



<http://www.IMPETUS-project.eu>

IMPETUS Project Deliverable: D3.1

Secure Smart City Tool Development initial report

Dissemination Status: Public

Authors: Michelangelo Ceci (CINI), Joaquin Garcia-Alfaro (IMT), Joaquín Luzón (INS), Joachim Levy, Moshe Rappoport (CINEDIT), Donato Malerba, Paolo Mignone, Annalisa Appice, Corrado Loglisci, Stefarino Ferilli, Nicola Di Mauro, Francesca Mazzia, Alessandro Balestrucci, Costantino Mele, Andrea Rizzello Bortone, Marco De Monte (CINI), Bruno Bonomini, Giulia Canilli (CPAD), Sandrine Bayle, Alexia Comte, Keren Saint-Hilaire (IMT), Berta Biescas, Laura Cebollero, Guillem Garcia, Sandra Cardoso, Aleix Cortines (INS), Osman Ibrahim, Simon Gjetrang, Juan Cabrera, Robert Lam, Eirik Bærulfsen (OSL), Radu Popescu, Andrei OGREZeanu, Dragos Trifan (SIV), Benjamin Preminger, Ron Shamir (SG), Thomas de Groot, Rafal Hryniewicz, Tije Oorwijn, Johan de Heer (THA), Axelle Cadière, Sébastien Courtin, Benoit Roig (UdN), Alberto Da Re (UNI), Paolo Mocellin (UPAD), Tobias Träbing, Rinat Villeval (XM)



About IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon 2020 Research and Innovation project that provides city authorities with new means to improve the security of public spaces in smart cities, and so help protect citizens. It delivers an advanced, technology-based solution that helps operational personnel, based on data gathered from multiple sources, to work closely with each other and with state-of-the-art tools to detect threats and make well-informed decisions about how to deal with them.

IMPETUS provides a solution that brings together:

- *Technology*: leverage the power of Internet of Things, Artificial Intelligence and Big Data to provide powerful tools that help operational personnel manage physical and cyber security in smart cities.
- *Ethics*: Balance potentially conflicting needs to collect, transform and share large amounts of data with the imperative of ensuring protection of data privacy and respect for other ethical concerns - all in the context of ensuring benefits to society.
- *Processes*: Define the steps that operational personnel must take, and the assessments they need to make, for effective decision making and coordination - fully aligned with their individual context and the powerful support offered by the technology.

Technological results are complemented by a set of practitioner's guides providing guidelines, documentation and training materials in the areas of operations, ethical/legal issues and cybersecurity.

IMPETUS places great emphasis on taking full and proper account of ethical and legal issues. This is reflected in the way project work is carried out, the nature of the project's results and the restrictions imposed on their use, and the inclusion of external advisors on these issues in project management.

The cities of Oslo (Norway) and Padova (Italy) have been selected as the site of practical trials of the IMPETUS solution during the project lifetime, but the longer-term goal is to achieve adoption much more widely.

The work is carried out by a consortium of 17 partners from 11 different EU Member States and Associated Countries. It brings together 5 research institutions, 7 specialist industrial and SME companies, 3 NGOs and 2 local government authorities (the trial sites). The consortium is complemented by the Community of Safe and Secure Cities (COSSEC) – a group established by the project to provide feedback on the IMPETUS solution as it is being developed and tested.

The project started in September 2020 with a planned duration of 24 months (possibly to be extended to 30 months).

For more information

Project Coordinator: Joe Gorman, SINTEF: joe.gorman@sintef.no
Dissemination Manager: Snježana Knezić, TIEMS: snjezana.knezic@gmail.com

Executive Summary

The main objective of this deliverable is to make a high-level description of the tools that are being used in IMPETUS and that conform the Cybersecurity Framework, or the Technologies that are being integrated and producing the project's toolkit. The tools descriptions' central objective is to let any stakeholders understand how the tools work and which kind of functionalities cover each of them. These descriptions will also extend how each of these tools are explained in the project proposal. We are also taking the opportunity to showcase an update of the actual status and maturity of each of the technologic solutions provided, as well as indicating the data sources and data delivery methods each tool makes use of. The document also includes the user manuals for each of the tools, which we consider as a key material to lay out the usability of each tool and understand better the capabilities that they offer.

An extensive cooperation with all WP3 participants has been conducted during the writing of this document, when we were mainly focused on understanding and defining the technological and ethical aspects of the technologies for public safety in smart city environments. The definition of the tools is serving a close collaboration with other WPs, that focus on Requirements, Ethics, Technical Development and Platform Integration, Operations and Platform Evaluation, as all of these areas are being developed in an iterative manner. The understanding of how the tools work and what they offer is of vital importance for many participants from different backgrounds and perspectives in the project.

During the definition process of the Secure Smart City Tool Development module, we have been able to know first-hand the maturity and readiness of each of the tools that the Cybersecurity Framework will contain. We had the chance to do an assessment of what is possible to obtain by using each of the different tools and how to generate more value to secure smart cities when combining them. Also, a joint work with WP2 to understand how to integrate the tools and how these tools will interact between them has been done, and that uses the information presented in this document as a basis.



Table of Contents

About IMPETUS.....	2
Executive Summary.....	3
List of Figures.....	7
List of Tables.....	7
List of Abbreviations.....	8
1 About this deliverable	9
1.1 Why would I want to read this deliverable?	9
1.2 Intended readership/users	9
1.3 Structure	9
1.4 Other deliverables that may be of interest	10
2 Secure Smart City Module Development	11
2.1 Initial Modular proposal	11
2.2 Actual status and decisions made	12
3 Social Media Detection tool (SMD).....	14
3.1 Responsible Partner	14
3.2 Tool internal/commercial name.....	14
3.3 Tool Technology Readiness Level (TRL).....	14
3.4 Data Sources.....	14
3.5 Tool data delivery	14
3.6 Tool Functionalities.....	15
3.6.1 Online data acquisition	15
3.6.2 Linguistic feature identification	15
3.6.3 Social Network Analysis	17
3.6.4 Hate Speech Detection	17
3.6.5 Real-Time Environment.....	18
3.6.6 Deanonimization	18
4 Weapon Detection tool (WD).....	19
4.1 Responsible Partner	19
4.2 Tool internal/commercial name.....	19
4.3 Tool Technology Readiness Level (TRL).....	19
4.4 Data Sources.....	19
4.5 Tool data delivery	19
4.6 Tool Functionalities.....	19
4.6.1 Weapon detection	19
5 Biological Risk Detection tool (BRD)	22
5.1 Responsible Partner	22
5.2 Tool internal/commercial name.....	22
5.3 Tool Technology Readiness Level (TRL).....	22
5.4 Data Sources.....	22
5.5 Tool data delivery	22
The data will be delivered using the Apache Kafka as a framework.	22
5.6 Tool Functionalities.....	22
5.6.1 Biocollector.....	22
5.6.2 ATP- analyser.....	23
5.6.3 Data sending	23
6 Breach & Attack Simulation tool (BAS)	25



6.1	Responsible Partner	25
6.2	Tool internal/commercial name.....	25
6.3	Tool Technology Readiness Level (TRL).....	25
6.4	Data Sources	25
6.5	Tool data delivery	25
6.6	Tool Functionalities	25
6.6.1	Fully automated APT simulation	25
6.6.2	Real-time visualization	26
6.6.3	Discover hard-to-find exposures that result from misconfigurations, vulnerabilities, misplaced credentials and poor user behaviour	26
6.6.4	Quickly get remediation recommendations and links to associated patches, data and tools	26
6.6.5	Greater realism than standalone security control validation	27
6.6.6	What-if analysis.....	27
6.6.7	SaaS, UI, System & Environment Management.....	28
7	Cyber Threat Intelligence tool (CTI)	29
7.1	Responsible Partner	29
7.2	Tool internal/commercial name.....	29
7.3	Tool Technology Readiness Level (TRL).....	29
7.4	Data Sources	29
7.5	Tool data delivery	29
7.6	Tool Functionalities	29
7.6.1	Detecting Zero Day Malware	29
7.6.2	Cyber Incidents Prevention + Detection + Incident Response	29
7.6.3	Enriching End Point Protection (IOCs)	30
8	Physical Threat Intelligence tool (PTI).....	31
8.1	Responsible Partner	31
8.2	Tool internal/commercial name.....	31
8.3	Tool Technology Readiness Level (TRL).....	31
8.4	Data Sources.....	31
8.5	Tool data delivery	31
8.6	Tool Functionalities.....	31
8.6.1	Identify if the current sensor data is anomalous or normal.....	31
8.6.2	Identify the class of threats of an unclassified sensor data	32
8.6.3	Switch remotely among the possible states of the anomaly detectors and event classifiers.....	32
9	Human Computer Interaction tool (HCI)	34
9.1	Responsible Partner	34
9.2	Tool internal/commercial name.....	34
9.3	Tool Technology Readiness Level (TRL).....	34
9.4	Data Sources	34
9.5	Tool data delivery	34
9.6	Tool Functionalities	35
9.6.1	Custom Sensor Set.....	35
9.6.2	Realtime Data Acquisition and Quality Check.....	36
9.6.3	Data Feature Extraction for personalized ML model	36
9.6.4	Personal Model Trainer	36
9.6.5	Assessment.....	36
9.6.6	Alert System	37
10	Physical Threat Response Optimization tool (PTRO).....	38
10.1	Responsible Partner	38
10.2	Tool internal/commercial name.....	38
10.3	Tool Technology Readiness Level (TRL).....	38
10.4	Data Sources	38
10.5	Tool data delivery	38



10.6	Tool Functionalities	38
10.6.1	<i>Data acquisition</i>	38
10.6.2	<i>Scenario anticipation/forecast</i>	38
10.6.3	<i>Communication</i>	39
11	Cyber Threat Mapping tool (CTM)	40
11.1	Responsible Partner	41
11.2	Tool internal/commercial names	41
11.3	Tool Technology Readiness Level (TRL)	41
11.4	Data Sources	41
11.5	Tool data delivery	41
11.6	Tool Functionalities	41
11.6.1	<i>Receive logs</i>	41
11.6.2	<i>Generate alerts</i>	41
11.6.3	<i>Correlate alerts</i>	42
11.6.4	<i>Visualize alerts</i>	42
11.6.5	<i>Timeline visualization</i>	42
11.6.6	<i>Additional information</i>	42
12	Future Work	44
13	APPENDIXES – USER MANUALS	46
	Members of the IMPETUS consortium	47



List of Figures

Figure 1. Social Media Detection (SMD) main dashboards.....	16
Figure 2. SMD dashboard visualizing the User Interactions Network.....	17
Figure 3. Weapon Detection tool (WD), SAMSON UI.	20
Figure 4. Weapon Detection for CCTV.	21
Figure 5. Integration of HCI in the IMPETUS platform.	35
Figure 6. Prelude-ELK flow chart showing the inputs, processes and outputs.	40

List of Tables

Table 1: List of Abbreviations.....	8
Table 2. Initial group of tools.	11
Table 3. New WP subdivision.	12
Table 4. TRL status of each of the tools.....	44



List of Abbreviations

Table 1: List of Abbreviations

Abbreviation	Explanation
WP	Work Package
TRL	Technology Readiness Level
SaaS	Software as a Service
UI	User Interface
GUI	Graphical User Interface
ATP	Adenosine TriPhosphate
LAN	Local Area Network
SOC	Security Operations Center



1 About this deliverable

1.1 Why would I want to read this deliverable?

The main goal of this document is to provide a complete and understandable high-level description of the nine tools that will constitute the IMPETUS integrated toolkit, covering the complete physical and cybersecurity value chain.

The tools are one of the central actives for the development of IMPETUS' Technologies or Cybersecurity Framework, which combined with the Operational and Ethical Framework will form the decision-making solution. A complete and understandable description of them will serve as a common source of information across the project participants and stakeholders. This document aims to serve as a common ground for further discussions, both in Work Package 3 (WP3) and the rest of the project activities.

The description of the tools is key for further and parallel processes in the project, including but not limited to the definition and integration of the platform, the user interface definition, the platform's usability, the requirements (platform, solution, frameworks, ethics) of the project and the project's piloting and validation of the platform.

1.2 Intended readership/users

The primary audience of the deliverable is the project consortium.

A secondary target audience are the stakeholders of the project: stakeholders of public safety solutions for smart cities, possible end-users and third-party technology providers.

1.3 Structure

This document consists of a set of sections (Sections 2-11) with the same structure, each of them describing one of the tools in the Cybersecurity Framework for IMPETUS. The structure of the sections was made based on a working document (spreadsheet). Each partner was provided with an identical template to fill the spreadsheet, letting the document authors to fill and format the sections.

Each of these chapters contains:

A high-level, understandable, and clear tool description and, if existing, the tool internal or commercial name.

- The Technology Readiness Level (TRL) determined for the tool, based on the status of each independent tool.
- A description of the data sources that each tool consumes and a brief explanation of how the data produced by the tool is or can be delivered and/or presented to the end-user.
- A structured description of each of the tool's functionalities, that includes the following fields:
 - Description
 - User roles
 - Maturity
 - Interface (service, methods, data structures)



1.4 Other deliverables that may be of interest

The work done in WP3 and the necessary adaptations of the tools for its integration in the IMPETUS platform, and to be aligned with the scope of the project is fully dependent on the rest of the project's results. However, this is a list of the deliverables that are strongly connected to WP3 and this deliverable:

- D1.1 - Local Context of Partner Cities
- D1.2 - Requirements for public safety solutions
- D2.1 - Platform architecture, requirement specifications and test plan
- D4.1 - Data analytics and ingestion-based access control initial report
- D9.1 - Exploitation strategy and plan

2 Secure Smart City Module Development

2.1 Initial Modular proposal

The initial modular proposal was defined considering the three following work package tasks:

- **Task 3.1 (Detection solutions).** The goal of this task was to combine proactive tools for threat identification, using data sources such as social media, surveillance camera feeds and other similar sensor measurements. Such data sources can be processed with artificial intelligence and statistics techniques (e.g., machine learning and natural language processing), in order to discover and warn urban safety operators about potential underlying threats affecting their systems.
- **Task 3.2 (Simulation & analysis solutions).** The goal of this second task was to combine the proactive information collected and processed in Task 3.1, with a second batch of tools providing threat analysis and decision-making features, such as automated processing of physical security threats and technical vulnerabilities affecting computational and networked resources, in order to simulate the consequences of each threat.
- **Task 3.3 (Intervention solutions).** The goal of this third task was to close the loop with reactive tools capable of facing the list of identified threats with the appropriate countermeasures. This includes the combination of different approaches targeting the affected systems, in order to autonomously evaluate changes in the environment and adapt them prior responding to the threats. For instance, by combining the monitoring process with the selection of response plans, both at physical and cyber layers.

Hence, the initial driving idea was to separate tools into three main modules used to:

- identify threats (T3.1),
- explore the consequences if those identified threats occur (T3.2), and
- prepare an optimized response to neutralize the threats (T3.3).

Following this modularity, nine tools were grouped according to the schema shown in Table 2.

Table 2. Initial group of tools.

Tool	Task
Social Media Detection (SMD)	Task 3.1: Detection solutions
Weapon & Face Detection (WFD)	
Biochemical Risk Detection (BRD)	
Breach & Attack Simulation (BAS)	Task 3.2: Simulation & analysis solutions
Cyber Threat Intelligence (CTI)	
Physical Threat Intelligence (PTI)	
Human computer interaction (HCI)	Task 3.3: Intervention solutions
Physical Threat response Optimization (PTRO)	
Cyber Threat response Optimization (CTRO)	

2.2 Actual status and decisions made

After some individual analysis on the tools, during the WP3 initial discussions, the modular approach (Detection solutions, Simulation & analysis solutions and Intervention solutions) seemed to be out of date.

While the tools could be superficially categorised by the modules defined, the type of activities, data sources and pace of progress didn't seem to be aligned among them. It made more sense to define the IMPETUS toolkit as a set of nine independent tools.

The platform definition processes that are being carry out in parallel to WP3 in WP1 (functional, non-functional and platform requirements) and WP2 (architecture and technical requirements) are even identifying integration scenarios where some tools that are prone to be sharing data amid themselves were not even included in the same module at the beginning. One clear example for this is the direct collaboration between cybersecurity tools: Cyber Threat Intelligence, Breach & Attack Simulation, and Cyber Threat Mapping Tool.

With regards to each preliminary defined module, the planned completion and/or integration of each tool (or some of its functionalities) is not always aligned with the rest of the tools integrated in that module. In terms of internal Work Package and Task organization, this situation made us consider that it was more efficient to track progress for each of the tools independently rather than keeping track of the completion of each of the initial tasks defined (T3.1 to T3.3).

The new WP subdivision is as shown in Table 3.

Table 3. New WP subdivision.

Current task	Initial task	Tool name (in DoA)	Updated tool/task name
T3.1.1	T3.1: Detection solutions	Social Media Detection (SMD)	Social Media Detection (SMD)
T3.1.2		Weapon and Face Detection (WFD)	Weapon Detection (WD)
T3.1.3		Biochemical Risk Detection (BRD)	Biological Risk Detection (BRD)
T3.1.4	-	-	WP3 Management and strategic planning
T3.2.1	T3.2: Simulation & analysis solutions	Breach & Attack Simulation (BAS)	Breach & Attack Simulation (BAS)
T3.2.2		Cyber Threat Intelligence (CTI)	Cyber Threat Intelligence (CTI)
T3.2.3		Physical Threat Intelligence (PTI)	Physical Threat Intelligence (PTI)
T3.3.1	T3.3: Intervention solutions	Human Computer Interaction (HCI)	Human Computer Interaction (HCI)
T3.3.2		Physical Threat Response Optimization (PTRO)	Physical Threat Response Optimization (PTRO)
T3.3.3		Cyber Threat Response Optimization (CTRO)	Cyber Threat Mapping Tool (CTM)



During the definition process of this toolkit, all WP3 participants also reached the consensus of establishing the term ‘tool’ as the correct way to refer to all of the different toolkit parts, since terms like ‘module’, ‘component’ or ‘solution’ were leading to confusion during the working sessions. Hence, the agreement was to always use the more appropriate term (‘tool’).

Moreover, some tool/subtask names were modified in order to be described more accurately:

- **Weapon Detection tool** was previously called Weapon and Face Detection. Currently, the Weapon Detection Tool constantly anonymizes all the biometric data unless an anomaly is detected (more details in section 4).
- **Biological Risk Detection tool** was previously called Biochemical Risk Detection, since this tool is a microbial air analyser rather than a biochemical agents detector.
- **Cyber Threat Mapping tool**, previously called Cyber Threat Response Optimization tool has been renamed to reflect better the tool purpose.



3 Social Media Detection tool (SMD)

The Social Media Detection tool, which commercial name is Insikt Spotlight, is a unique platform, which collects and analyses massive amounts of online public data to help Law Enforcement and Investigative Professionals detect specific written content, powered by Artificial Intelligence methods, Data Mining, Text Mining with Natural Language Processing, Deep Learning, Big Data Analysis, and Social Network Analysis in order to leverage cutting edge algorithms to surface hidden insights and cut through the noise to effectively neutralise and prevent terror, crime and threats affecting cities.

3.1 Responsible Partner

Insikt Intelligence - INS

3.2 Tool internal/commercial name

Insikt Spotlight - <https://www.insiktintelligence.com/our-solutions/spotlight-osint/>

3.3 Tool Technology Readiness Level (TRL)

TRL 7 - System prototype demonstration in operational environment

3.4 Data Sources

Social Media Detection will make use of encrypted anonymised data (text and metadata) from Social Media -Twitter, YouTube, TikTok- and comments sections from local newspapers in Padova - mattinopadova.gelocal.it- and Oslo - document.no, reset.no, vg.no and dagbladet.no.

Online Sources from Social Media:

- Twitter
- YouTube
- TikTok

Online Sources from Local Press:

- mattinopadova.gelocal.it
- document.no
- reset.no
- vg.no
- dagbladet.no

3.5 Tool data delivery

SaaS and UI

3.6 Tool Functionalities

3.6.1 Online data acquisition

Description	<p>The data is automatically acquired, given a frequency specified for each project. The sources of the data are:</p> <p>Online Sources from Social Media:</p> <ul style="list-style-type: none">• Twitter• YouTube• TikTok <p>Online Sources from Local Press:</p> <ul style="list-style-type: none">• mattinopadova.gelocal.it• document.no• reset.no• vg.no• dagbladet.no
User roles	Analyst - Investigator who looks for potential threats that are published, organized, promoted or enhanced in online social media and local newspapers.
Maturity	Ready - Scraper of local online newspapers of Padova and Oslo have been developed for the project.
Interface (service, methods, data structures)	By creating a project, the user selects which are the sources that want to include in the investigation. The tool Integrates scrapers adapted to each source. All the acquired data are showed in the dashboard as raw data and also within the different analysis.

3.6.2 Linguistic feature identification

Description	Seven different methodologies of Natural Language Processing [NLP, i.e., AI applied to text] are applied in 5 languages [English, Italian, Norwegian, French and Arabic] to analyse the content of the public online text from different perspectives: Concepts extraction, Key Ideas extraction, Topic classification, Hate Speech detection, Entities extraction, Hashtag detection and Sentiment analysis.
User roles	Analyst - Investigator who looks for potential threats that are published, organised, promoted or enhanced in online social media and local newspapers.
Maturity	Ready - New list of topics could be customised to improve the analysis if cities are interested. Norwegian NLP has been added for the project.
Interface (service, methods, data structures)	Computational linguistic methodologies: * post tagging, tokenization and stopword removal for text processing;

	<ul style="list-style-type: none"> * classification of topics based on cosine distances in 300 dimensional word embeddings; * detection of linguistic patterns to extract the key ideas and concepts of text; * network analysis applied to describe interactions between users. <p>Dashboard with graphs for user-friendly visualization of the results: bar plots, 2-D graphs, word clouds, tables and network graphs. Word embeddings allow to convert text to numerical vector, which is key for computational linguistic methods. SMD integrates the tokenizers based on XLMRoberta cross-lingual tokenizers and the aligned word embeddings trained in Wikipedia in English, Italian, Norwegian, French and Arabic. [Figure 1. Example of NLP Analysis]]</p>
--	---

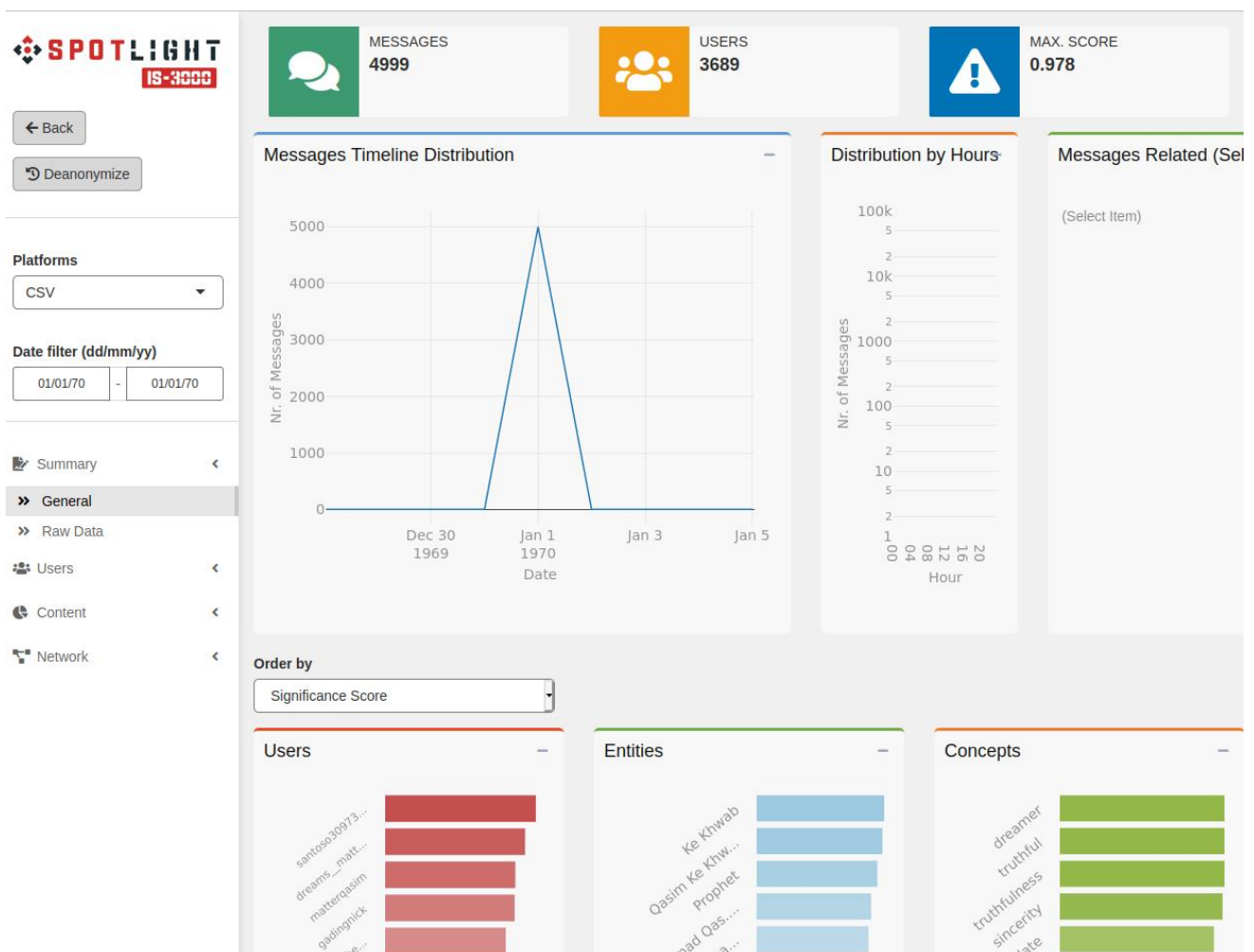


Figure 1. Social Media Detection (SMD) main dashboards.

3.6.3 Social Network Analysis

Description	Analysis of observed interactions creating relationships relations between authors within SM. This analysis gives information about the users in terms of their activity within the SM, and their score as influencers, spreaders, and the role they have. Communities within SM are also detected and analysed.
User roles	Analyst - Investigator who looks for information about relations between users within a SM [activity, influencers, spreaders, roles, communities].
Maturity	Ready - The feature of analysing networks based on the observed interactions has been verified and is working correctly.
Interface (service, methods, data structures)	The social network analysis is based on different metrics applied to the observed interactions. Afterwards, the interactions between the users are displayed in the dashboard. [Figure 2. SNA.]

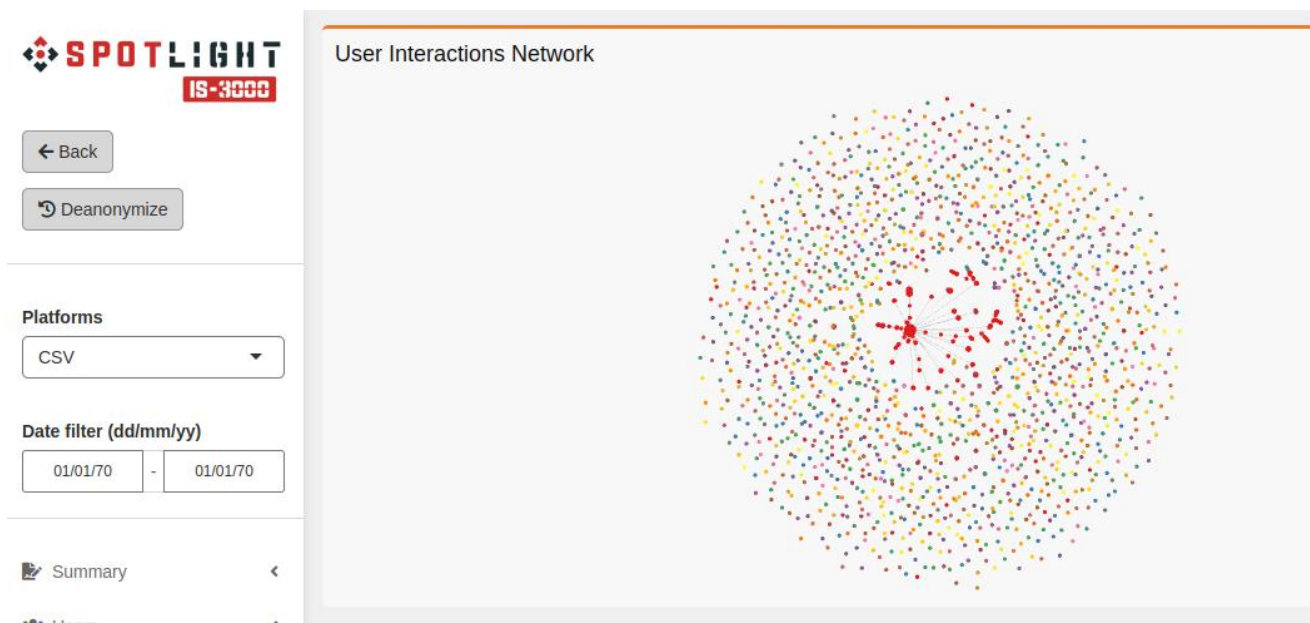


Figure 2. SMD dashboard visualizing the User Interactions Network.

3.6.4 Hate Speech Detection

Description	The texts extracted from the social media and the local newspapers are analysed to evaluate the degree of hate speech they have.
--------------------	--

User roles	Analyst - Investigator who looks for hate speech in online social media and local newspapers.
Maturity	Ready - These models can be improved along the project with new data sets of the cities.
Interface (service, methods, data structures)	Supervised machine language models trained from XLNetRoberta cross-lingual pre-trained model. Transfer learning methods applied to multilingual text classifiers of hate speech content.

3.6.5 Real-Time Environment

Description	The functionalities of Insikt Spotlight have been developed to run in a low processing time in all the workflow.
User roles	Analyst - Investigator who looks for potential threats that are published, organised, promoted or enhanced in online social media and local newspapers.
Maturity	Ready - Low processing time in all the workflow
Interface (service, methods, data structures)	Low processing time in all the workflow. Near-real time.

3.6.6 Deanonymization

Description	Functionality that allows to recover pseudonymised personal data by authorised parties.
User roles	Authorised analyst - Authorised parties for accessing to personal data.
Maturity	In progress - We are working in the implementation of this functionality and its integration in the dashboard.
Interface (service, methods, data structures)	The dashboard shows anonymised data by default. It means that all usernames and nicknames used in SM and local newspapers will be removed from the dashboard and substituted by encrypted codes. These codes can be converted to the original personal data by using the deanonymization functionality. The deanonymization will be only possible for those authorised user roles who will have a key that will allow the de-encryption.



4 Weapon Detection tool (WD)

SAMSON is an AI (artificial intelligence) that uses already installed CCTV cameras to detect small magazine fed weapons as well as assault rifles. The instant a weapon enters the camera field of view, SAMSON shares a real-time alert. Here is a detailed motion graphics workflow of the proposed solution: <https://workspace.cimediadcloud.com/r/GfA1BqXGH26U>

The anonymized Weapon Detection Tool constantly obfuscates/anonymizes people including their biometric data such as clothing, gender, face. When an anomaly is detected such as a small magazine fed handgun or assault rifle, then all biometric data is revealed and shared in real-time with the SOC's (Security Operation Control) dispatcher.

4.1 Responsible Partner

Cinedit

4.2 Tool internal/commercial name

SAMSON

4.3 Tool Technology Readiness Level (TRL)

TRL 6 – Technology demonstrated in relevant environment

4.4 Data Sources

4K CCTV (8 Mega Pixels) with IR leds (night mode on monochrome) with a shutter speed of at least 120th/sec.

4.5 Tool data delivery

UI, edge device, cloud service and AI retraining

4.6 Tool Functionalities

4.6.1 Weapon detection

Description	Using already installed CCTV cameras, SAMSON detects small magazine fed weapons. The instant a weapon enters the camera field of view, an alert is instantly shared with the relevant teams.
User roles	Dispatcher at SOC
Maturity	SAMSON is mature for indoor environments using 2MP, 3MP and 5MP (Mega Pixels) cameras. It can successfully detect weapons a few meters from the camera depending on the camera resolution
Interface (service, methods, data structures)	Alerts are displayed in our UI dashboard (see Figure 3 and Figure 4) and are pushed to a local directory.



Figure 3. Weapon Detection tool (WD), SAMSON UI.

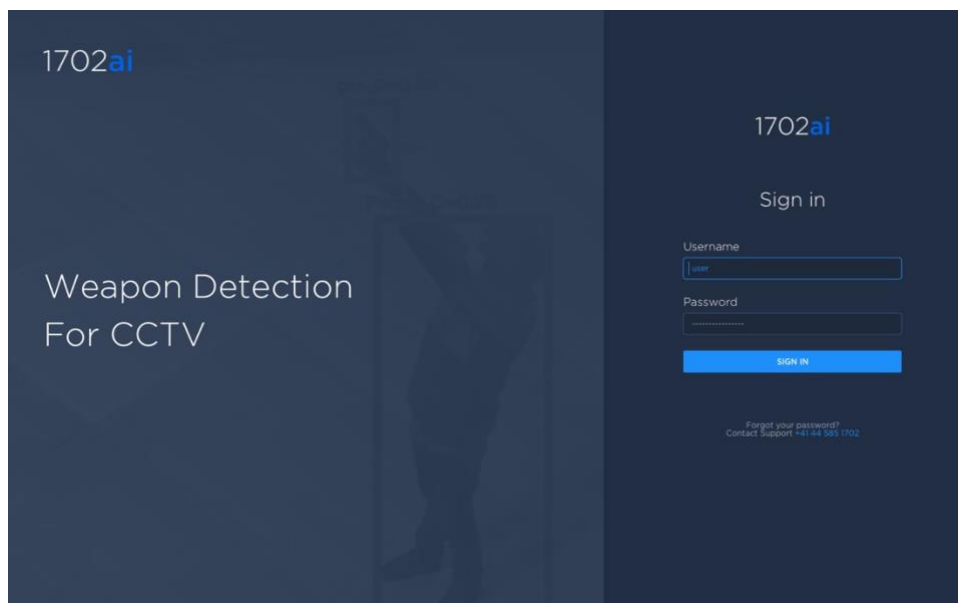


Figure 4. Weapon Detection for CCTV.



5 Biological Risk Detection tool (BRD)

The BRD is an air analyser aimed at detecting microorganism's concentration in public area (train station, subway, hospital, festival, theatre). The device will transmit these data to a monitoring station.

The tool is made up of two parts that are respectively air-biocollector and an ATP analyser. The biocollector collects and catches the airborne particles in water volume, this is the sample. The ATP analyser part is designed by GLBiocontrol and called GLOW'N'CARE. The method used is ATP-metry to quantify the microorganisms in the air. Indeed, ATP (Adenosine TriPhosphate) is easy to use, this organic compound provides energy to drive many processes in living cells and is found in all known forms of life as human cell, bacteria cell and fungi cell. It can therefore be assumed in case of biological threat, the concentration in ATP will be higher due to the bacteria concentration in the air.

The ongoing step is to *physically* and *digitally* connect both tools for creating the BRD. Indeed, the air caught in the volume is transferred in the ATP-analyser and the data is sent to the platform. The BRD prototype is aimed at reaching TRL 6 by being deployed in real environment. This procedure allows the BRD to be properly calibrated. Data aggregation is necessary in both partner cities to define what the relevant threshold is in case of a bio-terror attack. Additionally, the next goal is to deploy the BRD so it can be remotely controlled using the partner cities LAN.

5.1 Responsible Partner

UdN and IMT

5.2 Tool internal/commercial name

Microbial air analyser

5.3 Tool Technology Readiness Level (TRL)

TRL 6 – Technology demonstrated in relevant environment

5.4 Data Sources

The data collected is to define the concentration of microorganisms suspended in the air. Given our environmental data, we do not use anonymization or any pseudonymization.

5.5 Tool data delivery

The data will be delivered using the Apache Kafka as a framework.

5.6 Tool Functionalities

5.6.1 Biocollector

Description	The air-biocollector collects and catches air microorganisms in a small volume of water. The air-biocollector is compounded in an inlet for an automatic filling and an outlet to transfer the sample to the ATP analyser.
--------------------	---



User roles	Technician or operator
Maturity	TRL 6
Interface (service, methods, data structures)	A program has been developed to control a remote sequence. Plus, a local and html interface has been designed to drive the BRD remotely.

5.6.2 ATP- analyser

Description	<p>The ATP-analyser is a commercial device. It was modified and adapted to receive the air sample from the air-biocollector.</p> <p>The ATP-analyser is compounded in an inlet for receiving the air sample and a cell for measurements to define the concentration of microorganism present in the air.</p>
User roles	Technician or operator
Maturity	TRL 7
Interface (service, methods, data structures)	A specific program allows to communicate and to automate all the measurements.

5.6.3 Data sending

Description	The sent data includes four types of information: ATP levels, the internal standard values, ATP concentrations as well as the ATP concentration per unit of air.
User roles	Technician or operator
Maturity	TRL 6
Interface (service, methods, data structures)	Below is a sample of shared data output:

Date/Time	R0	R1	R2	Conc: bacteria concentration pg/ml	AirConc: bacteria concentration pg/m3
10-08-2020 17:49:20	888	835	835	151011	Conc: 1.51011, AirConc: 14.171 pg/m3
10-08-2020 18:38:50	888	885	885	2246	R2: 213279, Conc: 9.9189, AirConc: 9.1802 pg/m3
10-08-2020 18:38:51	888	885	885	1877	R2: 238278, Conc: 9.4278, AirConc: 9.1801 pg/m3
10-08-2020 18:57:51	888	885	885	2219	R2: 419823, Conc: 9.3583, AirConc: 9.1129 pg/m3
10-08-2020 20:38:51	888	885	885	2733	R2: 382318, Conc: 9.6773, AirConc: 9.1129 pg/m3
10-08-2020 21:38:49	888	885	885	2132	R2: 359847, Conc: 9.4985, AirConc: 9.1129 pg/m3
10-08-2020 21:50:40	888	885	885	138	R2: 329847, Conc: 9.3888, AirConc: 9.0888 pg/m3
10-08-2020 22:31:40	888	885	885	2504	R2: 437338, Conc: 9.3583, AirConc: 9.0987 pg/m3
10-08-2020 22:37:40	888	885	885	1876	R2: 401379, Conc: 9.4588, AirConc: 9.0823 pg/m3
10-08-2020 23:43:43	888	885	885	2412	R2: 478888, Conc: 9.5888, AirConc: 9.0848 pg/m3
11-08-2020 00:18:39	888	885	885	272	R2: 2987, R2: 378852, Conc: 9.8488, AirConc: 9.0888 pg/m3

R0: Background signal noise.

R1: Measure of ATP in RLU (Relative Light Unit)

R2: The measure in RLU after addition of internal standard (1000 pg of ATP).

Conc: Quantity in pg of ATP/ml

AirConc: Concentration of ATP per unit of air (m³)

The analysis results are stored in a .csv file in the BRD and sent through secured FTP to the IMPETUS platform. The data history can be downloaded from the BRD dashboard as a log file.



6 Breach & Attack Simulation tool (BAS)

XM Cyber continuously calculates all cyber-attack paths using simulated attacker techniques. Using the resulting data gives your security and network teams an attack-centric view into risks, regardless of other security scores or vulnerability notices. Now organizations can optimize their time and resources by prioritizing remedial actions based on real threats in your actual environment.

Hackers explore every opening, waiting for changes that get them closer to your critical assets. The best defence is to take the same approach – be proactive in searching for attack paths.

- Run risk-free with no impact to any production environment.
- Discover cyber risks as they arise by continuously looking for attack vectors.
- Validate remediation efforts and track the overall security posture and risk level.
- Discover hard-to-find exposures that result from misconfigurations, vulnerabilities, misplaced credentials and poor user behaviour.

6.1 Responsible Partner

XM Cyber Ltd.

6.2 Tool internal/commercial name

XM Cyber

6.3 Tool Technology Readiness Level (TRL)

TRL 6 – Technology demonstrated in relevant environment

6.4 Data Sources

XM Cyber Development, Research Teams and XM Cyber Sensors

6.5 Tool data delivery

SaaS, UI

6.6 Tool Functionalities

6.6.1 Fully automated APT simulation

Description	Manual advanced persistent cyber threat testing is simply ineffective in most rapidly evolving contexts. The dynamism of most networks makes a manual approach fundamentally flawed. Prioritized remediation of security gaps: This feature provides instant feedback on which cyber security issues are most pressing and enables immediate fixes.
User roles	Security Architect - read & write on scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation . The sensor represents a small, passive and lightweight software.



Interface (service, methods, data structures)	UI step by step configuration through Scenario Definition
--	---

6.6.2 Real-time visualization

Description	Visually see all the cyber-attack paths associated with a particular alert and drill down for specific details. Essentially, see how attackers can pivot in your environment and use multiple vulnerabilities and exposures to form new attack vectors that lead to business-sensitive assets
User roles	Security Analyst - read-only access to scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	Pending automatic pen test configuration in UI (point 1)

6.6.3 Discover hard-to-find exposures that result from misconfigurations, vulnerabilities, misplaced credentials and poor user behaviour

Description	By continuously running fully automated APT simulation and combining critical IT security risks (e.g., Software Vulnerabilities with Misconfigurations and User Behaviour) all exposures towards critical assets or pivoting points in the network are identified.
User roles	Security Analyst - read-only access to scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	UI step by step configuration through Scenario Definition

6.6.4 Quickly get remediation recommendations and links to associated patches, data and tools

Description	
User roles	Security Analyst - read-only access to scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	Pending automatic pen test configuration in UI (point 1)

--	--

6.6.5 Greater realism than standalone security control validation

Description	Rather than simply testing controls, this approach allows you to gain true visibility into all cyber-attack paths and lateral movement. The importance of this feature was underlined when one of the world's largest financial institutions suffered a severe breach while relying on security control validation products. The hacker assumed the identity of an employee to move undetected across security controls, ultimately taking advantage of poor IT hygiene and (all-too-frequent) human judgment errors.
User roles	Security Analyst - read-only access to scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	Pending automatic pen test configuration in UI (point 1)

6.6.6 What-if analysis

Description	<p>APT simulation and remediation are designed to work within dynamic environments, transcending one of the key limitations of manual tests. This approach also helps organizations optimize their cyber security investments while minimizing the risk and impact of a breach.</p> <p>This approach can also confirm what-if analysis based on the location of a breach and the digital assets that were targeted. It also uses actual user behaviour to identify real attack vectors. Meanwhile, overall IT hygiene is improved by reducing misconfigurations and the possibility of human error.</p>
User roles	Security Architect - read & write on scenarios and campaigns, without access to system configuration
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	Pending automatic pen test configuration in UI (point 1)



6.6.7 SaaS, UI, System & Environment Management

Description	The system has zero disruption to profunction environment on the sensors technologies IE - 0.02MB of RAM needed for checking all the attach conditions to a successful cyber-attack without executing any malicious payload
User roles	Administrator - full access to all XM Cyber system elements and configuration options, including user management
Maturity	Ready - pending sensor implementation. The sensor represents a small, passive and lightweight software.
Interface (service, methods, data structures)	Pending on boarding IMPETUS

...



7 Cyber Threat Intelligence tool (CTI)

Darkfeed is a feed of malicious indicators of compromise, including domains, URLs, hashes, and IP addresses.

It relies on Cybersixgill's vast collection of deep and dark web sources and provides unique and advanced warnings about new cyberthreats.

It is automated, meaning that IOCs (indicator of compromise; hashes, IPs, Domains and URLs) are extracted and delivered in real-time, and it is actionable, meaning that its consumers will be able to receive and block items that threaten their organization.

7.1 Responsible Partner

Sixgill

7.2 Tool internal/commercial name

Cybersixgill Darkfeed

See product marketing here - <https://www.cybersixgill.com/products/darkfeed/>

7.3 Tool Technology Readiness Level (TRL)

TRL 9 - Actual system proven in operational development

7.4 Data Sources

Threat intelligence extracted from deep/dark web sources

7.5 Tool data delivery

API

7.6 Tool Functionalities

7.6.1 Detecting Zero Day Malware

Description	Darkfeed detects attacks under development, before they are deployed in the wild and detected by other security vendors
User roles	
Maturity	Mature/ready - already available and in production
Interface (service, methods, data structures)	API, integrations to leading SIEM/SOAR/TIP systems

7.6.2 Cyber Incidents Prevention + Detection + Incident Response

Description	Sixgill provides its customers with the ability to investigate a specific threat or incident across its wide datasets from the Dark, Deep and Clear web. This include inter alia enrich the investigation with more context, attribute an incident to a specific threat actor and more
--------------------	--



User roles	
Maturity	Mature/ready - already available and in production
Interface (service, methods, data structures)	API, integrations to leading SIEM/SOAR/TIP systems

7.6.3 Enriching End Point Protection (IOCs)

Description	Sixgill provides security vendors with a feed of IOCs appearing on the underground (domains, IPs, Hashes etc.), enriched with context. This includes inter alia attributing them to a specific actor, providing their risk score and more.
User roles	
Maturity	Mature/ready - already available and in production
Interface (service, methods, data structures)	API, integrations to leading SIEM/SOAR/TIP systems



8 Physical Threat Intelligence tool (PTI)

Algorithms for the construction of anomaly detection models and event classification models.

8.1 Responsible Partner

CINI

8.2 Tool internal/commercial name

The tool includes two Machine Learning algorithms: Spark-GHSOM1 and DENCAST2 which can perform Anomaly Detection and Event Detection. The algorithms are now being integrated into the PTI tool.

8.3 Tool Technology Readiness Level (TRL)

TRL 4 – Technology validated in-house

8.4 Data Sources

Structured (possibly labelled) data from sensors. The data are automatically generated by the sensors and, in the general scenario of IMPETUS, they should not contain any personal data. If any personal data is provided, these data will be removed or anonymized by means of rolling hashing functions. The tool is able to process geo-referenced time series for any measure that can be collected by available sensors (e.g., temperature, PM10, pedestrians flow, traffic).

8.5 Tool data delivery

SaaS -> 1st version delivery: Sept 2021. 2nd version delivery: July 2022

8.6 Tool Functionalities

8.6.1 Identify if the current sensor data is anomalous or normal

Description	Functionality that allows the system to notify when an anomalous phenomenon occurs. An anomaly is identified when a time series does not follow the expected behaviour, according to historical data and according to the behaviour of data in the (spatial) neighbour
User roles	Analyst - Who can check what caused the anomaly to emerge by analysing the importance of the variables under analysis

¹ Ameya Malondkar, Roberto Corizzo, Iluju Kiringa, Michelangelo Ceci, Nathalie Japkowicz: Spark-GHSOM: Growing Hierarchical Self-Organizing Map for large scale mixed attribute datasets. Inf. Sci. 496: 572-591 (2019)

² Roberto Corizzo, Gianvito Pio, Michelangelo Ceci, Donato Malerba: DENCAST: distributed density-based clustering for multi-target regression. J. Big Data 6: 43 (2019)

Maturity	Ready - It depends also by the integration with the other tools, but the big data analytics method is currently capable to process a dataset by catching possible and interpretable anomalies through a ranking of the variables under analysis
Interface (service, methods, data structures)	The IMPETUS platform receives the alert, which represents the anomaly, from the tool. The dashboard can ask the tool to notify which sensor and/or variable of analysis are relevant for the anomaly and ask some aggregate data to show the trend of such variables.

8.6.2 Identify the class of threats of an unclassified sensor data

Description	Functionality that allows to notify different users when a specific threat is identified from the sensor data. The tool is able to process geo-referenced time series for any measure that can be collected by available sensors (e.g., temperature, PM10, pedestrians flow, traffic).
User roles	Analyst - Who can check what type of threat the current data is referring to among the set of predefined threats. If data are provided in streaming, the alerts can be generated in real time and the analyst can act immediately.
Maturity	The event classifier method is already implemented but we need adapt it and to test it with some annotated data. Testing will be completed in the next three months.
Interface (service, methods, data structures)	The IMPETUS dashboard receives the alert, which represents the identified threat, from the tool. The dashboard can ask the tool to notify which sensor and/or variable of analysis are relevant for the anomaly and ask some aggregate data to show the trend of such variables.

8.6.3 Switch remotely among the possible states of the anomaly detectors and event classifiers

Description	The machine learning model states could be changed via REST APIs to explicitly switch from one state to another depending on the specific needs
User roles	Analyst - Investigator who looks at the current state of the anomaly detector or event classifier and decides to switch from a particular state to another for a particular reason. For example, the user can manually force the learning process (training phase) in order to update the models on the basis of new



	data arrived. If the used does not manually force the start of learning process, it is automatically started according to some periodicity.
Maturity	In progress - The services have to be adapted. The backend is already implemented
Interface (service, methods, data structures)	Machine learning methods for the anomaly detection and for the event classifier must trained from a batch of data for the initial state, from a batch or mini-batch of data for the update, and they work at prediction state with batch or mini-batch of data. The algorithms could automatically identify when they should switch from one state to another. Moreover, the user could manually switch from one state to another



9 Human Computer Interaction tool (HCI)

Human computer interaction (HCI) tool assesses human operator mental workload based on neuro-physiological measurements.

9.1 Responsible Partner

Thales

9.2 Tool internal/commercial name

HCI

9.3 Tool Technology Readiness Level (TRL)

TRL 6 – Technology demonstrated in relevant environment

9.4 Data Sources

The HCI Tool is dependent on the operator's neuro-physiological signals that are captured through the tools' sensor set. The sensors will be chosen depending on the user preference and will likely encompass an EEG (ElectroEncephaloGram) sensor, to capture brain activity, and a PPG (Photoplethysmogram) sensor to measure heart rate. Both sensors are built in a single device (a headband). The training data will be collected once, on a personal basis, in order to create a personalized model for each individual. An assessment model will be created based on that data and then the data will be anonymized by removing the references to the individual. The assessment model will be deployed on a secured USB drive (cf. Figure 5), which will be in the possession of the individual who the model belongs to.

9.5 Tool data delivery

The HCI Tool sends real-time Assessment and Alert Data on the operator and team's workload state. The tool can also send Data Quality Alerts and information about the HCI tool system state.

The HCI Tool service will be deployed as a module within the IMPETUS Platform Product on premisses. The sensor set and corresponding data acquisition units will be deployed on site.

See figure 5 below for an overview of the integration of HCI tool in IMPETUS platform.

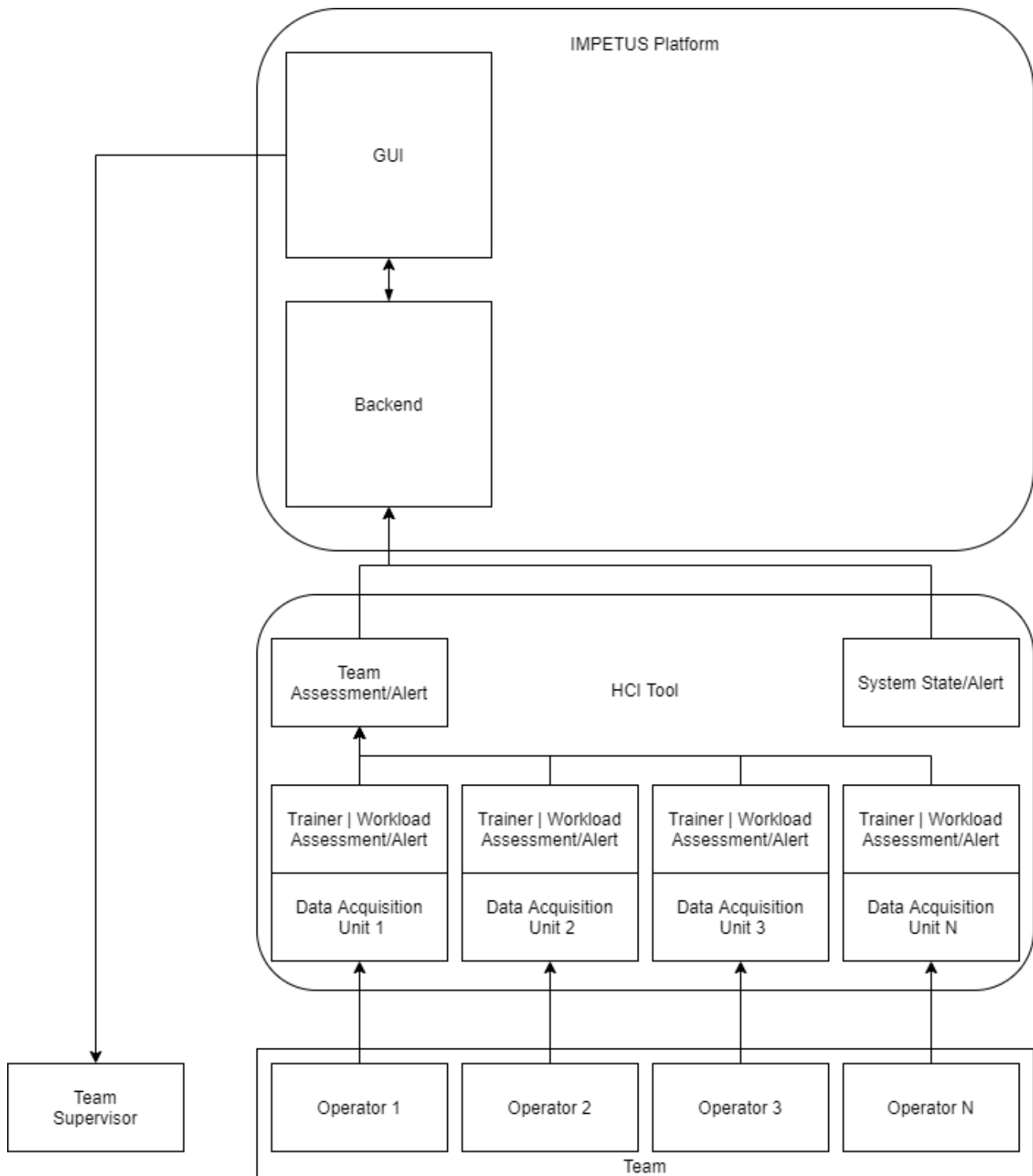


Figure 5. Integration of HCI in the IMPETUS platform.

9.6 Tool Functionalities

9.6.1 Custom Sensor Set

Description	A custom sensor set is designed based on the task and user requirements, as described in chapter 9.4
User roles	SOC Operator, HCI tool Technician

Maturity	Off the shelf sensors, signal acquisition software operational.
Interface (service, methods, data structures)	physical contact, one set per desk

9.6.2 Realtime Data Acquisition and Quality Check

Description	The Data Acquisition is used to acquire sensor data from an operator and check for data quality.
User roles	SOC Operator, HCI tool Technician
Maturity	In progress, first version operational
Interface (service, methods, data structures)	debug UI, alerts to IMPETUS PLATFORM

9.6.3 Data Feature Extraction for personalized ML model

Description	Realtime feature extraction for ML model
User roles	HCI tool Technician
Maturity	In progress, first version operational
Interface (service, methods, data structures)	debug UI, LSL (Lab Streaming Layer)

9.6.4 Personal Model Trainer

Description	Train the personal workload assessment Machine Learning model. Done one time per operator, using a custom calibration task.
User roles	HCI tool Technician
Maturity	In progress. Operational in 09.2021
Interface (service, methods, data structures)	debug UI, model put on secured USB stick

9.6.5 Assessment

Description	Realtime assessment of operator sensor data
User roles	SOC Operator, SOC Team Supervisor
Maturity	In progress. Framework has been developed. Optimizing on feature selection. Operational in 09.2021



Interface (service, methods, data structures)	personal unit with model loaded (secured USB stick)
--	---

9.6.6 Alert System

Description	Operator alerts on basis of the assessments
User roles	HCI tool Technician
Maturity	In progress. Module has to be adapted to the IMPETUS platform (under design). Operational in 09.2021
Interface (service, methods, data structures)	Tool internal message communication bus (MQTT), alerts sent to IMPETUS PLATFORM (Kafka)

10 Physical Threat Response Optimization tool (PTRO)

The PTRO tool will provide efficient exodus ways given different scenarios possible. It will be used both to a better management of organised events (such as concert) and in case of critical events (such as a criminal attack). The prediction tools developed by UPAD will take into consideration different variabilities and, in case of alert, it will be used by the police and emergency forces to manage in a better way the citizens exodus and the arrival of the police/first aid operators. In addition, when needed, it will be combined with a broad communication tool, such as the Trio App for Oslo or a SMS alert system in Padova.

10.1 Responsible Partner

CPAD

10.2 Tool internal/commercial name

There's not commercial approach for this tool.

10.3 Tool Technology Readiness Level (TRL)

TRL 3

10.4 Data Sources

TBD

10.5 Tool data delivery

TBD

10.6 Tool Functionalities

10.6.1 Data acquisition

Description	Thanks to the sensors of the city many data will be acquired
User roles	operator/technician
Maturity	TBD
Interface (service, methods, data structures)	TBD

10.6.2 Scenario anticipation/forecast

Description	An elaboration of the data will lead to a simulation of the most likely scenario of exodus in different conditions
User roles	operator/technician
Maturity	The tool is already finalized on a theoretical level, but it will be developed on a real scenario for the first time.
Interface (service, methods, data structures)	TBD



10.6.3 Communication

Description	In case of need it will be possible to communicate useful exodus information to the population or to the police/emergency forces. Cities are free to develop the communication tool as they prefer. CPAD: SMS service to citizen, OSLO app Trio.
User roles	Police officers
Maturity	Both the tools proposed by the Cities are already existing. They just need to be connected with the IMPETUS platform
Interface (service, methods, data structures)	TBD

11 Cyber Threat Mapping tool (CTM)

The Cyber Threat Mapping tool is based in Prelude OSS, the freeware version of Prelude SIEM³, which is a Security Information and Event Management (SIEM) tool, for the generation and reporting of cybersecurity alerts. Under the scope of the IMPETUS project, we will refer to either Prelude OSS or Prelude SIEM as Prelude, for simplicity reasons. It is composed of monitoring software that collects and processes events created by other tools (e.g., events stored in the log files of an antivirus, network firewalls or intrusion detection systems). It can also be used to enrich and process inputs from other cybersecurity tools (e.g., XM Cyber's BAS tool), by using the IDMEF alert standard format (cf. RFC 4765⁴ for further details). Additionally, alerts can also be displayed and explored by security analysts via graphical user interface (GUI) dashboards.

In the IMPETUS project, Prelude will be extended with the use of the ELK stack⁵, which is the abbreviation for three open-source projects, namely Elasticsearch, Logstash and Kibana. The goal of the Cyber Threat Mapping tool is to add further processing and reporting capabilities to Prelude, as well as to provide new dashboards to cybersecurity analysts. Hereinafter, we will refer to Prelude-ELK to the extended tool used in IMPETUS. The flow chart in Figure 6 illustrates the idea.

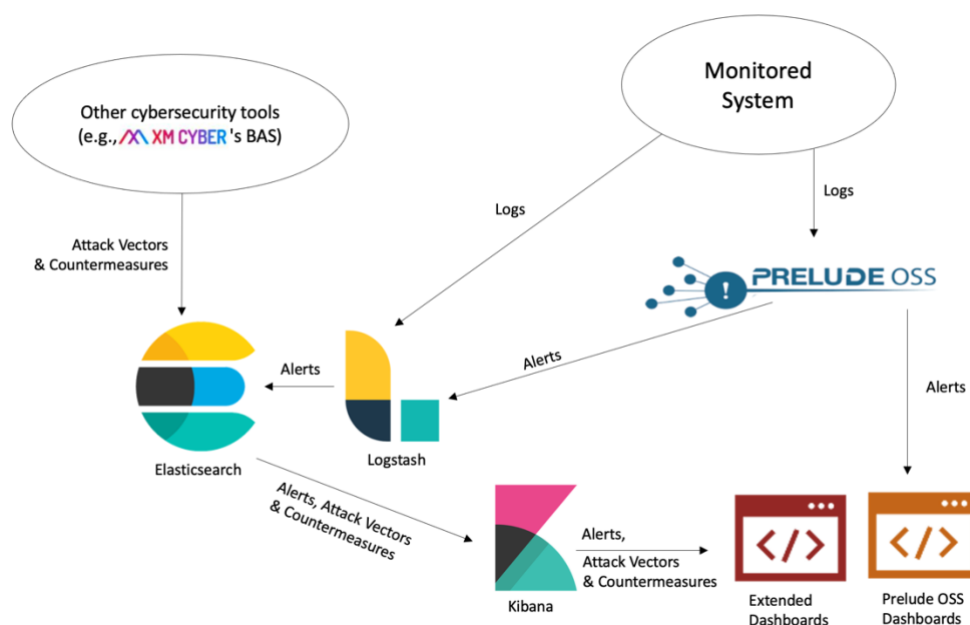


Figure 6. Prelude-ELK flow chart showing the inputs, processes and outputs.

Elasticsearch allows indexing and processing unstructured data. It also provides a distributed web interface to access the resulting information. Logstash is the parsing engine associated with Elasticsearch for collecting, analysing, and storing logs. It can integrate many sources simultaneously.

³ Cf. <https://www.prelude-siem.com/> and <https://www.prelude-siem.org/> for additional details about both versions.

⁴ The Intrusion Detection Message Exchange Format (IDMEF), available at <https://tools.ietf.org/html/rfc4765>

⁵ Additional information about the ELK stack is available at <https://www.elastic.co/what-is/elk-stack>



Finally, Kibana is a data visualization platform that provides visualization functionalities on indexed content in Elasticsearch. Users can create dashboards with charts and maps of large volumes of data.

11.1 Responsible Partner

IMT

11.2 Tool internal/commercial names

Prelude SIEM (<https://www.prelude-siem.com/>) – This tool is developed by a third party.

Prelude OSS (<https://www.prelude-siem.org/>) – Also developed by a third party.

ELK Stack (<https://www.elastic.co/what-is/elk-stack>) – Developed by third parties.

11.3 Tool Technology Readiness Level (TRL)

TRL 6 – Technology demonstrated in relevant environment

11.4 Data Sources

Unstructured recording of events (e.g., log files from an operating system or network device) using the syslog format (cf. RFC 5424⁶).

11.5 Tool data delivery

Web interface

11.6 Tool Functionalities

11.6.1 Receive logs

Description	Prelude-ELK is installed as a service on a Docker container, configured to receive syslog files from the components of the monitored system, using events messages on an IP network.
User roles	Security analysts via dashboards
Maturity	TRL 6 - Dockerised version of Prelude-ELK, composed of VMs, containers and configurations.
Interface (service, methods, data structures)	Use of RFC 5424 (syslog) interface for the collection of logs.

11.6.2 Generate alerts

Description	Based on automated rules to generate cybersecurity IDMEF alerts.
User roles	Security analysts via dashboards
Maturity	TRL 6 - Dockerised version of Prelude-ELK, composed of VMs, containers and configurations.

⁶ <https://tools.ietf.org/html/rfc5424>

Interface (service, methods, data structures)	Prelude-ELK already installed on the containers. An alert database, in which the alerts of Prelude-ELK will be stored, is also installed and configured as a container.
--	---

11.6.3 Correlate alerts

Description	Based on automated rules to correlate and generates cybersecurity alerts. For example, when a user tries to get remote access several time on a machine, Prelude-ELK will correlate previous alerts into a new 'Brute Force' alert.
User roles	Security analysts via dashboards
Maturity	TRL 6 - Dockerised version of Prelude-ELK, composed of VMs, containers and configurations.
Interface (service, methods, data structures)	Prelude-correlator tool and required scripts, already installed on a container in the Dockerised version of Prelude-ELK.

11.6.4 Visualize alerts

Description	Visualization of events and processed alerts, either in raw, IDMEF or additional formats.
User roles	Security analysts via dashboards
Maturity	TRL 6 - Dockerised version of Prelude-ELK, composed of VMs, containers and configurations.
Interface (service, methods, data structures)	Standard and extended Prelude-ELK dashboards, already installed on containers in the Dockerised version of Prelude-ELK.

11.6.5 Timeline visualization

Description	Visualization of events and processed alerts, either in raw, IDMEF or additional formats, and its distribution across time (e.g., using chart bar diagrams).
User roles	Security analysts via dashboards
Maturity	TRL 6 - Dockerised version of Prelude-ELK, composed of VMs, containers and configurations.
Interface (service, methods, data structures)	Standard and extended Prelude-ELK dashboards, already installed on containers in the Dockerised version of Prelude-ELK.

11.6.6 Additional information



Additional information about the Cyber Threat Mapping tool, and Prelude-ELK, is available in the user manual appendix.

12 Future Work

At this point, a general observation regarding the tools for the IMPETUS project is that the maturity of the toolkit overall is pretty promising. If we compare the Technology Readiness Level (TRL) of the starting point for each of the tools in the project's definition, we will see that many of the tools are in progress or even have achieved the expected level of maturity for the end of the project.

Table 4. TRL status of each of the tools

Tool	GA – Start TRL	GA – End TRL	D3.1 - Actual TRL
Social Media Detection (SMD)	6	7	7
Weapon Detection (WD)	6	7	6
Biological Risk Detection (BRD)	5	7	6
Breach & Attack Simulation (BAS)	6	7	6
Cyber Threat Intelligence (CTI)	6	7	9
Physical Threat Intelligence (PTI)	5	7	4
Human Computer Interaction (HCI)	6	7	6
Physical Threat Response Optimization (PTRO)	6	7	3
Cyber Threat Mapping Tool (CTM)	5	7	6

However, there are some exceptions that we must certainly consider and clarify. First of all, during the development of WP3, we established the EARTO TRL Scale⁷ as the standard for determining the maturity level of each of the tools. This standardization process was not considered during the Grant Agreement writing phase, so some small deviations could be contemplated.

On the other hand, the PTRO tool has been modified after detecting some conflicting with the scope of the specifications included at the beginning of the project. In order to align with the user requirements (in WP1) and to optimize the PTRO tool impact, this tool will need further development and adaptation. To reflect the situation, we consider it more appropriate to categorise PTRO tool maturity as TRL 3 for now. A detailed report of the new status of the PTRO tool (and all the other tools) will be provided to the reader in *D3.2 - Secure Smart City Tool development final report*.

The PTI TRL level included in the proposal was considering the maturity of the algorithms used in it (Spark-GHSOM⁸ and DENCAS⁹) but not the tool overall, which is still under development. We have

⁷ https://www.earto.eu/wp-content/uploads/The_TRL_Scale_as_a_R_I_Policy_Tool_-_EARTO_Recommendations_-_Final.pdf

⁸ <https://www.sciencedirect.com/science/article/pii/S0020025518309496>

⁹ <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0207-2>



corrected the situation in this document by indicating the actual TRL of the tool (TRL 4 for now). The expected final maturity of the tool (TRL 7) is expected to be accomplished.

Another relevant perspective regarding the diversity, in terms of maturity and divergent projection of each of the tools, is to highlight that not only the maturity level is planned to be different for all the tools at the beginning and the end of the project. The partners have also different objectives regarding their tools. Some of the tools are mature enough to be integrated in the IMPETUS platform, with no other development expected. However, other tools will require the development or the modification of components -such as data connectors or operational capabilities- that will bring the opportunity to the responsible partners to obtain a much more mature product. Lastly, other tools, in a development status (also without an existing product), will have the opportunity to develop new capabilities that will be specifically addressed by the IMPETUS project.

The development of the WP3 tools and its integration to the IMPETUS platform is an iterative process that needs to be aligned and synchronized with the results of the rest of WPs in the project, from the definition of the platform and its architecture (WP2), the iteration over the user requirements (WP1), the platform validation (WP7), the user interface definition (WP4), the compliance with legal and ethical aspects and frameworks (WP5 and WP11), etc. This collaborative workflow will be reflected in the next deliverables produced in WP3 and will be a definitive condition for the development of the toolkit, the maturity level achieved by each of the tools and its integration in the IMPETUS ecosystem.












13 APPENDIXES – USER MANUALS









The last pages of this document include user manuals from most of the tools described in the deliverable. Due to low maturity at this point of the project, no manual is available for the PTRO tool. The manuals are provided in the following order:

1. Social Media Detection tool (SMD)
2. Weapon Detection tool (WD)
3. Biological Risk Detection tool (BRD)
4. Breach & Attack Simulation tool (BAS)
5. Cyber Threat Intelligence tool (CTI)
6. Physical Threat Intelligence tool (PTI)
7. Human Computer Interaction tool (HCI)
8. Cyber Threat Mapping tool (CTM)

Members of the IMPETUS consortium

	SINTEF, Strindvegen 4, Trondheim, Norway, https://www.sintef.no	Joe Gorman joe.gorman@sintef.no
	Institut Mines Telecom, 19 place Marguerite Perey, 91120 Palaiseau, France, https://www.imt.fr	Joaquin Garcia-Alfaro joaquin.garcia_alfaro@telecom-sudparis.eu
	Université de Nîmes, Rue du Docteur Georges Salan CS 13019 30021 Nîmes Cedex 1, France, https://www.unimes.fr	Axelle Cadere axelle.cadere@unimes.fr
	Consorzio Interuniversitario Nazionale per l'Informatica, Via Ariosto, 25, 00185 – Roma, Italy, https://www.consortio-cini.it	Donato Malerba donato.malerba@uniba.it
	University of Padova, Via 8 Febbraio, 2 - 35122 Padova, Italy, https://www.unipd.it	Giuseppe Maschio giuseppe.maschio@unipd.it
	Biotehnoloogia ja Meditsiini Ettevõtluse Arendamise Sihtasutus, Tiigi 61b, 50410 Tartu, Estonia, https://biopark.ee	Sven Parkel sven@biopark.ee
	SIMAVI, Complex Victoria Park, Corp C4, Etaj 2, Șos. București – Ploiești, nr. 73 – 81, Sector 1, București, Romania, https://www.simavi.ro	Gabriel Nicola Gabriel.Nicola@simavi.ro Monica Florea Monica.Florea@simavi.ro
	Thales Nederland BV, Zuidelijke Havenweg 40, 7554 RR Hengelo, Netherlands, https://www.thalesgroup.com/en/countries/europe/netherlands	Johan de Heer johan.deheer@nl.thalesgroup.com
	Cinedit VA GmbH, Poststrasse 21, 8634 Hombrechtikon, Switzerland, https://www.cinedit.com	Joachim Levy j@cinedit.com



	Insikt Intelligence, Calle Huelva 106, 9-4, 08020 Barcelona, Spain, https://www.insiktintelligence.com	Dana Tantu dana@insiktintelligence.com
	Sixgill, Derech Menachem Begin 132 Azrieli Tower, Triangle Building, 42nd Floor, Tel Aviv, 6701101, Israel, https://www.cybersixgill.com	Benjamin Preminger benjamin@cybersixgill.com Ron Shamir ron@cybersixgill.com
	XM Cyber, Galgalei ha-Plada St 11, Herzliya, Israel https://www.xmcyber.com	Lior Barak lior.barak@xmcyber.com Menachem Shafran menachem.shafran@xmcyber.com
	City of Padova, via del Municipio, 1 - 35122 Padova Italy, https://www.padovanet.it	Enrico Fiorentin fiorentine@comune.padova.it Stefano Baraldi Baraldis@comune.padova.it
	City of Oslo, Grensen 13, 0159 Oslo, Norway, https://www.oslo.kommune.no	Osman Ibrahim osman.ibrahim@ber.oslo.kommune.no
	Institute for Security Policies, Kruge 9, 10000 Zagreb, Croatia, http://insigpol.hr	Krunoslav Katic krunoslav.katic@insigpol.hr
	International Emergency Management Society, Rue Des Deux Eglises 39, 1000 Brussels, Belgium, https://www.tiems.info	K. Harald Drager khdrager@online.no
	Unismart – Fondazione Università degli Studi di Padova, Via VIII febbraio, 2 - 35122 Padova, Italy, https://www.unismart.it	Alberto Da Re alberto.dare@unismart.it



IMPETUS

First draft version - Example

Social Media Detection tool - Spotlight - User Manual



Uncovering Hidden Intelligence

General Information	3
Overview	3
Languages Retrieved/Analysed	3
Analysis	3
NLP Features	4
Significance Score	4
Hate Speech Score	4
Sources of Information	6
Dashboards	7
Overview	7
Content of the dashboards	8
Menu bar	8
General - Summary	8
General - Raw Data	9
Content - Messages	9
Content - NLP features (concepts, entities, topics, key ideas, hashtags)	10

General Information

Overview

The objective of this manual is to show Spotlight's capabilities in the following use cases:

Monitoring different Social Media platforms and digital newspapers to detect messages and relationships suspicious of being a threat in the cities of Padova and Oslo.

Data sources in these use cases are:

Use case	Data sources
Padova	Social Media: <ul style="list-style-type: none">• Twitter• Youtube• TikTok
	Local Press: <ul style="list-style-type: none">• mattinopadova.gelocal.it
Oslo	Social Media: <ul style="list-style-type: none">• Twitter
	Local Press: <ul style="list-style-type: none">• document.no• reset.no• vg.no• dagbladet.no

Languages Retrieved/Analysed

AI will be applied to text in 5 languages:

- English
- Italian
- Norwegian
- French
- Arabic

Analysis

Description of the features extracted from the Natural Language Processing engine also referred to as the NLP engine from here onwards.

NLP Features

The core of Spotlight is an NLP engine that analyzes all the messages and extracts and abstracts the following information:

Feature	Definition	Values
Concept	Terms included in the message	List of words
Entity	People, organizations, and places included in the message.	List of words
Topic	Message topic	List of topics
Sentiment	Author's attitude towards a person, product, topic, etc. (positive, negative, or neutral).	-5 (very negative) to +5 (very positive)
Hashtags	Hashtags included in the message.	List of hashtags

Significance Score

This Score evaluates the importance of a message based on the chosen domain to be analyzed in the project - specific context* or engagement. In case the chosen domain is 'Engagement', the Score measures how a message is ranked in the social media from the point of view of its engagement (number of shares, comments and received likes) , the impact of its author in SM (number of friends and followers) and the PageRank metric.

*Which in this case are the potential threats and extremists in the cities of Padova and Oslo.

The scale of such a score is ranged from 0 to 1, and each subsection of such a range has a different meaning. These are the following:

Ranged Values	Definition
0 - 0.4	Low significance score and impact in SM
0.4 - 0.6	Light significance score and impact in SM
0.6 - 0.8	High significance score and impact in SM
0.8 - 1	Very high significance score and impact in SM

Hate Speech Score

This score measures the probability of a text to have hate speech content:

- Personal attacks: threats against people or organizations.
- Bigotry, hate speech against minorities, groups, countries, etc.

Values	Probability
0.0 - 0.5	No hate speech
0.5 - 0.7	Low
0.7 - 0.9	High
0.9 - 1	Extreme

Dashboards

Overview

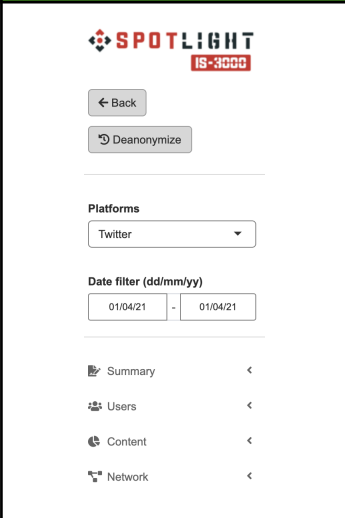
Summary	General	Summary of all the content.
	Raw data	Table with all the data analyzed in the dashboard.
Users	General	Summary of all the users information, including all the scores. <u>Disclaimer:</u> Only some specific roles will have permissions to <u>anonymize/deanonymize</u> usernames.
Content	Messages	Scores at a message level.
	Concepts	Main concepts written in the message.
	Entities	Entities mentioned in the messages.
	Topics	Message topics (defined by the user).
	Key-ideas	Message topics (not pre-defined).
	Hashtags	Hashtags used.
Network	Interactions	A network of the observed interactions based on the mentions. Detection of influencers or discovering new suspicious users.
	Disruption	Networks are disrupted by different internal and external interactions. Six criterias are defined and users are ranked based on them.

All the social media data sources are shown in the same dashboard, for the sake of simplicity, including dashboards to analyze the message contents and to extract information

about the users. All local newspapers for each city will be also displayed in the same dashboard.

Content of the dashboards

Menu bar

Graph	Content	Capabilities
	Summary of all the data retrieved and analyzed	<p>Filter all the data shown in the dashboard's tabs by:</p> <ul style="list-style-type: none"> • Date • Data source <p>Choose the dashboard tab.</p>
Hints	Daily updates.	Choose a period of time of the current day to review the daily updates.
	Specific data source.	Filter by data source to show all the data of a specific platform.

SPOTLIGHT IS-3000

← Back

↺ Deanonimize

Platforms

Twitter

Date filter (dd/mm/yy)

01/04/21 - 01/04/21

Summary

Users

Content

Network


Data deanonymization (only for authorised users)

Choose the data source to fill the dashboard

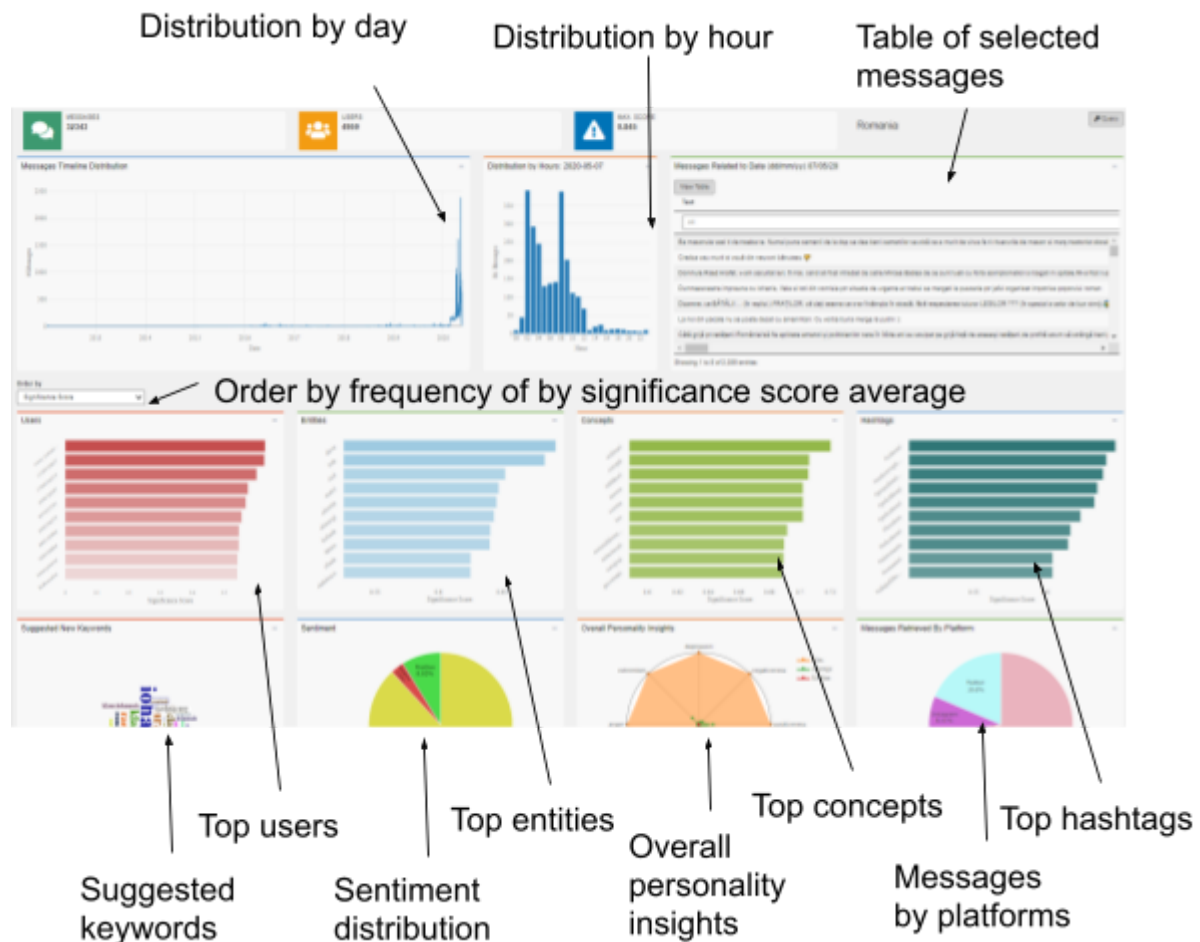
Filter by date: choose a period of time

Menu bar with all the dashboards

General - Summary

Graph	Content	Capabilities
	Summary of all the data retrieved and analyzed	<ul style="list-style-type: none"> • Number of messages by day. • Number of messages by hour. • Table of messages by day. • Top values of users, entities, concepts and hashtags. • Suggested keywords for new projects/searches. • Sentiment distribution. • Overall personality insights. • Messages by platforms.
Hints	Daily updates.	Click over one day to get all the messages of this day
	Order values by frequency	Choose order by frequency to show the most frequent terms and more active users.

	Order by Significance Score	Choose order by Significance Score to show terms and users in messages with high Significance Score.
	Messages containing a term	Click on a bar to show all the messages with this content.
	Suggested keywords	Terms that can be used for future searches
	Personality insights	<p>Personal insights are scores evaluated from words that could express signs of depression, anger, disgust, positiveness or negativeness.</p> <p>Overall sentiment intensity among all those five emotions.</p>



Ordered by frequency:

- The dashboard shows the most frequent terms and more active users.

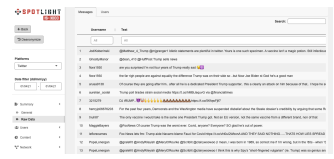
Ordered by Significance Score:

- Most frequent terms in messages with high Significance Score, that is, in terms of messages with high relevance to a given context.

General - Raw Data

Raw data page contains all the data analyzed in the project, in a table format.

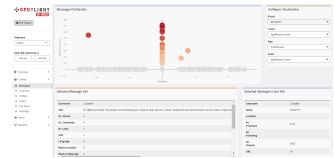
It is useful for searching and filtering across all the information collected and showing them in a table format.

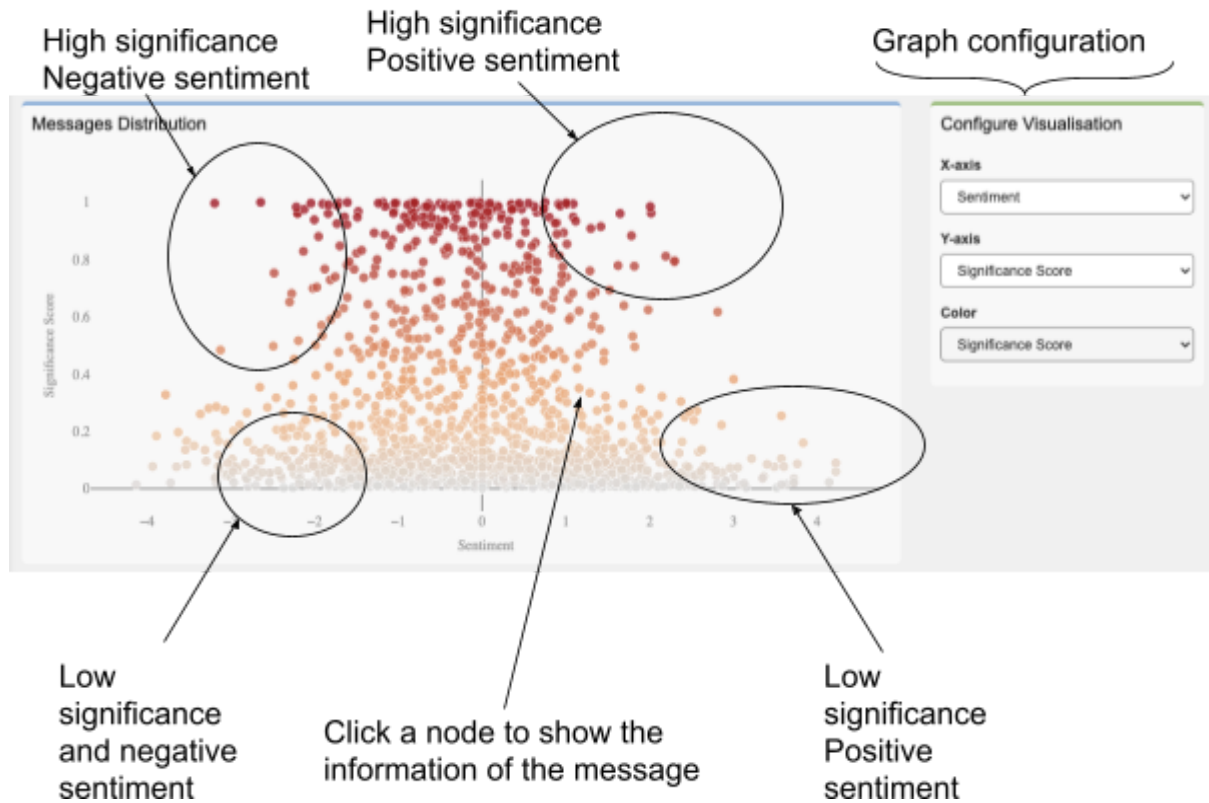
Graph	Content	Capabilities
	<ul style="list-style-type: none"> • Table with all the data. • Table with the content of a specific message. • Filters. 	<p>Filter by:</p> <ul style="list-style-type: none"> • Username (see disclaimer about data anonymized in Overview section) • Text • Nr. Shares (Rank) • Nr. Comments (Rank) • Nr. Likes (Rank) • URL • Reply to Author • Reply to Message • Timestamp (Rank) • Significance Score (Rank) • Sentiment (Rank) • Date (Rank)
Hints	Discover influence content.	Filter by Significance Score above 0.5 to discover messages with high relevance.
	Daily updates.	Filter by time to check the daily new content.
	Discover negative-positive messages	Filter by Sentiment below -0.5 (above +0.5) to discover negative (positive) messages.

Content - Messages


The Messages page contains all the messages retrieved, making letting the user scroll through or filter them.

See disclaimer about data anonymized in Overview section

Graph	Content	Capabilities
	Significance Score, Hate speech, and Sentiment of all the messages	Three dimension (X-axis, Y-axis and Color) graph configuration can be set among the following concepts: <ul style="list-style-type: none"> • Significance Score • Hate Speech • Sentiment • Positiveness • Negativeness • Depression • Anger • Disgust
Hints	Discover top messages in terms of impact and positive / negative sentiment.	Select all the top - right messages.
	Discover messages with very positive (or negative) content.	Select all the top messages.
	Discover messages with high impact.	Select all the messages to the right.



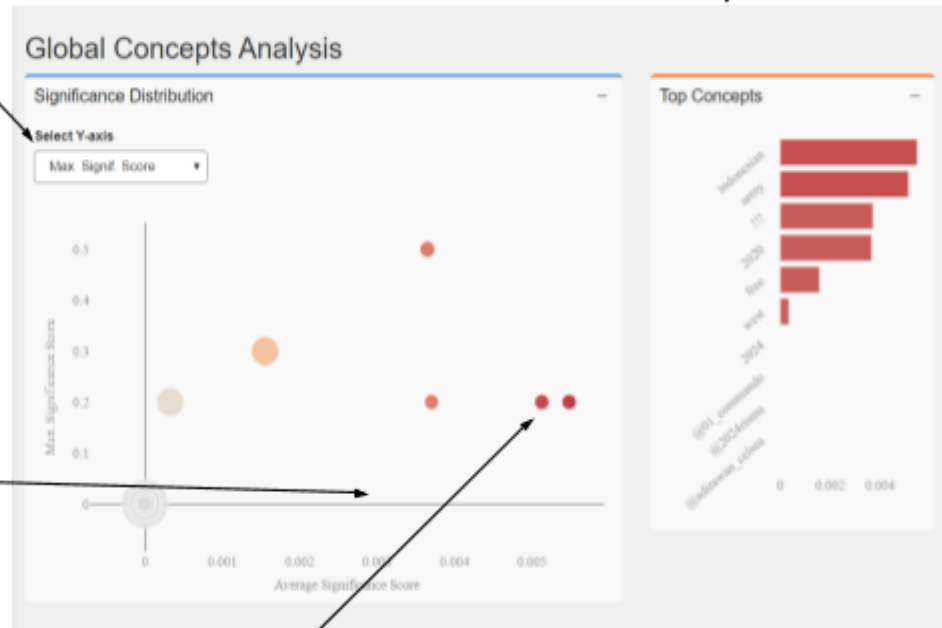
Content - NLP features (concepts, entities, topics, key ideas, hashtags)

Graph	Content	Capabilities
	<ul style="list-style-type: none"> Graphs with the features in messages having the highest Significant Scores: <ul style="list-style-type: none"> Topics Concepts Hashtags Entities Key ideas 	<p>Select features to visualize evolution.</p>
Hints	Discover trends in the conversation.	Choose different time periods to check the trends in these periods of time.

Most frequent concepts

Choose the y axis score

X axis Significance score



Click the node to show the information about the concept

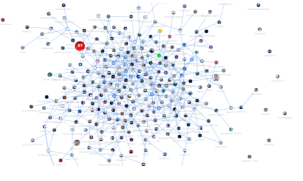
With the Significance distribution graph we can discover the following information:

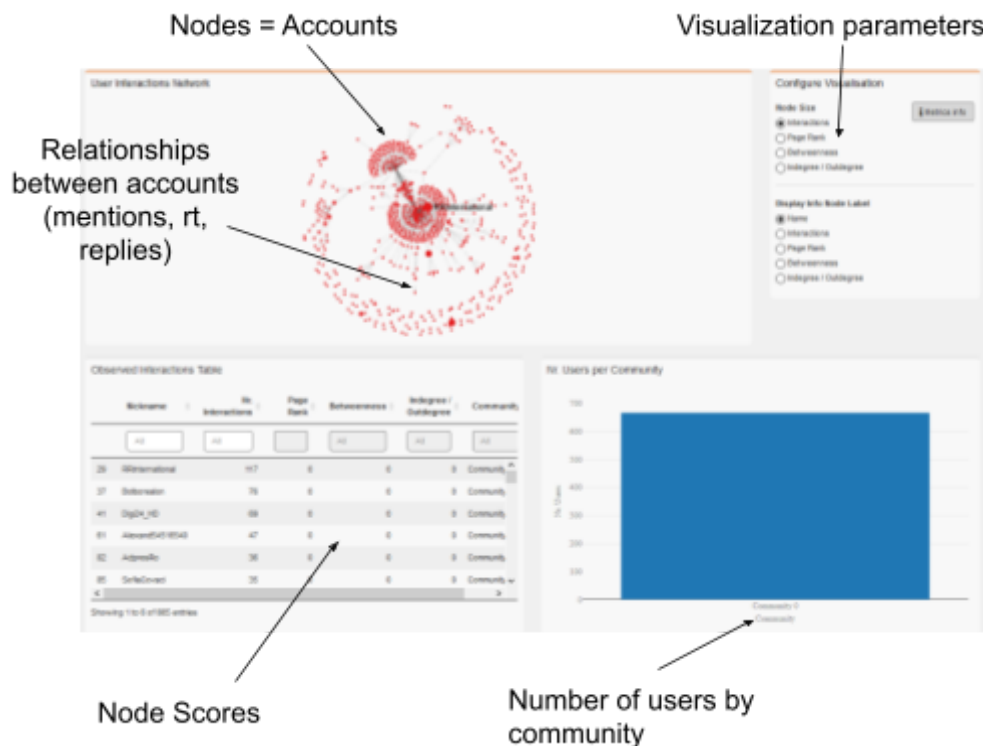
Dashboard	Meaning	Useful for
Concepts	Concepts used in the most significant/important or the main messages.	Discover new concepts users are writing about.
Entities	Entities that appear in the most significant/important or the main messages.	What are they writing about in terms of people, locations and organizations?
Topics	Topics	Understand the main topics of interest of the more significant users.
Key Ideas	Key ideas used in the most significant/important or the main messages.	A way to detect trending topics in the most significant/important or the main messages.
Hashtags	Hashtags used in the most	Discover hashtags that are being used

	significant/important or the main messages.	in the main messages.
--	---	-----------------------

Network - Interactions

See disclaimer about data anonymized in Overview section

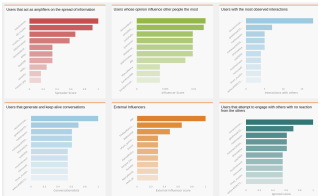
Graph	Content	Capabilities
	The network of accounts.	Accounts of the shared community (followers of both target accounts). The relationship between them is extracted by the interaction between them (mentions, rt, replies).
Hints	The network of specific accounts.	Select one node to check the links to other accounts.
	Node size.	The size of the node is proportional to the account activity.



The network contains only the top 300 accounts of the shared community (based on their influence score).

Network - Disruption

See disclaimer about data anonymized in Overview section

Graph	Content	Capabilities
	<p>Graphics with top users based on disruption criterias.</p>	<ul style="list-style-type: none"> • Top users that act as amplifiers on the spread of information • Top users whose opinion influence other people the most • Top users with the most observed interactions • Top users that generate and keep alive conversations • Top external users to the discussion that does not interact with the network • Top users attempting to engage with others with no reaction from them
Hints	Amplifiers of the spread of information	Users that are spreading the information through the network, by means of multiple interactions and observations.
	Top influencers	Users that drive the conversations and are mentioned a lot within the network.
	Users with most observed interactions	Users that interact the most with the network.
	Users that generate and keep alive conversations	Users that continue interacting in conversations that they started within the network.
	External influencers	Users not active in the discussion, not belonging to the network but mentioned a lot in the conversations.
	Users not able to engage	These users start interaction with the network but don't obtain any reaction.

Amplifiers of the spread of information

Top influencers

Users with most observed interactions



Users that generate and keep alive conversations

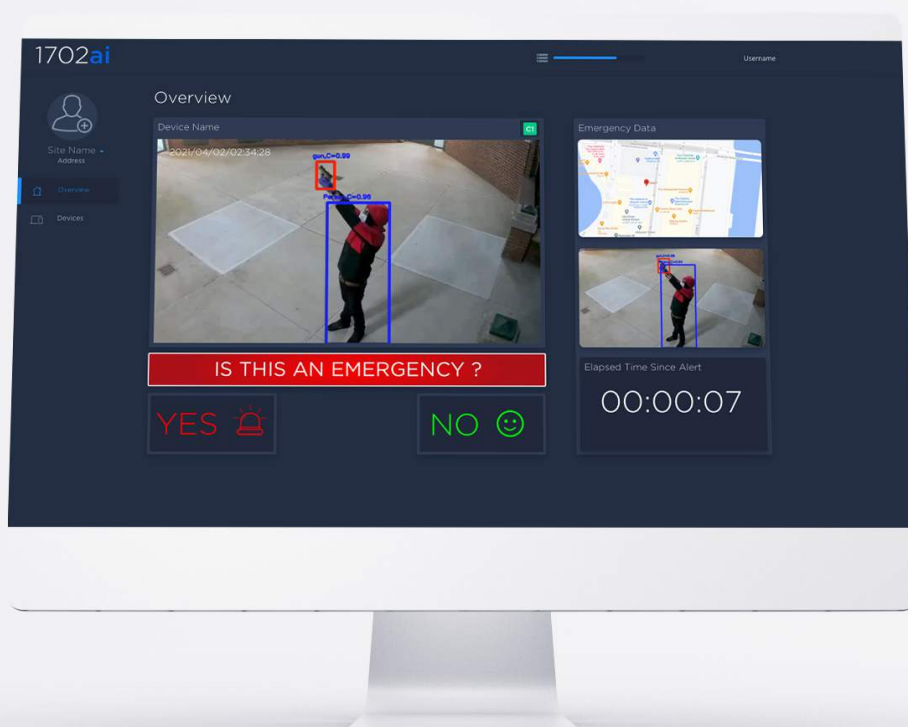
External influencers

Users not able to engage

1702ai SAMSON

User Manual V 1.0

Add gun detection to your existing RTSP/IP camera.



1702ai SAMSON

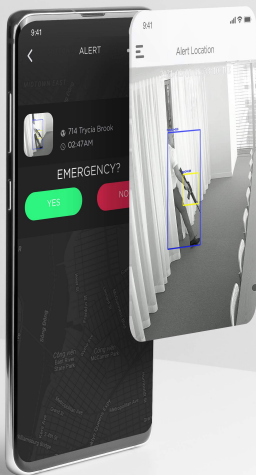
User Manual V 1.0

Add gun detection to your existing RTSP/IP camera.

SAMSON V 1.0 is an AI that detects small magazine-fed weapons in real-time using RTSP/IP cameras.

With SAMSON, the instant a weapon enters the camera field of view, alerts are shared with your dispatcher so they can be shared to the relevant teams. SAMSON provides instant situation awareness to first responders.

SAMSON saves lives, prestigious reputation and tremendous amounts of money.



1702ai SAMSON

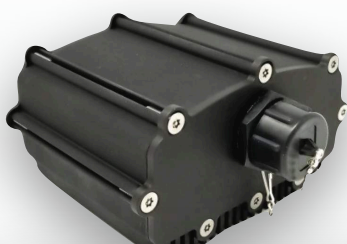
User Manual V 1.0 // INDEX

- Page 2 > Intro
- Page 3 > Index
- Page 4 > Falcon bOX Overview
- Page 5 > SAMSON Requirements
- Page 6 > SAMSON Sign In & Alert
- Page 7 > Add / Edit / Delete Device
- Page 8 > Add AI Edge Device
- Page 9 > Add Security Camera
- Page 10 > Start SAMSON
- Page 11 > SAMSON Alerts
- Page 12 > Undo & False Alerts
- Page 13 > History Tab
- Page 14 > Health Tab
- Page 15 > Retraining Tab

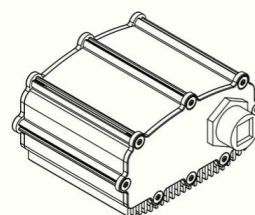
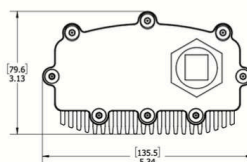
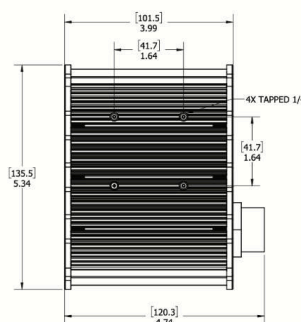
1702ai SAMSON

SAMSON Uses Our FALCON bOX To Add AI Gun Detection To Your RTSP/IP Camera

Falcon bOX is a rugged IP-67 embedded system that connects to your CCTV IP network. It is capable of reading several RTSP's and enables your existing video surveillance cameras to detect guns.



DIMENSIONS



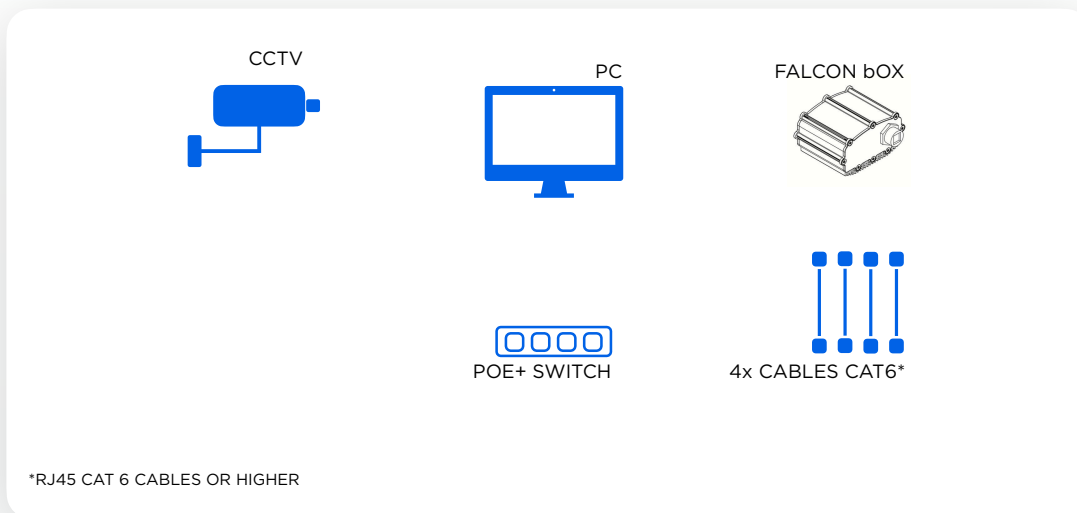
GENERAL	
# of IP cameras supported	1 to 4 (Dependent on the AI models implemented)
Max Resolution (per camera)	4K
Image Rate (per camera)	60 FPS
Video Input	H.264 & H.265 Input Supported
Max Frame Rate	60 FPS @ 4K
Privacy	hardware enforced privacy regions, GDPR compliant.
Web Browser Compatibility	Chrome, Firefox, and Microsoft Edge Browsers supported
PROCESSOR	
GPU	256 cores
Compute Performance	133 Teraflops
CPU	Dual-Core 1.5 64-Bit CPU and Quad-Core ARM
Memory	8 GB 128-bit LPDDR4 1600MHz
NETWORK	
Protocols	IPv4, IPv6, TCP, UDP, ARP, HTTP, HTTPS, DHCP, DNS, NTP, RTP/RTCP, RTSP
Streaming Protocols	Unicast(RTSP with configurable port + handle), Multicast(RTSP with configurable port and address ranges).
Authentication/Security	TLS Encrypted communication by default
PERIPHERALS	
Storage	NVMe SSD 1.2 and 4TB, BAI Cloud
SD Card	UHS Speed Class 1 or 3 Supported up to 30 MB/s (ships with 32GB card)
Audio	NA
ELECTRICAL	
Ports	PoE+ Female Ethernet Port
Network Cable Type/Speed	Cat5e or greater required @ 1000Mbps
Power Input	PoE+ (IEEE 802.3at)
Power Consumption (maximum)	25.5 W sustained, 30 W peak
MECHANICAL	
Camera Mount	2x 1/4-20 2" space bottom mount
Weight	2.43 lbs, 1102 kg
Dimensions (L x W x H)	9.5"x3"x3.5"
Housing Material	Aluminum

ENVIRONMENTAL	
Operating Temperature Range	NEMA TS2 which is -34°C to +74°C (~29.2F to 165.2F)
Operating Humidity	18 to 95% humidity over the range
Ingress Protection	IP67
Shock/Vibration	the ability to withstand 0.5g @ 5 to 30Hz vibration, and 10g's of shock
CERTIFICATIONS	
FCC, NEMA, IP67RoHS,CE	
OPTIONS	
Name	Description
NVMe M.2 Storage	Non-Volatile Memory Express (NVMe) SSD storage: 1TB, 2TB, or 4TB
SD Card Storage	UHS-1 16GB to 512GB SD Card
WiFi/Bluetooth Module	BAI PCB module that provides WiFi and Bluetooth capability onboard the DNN Cam
GPS/MJU Module	GPS - 20Hz Global position 3m; IMU - inertial measurement unit for anti tampering.
4G Module	Sierra Wireless 4G LTE modem with SIM / eSIM

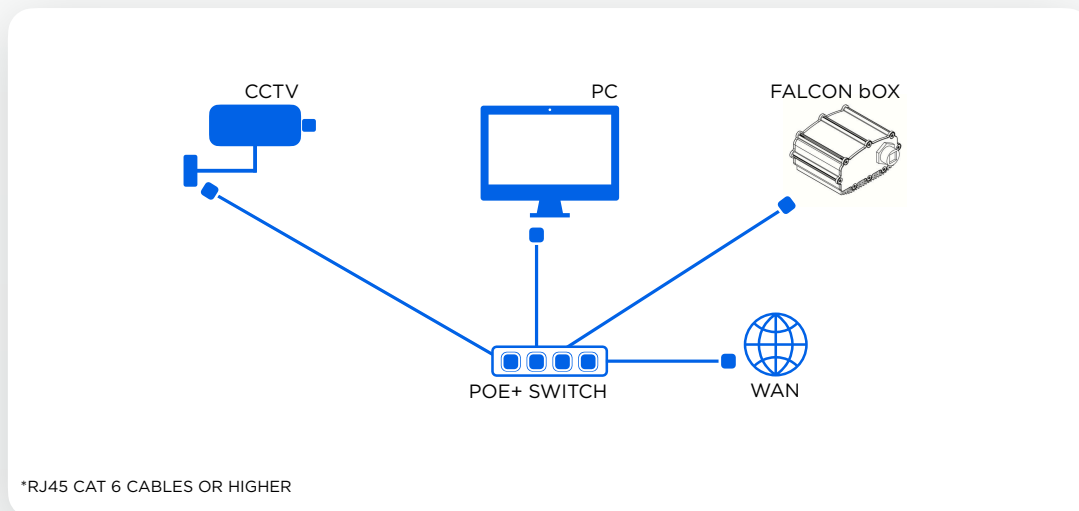


1702ai SAMSON

SAMSON Requirements

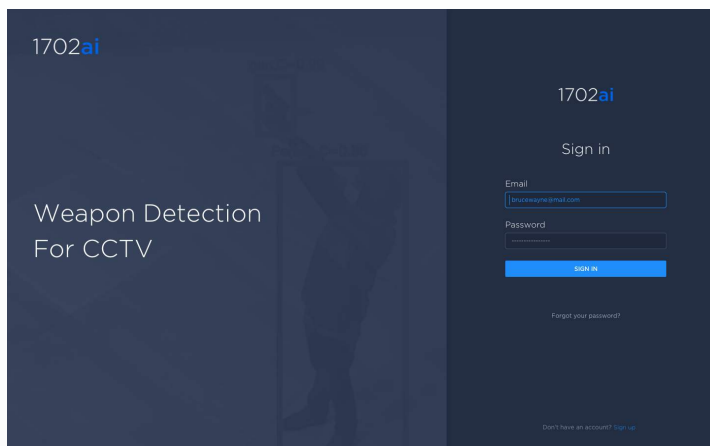


SAMSON Hardware Set Up



1702ai SAMSON

SAMSON Sign In



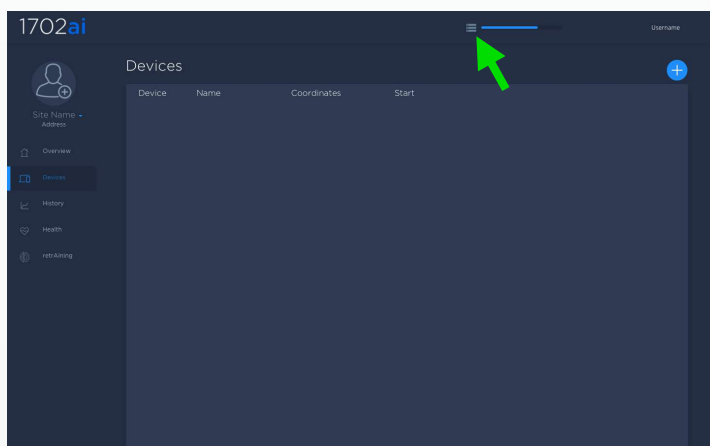
USING PC



Connect the Flacon bOX and PC to the same LAN. From the PC open a web browser, in the url address bar, type in the FALCON bOX IP address and sign in using your username and password.

If you do not have a password, click Sign Up.

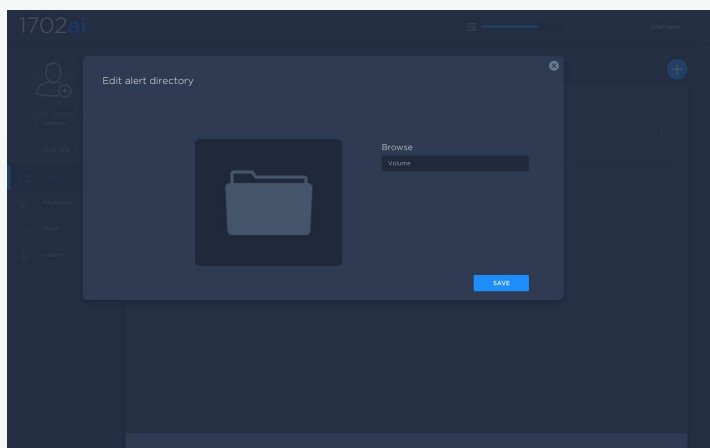
SAMSON Add Alert Directory



USING PC



Once logged in click the hard drive icon (green arrow) and choose a directory where the alerts will be written.



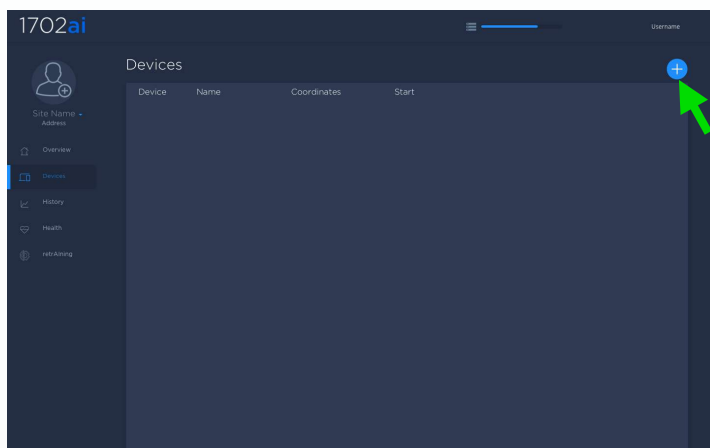
USING PC



Browse and select a directory. When the directory is selected click SAVE.

1702ai SAMSON

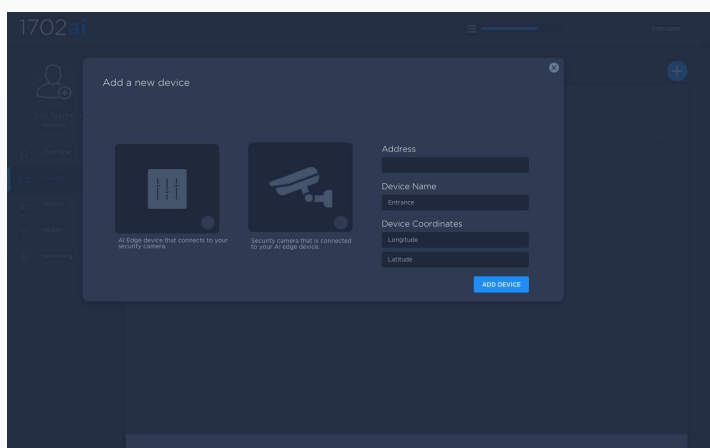
SAMSON Add Device



USING PC



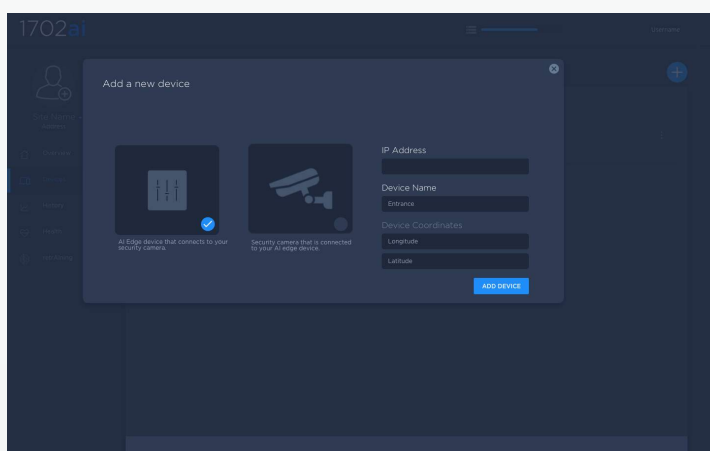
To add your first device, click the PLUS sign (green arrow).



USING PC



By default, the first device must be an AI edge device. Select AI Edge device and click ADD DEVICE.



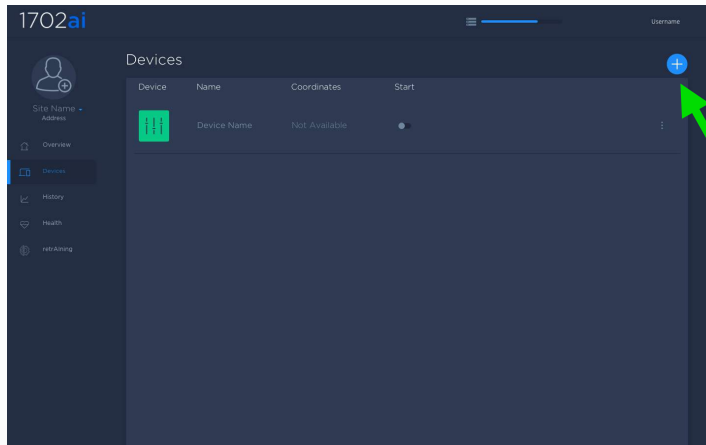
USING PC



Type the IP address of your Falcon bOX and Add a Name that will identify your Falcon bOX. The device coordinates are greyed out and not required as it is an input value related to security cameras only.

1702ai SAMSON

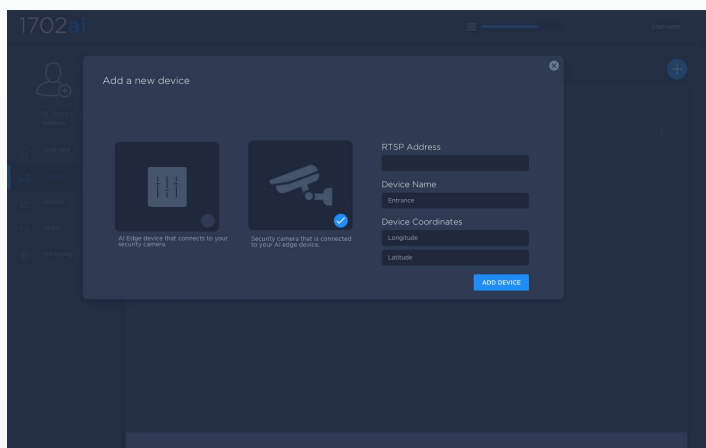
SAMSON Add AI Edge Device



USING PC



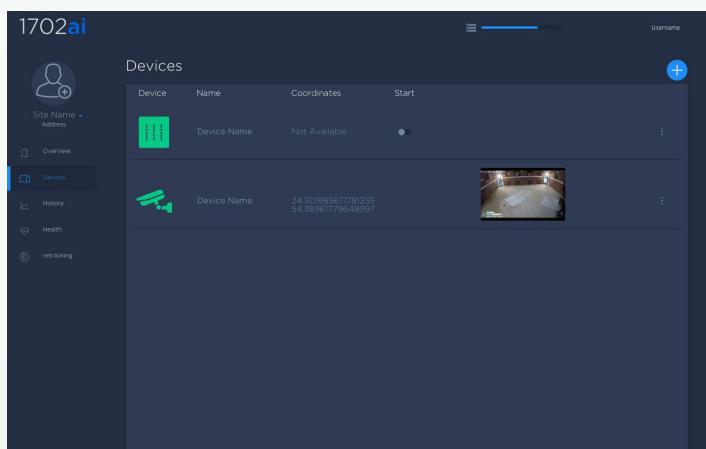
To add a Security Camera, click the blue plus sign. (Green Arrow)



USING PC



Select Security Camera, add the RTSP url, add a Device Name and input coordinates.



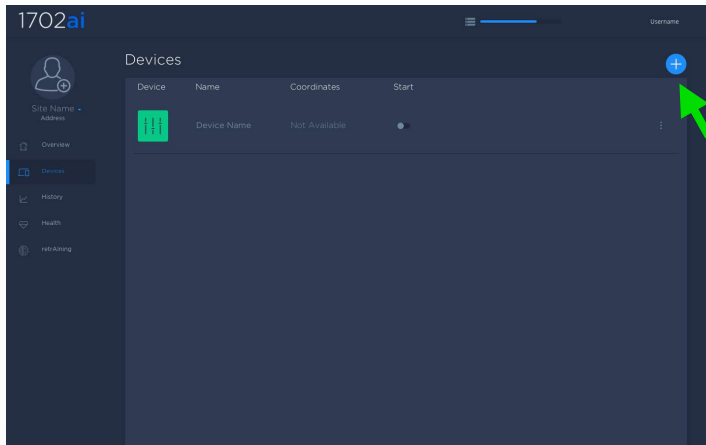
USING PC



If the RTSP url is correct, a low resolution thumbnail populates the security camera browser.

1702ai SAMSON

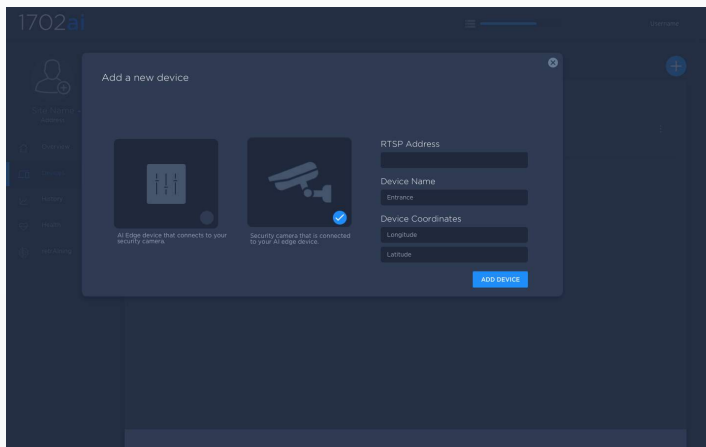
SAMSON Add Security Camera



USING PC



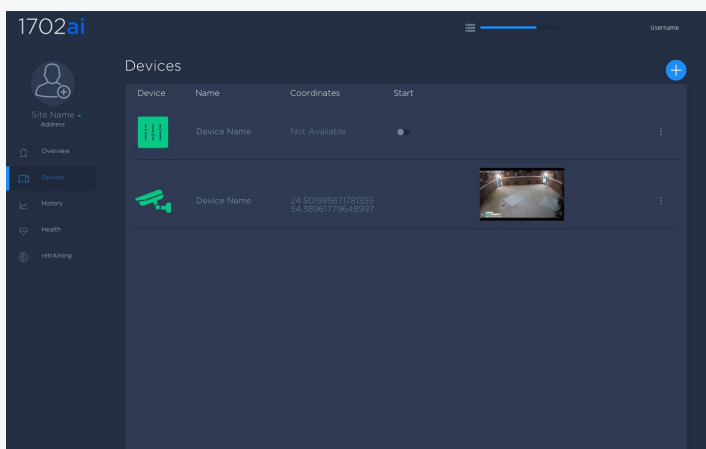
To add a Security Camera, click the blue plus sign. (Green Arrow)



USING PC



Select Security Camera, add the RTSP url, add a Device Name and input coordinates.



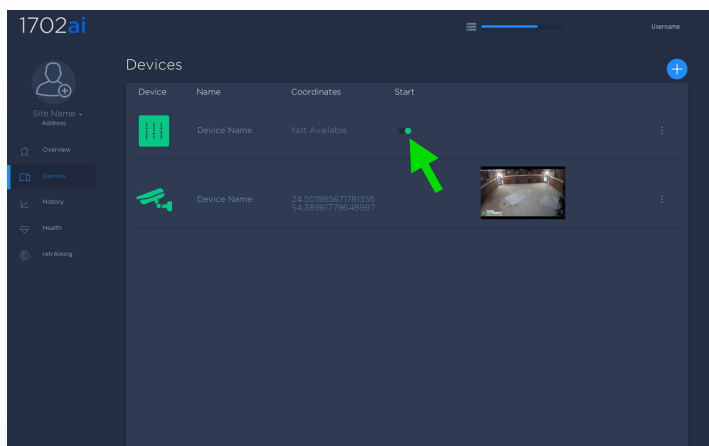
USING PC



If the RTSP url is correct, a low resolution thumbnail populates the security camera browser.

1702ai SAMSON

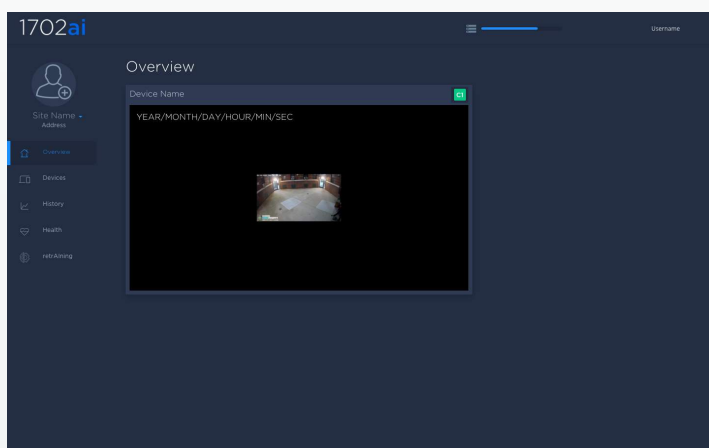
SAMSON Start



USING PC



To run SAMSON slide the Start button to the right (green arrow).



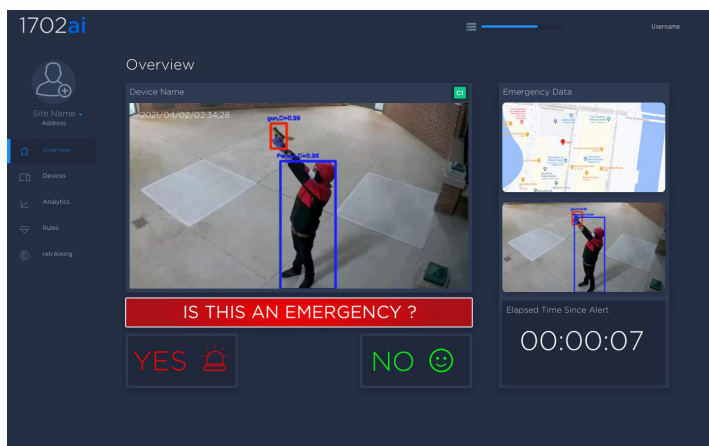
USING PC



Click on Overview, due to Data Privacy reasons, only a low resolution stream is shown.

1702ai SAMSON

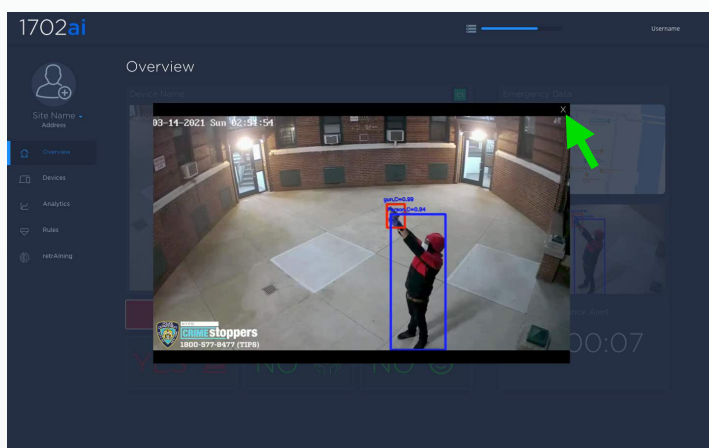
SAMSON Alert



USING PC



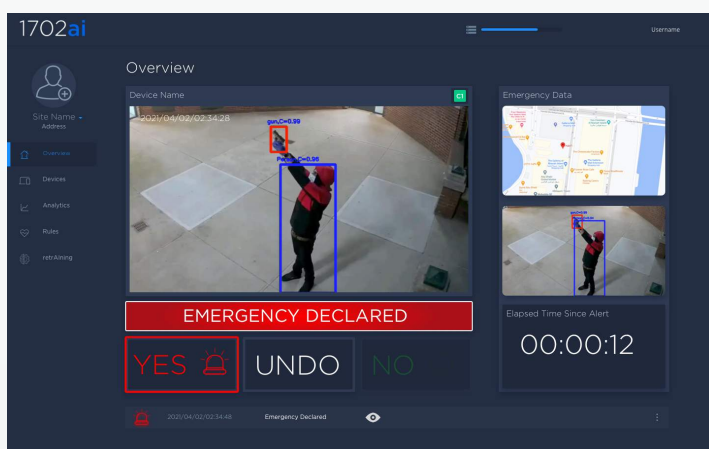
In Red Alert mode, a pop up populates the UI. The end user must validate the Emergency.



USING PC



When the user clicks on the still image, a jpeg is enlarged. Click the X (Green Arrow) to close the jpeg image. If the map is selected, a second web browser window will open and displays the alert location using your default map provider.



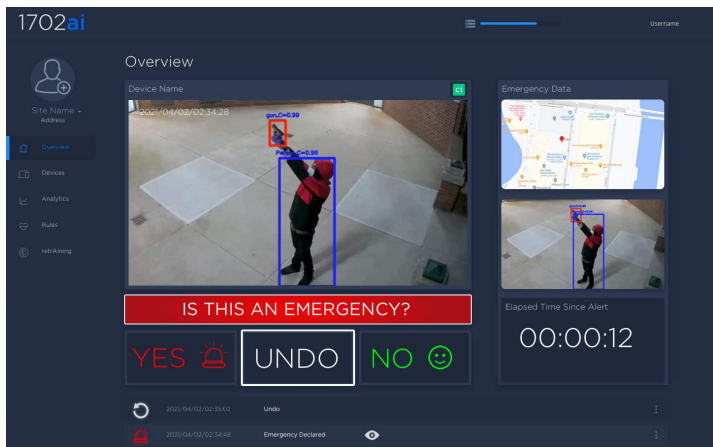
USING PC



When the end user selects YES a txt file is created in the alert directory. Then alert can be automatically escalated to the VMS of your choice.

1702ai SAMSON

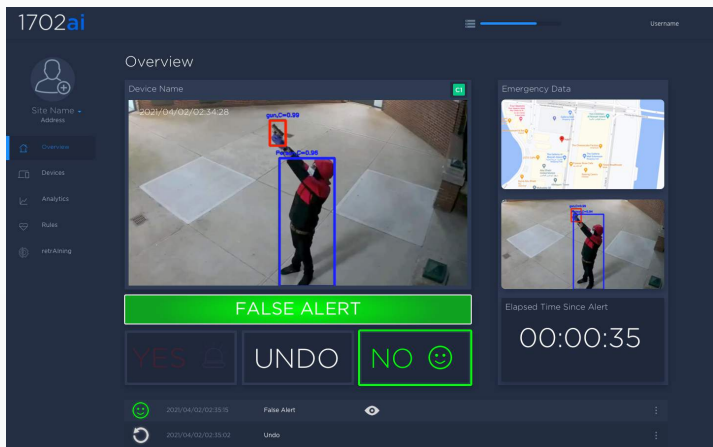
SAMSON Alert



USING PC



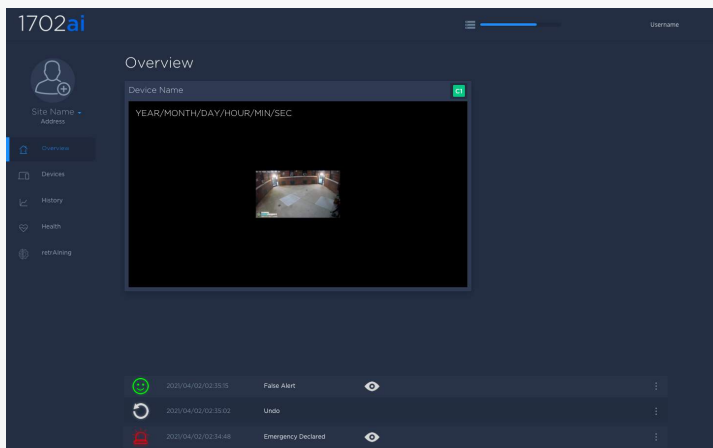
After an emergency is confirmed, when the end user selects UNDO, a text file is created in the alert directory to cancel the alert. UNDO can be automatically escalated to the VMS of your choice.



USING PC



In red alert mode, when the end user selects NO, the emergency is a FALSE ALERTS. A text file is created in the alert directory. The RAW video file of the FALSE ALERT is then pushed to 1702ai's CLOUD so SAMSON can be retrained in order not to produce the same FALSE ALERT.



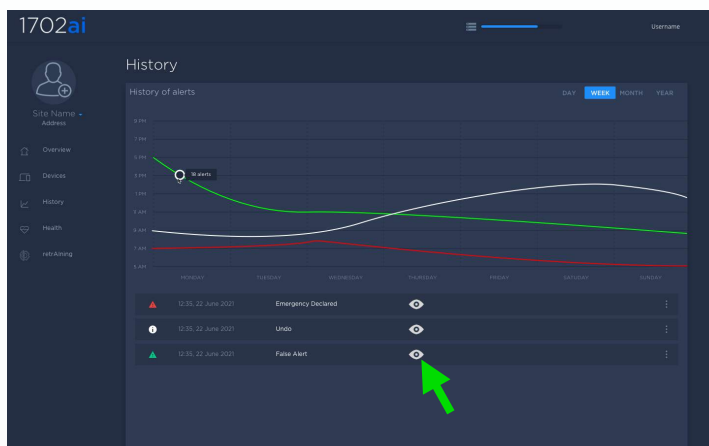
USING PC



By default, 10 seconds after an EMERGENCY is validated as NO, the overview UI becomes idle and a log is displayed below the stream.

1702ai SAMSON

SAMSON History



USING PC



In the History tab, the alert log displays all events using a GUI (Graphic User Interface). To visualise an alert, click on the eye (green arrow). It opens the alert directory where the alert is written.

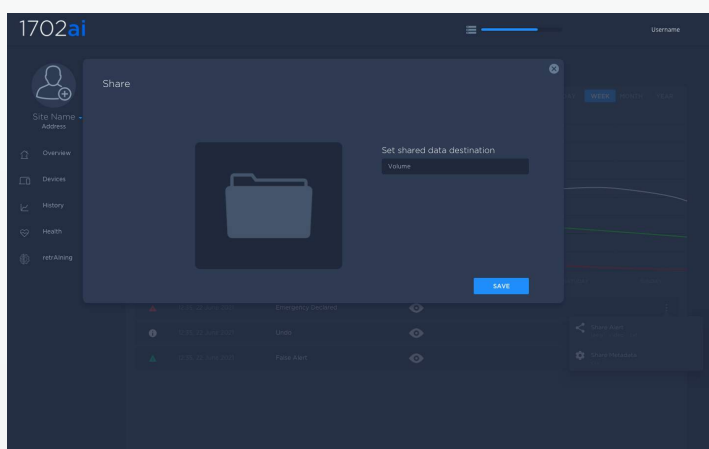


USING PC



In the history menu, each alert can be shared by clicking the three dots menu (green arrow). When selected a floating menu displays Share Alert or Share Metadata.

Using Share Alert, the jpeg - videos and text files generated by the alert can be shared in the directory of your choice. The Share Metadata shares a csv file that includes fps, time stamps, frame size and confidence.



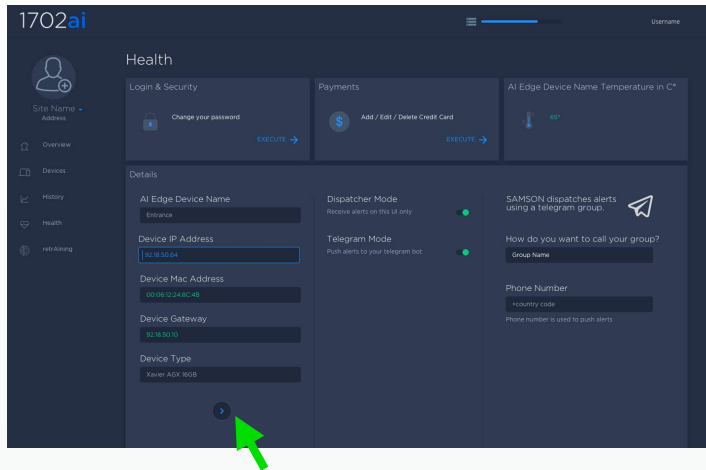
USING PC



When using Share Alert, the end user must specify the destination directory where the alert files have to be shared.

1702ai SAMSON

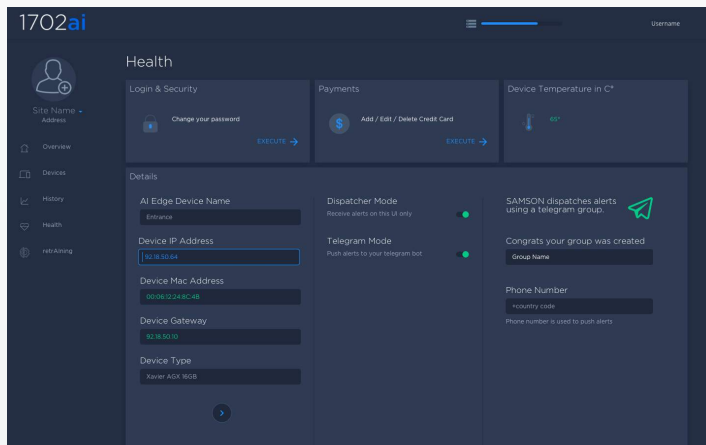
SAMSON Health



USING PC



The Health tab allows the end user to change the login credentials and set up the account for credit card payment. Using the right arrow (Green Arrow) the user can swipe through the devices that are connected. When Dispatcher Mode is on, when in red alert mode, the UI will generate pop ups for each alert. When Telegram Mode is on, all alerts are pushed to a Telegram Bot.



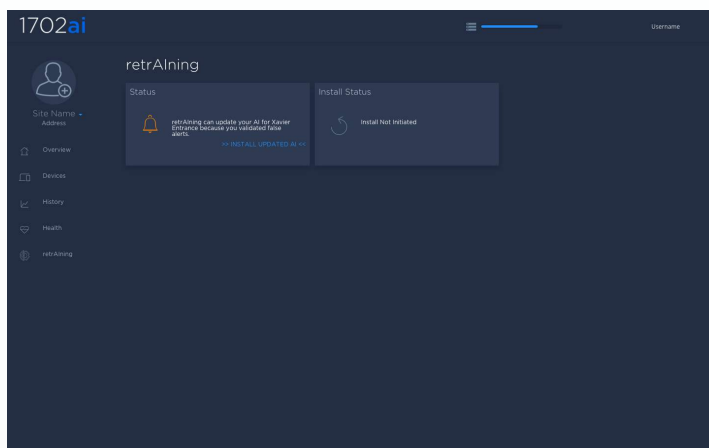
USING PC



When Telegram Mode is selected, SAMSON creates a Bot where the alerts are pushed. It is mandatory to add a telephone number for SAMSON to work with Telegram and have the LAN connected to the internet.

1702ai SAMSON

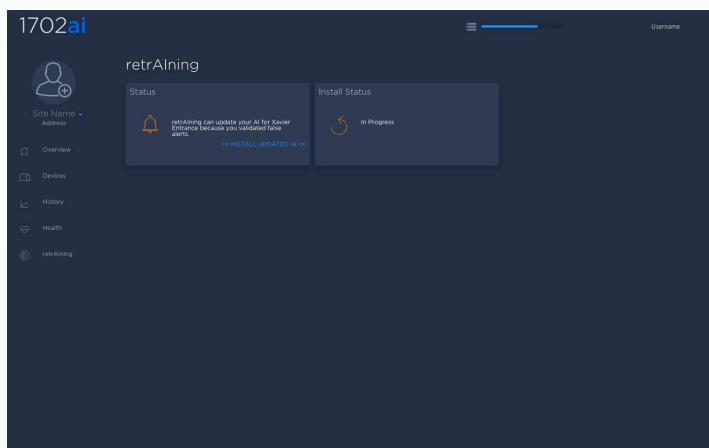
SAMSON RetrAlning



USING PC



In the History tab, the alert log displays all events using a GUI (Graphic User Interface). To visualise an alert, click on the eye (green arrow). It opens the alert directory where the alert is written.

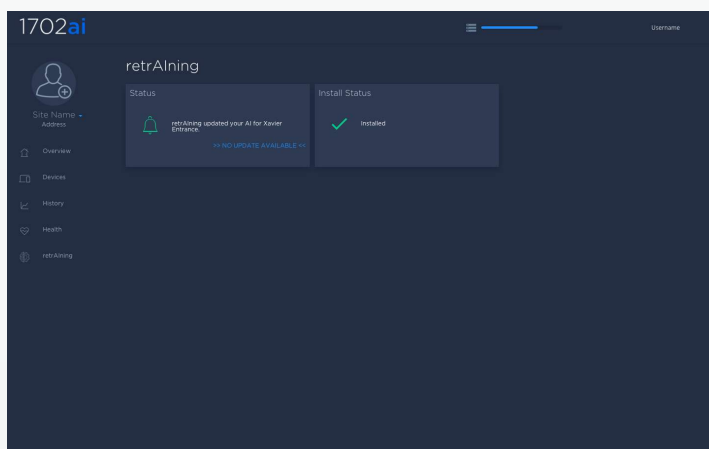


USING PC



In the history menu, each alert can be shared by clicking the three dots menu (green arrow). When selected a floating menu displays Share Alert or Share Metadata.

Using Share Alert, the jpeg - videos and text files generated by the alert can be shared in the directory of your choice. The Share Metadata shares a csv file that includes fps, time stamps, frame size and confidence.



USING PC



When using Share Alert, the end user must specify the destination directory where the alert files have to be shared.



BRD – Biochemical Risk Detection - User Manual



I. General information

1.1 Overview

The Biochemical Risk Detection (BRD) is an air analyser to detect a bacterial concentration in the cities. The BRD should be associated with Impetus platform. In this case, if a critical bacterial concentration is detected an alert is sent by the Impetus platform (Figure 1).

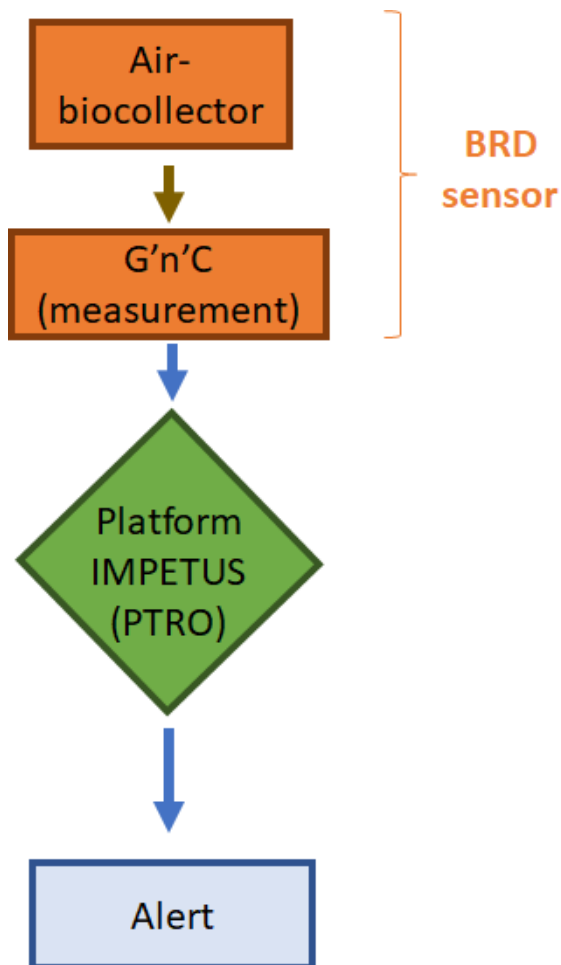


Figure 1: General system

1.2 Technical data

The BRD is made up of an Air-biocollector part and a measurement part (Glow'n'care) (Figure 2). The two parts of the BRD are described below. Moreover, a local interface commands the different tools. The devices can be commanded at the distance through an html dashboard.



Air- Biocollector

Glow'n'care

Figure 2: BRD

The main specifications in terms of dimension, weight, power, language etc. are described Table 1.

Table 1: Main specifications

Air-Biocollector	
Dimension (H*W*D)	60x51x24 cm
Weight	21 kg
Power	220 VAC power supply
Language	EN
Sample flux rate	12.5L/min
Sampling Modes	Manual, Automatic
Glow'n'care	
Dimension (H*W*D)	62x65x25 cm
Weight	20 kg
Power	220 VAC power supply
Language	FR

Part A description: Air-Biocollector

This part was designed for IMPETUS project. This tool catches and concentrate air microorganisms in the small water volume.

An air-biocollector is connected to an air flow and water pump. The collected sample is pumped by the Glow'n'Care for measuring the ATP (Figure 3).

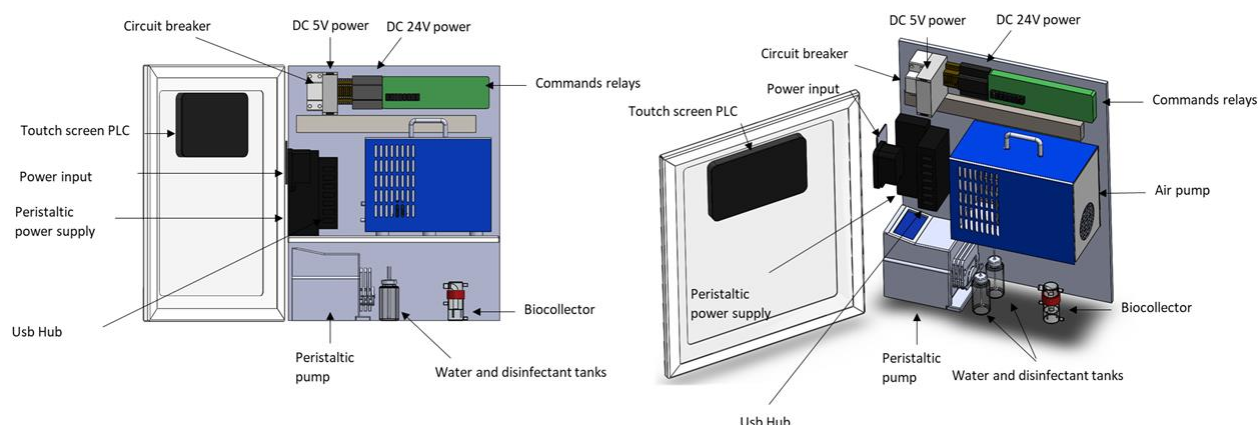


Figure 3: Air-Biocontrol

Part B description: Glow'n'care

Glow'n'care (G'n'C) was designed by GLBiocontrol this device intended for on-line monitoring of concentration of microorganisms (biomass) contamination in drinking water (Figure 4).

This technology is based on the measurement of the ATP concentration by bioluminescence. Indeed, all microorganisms (except viruses) contain ATP as primary source of energy. The ATP concentration in a sample is correlated with the biomass. The principle of the measure is as follows:

- Lysis of microorganisms with the aim to release the ATP in the medium
- Transformation of ATP in light (bioluminescence) by the following reaction:



The reaction is catalysed by luciferase. The principle of the reaction is illustrated Figure 5.

Addition of a standard allows to correlate light quantity to ATP concentration. Furthermore, one femtogram of ATP is similar to the ATP average concentration per bacteria.

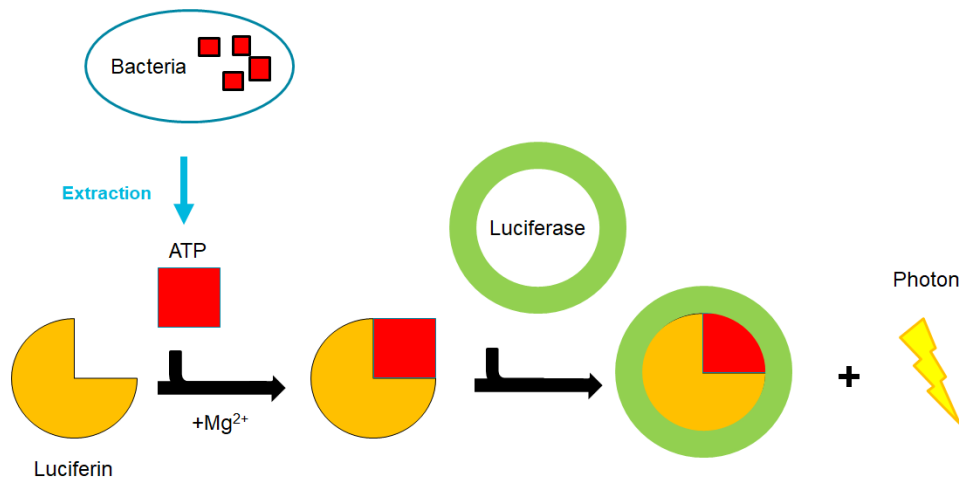


Figure 4: ATP- reaction

The G'n'C monitoring module is shown in Figure 5. Different tanks are present and contain:

- An extractant solution, this solution allows to lyse the bacteria to spread ATP
- A dendridag solution that contain all the enzymatic reactants (luciferin, luciferase etc.)
- A solution of ATP: added after the measure, this solution is an internal standard.
-

Figure 5: G'n'C. All solutions used for experimentation are manufactured by GLBiocontrol

II. Dashboard

2.1 Overview

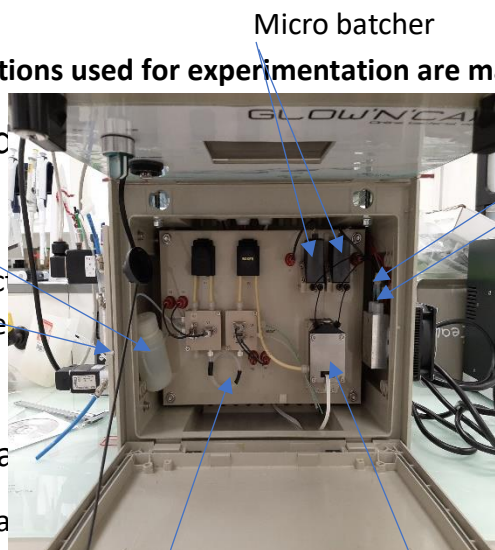
Glow'n'care was connected to a computer to communicate with the micro batcher.

2.2 Content of the dashboard

Four dashboards are available.

Automatic mode

By clicking on "Measure" the automatic mode starts, all steps come one after one automatically to realise the air collect to analyse. The automatic dashboard mode is presented Figure 6.



Principle parameters of the microorganisms sampling are specified on the left of the screen. The results are in the right part of the screen. The GNC indication allows to control the communication with the GNC module

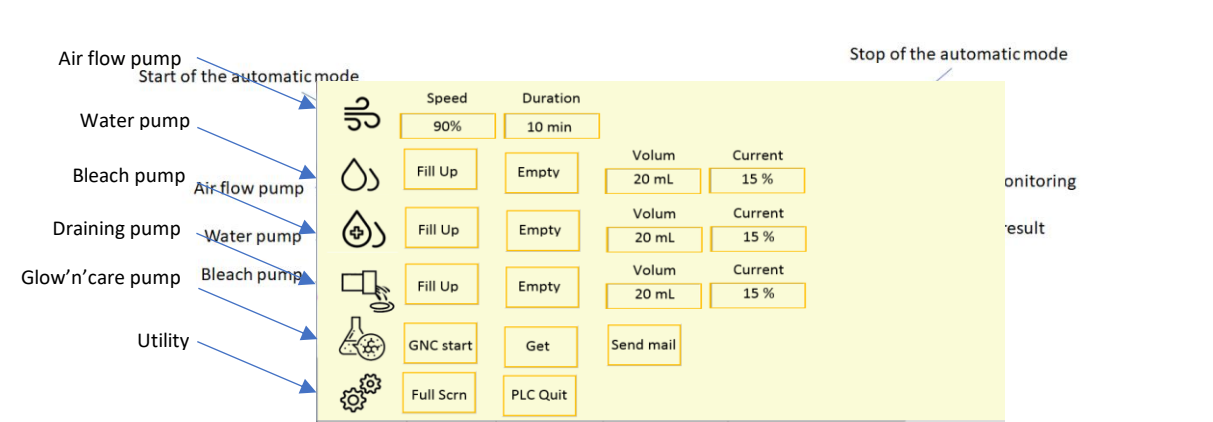


Figure 6: Automatic mode

Manual mode

A manual mode has been incorporated to perform sequential measurement. In this page, the parameters of the measure could be filled. The parameters set on this interface will be used when the automatic mode is launched (Figure 7).

Figure 7: Manual mode

Parameter

The parameters tab allows to set the parameters for sending data (Figure 8).

The screenshot shows the 'BactAirIA' application window with the 'Param' tab selected. The 'Receiver' field is filled with 'biotech@biotech.com'. The 'Server' field is 'smtp.UDN.com' and the 'Port' field is '587'. The 'Message' field contains 'Udn_Automate results!'. The status bar at the bottom displays 'SoftVer:1.3', 'Wlan:Up @ 192.168.1.188', 'Eth0:Up @ 192.168.1.188', 'eMail ok', and 'Client Connected: 1'.

Figure 8: Email Parameter

History

The history tab contains all data performed with the device (Figure 9). This dashboard contains the following information:

- the date and the hour of the measurement
- There are 5 columns of data. The first R0 corresponds to background signal noise in RLU.

The second column R1, measure of ATP in "air sample" in RLU.

The third column R2 is the measure in RLU obtained in the sample after the addition of the internal standard (1000 pg of ATP).

The fourth column is the concentration of bacteria in ATP in pg/ml.

The last one column is the concentration of bacteria in air (pg/m³)

The following calculation is applied:

$$[\text{ATP}]_{\text{pg/mL}} = (\text{R1}/(\text{R2}-\text{R1})) * 1000$$

The concentration of bacteria in air correspond to the expression of the concentration of ATP per unit of air (m³).

For example: 120L of air are collected and concentrated in 20 mL of water. Only one milliliter is analyzed by ATP metry. The concentration of ATP per m³ of air is calculated as

$$\text{follows:} [\text{Air}] = ([\text{ATP}] * 20) / 120$$

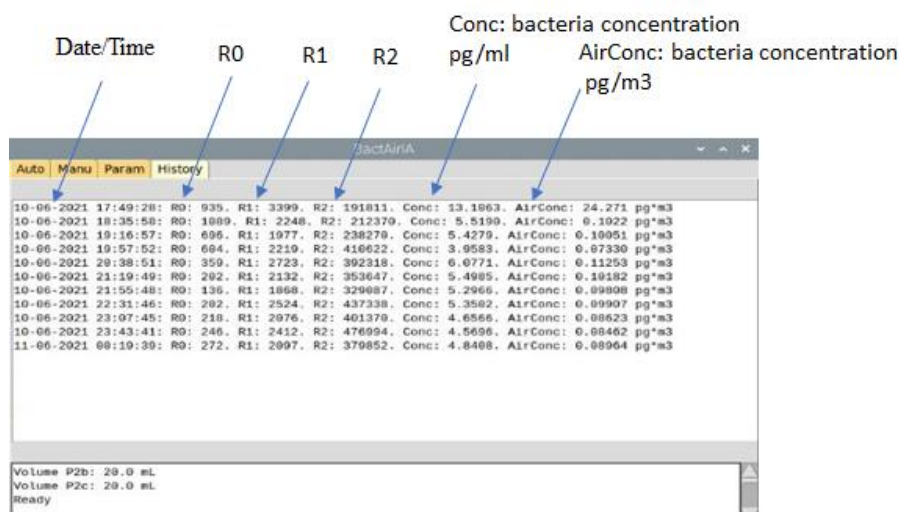


Figure 9: History

data

III. Global schematic of Biochemical Risk Detector

The operation scenario is described in Table 2. Each measure cycle is composed of 11 steps in order to ensure complete measurement, washing and disinfection of the BRD.

Table 2: Operation scenario for air analysis

STEP	ACTION
Step 1	System purge
Step 2	Clean solution filling
Step 3	System purge
Step 4	Water filing
Step 5	System purge
Step 6	Water filing
Step 7	Pompe ON
Step 8	Sample analysis
Step 9	Data sent

Step 10	System purge
Step 11	STAND-BY

The steps of the BRD operation are further described here below. For each step, the dashboard is presented.

STEP 1: System purge

This step aims to remove stagnant water from the air-biocollector using tank water (Figure 10). As stagnant water enables bacterial growth, the pipes need to be flushed out to avoid filter contamination for measuring only the organism from air.

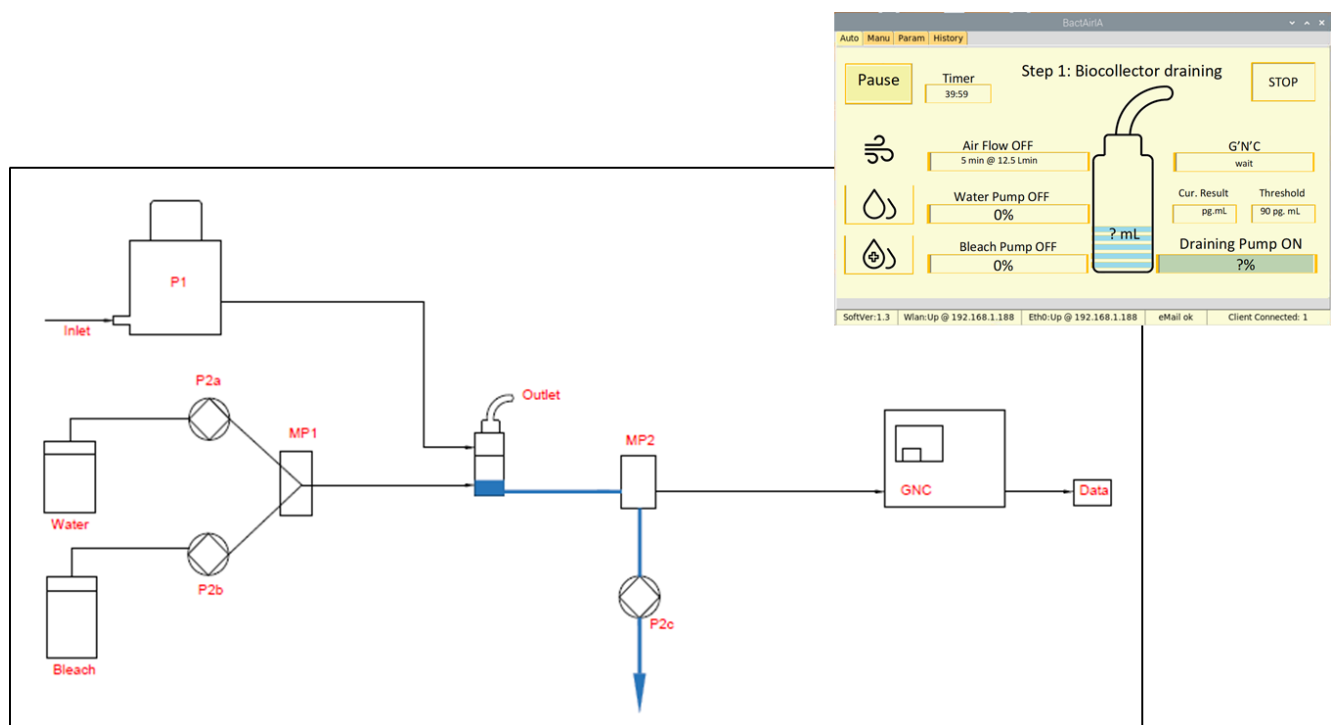


Figure 10: STEP 1 - System purge

STEP 2: Clean solution filing

After sampling and measurement, the air-biocollector must be disinfected to limit the formation and growth of organism. A solution of bleach is used as a disinfectant (Figure 11).

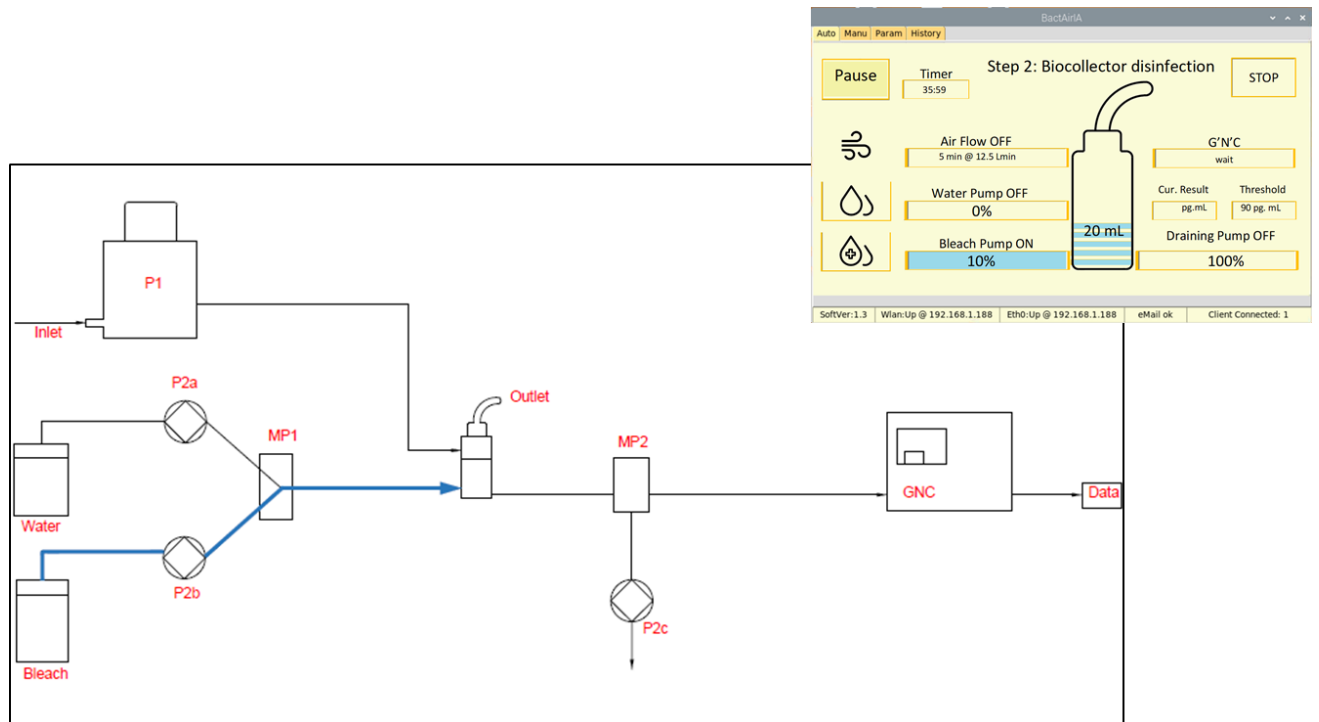


Figure 11: STEP 2 - Clean solution filing

STEP 3: System purge

This step aims to remove the disinfectant (in blue). The peristaltic pump P2C is activated (Figure 12).

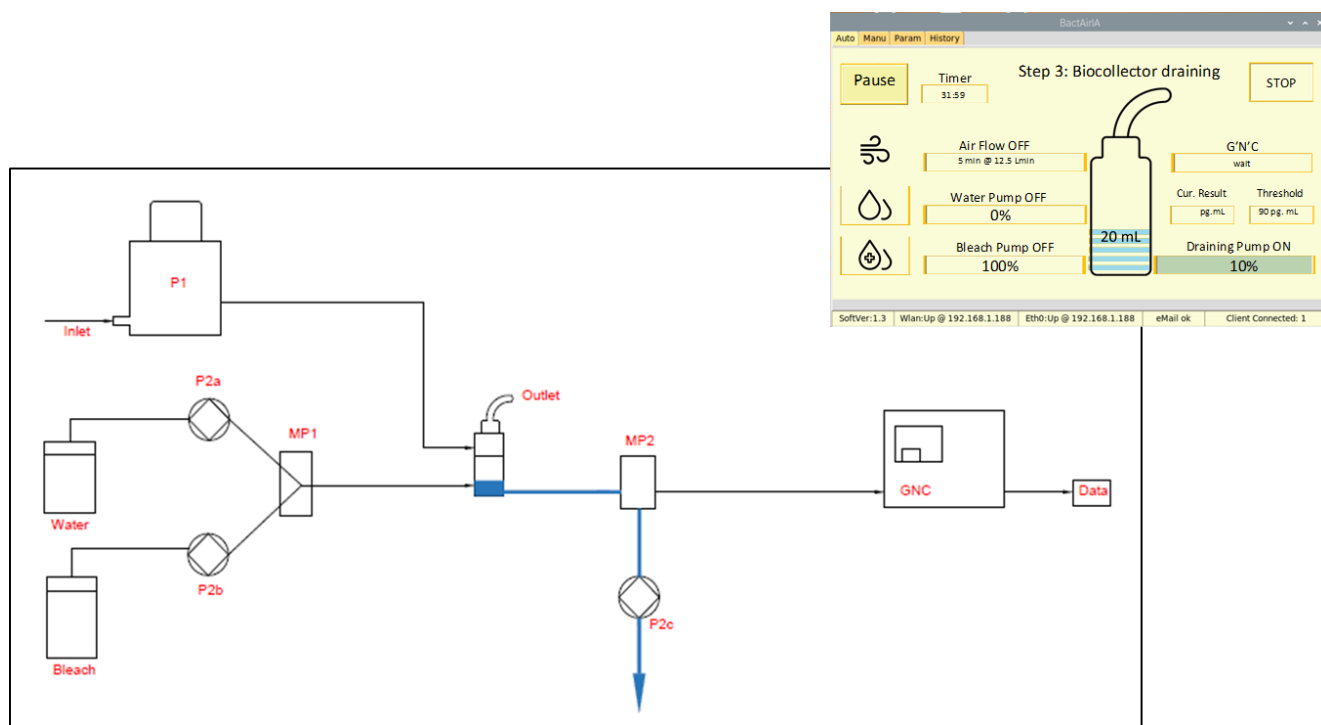


Figure 12: STEP 3 - System purge

STEP 4: Water filling

The air-biocollector is filled with sterile water to remove the bleach of the system. The peristaltic pump P2a is activated (Figure 13).

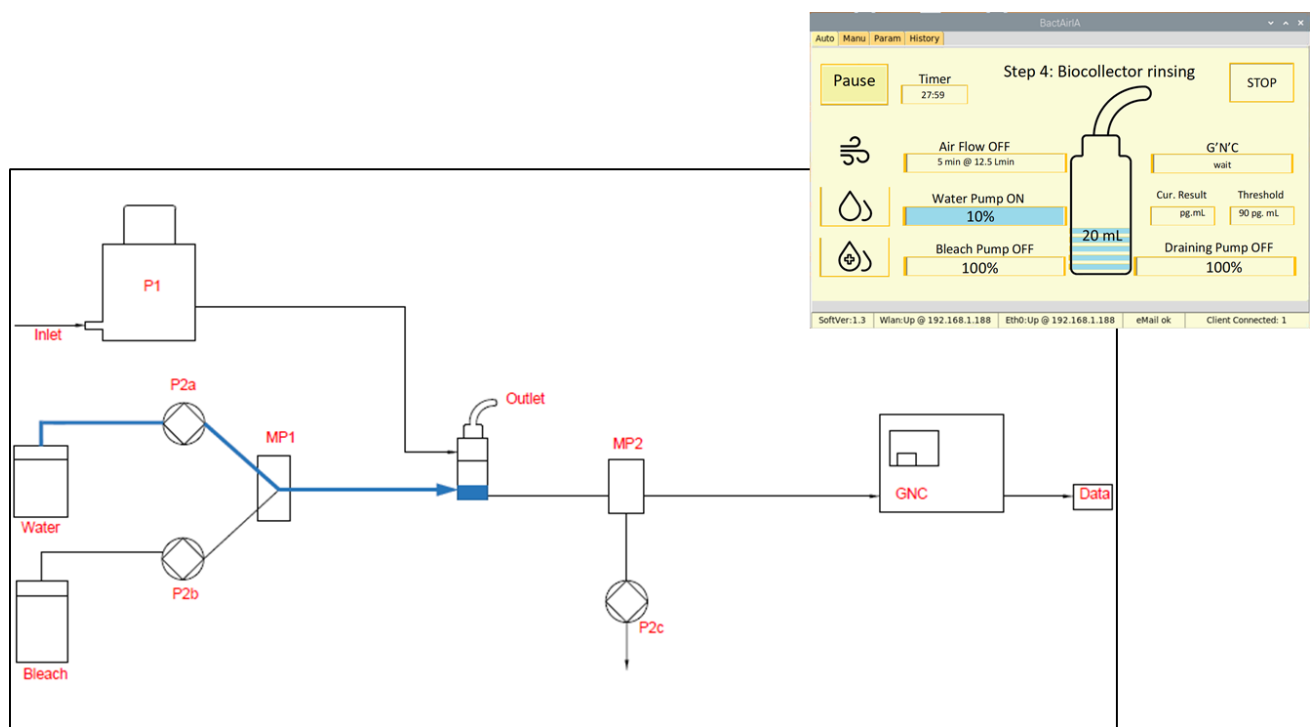


Figure 13: STEP 4 - Water filing

STEP 5: System purge

This step aims to remove the water (in blue). The peristaltic pump P2C is activated (Figure 14).

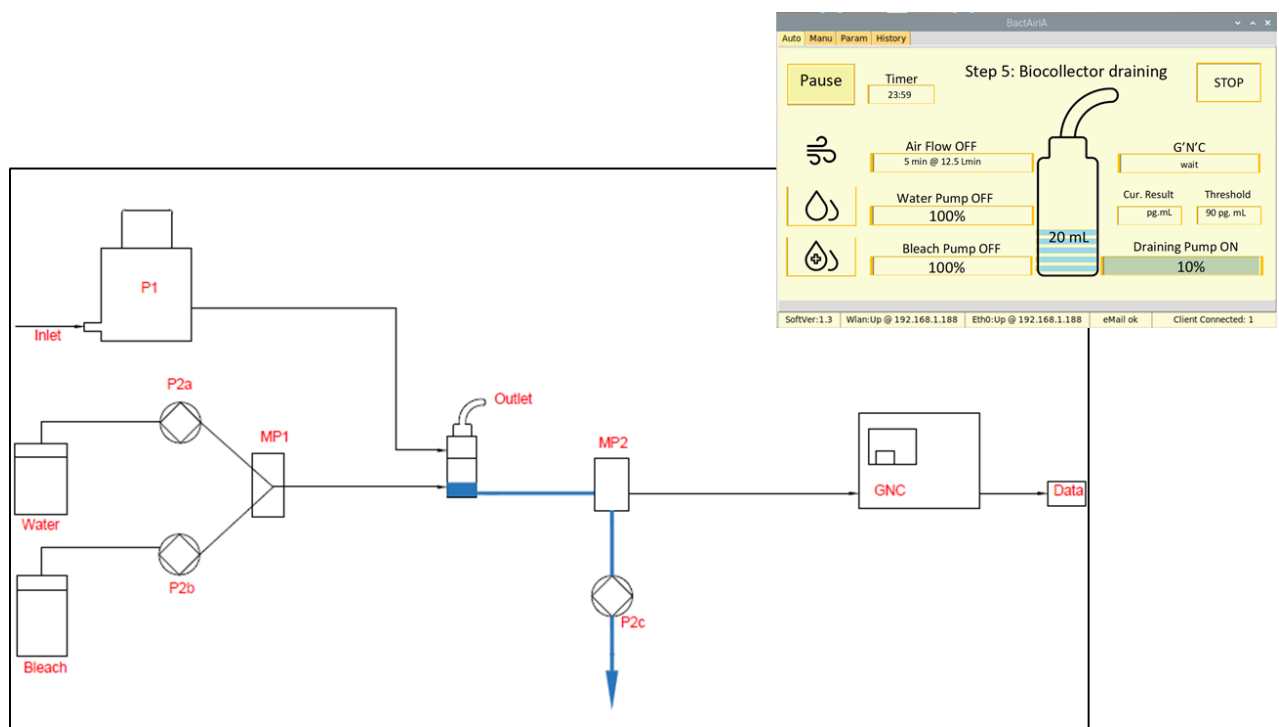


Figure 14: STEP 5 - System purge

STEP 6: Water filling

The air-biocollector is filled with sterile water to collect the microorganisms of the air. The peristaltic pump P2a is activated (Figure 15).

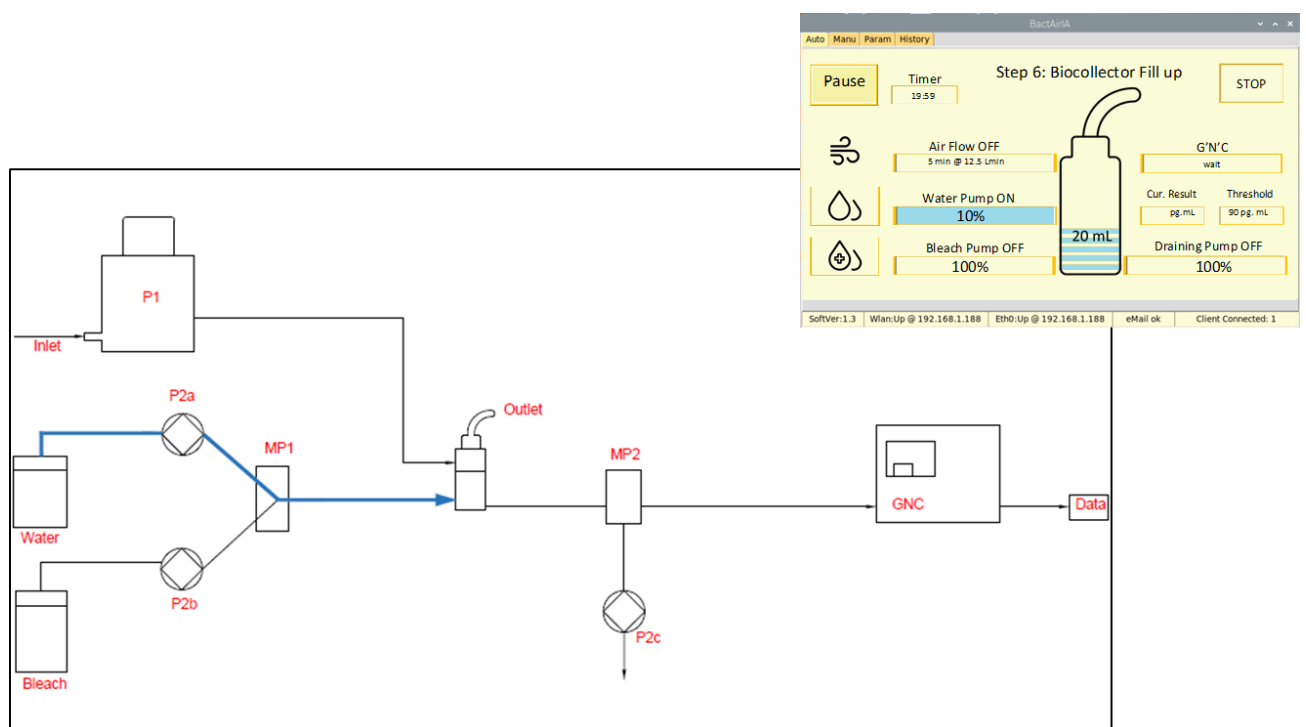


Figure 15: STEP 6 - Water filing

STEP 7: Air pump P1

During 10 minutes the “Air pump P1” connected with the air-biocollector performs the air sampling. This pump is turn “off” after 10 min (Figure 17).

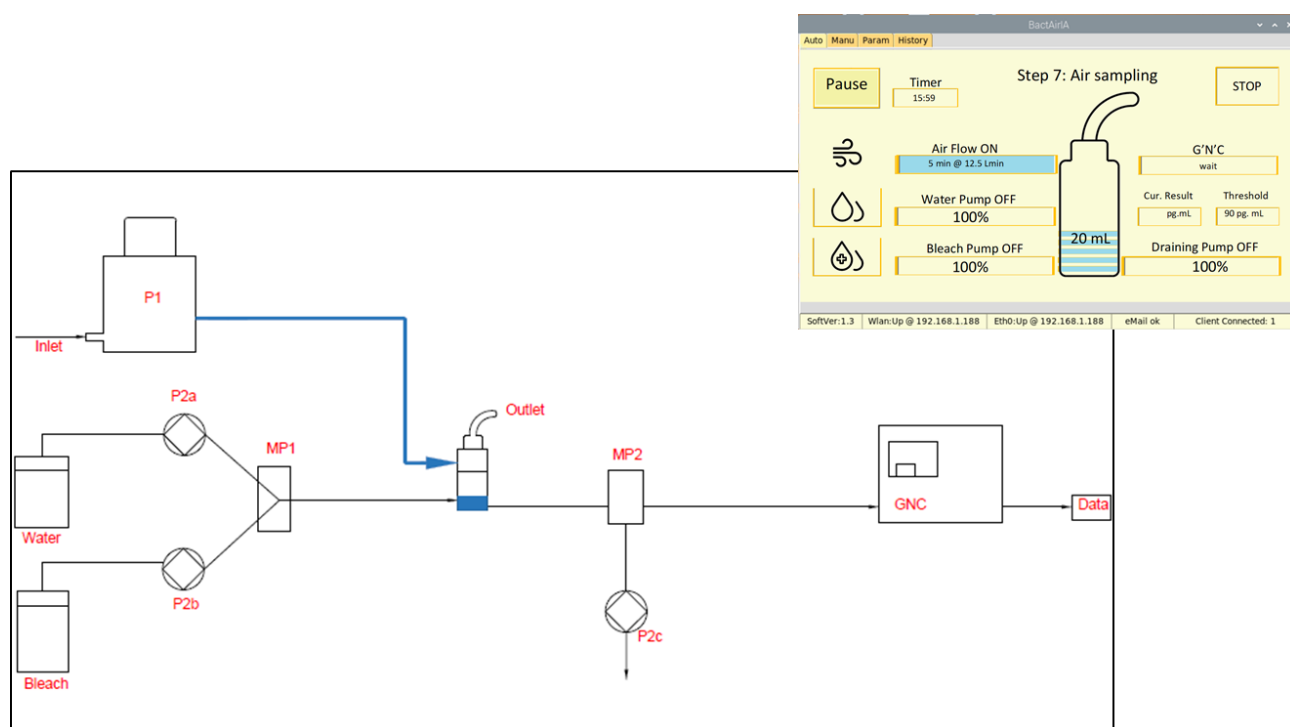


Figure 17: STEP 7 - Air pump P1

STEP 8: Sample analysis

1 mL of sample is pumped by the G'n'C pump to be analyzed (Figure 18).

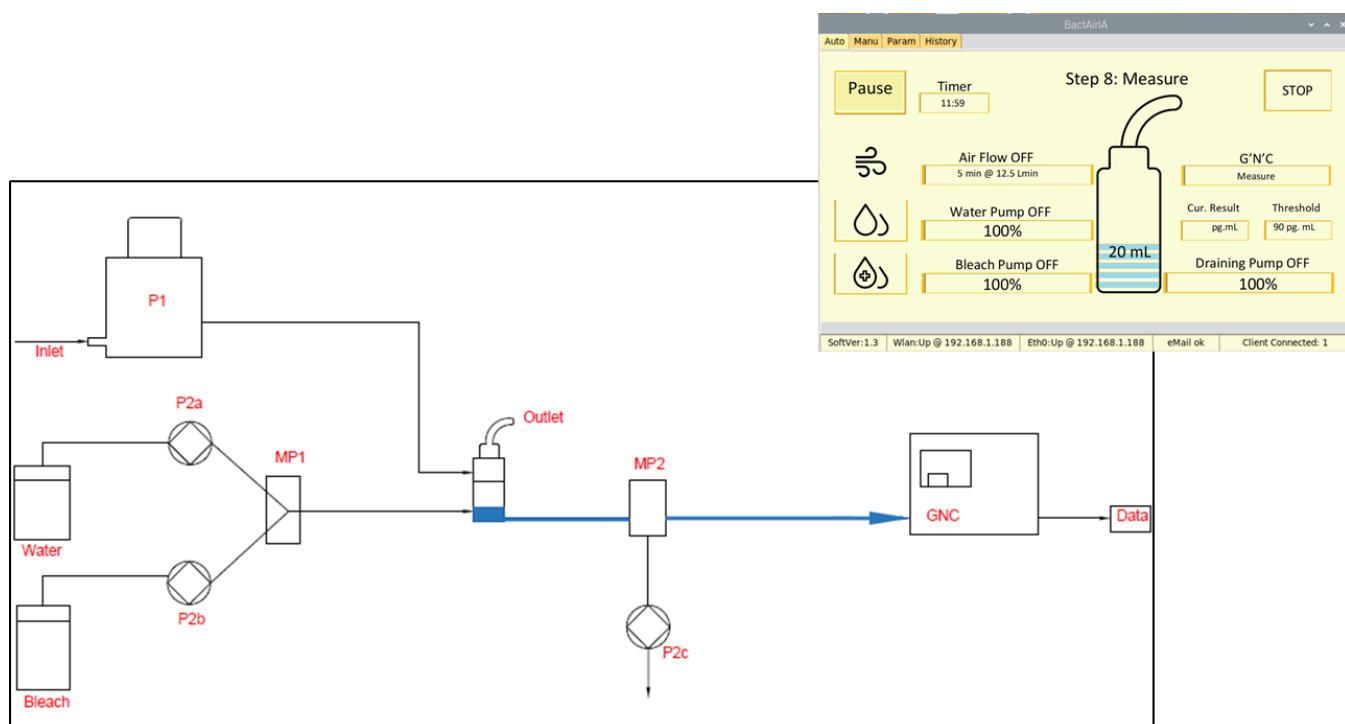


Figure 18: STEP 8 - Sample analysis

STEP 9: Data sent

Data is sent to the Impetus platform by an e-mail (Figure 19).

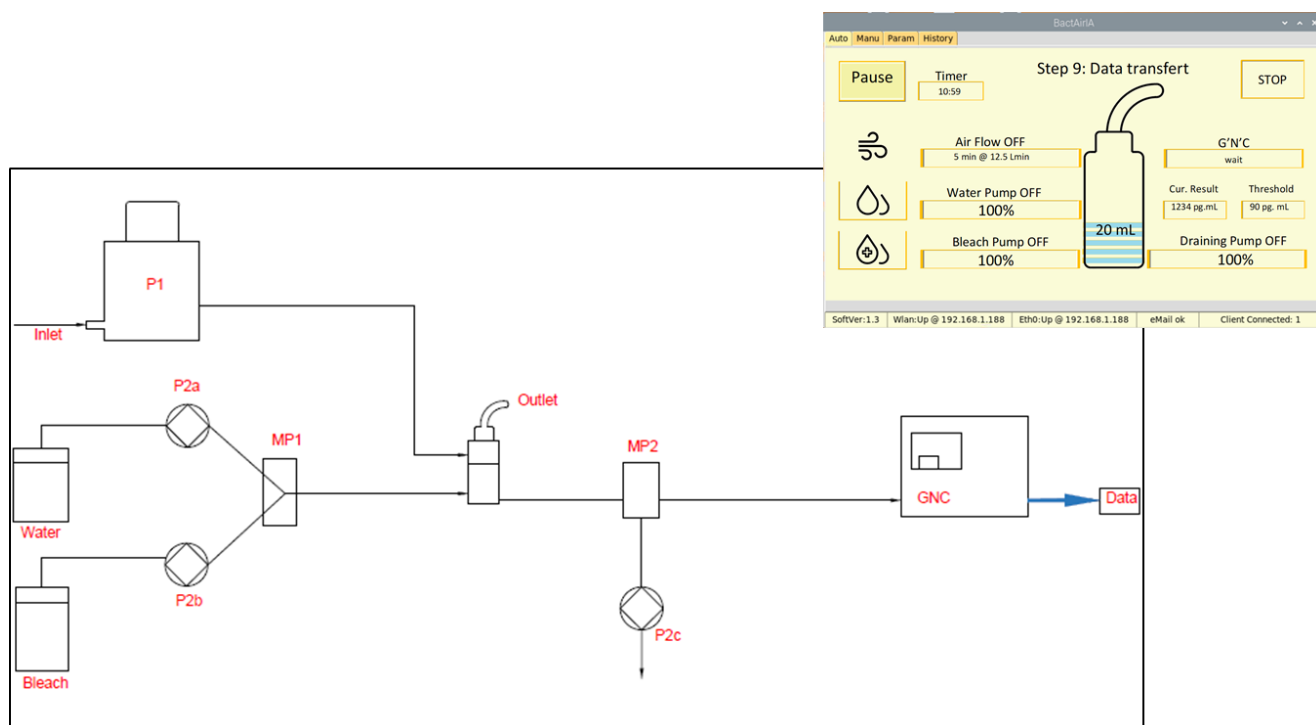


Figure 19: STEP 9 - Data sent

STEP 10: System purge

This step aims to remove stagnant water from the air-biocollector using tank water. The pump P2C is activated (Figure 20).

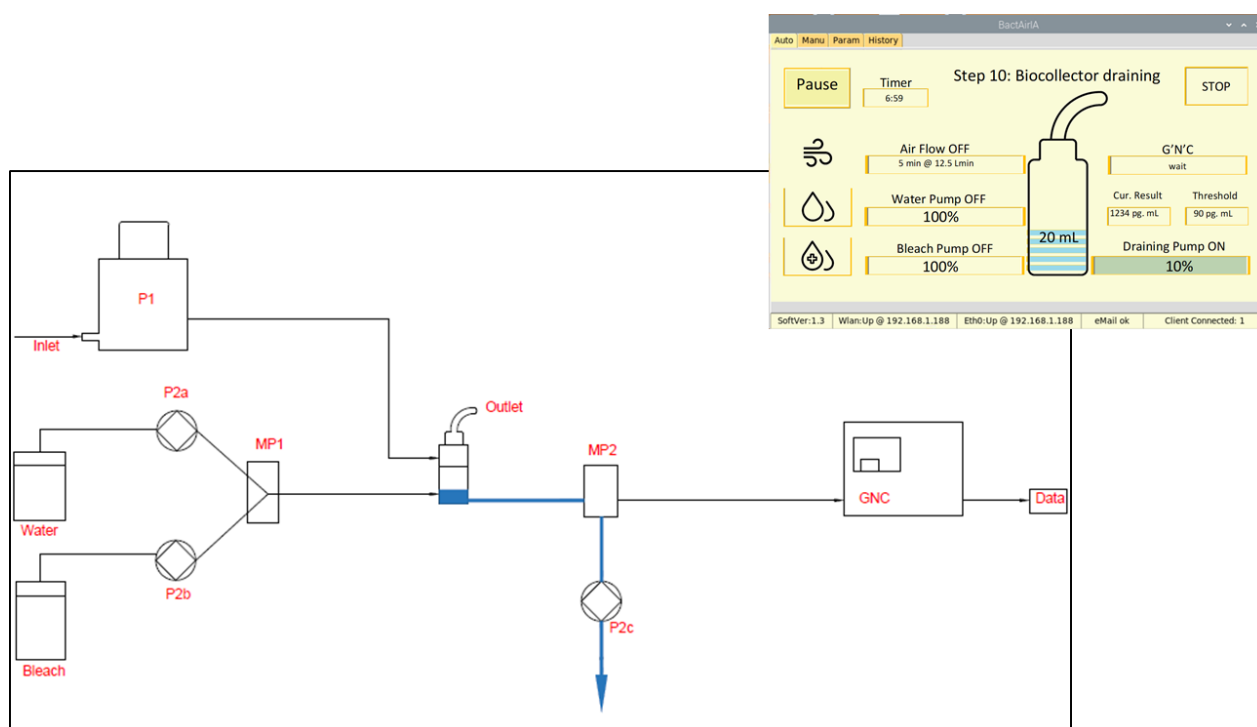


Figure 20: STEP 10 - System purge

STEP 11: System standby

The pipes and the measurement cell remain with disinfectant until the next sampling to limit microorganism growth.

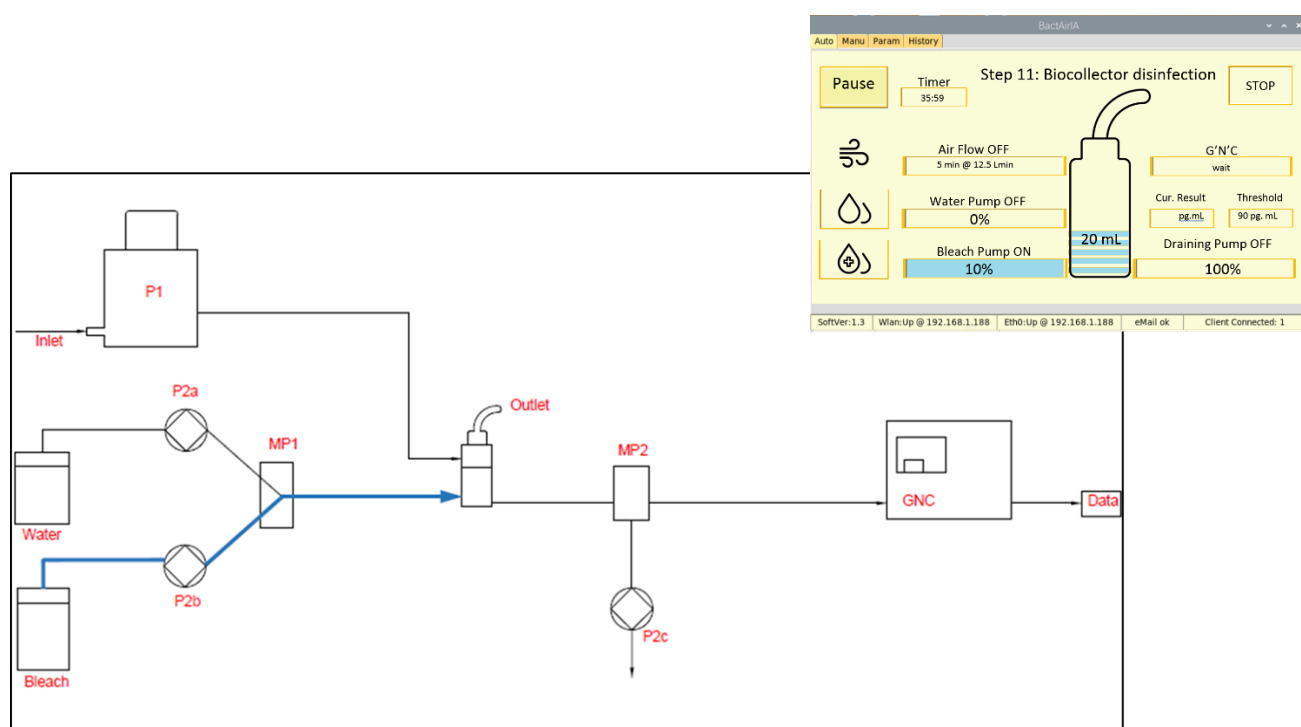


Figure 21: STEP 11- System standby

IV. Data collected by the platform

The data sent to the platform are in the same organization and calculi as presented in the dashboard.

The data are sent by e-mail as text in a CSV file.

```
# prv=Defi Systems,v151126

# pr=100,3600,24,20

# begin

2016:02:05 11:27:49 28239 328175 94.150 15.69

2016:02:05 11:44:36 12260 319248 39.936 6.65

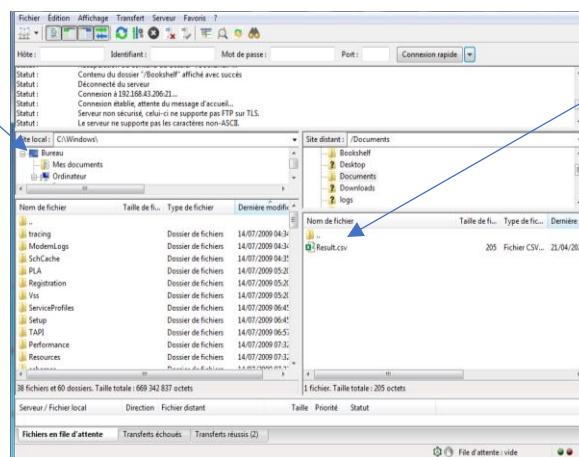
2016:02:05 11:59:26 37133 344464 120.824 20.13

# end
```

Figure 22: Example of sent data

If the data are not sending in this case the data are saved in FTP (File Transfer Protocol)

Platform desktop



Data file

Figure 23: Repository access

V. Data interpretation by the platform

To allow a good interpretation by the platform, it is necessary to obtain a couple data in each city's partners. Indeed, the air always contains microorganisms indoor or outdoor but the microorganism concentration depends of different parameters as seasons, the human activity, number of people in the room, ventilation system, the reservoirs (compost, animals...), geographical location. For all these reasons, the alert thresholds must be adjusted to the city of application as soon as possible.



XM Cyber User Guide

Version 1.35

2021





The information, data and drawings embodied in this in this document (collectively the "Document") are strictly confidential and are being furnished solely for informational purposes. They are not to be used for any other purpose or made available to any other person or reproduce in whole or in part without the express prior written consent of XM LTD (the "Company"). Any form of reproduction, dissemination, copying, disclosure, modification, distribution and or publication of the Document outside of the planned project scope is strictly prohibited. This Document was prepared by the Company and contains selected information pertaining to the Company and does not purport to be all-inclusive. Neither the Company nor any of its respective officers or employees make any representation or warranty, expressed or implied, as to the accuracy or completeness of this Document and no legal commitments or obligations shall arise by reason of this Document.



Table of Contents

INTRODUCTION	3
XM Cyber Features	3
Benefits from XM Cyber Deployment	3
How to Use this Manual	3
OVERVIEW	4
XM Cyber Architecture	4
XM Cyber Workflow.....	6
GETTING STARTED	7
XM Cyber Deployment	7
Starting the XM Cyber Application	8
THE DASHBOARD	10
Dashboard Display	10
THE SCENARIO HUB	13
Scenario Display	14
Viewing Campaigns.....	15
CREATING AND MODIFYING SCENARIOS	20
Creating a New Scenario	20
Manually Generating a Campaign from a Scenario	29
THE BATTLEGROUND	30
Navigating to the Battleground.....	30
Understanding the Battleground Screen.....	31
Campaign Visualization.....	35
REPORTS	45
How to Access Reports	45
Report Navigation.....	46
Understanding Reports	47
Other Reporting Capabilities	54
SYSTEM CONFIG	55
System Config Tabs and Links	55
XM Cyber Terminology – Glossary.....	73
User Manual and UI Conventions.....	76



INTRODUCTION

XM[®] Cyber provides the first fully automated APT (Advanced Persistent Threat) Simulation Platform to continuously expose all attack vectors, above and below the surface, from breach point to any critical organizational asset. This continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of security gaps. XM Cyber operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of hackers.

XM Cyber provides organizations with a clear, up-to-date understanding of where and how hackers can (and will) infiltrate their network and compromise critical assets. The platform is meticulously designed to work safely in an organizational network, simulating malicious methods without disrupting network availability or causing harm to critical assets.

XM Cyber Features

- Automated generation of actionable and prioritized remediation reports
- Customized attack scenarios from any starting point to any target asset
- Comprehensive and up-to-date attack methods
- Fully secure simulation based on real user actions implemented in real-time
- Detailed visual display of the attacker path(s) to critical assets
- Comprehensive reports on organization cybersecurity status and posture

Benefits from XM Cyber Deployment

- Easy deployment and rapid returns on security investment
- Accompanies changes to networks and asset distribution
- Scalable Architecture
- Reduces risk from non-optimal security hygiene
- Optimizes use of cyber resources, digital and human

How to Use this Manual

This manual is intended for security practitioners and analysts, and IT personnel. It explains how to use XM Cyber to run virtual APT (Advanced Persistent Threat) campaigns to test the viability of your company's cybersecurity and uncover exploitable vulnerabilities.

The document assumes that XM Cyber has already been installed on Windows and Linux servers as explained in the *XM Cyber Installation Manual*.



OVERVIEW

This section provides an overview of XM Cyber functioning, details on system components, and an outline of how to work with XM Cyber. A short glossary at the end of this guide assists in understanding key concepts and terminology. Instructions and requirements for installing the components of the XM Cyber virtual APT system are found in the *XM Cyber Installation Manual*.

Safe and Continuous Operation

XM Cyber simulates, assesses, and validates cyber-attacks using knowledge of APT techniques catalogued by XM Cyber. XM Cyber addresses real user behavior and actual exploits across a wide spectrum of attack scenarios to expose blind spots – bad configurations, latent vulnerabilities and other weak points. The attacks use real-world techniques but XM Cyber simulations are run safely without affecting network availability or user experience.

Comprehensive Approach

XM Cyber provides visibility along an entire attack path, from breach points to critical assets, followed by prioritized and actionable remediation guidance. XM Cyber operates as an automated purple team, continuously combining red team (attack) and blue team (defense) techniques to help you optimize allocation of resources and deliver measurable return on security investments.

XM Cyber Architecture

To perform attack simulations, XM Cyber deploys software across the organization to manage, monitor and analyze simulated attacks using the following components:

Sensors

Sensors are lightweight passive software agents deployed on user computers and servers across the organization that monitor and report on the state of network nodes and sub-nets in support of APT simulations (campaigns). XM Cyber sensors communicate with the South server over a secure SSL/TLS channel. Sensors contain host self-defense to protect themselves from attack, via signature validation of executed code, and resource monitoring.

Sensors can be installed on computers running Windows, Linux and MacOS. They can run on physical or virtual devices with the supporting operating systems. The sensors continuously capture information from systems and can identify changes in the network and devices that effect the risk of assets. For an accurate security assessment, organizations must deploy sensors on at least 10% of network nodes distributed across different network segments, departments and device types.

North Server

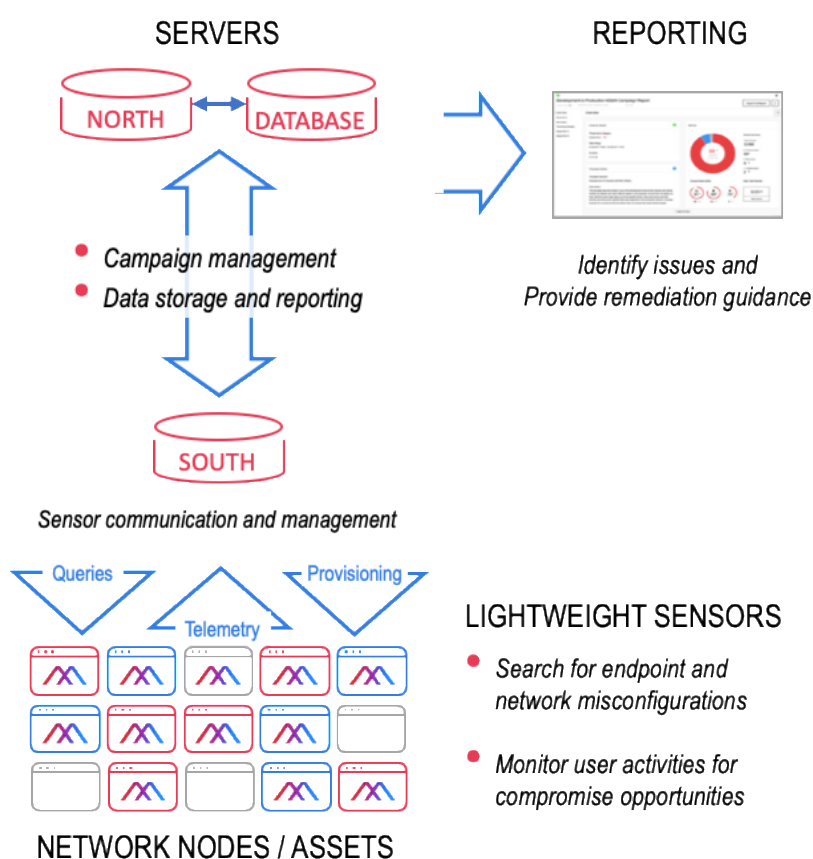
The North Server hosts the main XM Cyber software components under Linux (CentOS/RHEL 6/7). The North Server is responsible for running campaigns that simulate attacks, including discovering weaknesses and exploiting them. The North Server also analyzes data collected during campaigns and generates reports that highlight vulnerabilities and offer remediation plans postmortem. The server can reside either on premises or in the cloud.

Database Server

XM Cyber requires a NoSQL database (MongoDB) to store information collected from the sensors deployed throughout the network, before, during and after campaigns. The Database Server can be hosted on premises or in the Cloud. For smaller organizations, the database can reside on the North Server.

South Server

The South Server runs Windows Server Edition and manages communication between the North Server and sensors during campaigns. It also provisions sensor node with up-to-date binaries to the sensors.



XM Cyber Architecture

XM Cyber Gateway (not pictured)

For air-gapped or otherwise isolated sub-networks, a computer may be assigned to act as a gateway, relaying and regulating communication between sensors in the segment and the South Server.

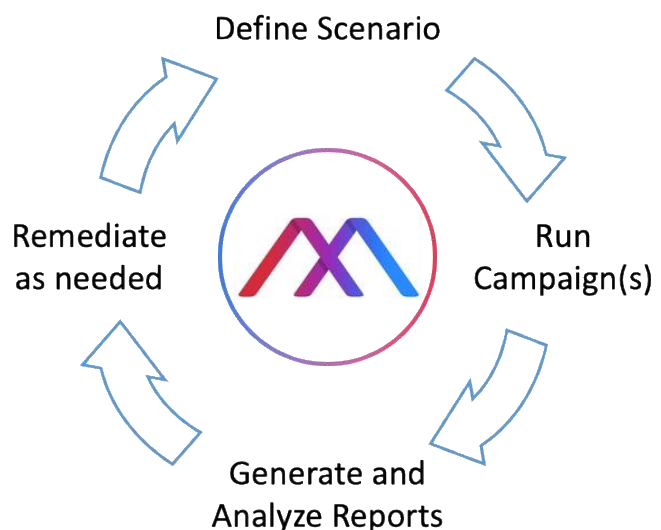
XM Cyber Workflow

After XM Cyber is installed, XM Cyber can run APT simulations (campaigns) in each Scenario. Scenarios are created by customers depending on the business risk they want to assess. Within each Scenario, campaigns are activated to begin at an endpoint in the network, which is deemed vulnerable. Defining scenarios is explained in [Creating and Modifying Scenarios](#).

Once a scenario has been created in XM Cyber, the system can execute campaigns either automatically or manually.

A typical workflow is as follows:

1. Create a Scenario around a particular risk, e.g., starting from a remote office, is an organization's PCI network accessible?
2. Once the scenario is configured with one or more breach points, assets and a schedule, the campaign will run. Users can view a graphic simulation of the APT in real time (*battleground*) and observe endpoints that are discovered to be compromised or vulnerable. Campaigns can be set to run automatically at specified times or can be activated manually whenever desired.
3. Generate reports that identify security problems and provide remediation guidance for overcoming them.



The XM Cyber workflow



GETTING STARTED

This chapter explains how to begin running campaigns with XM Cyber. It also introduces the XM Cyber user interface and explains the information it displays.

XM Cyber Deployment

Getting Started with XM Cyber involves the following steps:

1. On-premises - Install XM Cyber on the North, South and Database servers as explained in the *Installation Manual*. The XM Cyber team can provide assistance with this step.
2. Cloud-hosted – for cloud-based configurations, no server installation is required.
3. Deploy XM Cyber sensors on servers and workstations across an on-premise and/or cloud environment, whose security is being checked. Administrators can deploy sensors across their environments and include those sensors as part of their base images.

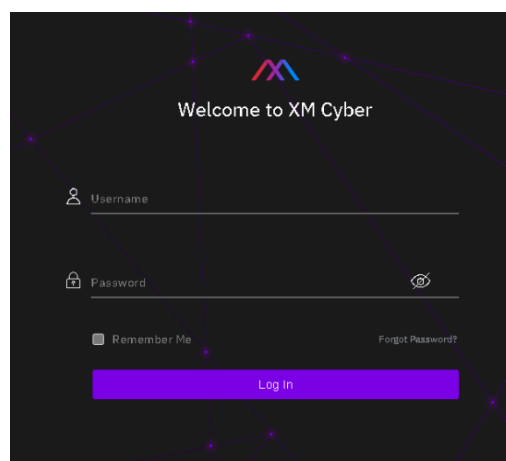
Optional – XM Cyber can provide guidance on sensor deployment based upon analysis of your network topology and security measures in place. To support this analysis, XM Cyber asks that users fill out a questionnaire that describing their system security.

4. Start the XM Cyber application and specify parameters for a scenario from the **Scenarios** screen (see [SCENARIO HUB](#) below). The scenario specifies which computers will be breach points for the start of the campaign, as well as other parameters such as the timing and duration of the campaign.
5. Start and run the campaign from the XM Cyber application.

Starting the XM Cyber Application

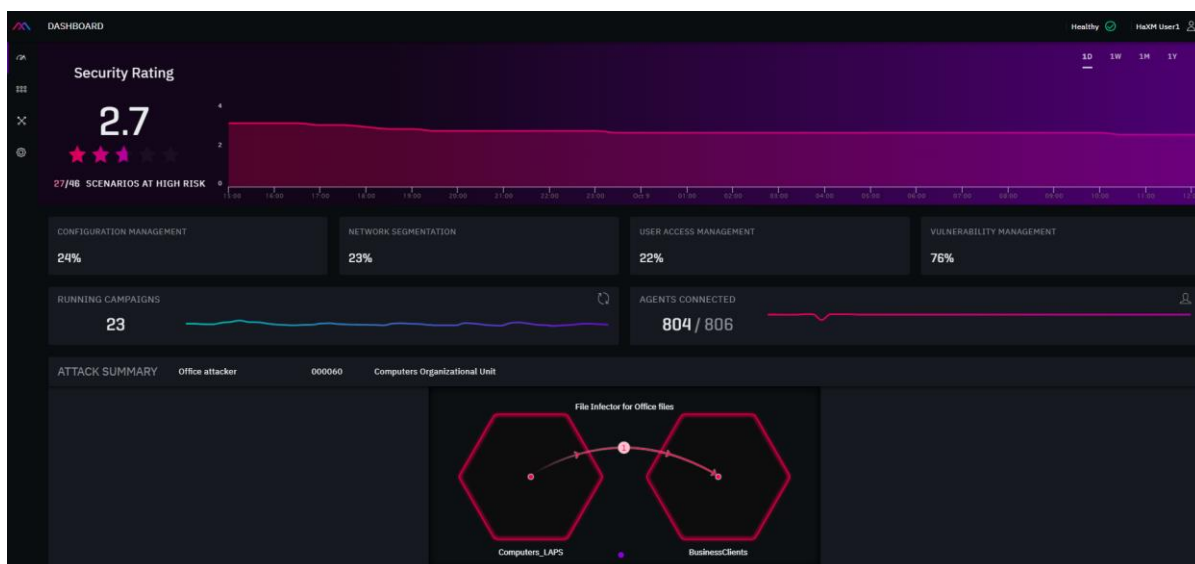
Launch XM Cyber by doing the following:

1. From an Internet browser*, enter the IP address of the North Server or the URL of a cloud instance provided by XM Cyber and press Enter to reach the XM Cyber login screen.
2. Log in with your username and password; the XM Cyber dashboard appears if you forgot your password, click Forgot Password on the login screen to initiate a password reset sequence via your registered email address.



XM Cyber login screen

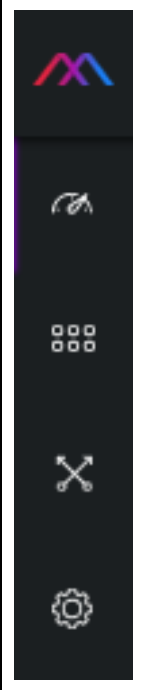
Note – XM Cyber supports SSO with OpenID Connect and OAuth2.



The XM Cyber Opening Screen

* Chrome and Firefox are recommended browsers

At the left side of the screen is the *XM Cyber Sidebar* that enables navigation around XM Cyber.

	<p>XM Cyber Sidebar Icons and Functions</p> <p>DASHBOARD: Provides an overview of your organization's security posture, including security ratings over time, and measurements of factors affecting it. The dashboard also displays information on currently running campaigns, the number of active sensors, as well as an attack summary.</p> <p>SCENARIO HUB: Displays information on campaigns and campaign scenarios. This screen also enables you to create and modify scenarios that specify the parameters of campaigns. See SCENARIO HUB for details.</p> <p>BATTLEGROUND: Displays a graphic representation of a scenario and campaign. Information on the origin, target, and method of each attack is displayed at varying levels of granularity. Complete campaigns can also be viewed and replayed. See THE BATTLEGROUND for details.</p> <p>SYSTEM CONFIG: Contains tabs displaying the health of the system, information on the sensors deployed across the system, and administration details. See SYSTEM CONFIG for details.</p>
---	---

THE DASHBOARD

The **Dashboard** provides information to help assess your organization's security posture, as well as displaying essential information on XM Cyber operation, including the number of campaigns currently running, the number of connected sensors, a summary of attacks that occurred in the course of campaigns, and the overall health of the XM Cyber system.

Dashboard Display

Security Rating

At the top of the dashboard is a graph that displays security ratings over time:



Security Rating Graph

The **Security Rating** is derived from scenario attributes – number/type of assets, paths to assets, complexity, likelihood of compromise, etc. Applying remediation (e.g., to reduce or eliminate attack paths) will increase the security rating, indicating better IT hygiene.

The **Security Rating** graph displays a time span with security ratings ranging from 1 – 5, in increments of .1. You can scale timespan to cover days, weeks, months, or a year by clicking the buttons at the top right of the graph. These buttons indicate the last 24 hours (day), the previous seven days (week), the prior 30 days (month), or a full 365 days (year). The percentages for security factors such as configuration management, network segmentation, etc. change to indicate the measurement for the time span selected.

Placing the cursor on the graph displays a purple marker that you can drag to a point on the graph showing the security rating for a specific date and time.

Utilization Statistics pane

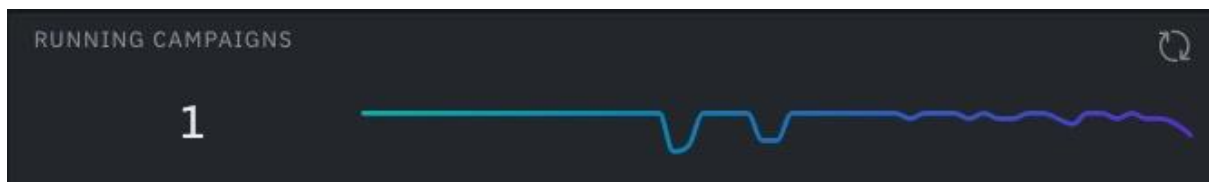
Just below the Security Rating pane is the Utilization Statistics area. It shows statistics for Configuration Management, Network Segmentation, User Access Management and Vulnerability Management. You can find additional information on these metrics in *Findings Reports* in the [Reports](#) section of this document.

CONFIGURATION MANAGEMENT	NETWORK SEGMENTATION	USER ACCESS MANAGEMENT	VULNERABILITY MANAGEMENT
95%	4%	1%	4%

Utilization Statistics pane

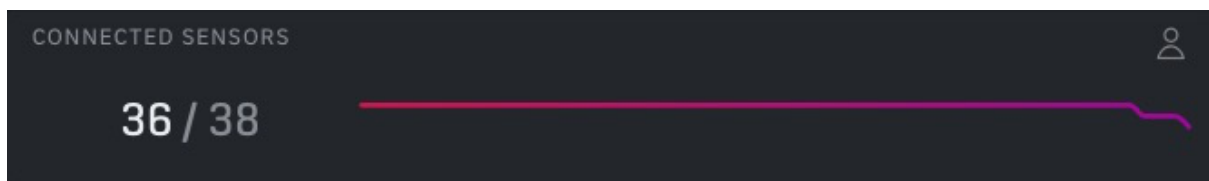
Running Campaigns pane

This graph enables you to display the number of running campaigns for a specific time. The time span of the graph changes according to the time span button (day, week, month or year) selected at the top right of the dashboard. Placing the cursor on the graph displays a marker that you can use to locate a specific time.

*Dashboard Running Campaigns pane*

Connected Sensors pane

This graph indicates the number of connected sensors. Similar to the other graphs, the time span changes according to the time span button that you selected and placing your cursor on the graph enables you to locate a specific time.

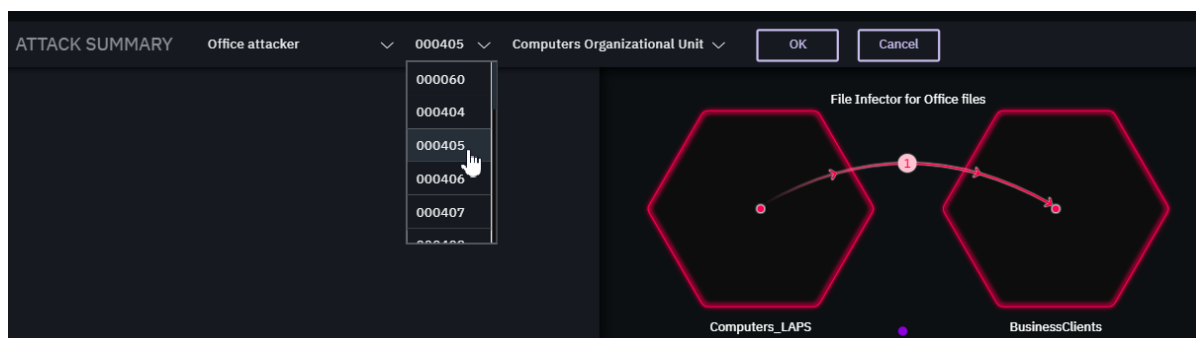
*Connected Sensors pane*

Clusters






Clusters are groupings of computers or subnets, by type, that appear on the Dashboard as hexagons in the **Attack Summary** pane described below. You can select the type of clusters to be displayed – Network Subnet, Domain/Workgroup, Computer Organization Unit, or User Organizational Unit.

Attack Summary

An **Attack Summary** provides information on the first device in a cluster compromised by an attack. The **Dashboard Attack Summary** displays information on the attacking device and target, as well as the method of attack. The **Dashboard Attack Summary** area enables you to select from a list of scenarios, campaigns, and cluster types in which an attack occurred.

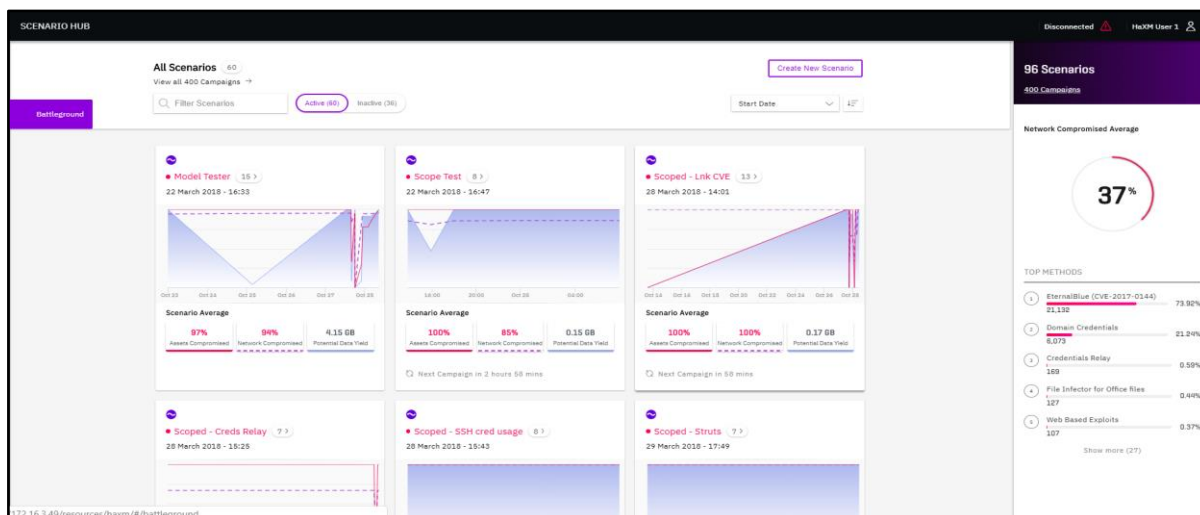
*Attack Summary*

To change the displayed attack:

1. At the right of the Attack Summary area, click the Edit button  to display a dropdown list of icons .
2. Click the first drop-down list button  at the left to display a list of scenarios and select one.
3. Click the next drop-down list button  to display a list of campaigns and select one.
4. Click the next drop-down list button  to select a cluster type.
5. Click OK.
6. The display changes to show the cluster from which the attack originated and the cluster containing the device that was compromised (see figure above).
7. To view the attack on the Battleground, click the Battleground button in the Sidebar. The Battleground Attack Summary provides details about the specific devices involved in the attack and provides information about the method of attack.

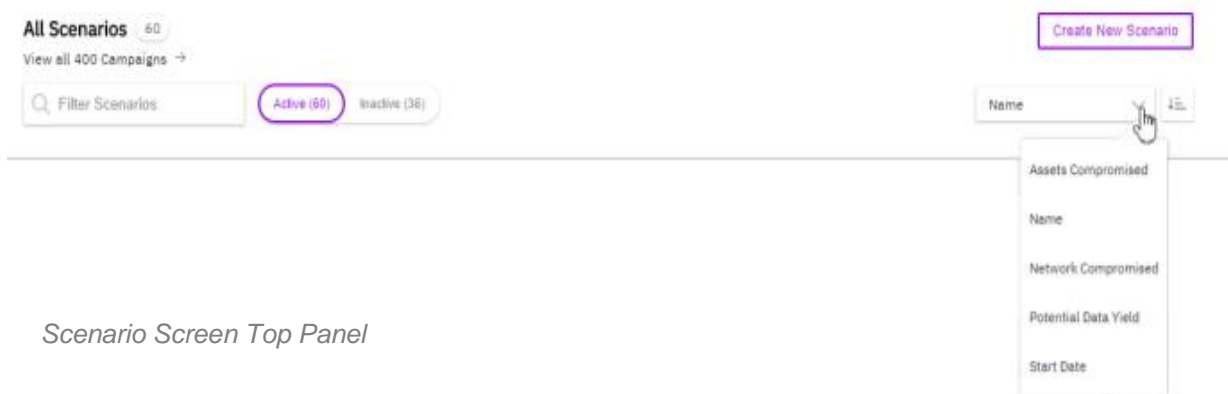
THE SCENARIO HUB

The **Scenario Hub** displays user-created XM Cyber scenarios laid out in a grid. Each scenario represents a mission for the APT simulation engine. A scenario in the grid may display currently running campaigns, past campaigns, or scheduled campaigns not yet begun.



Scenario Hub

At the top of the screen is a panel that shows the number of scenarios displayed on the screen **All Scenarios 60**, a text entry / search box **Filter Scenarios** to filter the scenarios displayed, buttons to display active or inactive scenarios **Active (60)** **Inactive (36)**, and a Sort pulldown menu **Name** to sort the displayed scenarios according in ascending or descending order. You use the **Create New Scenario** button **Create New Scenario** to create and configure a new scenario (see [CREATING AND MODIFYING SCENARIOS](#) below.)



Scenario Screen Top Panel

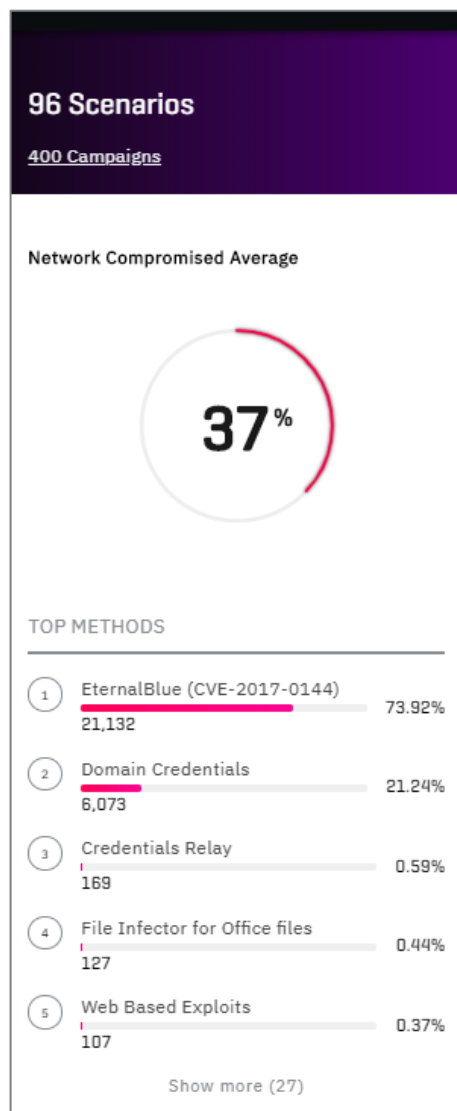
At the right side of the **Scenario Hub** is an information pane that displays the total number of scenarios in the system, the total number of campaigns run by the scenarios, the average percentage of the network compromised by the total of all campaigns, and a list of the top methods that compromised the network.

Scenario Display

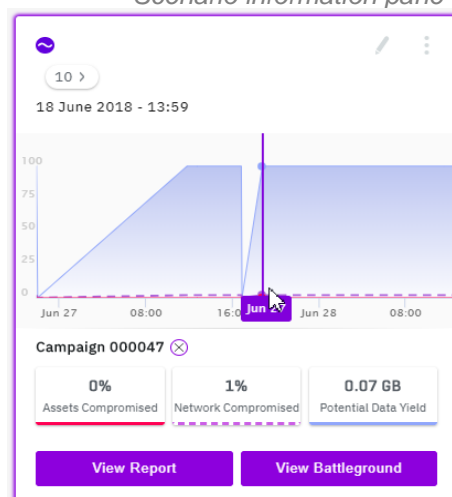
Scenarios are displayed in a grid, with each square (scenario “card”) highlighting scenario name and creation date. For scenarios in completed campaigns, the scenario display includes statistics on the percentage of compromised network and assets, as well as data yield in gigabytes. The bottom margin displays the number of hours and minutes until the next campaign scheduled by the scenario will run.

A typical scenario card is pictured in the Example Scenario pictured to the right. Note the graph in the center representing a timeline of campaigns that have completed for that scenario. Placing the cursor on the graph displays a date and the name of the campaign run by the scenario on that date. For example, in the figure, on June 27 the scenario ran Campaign 000047. The graph also depicts the percentage of assets compromised (red line), network compromised (dashed purple line), and the data yield (blue line) for the campaign. At the top left, above the scenario name, is a symbol that indicates the current status of the scenario: Active or Inactive .


Clicking on the graph displays two buttons at the bottom enabling you to **View Report** or **View the Battleground** for the selected campaign.



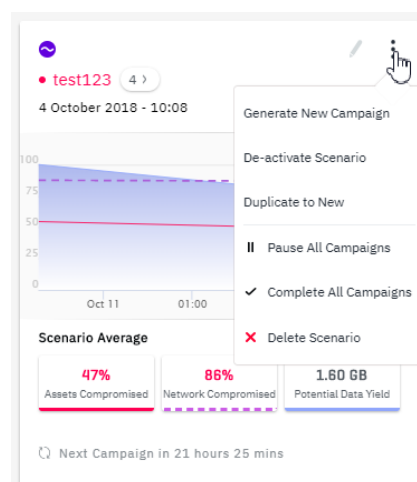
Scenario information pane



Example Scenario

At the top of each scenario card is a **More** button . Clicking the button displays a list of options enabling you to Generate a new campaign, as well as options to Activate/De-activate the scenario, Duplicate to New, Pause all campaigns run by the scenario, Complete all campaigns, or Delete the scenario:


Clicking a Scenario card selects it and displays the relevant details in the Information pane at the right of the screen.

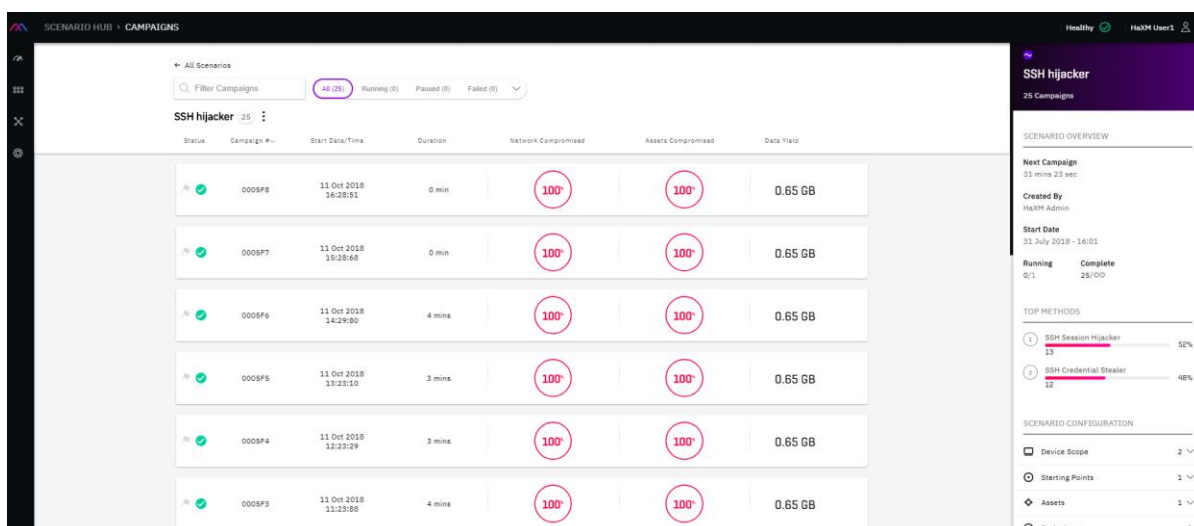


Scenario options

Viewing Campaigns

Viewing a Campaign from Scenarios

At the top of each scenario display, near the scenario name, is a button showing the number of campaigns run by the scenario to date: . Clicking this button displays the campaign on a screen as follows:

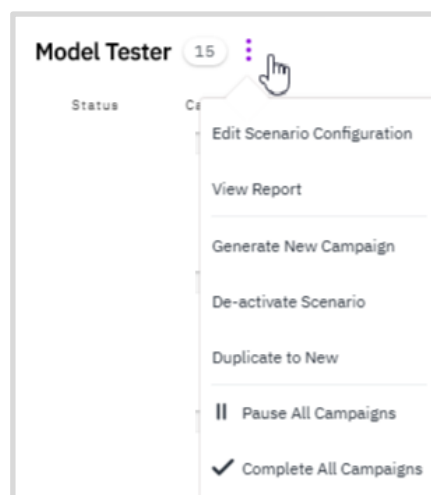


Status	Campaign #	Start Date/Time	Duration	Network Compromised	Assets Compromised	Data Yield
✓	0005F8	11 Oct 2018 16:28:51	0 min	100%	100%	0.65 GB
✓	0005F7	11 Oct 2018 19:28:46	0 min	100%	100%	0.65 GB
✓	0005F6	11 Oct 2018 14:28:40	4 mins	100%	100%	0.65 GB
✓	0005F5	11 Oct 2018 13:28:35	3 mins	100%	100%	0.65 GB
✓	0005F4	11 Oct 2018 12:28:29	3 mins	100%	100%	0.65 GB
✓	0005F3	11 Oct 2018 11:28:26	4 mins	100%	100%	0.65 GB

Scenario Details Screen






The top of the screen displays the name of the campaign scenario and a **More** button with the following options:

- Edit Scenario Configuration,
- View Report,
- Generate New Campaign,
- De-activate Scenario,
- Duplicate to New,
- Pause All Campaigns,
- and Complete All Campaigns.



Campaign Scenario Options

The remainder of the screen displays a list of campaigns already run or are currently being run by the scenario. For each campaign, the following information is displayed:

Status: Completed , Currently running , Paused , or Failed . A campaign can also be flagged  for tracking, by clicking the Flag icon to the left of the campaign.

Campaign number: a unique number assigned by XM Cyber that identifies the campaign.

Start Date: the date on which the campaign started.


Duration: the number of hours and minutes the campaign has run.

Network Compromised: the percentage of the user network compromised. The number in the center of the circle represents the actual percent. A completed circle around the percent signifies 100 percent, while lower percentages appear within incomplete circles. For currently running campaigns, the circle and its percentages change in real time, reflecting how much of the network has been compromised so far by the campaign.

Assets Compromised: the percentage of assets that have been compromised by the campaign. The percentage is displayed in the same way as Network Compromised (see above).

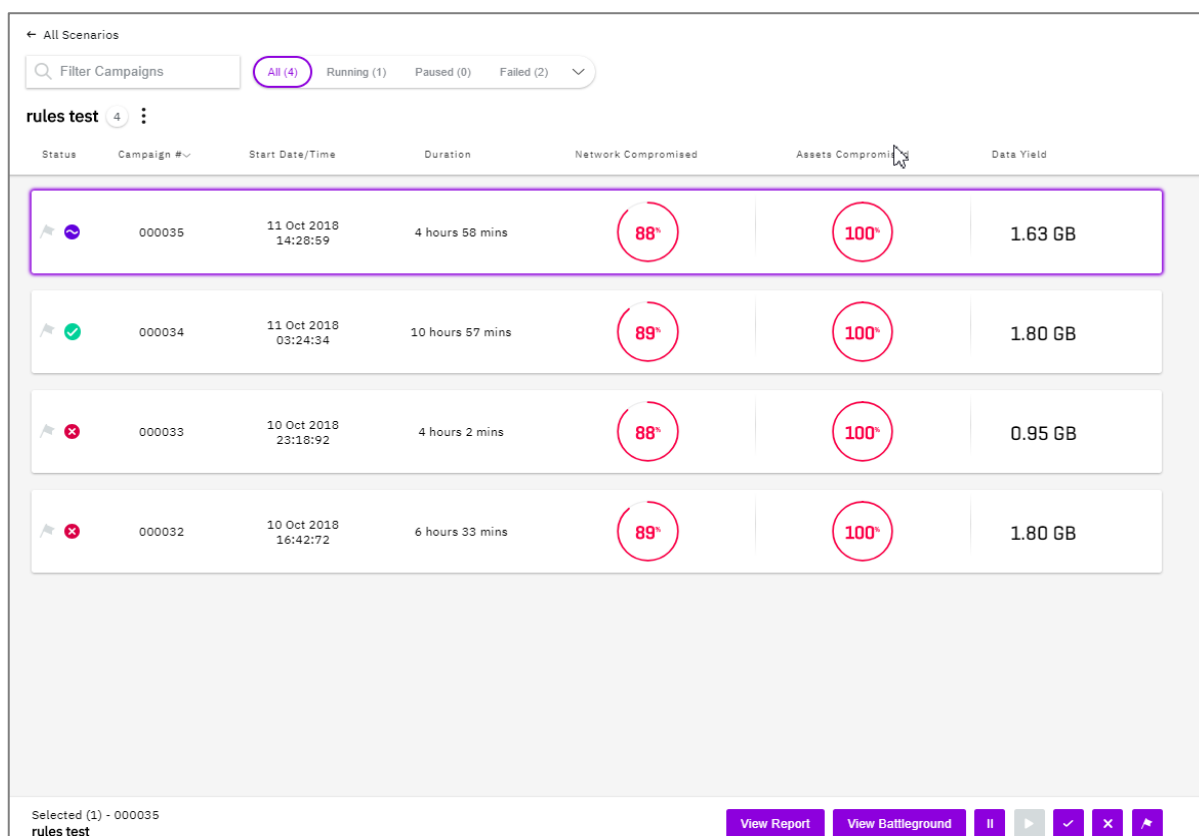
Date Yield: The amount of data potentially exfiltrated by the campaign in gigabytes.





Clicking a heading enables you to sort the list by that heading in ascending/descending order. You can also filter the list of campaigns using the buttons at the top of the campaign list (All, Running, Paused, Failed, Completed, and Flagged).

For each campaign, placing the cursor at the far-right of the information-row reveals a More button  with the following options: View Battleground, View Report, Delete. For campaigns that are currently running, there is also an option to pause the campaign.





Viewing Information on a Selected Campaign

Clicking on a campaign in a scenario campaign list selects the campaign and displays a panel of buttons at the bottom of the screen:










Status	Campaign #	Start Date/Time	Duration	Network Compromised	Assets Compromised	Data Yield
	000035	11 Oct 2018 14:28:59	4 hours 58 mins	88%	100%	1.63 GB
	000034	11 Oct 2018 03:24:34	10 hours 57 mins	89%	100%	1.80 GB
	000033	10 Oct 2018 23:18:92	4 hours 2 mins	88%	100%	0.95 GB
	000032	10 Oct 2018 16:42:72	6 hours 33 mins	89%	100%	1.80 GB

Selected (1) - 000035
rules test

View Report View Battleground    

Scenario Campaign List Buttons

The buttons enable you to view a report or view the campaign battleground   as well as performing other functions: pause/resume  , force completion of the campaign , delete the campaign , or flag the campaign .

Selecting a campaign also displays further information about the campaign on the Information pane at the right of the screen:

The top of the Information pane displays Start Date, End Date, and Duration of the selected campaign.

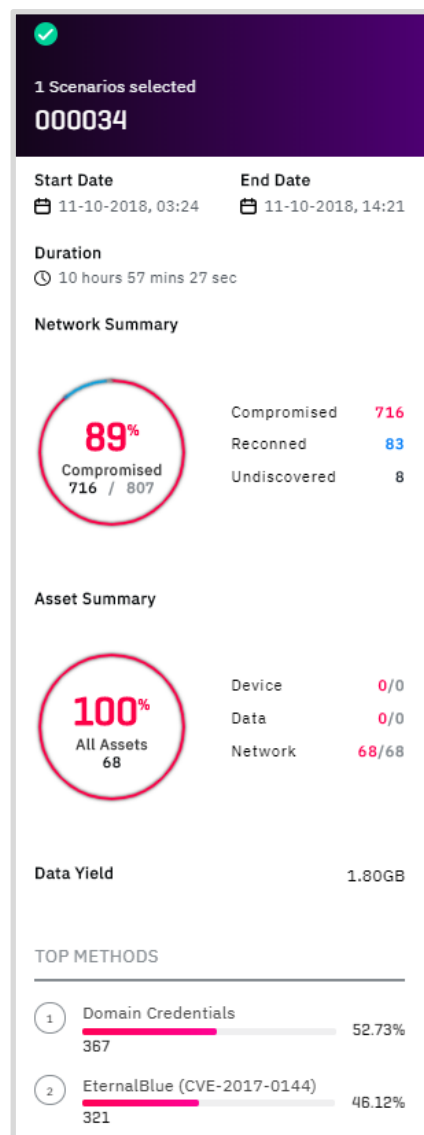
The **Network Summary** details the number of entities (devices, data, network, or cloud) in the network that were Compromised, Reconned, or that remained Undiscovered by the campaign. Placing the cursor over one of these categories changes the display in the circle to reflect the percentage of these categories. The percentage is displayed as red for Compromised, blue for Reconned, and gray for Undiscovered, with parts of the circle around the percentage, color-coded accordingly. For example, Figure 13. represents the number and percentage of the network that was compromised.

The **Asset Summary** provides details on the assets that were compromised in the campaign. The summary shows statistics for three asset categories: Device, Data, and Network assets. As with the Network Summary, placing the cursor on one of these categories displays the percentage of such assets in the circle.

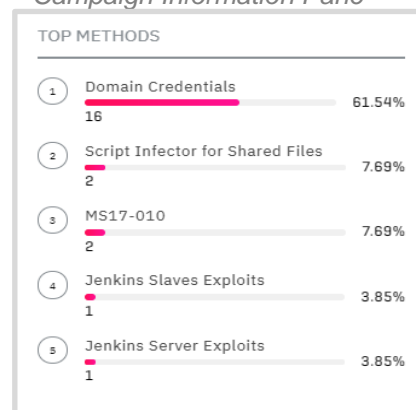
The Data Yield for the campaign is displayed in gigabytes below the Network and Asset summaries.

The Information pane also lists the **TOP METHODS** used by the campaign that were successful in compromising the network. The name of each method is listed along with the number of devices compromised by the method, as well as the percentage of the network compromised by that method. The percentage is also displayed graphically as a section of red along a grey line:

Clicking the name of a method displays a **Campaign Report**, with links to additional details, including information on how methods function.



Campaign Information Pane



Example Top Methods Listing



Findings
Credentials Relay

Compromised 3 devices, representing 0.45% of total compromised devices, using Credentials Relay

3 0.45%

Details

Rating
Severity: High
Complexity: High

Category
Configuration Management

Description
Credential Relay enables remote code execution on Windows hosts given an SMB MITM/inbound NTLM connections from windows machines. An attacker can perform a relay attack to gain credentials using the SMB protocol via a MITM between a connecting client and a target server. The attacker can relay the NTLM challenge/response authentication when a victim tries to access an attacker-controlled machine, and get access to another server using the victim's credentials.

Related MITRE ATT&CK Techniques
T1187, T1171

[Exclude](#)

Affected Devices
USERBB31 USERBB40 USERBB46

Remediation

Best Practice

- Enforce SMB signing on both clients and servers.
- Disable "editing mode" (force protected mode) for network files.
- Register endpoints DNS names (to avoid NBNS/LLMNR lookups)

Actionable Advice

Method Details Report Section

Scrolling to the bottom of the Campaign Information pane displays the Scenario Configuration, containing the following information and pop-downs:

Scope (all): the number of entities included in the scenario.

Breach Points: the number of devices that were the starting points for the scenario. Clicking this number lists the names of the devices in a pop-down.

Assets: the number of assets in the scenario. Clicking the number displays the names of the assets that are part of the scenario in a pop-down.

Exclusions: the number of attack methods that were excluded from the campaign. Clicking this number displays the names of the attack methods that were excluded.

Scenario Configuration		
	Scope (All)	131
	Breach Points	1
	Assets	2
	Exclusions	--

Scenario Configuration info

CREATING AND MODIFYING SCENARIOS

This chapter explains how to create or modify the scenarios that specify the parameters for running campaigns. Scenario parameters determine the following:

- campaign scope
- the breach point (entity or entities from which the campaign starts)
- rules for which devices are defined as assets
- duration of the campaign
- campaign schedules

and other attributes of a campaign.

Creating a New Scenario

You can create a scenario by clicking the New Scenario button at the top of the Scenario Hub screen and naming the scenario.

Clicking Confirm begins the Scenario definition process, beginning with Scope.

Scenario Name

Please provide a unique name for the scenario.

Attacker123

Cancel Confirm

Scenario Name dialogue box

1 Scope 2 Define Breach Points 3 Define Assets 4 Exclusions 5 Settings Cancel

Scope Rules

All Entities are selected


Define Scope rules that dynamically identify matching devices and tag them as Scope

Scope (125) All Entities

Search: TEXT .* Ab Show/Hide

Name ^	Type	OS	Labels	Domain / Workgroup	IP	Scope Rules
<input type="checkbox"/> AdminRole	AWS Role					Found 1 Rule
<input type="checkbox"/> artiom	AWS User					Found 1 Rule
<input type="checkbox"/> artiom AKIA*...	AWS Access K					Found 1 Rule
<input type="checkbox"/> artiom-test-a...	AWS Role					Found 1 Rule
<input type="checkbox"/> Assaf	AWS User					Found 1 Rule
<input type="checkbox"/> avishaya	AWS User					Found 1 Rule
<input type="checkbox"/> avishaya AKI...	AWS Access K					Found 1 Rule
<input type="checkbox"/> AWSServiceR...	AWS Role					Found 1 Rule

Initial Scenario Scope screen


Then proceed through the following steps, using the Plus button  to add attributes at each stage and the Next and Previous links at the bottom of the screen to move through the various steps.


1. Define the **Scope** of campaigns run by the scenario. By default, all Entities are included.
2. Define **Breach Points** for campaigns run by the scenario.
3. Define **Assets** – device, data, network and cloud assets for campaigns run by the scenario.
4. Add **Exclusions** for specific methods, pathnames, or credentials from campaigns run by the scenario.
5. Configure scenario **Settings** to edit scenario name, add an optional description, and specify settings for scheduling campaigns and duration.

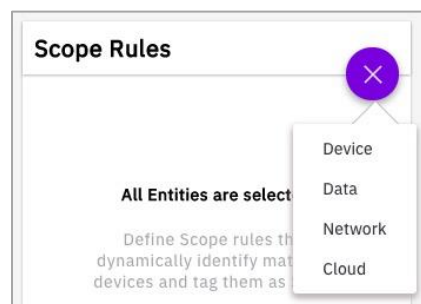
Note that returning to earlier steps requires that you repeat the subsequent steps and reset the parameters for each step (i.e., if you return to step 3, you must repeat steps 4 and 5).

The following section describes each scenario creation step in detail.

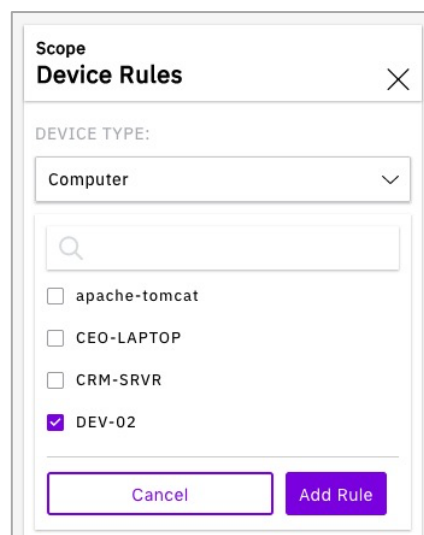
Step 1: Define Scope Rules

This step defines the rules that identify which entities (Devices, Data, Network or Cloud) are included in the scope of campaigns run by the scenario. All entities are included by default and XM Cyber recommends not limiting the scope without specific requirements to do so. Clicking the **Plus** button  lets you add a new rule specifying the exact entities to include in a scenario.

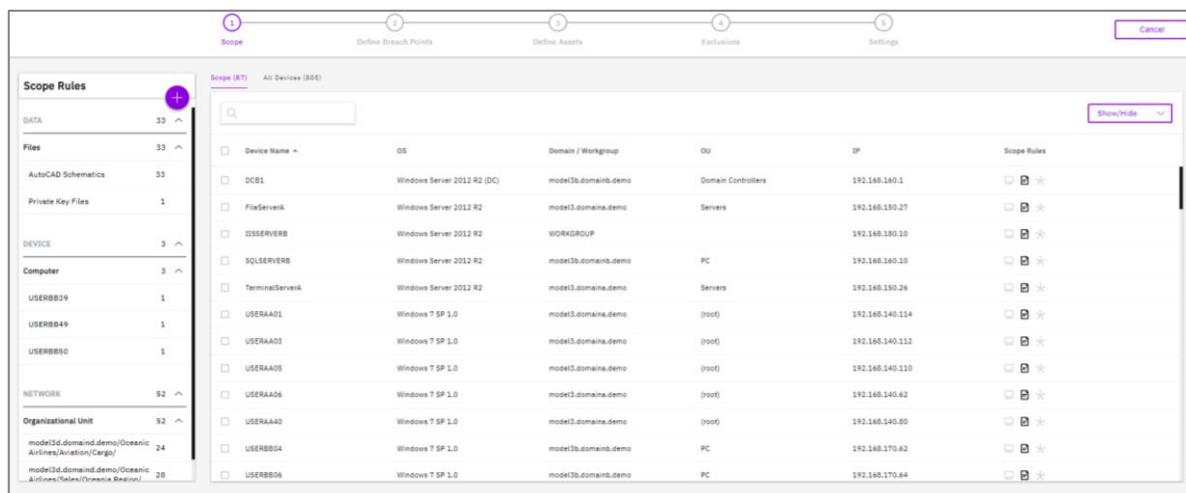
For each entity type in the pull-down, proceed to add scope rules by clicking **Add Rule**  and choosing from the listing, as illustrated for **Devices** with **Device Type** set to Computer.



Choosing Scenario Scope



Selecting Entities and Types



Set Scope Rules Screen

Once you choose your desired entity types and entities (Devices, Data, Network and Cloud) for inclusion in the scenario, they will appear in the **Scope Rules** listing.

You can display all entities in the system by clicking the **All Entities** tab (not just those in the current rule set). You can then add entities to the scope of the scenario by selecting it on the **All Entities** tab and clicking **Add** at the bottom of the screen. Similarly, you can remove devices from the scenario scope by selecting the device(s) on the **Scope** tab and then locating the selected devices on the **All Entities** tab and clicking Remove at the bottom of the screen.

You can also customize which columns are displayed on the **Scope** and **All Entities** tabs by using the **Show/Hide** button at the right of the screen.

When you are finished setting the Scope Rules, click **Next**, **Define Breach points** at the bottom right of the screen.

Scope Rules	
linuxbb01	1
linuxbb01	1
Artiom08	0
linuxbb01	1
linuxbb01	1
linuxbb01	1
USERBB47	1
USERBB50	0
USERDD388	0
REMOVED SCOPE 3 ^	
Artiom08	
USERDD388	
USERBB50	

Scope Rules Pane Including Removed Scope

Step 2: Define Breach Points

The **Define Breach Points** screen enables you to select entities (Device, Data, Network or Cloud) as breach points for the scenario. By default, no breach points are defined in a scenario and at least one is required. It is advised to start defining a campaign using entities considered most vulnerable to a hacker. For example, these entities might be specific computers, network domains, or cloud users/tokens.

As you add entities (if they are actually present in your environment), each is displayed as a rule in the **Breach Points Rules** pane and in the Breach Points listing on the right hand part of the screen.

As with determining Scope in the previous section, you can use the **Breach Points** tab to delete breach points and the **All Entities** tab to add them to a given rule.

Breach Points Rules	
DATA	0 ^
Files	0 ^
Database Files	0
Outlook Mailboxes	0
DEVICE	0 ^
Computer	0 ^
USERBB39	0
USERBB49	0
USERBB50	0
NETWORK	0 ^
Domain	0 ^
model3.domain.demo	0

Breach Points Rules pane

Breach Points (2)		All Entities					
<input type="text"/>		<input type="text"/>					
Name ^	Type	OS	Labels	Domain / Workgroup	IP	Breach Point Rules	
<input type="checkbox"/> DEV-02	Sensor	Windows 7 S...	spooler	dev.model.demo	192.168.251.19	Found 1 Rule	
<input type="checkbox"/> spring-break	Sensor	Windows 7 S...	java	WORKGROUP	192.168.230.100	Found 1 Rule	

Breach Points Tab display

NOTE: You must define at least one breach point before proceeding to the next stage.

After defining breach points, click **Next, Define Assets** Next **Define Assets** → at the bottom of the screen.

Step 3: Define Assets

The Define Assets screen enables you to define rules that identify assets within your system. By default, no assets are defined for a scenario and at least one asset is required. Asset rules can be defined for entities known to XM Cyber, as with scope and breach points. For example, a device may be considered an asset if it performs a specific role such as a server, if it stores data contained in specific files, or if it is located in a certain subnet or workgroup.

To create an asset rule, click the **Plus** button to choose the asset type and see the available entities for that type. You can use the **Assets** and **All Entities** tabs in the main pane to view/remove assets already included or to add new ones from **All Entities**.

Assets
Network Rules [X]

NETWORK TYPE:

Select... [v]

Credential Mapping

Domain

Organizational Unit

Subnet

Workgroup

Asset Rules for Networks

Assets (9)		All Entities					
Name ^		Type	OS	Labels	Domain / Workgroup	IP	Asset Rules
<input type="checkbox"/>	cf-templates-...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	cf-templates-...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	cf-templates-...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	cf-templates-...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	cg-secret-s3-...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	customerdata...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	nodetlv2020.l...	AWS S3 Bucket					Found 1 Rule [≡]
<input type="checkbox"/>	xm-lambda-tr...	AWS S3 Bucket					Found 1 Rule [≡]

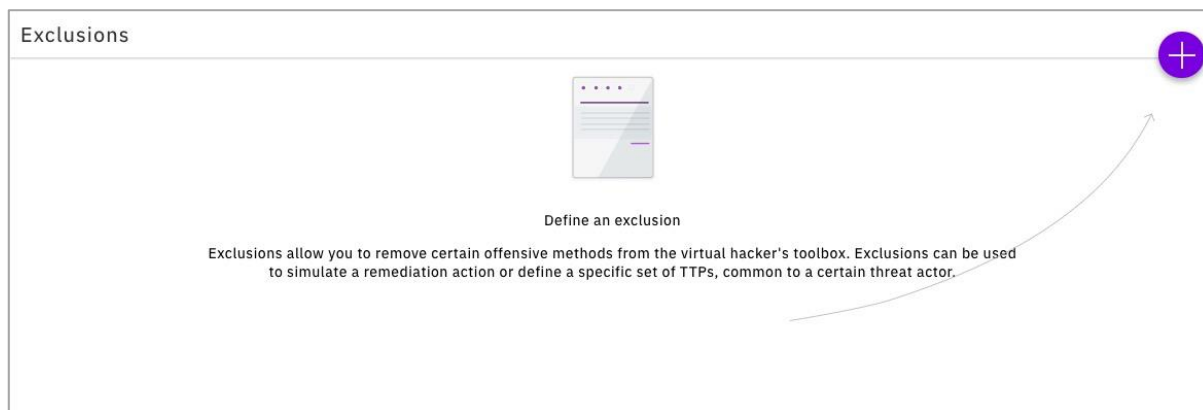
Define Assets Screen Showing Rules for Cloud Assets

Asset rules may overlap and specify the same device. For example, the same computer may conform to the rule for a specific computer name as well as fulfill a role included in the device rules, such as Web Server.

After defining assets, click **Exclusions** at the bottom of the screen to move to the next step.

Step 4: Exclusions

You can exclude specific methods or parameters, such as CVEs and credentials, from participation in scenarios. Exclusion enables you to customize scenarios to control how they affect your network. For example, you can remove a method to simulate a remediation action.

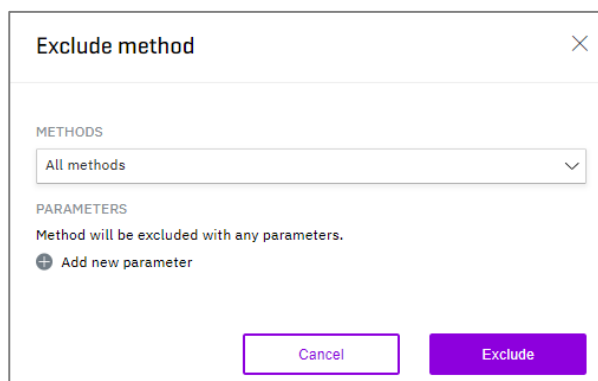


Initial Exclusions screen

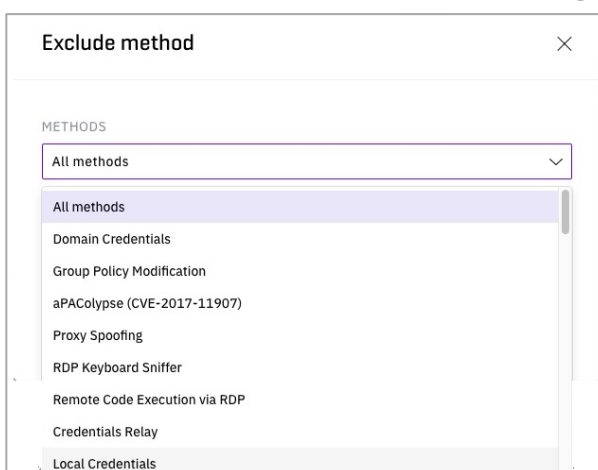
There are no exclusions defined by default and none are required to move to the next step.

To exclude a method:

1. Click the **Plus** button to create an **Exclusion**
2. Click the **Methods** drop-down to select a method type. By default, all methods found in the environment will be excluded.



Exclude methods dialog



Method selection drop-down

3. To add a parameter to the method, underneath **Parameters**, click the **Add new parameter** button and select a parameter type from the Parameters dropdown:
4. To add an additional parameter, click the **Add** button at the right of the **Parameter** box. To remove a parameter, click the at the right of the parameter to remove.

Providing method parameters

5. After adding parameters to the method, click the **Exclude** button . The method, along with its type and parameters, is displayed on the **Exclusions** screen.

After adding exclusions, click **Settings** at the bottom of the screen to move to the last step, **Settings**.

Step 5: Settings

In this step, the **Settings** screen lets you further customize various attributes of a scenario

Scenario Settings Screen


This screen contains the following configuration options:

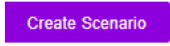


Scenario Name	Edit the scenario name visible in various contexts.
Description	Enter an optional description for the scenario.
Maximum Running Campaigns:	Specify the maximum number of campaigns that can be run concurrently by the scenario.
Complete Campaigns:	Specify the conditions to terminate the campaign: when the entire network is compromised, or when all assets are compromised. You can choose either or both options. Selecting neither will run the campaign for the duration specified in Campaigns run for .
Campaigns run for:	Specify the duration of campaigns run under the scenario.
Multiple Attack Vectors:	Recommended to enable Allows assets to be compromised multiple times via different attack vectors. After the first attack, an asset can be compromised again via another attack vector, to find all compromises and report them in order of complexity.
Generate Campaigns Now:	Select for generating new campaigns immediately or later, at your convenience.

When you are finished entering the settings, click **Review** at the bottom of the screen.

Step 6: Review

This final step lets you review the scenario settings. You can change settings by clicking the **Edit** button  at the top right corner of each step encountered above (Scope, Breach Points, etc.).

When you are satisfied with the settings, click the **Create Scenario** button  at the bottom of the screen. The Scenario is now displayed as a card on the **Scenario Hub** screen.

Review

New Scenario

Cancel

Settings

SCENARIO NAME

⊖ New Scenario

MAXIMUM RUNNING CAMPAIGNS

1

CAMPAIGNS RUN FOR

01:00:00

CAMPAIGN GENERATED

Every 1 days 0 hours

Starting 03 Apr 2020

Will generate now

DESCRIPTION

a very boring scenario

SCENARIO CREATED BY

billw

MULTIPLE ATTACK VECTORS

Disabled

SCOPE

144/144

BREACH POINTS

7/144

ASSETS

9/144

METHOD EXCLUSIONS


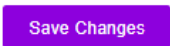
1

Review Screen

Editing Scenario Settings

You can edit the settings of any scenario on the **Scenario Hub** screen. You can change all settings including scope settings, breach points, assets, and scheduling settings.

To edit a scenario:

1. On the **Scenario Hub** screen, select a scenario and at the upper right of the card, click the **Edit** button. The Review screen appears (see above).
2. Review the settings and click the **Edit** button  at the top right of the step whose settings you want to edit. A screen will appear enabling you to edit the settings of the selected step.
3. After completing the settings for a particular step, click the **Save Changes** button  at the lower right of the screen.

NetBackup 1 >

28 June 2018 - 17:15

First campaign in progress

Template Average

0%

Assets Compromised

0%

Network Compromised

0.00 GB

Potential Data Yield

Next Campaign in 23 hours 14 mins

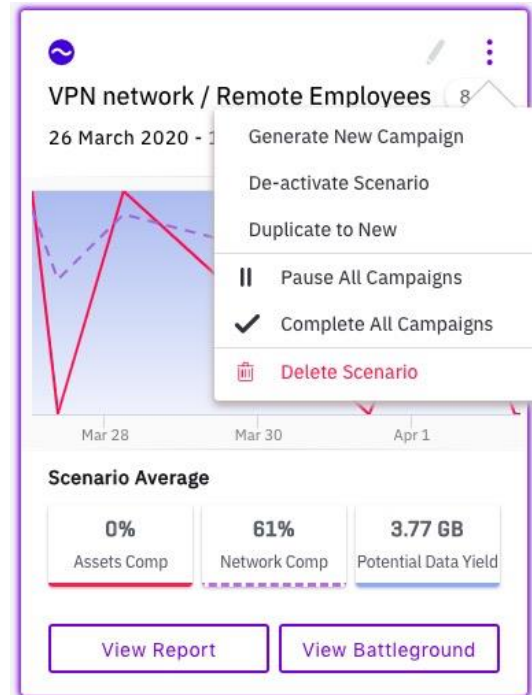
Scenario card with Edit button

4. After completing your edits, click **Close**.

Manually Generating a Campaign from a Scenario

To start a campaign manually from an existing scenario:

1. On the **Scenarios** screen, select the scenario from which you want to start the campaign.
2. At the top of the scenario's card, click the **More** button (three dots) and click **Generate New Campaign**.
3. A new campaign is generated according to the scenario settings.



Generate New Campaign from drop-down

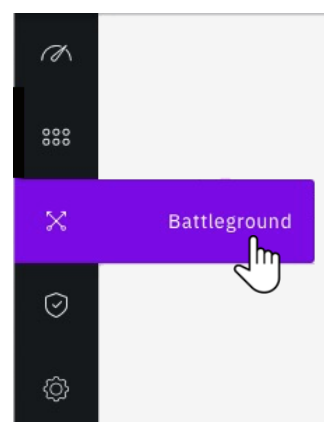
THE BATTLEGROUND

The **Battleground** offers a real-time graphical view of the progress of an ongoing campaign. The Battleground can also play back a completed campaign. The **Battleground** provides layers of information that reflect the progress of a campaign and a timeline. Information includes the identity of each node participating in the campaign, its status at any time in the campaign (compromised, reconnected, or undiscovered), as well as listing events that caused the change of status.

Zoom out to display the top layer of information with a bird's eye view of organizational units, workgroups, subnets, etc. By zooming in, you view a graphical representation of each device in the campaign along with its identity, a timestamp of the event that changed its status, and the source of the event.

Navigating to the Battleground

There are multiple ways to display the **Battleground** screen. The simplest path is to click the **Battleground** button on the main navigation strip on the left-hand side of the XM Cyber display.



Selecting Battleground from the navigation strip

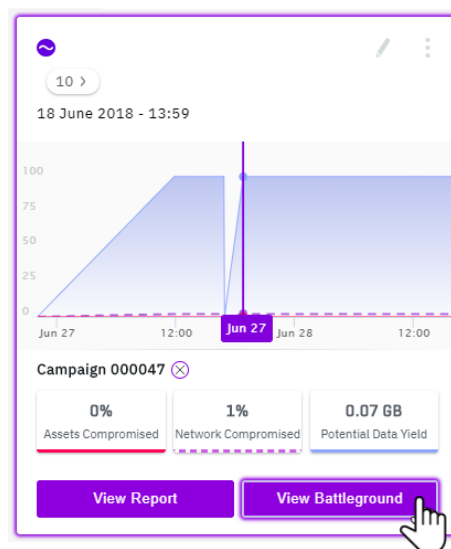
To display the **Battleground** for a campaign:

1. On the **Scenario Hub** screen, select a scenario card.
2. Then, do one of the following:

- Use the slider in the selected card to locate a campaign along the displayed timeline and click once. Click the **View Battleground** button that appears at the right bottom corner of the card:

—OR—

- Click the oval next to the scenario name displaying the number of campaigns run by the scenario. From the displayed list of scenarios select a campaign and click the **View Battleground** button at the bottom of the screen.



Battleground Button on Scenario display

Status	Campaign #	Start Date/Time	Duration	Network Compromised	Assets Compromised	Data Yield
	000006	21 Oct 2018 15:57:46	37 mins	87%	74%	0.97 GB
	000005	21 Oct 2018 11:46:45	4 hours 2 mins	85%	91%	1.14 GB
	000004	21 Oct 2018 11:28:03	15 mins	3%	69%	0.35 GB
	000003	20 Oct 2018 22:58:47	12 hours 26 mins	86%	91%	1.19 GB
	000002	20 Oct 2018 17:35:39	5 hours 21 mins	85%	91%	1.19 GB

Selected (1) - 000005
kiril-test

View Report View Battleground

Viewing the Battleground from a Campaign

–OR–

- On the **Scenario Hub** screen, select a scenario, and on the **Scenario Information** pane that appears at the right of the screen, click the **Campaigns** link under the scenario title. A similar list of campaigns is displayed. Select a campaign and click the **View Battleground** button at the bottom of the screen.

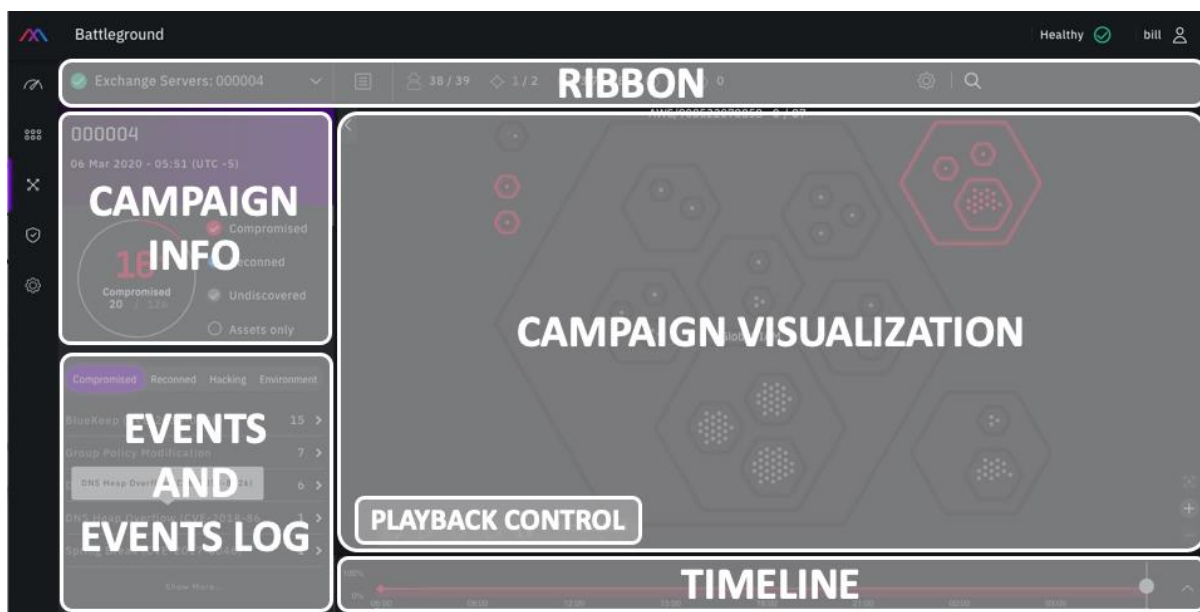
Understanding the Battleground Screen

Below is the opening battleground display.

The **Battleground** screen displays several key pieces of information and features controls to adjust your view of the Battleground, as follows

Screen Layout

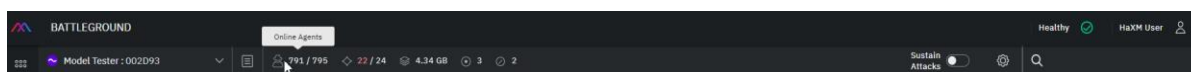
The screen is broken into a number of functional areas: Campaign Info, Ribbon, Events and Event Log, Campaign Visualization, Timeline and Playback Control. The following sections describe each in detail.



Battleground Screen Layout

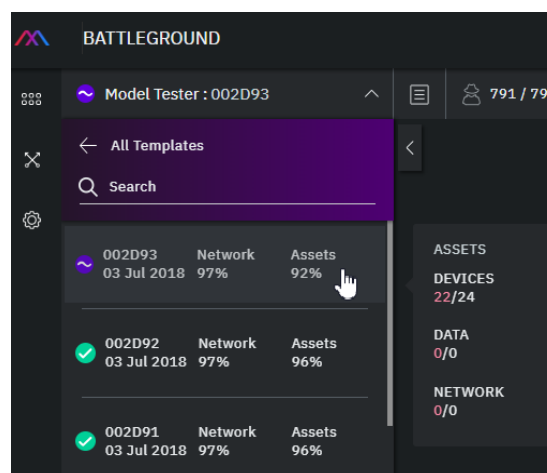
Ribbon

At the top of the screen is a ribbon displaying information and display controls.



Battleground Ribbon

On the left-hand side of the ribbon, above the central display, is displayed the name of the scenario and campaign. For example, in the figure above, the campaign 000093 is running under the Model Tester scenario. The ribbon includes a button for displaying reports on the campaign and scenario, as well as icons indicating the number of online sensors, the number of compromised assets compared to the total number of assets, the data yield in gigabytes, the number of breach points, and the number of exclusions.




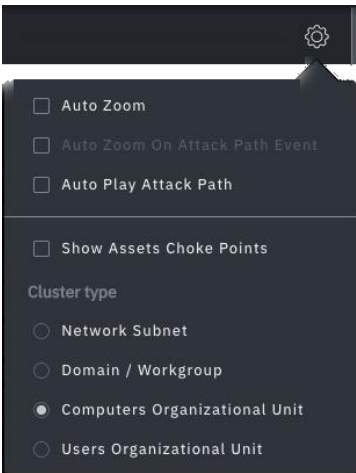
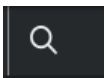
Dropdown – other campaigns in the same scenario

Clicking the dropdown menu next to the **scenario: campaign name** displays a list of other campaigns run by the same scenario. Each campaign in the list displays the date and

time of the start of the campaign as well as percentages of the network and assets that were compromised. Clicking a campaign displays the associated **Battleground**.

Hovering over a campaign in the list displays additional information on the number of devices, data, and network assets compromised in the campaign.

The ribbon has buttons that enable control of the display, described in the following table.

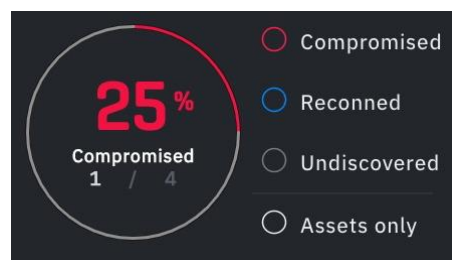
Ribbon Elements	Function
 	<p>Settings - displays a dropdown menu with two sections.</p> <p>The upper section displays options to customize the display:</p> <p>Auto Zoom: zooms on devices in close proximity to attacks displayed in the Events and Event log area.</p> <p>Auto Zoom On Attack Path Event: Automatically zooms into a selected attack path as a user steps through them</p> <p>Auto Play Attack Path: zooms on attack path(s) during playback of past campaigns</p> <p>Show Assets Choke Points – highlight devices presenting the greatest risk to the environment</p> <p>Cluster Type</p> <p>The lower section of the menu is labeled Cluster type and displays options to enable display of the Battleground in a grouping of computers by the following criteria: Network Subnet, Domain/Workgroup, Computers Organizational Unit, or Users Organizational Unit.</p>
	<p>Search – enables search for strings in the Battleground. For example, to find and display a list of all computers with Server in their name. Clicking an item in the list zooms in on the item.</p>

Campaign and Event Info Panel

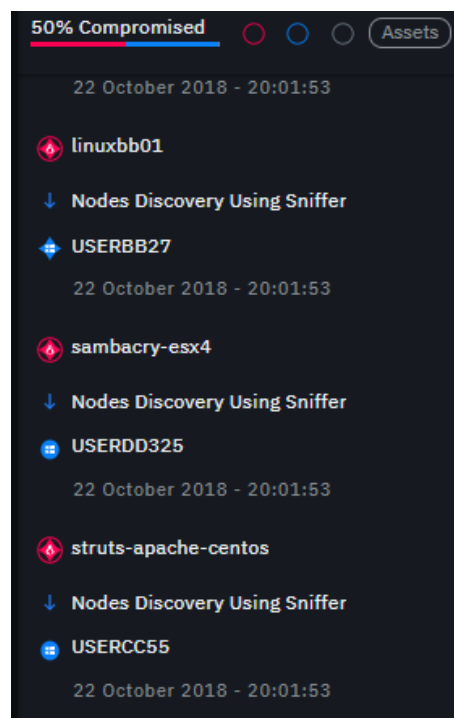
The left-hand area of the **Battleground** screen features a panel displaying general information on the campaign, a summary of compromised devices and methods of compromise, and access to more detailed logs of compromise events.

The large circle on the left of the Tracker shows the percentage of compromised devices reflecting selections on the Campaign Visualization. This circle changes to a small horizontal bar with scrolling down the list of methods. The smaller circles on the right of the Tracker (Compromised, Reconned, Undiscovered and Assets Only) are actually buttons. These buttons let you filter the visualization to show only clusters with the associated status, i.e., clicking **Compromised** will highlight compromised clusters in white and redraw all others in black (but not fully hide them). Filtering also recalculates the value in the larger tracker circle.

Clicking on the methods listed below the tracker changes the **Battleground** visualization to show only devices compromised by that method. Note that the number of devices compromised by a given method is displayed above the methods list. These selections determine the content display on the **Battleground**. Clicking on the lines in this area displays details about the **Battleground**, such as **Compromised** or **Reconned**.



Compromised Device Tracker



Compromise methods in use

The bottom part of this panel features four event-type tabs that follow the MITR ATT&CK TTP:

- **Compromise** - a device or asset can be compromised
- **Recon** - a device or asset can be discovered
- **Hacking** - an action an attacker would take to modify a system
- **Environment** - user and device behaviors

With listings of the methods encountered of the type specified by the tab. Clicking on the method opens a log of attacks made thus far in a campaign, showing the number of attacks and a list of the attacks themselves.

Each attack shows the device IP address of the origin of the attack and the name of the device under attack, and the date and time of the attack. Colored symbols indicate whether the attack resulted in a compromised or reconned device (red circles indicate compromise, blue, recon).

Clicking a log entry displays the attack on the **Battleground** visualization panel.



Attack methods and event log

Campaign Visualization

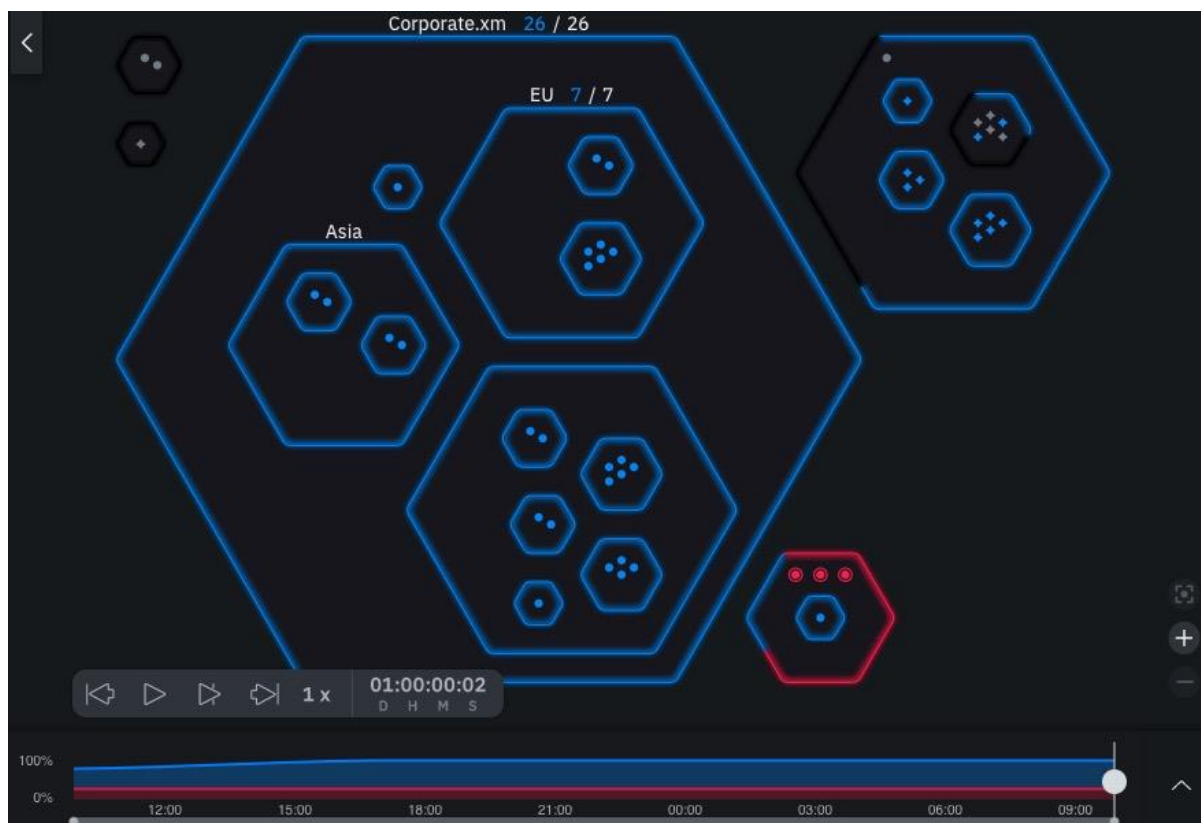
The **Campaign Visualization** panel is the main focus of the Battleground, where the “action” occurs. The rest of this section will concentrate on this panel and its uses.

Battleground Opening Display: Viewing Clusters

Upon opening a campaign **Battleground**, XM Cyber displays the clusters involved in the campaign. Clusters appear as hexagons filled with circles representing monitored devices.

By default, the display shows clusters organized by Microsoft Active Directory organizational units. Clicking the **Settings** button on the ribbon allows changing the display as explained in the table above.

As devices in a cluster progressively become compromised or reconned, the sides of the hexagon in which they are grouped turn red or blue, respectively. At the edge of each hexagon are displayed the total number of devices in the cluster and the number of compromised nodes.



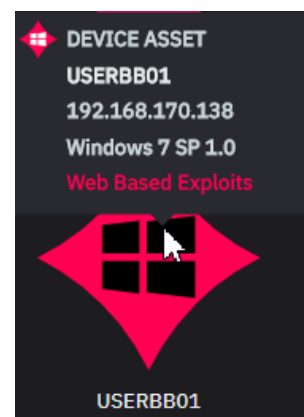
Opening Battleground Display Showing Clusters displayed by Organization Unit

Hovering over the edge of a cluster displays the cluster IP address and percentage of compromised devices in it.

















By using the mouse wheel or the **Zoom** buttons at the right side of the screen, you can display more information for each device. Icons in the hexagon represent devices according to the following scheme.

Device names are displayed below the icon. Hovering over the icon displays its IP and operating system, and the compromise or recon method for the device.

Assets are indicated by diamond shaped icons. described in the table below.



Hovering over a Device icon

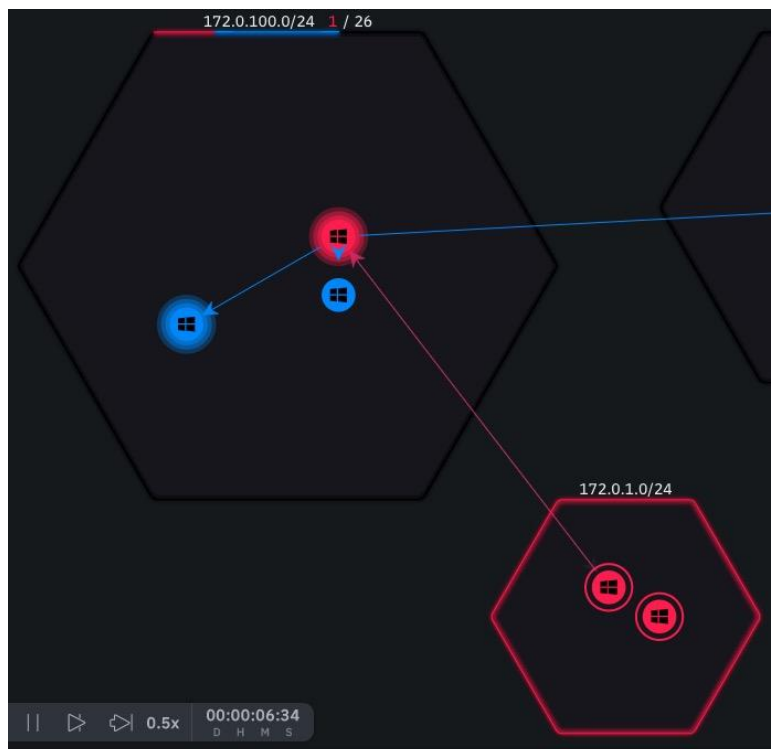
	Compromised breach point (Windows device)
	Compromised Windows device
	Reconned Windows device
	Disconnected reconned Windows device
	Undiscovered Windows device
	Disconnected undiscovered Windows device
	Compromised breach point (Windows device asset)
	Compromised Windows device asset
	Reconned Windows device asset
	Undiscovered Windows device asset
	Compromised Linux device asset
	Reconned Linux device asset
	Undiscovered Linux device asset
	Compromised Linux device
	Reconned Linux device
	Undiscovered Linux device

Cluster device icon descriptions

Viewing Attacks

Events that cause nodes to be compromised or reconned are indicated as red/blue arrows. For currently running campaigns, arrows appear in real time to indicate attacks in progress. To view attacks that have already occurred, click on the node.

An arrow appears leading from the attacking device to the compromised or reconned node. If the attacking node itself was compromised from a breach point, an arrow is displayed showing that as well:

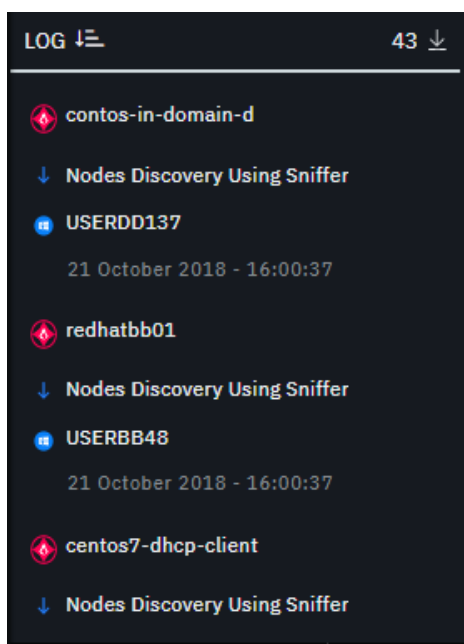


Viewing attacks in progress

Note that the arrows come and go as the simulation progresses, in real-time or across the time-line of a recorded attack.

Details of attacks that have occurred up to the time specified on the timeline are represented in the **LOG** area on the panel at the left of the screen:


You can also scroll through the log to view all attacks. To view the attack on a specific node, click the node on the **Battleground** display; the **LOG** jumps to the attack that compromised or reconned the node:

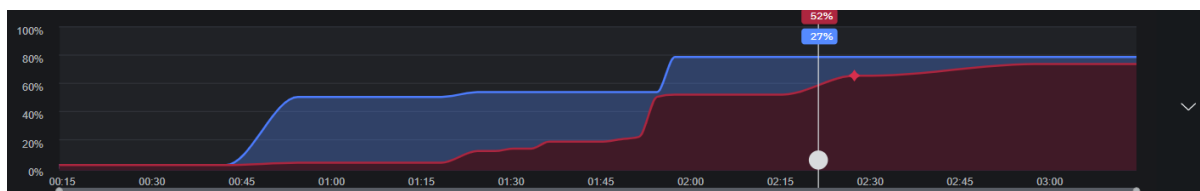


Log Area Displaying Attack information



Attack log details

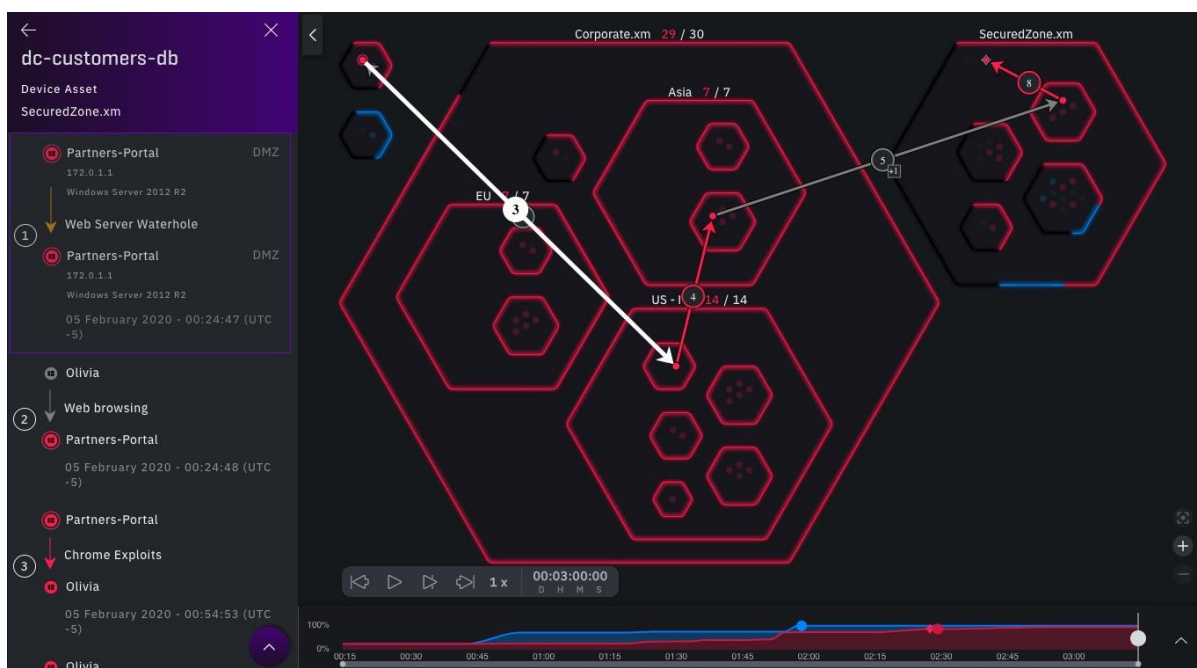
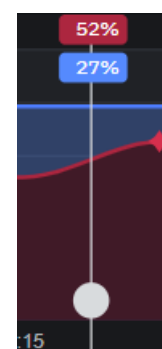
The campaign **Timeline** is displayed at the bottom of the screen. The **Timeline** displays time in increments that you can specify as explained below. The full **Timeline** also displays a graph indicating the percentage of devices that the campaign has compromised. To display the timeline together with its graph, click the **Timeline Display** button  at the right bottom corner of the screen. The **Timeline**, together with its graph, appears at the bottom of the screen



Timeline Display

The white marker can be dragged to an exact time on the **Timeline** and displays the percentage of the system compromised up until that time

Clicking a point on the timeline displays attacks that have occurred up until that time on the **LOG**. You can easily scroll the **LOG** upward from the last attack to view previous attacks. Clicking at the right side of the attack display on the **LOG** displays the attack graphically on the **Battleground**:



Attach log entries correspond to Battleground arrows







The **Timeline** also displays red and blue markers to indicate the attacks that occurred at that time. Double-clicking a marker on the **Timeline** jumps to the corresponding attack on the log. Compromised assets are indicated by red diamond markers on the timeline.

Modifying time intervals on the timeline

You can increase or decrease the time interval displayed on the **Timeline** by expanding or contracting the bar underneath the timeline, at intervals between 1 second and 15 minutes.

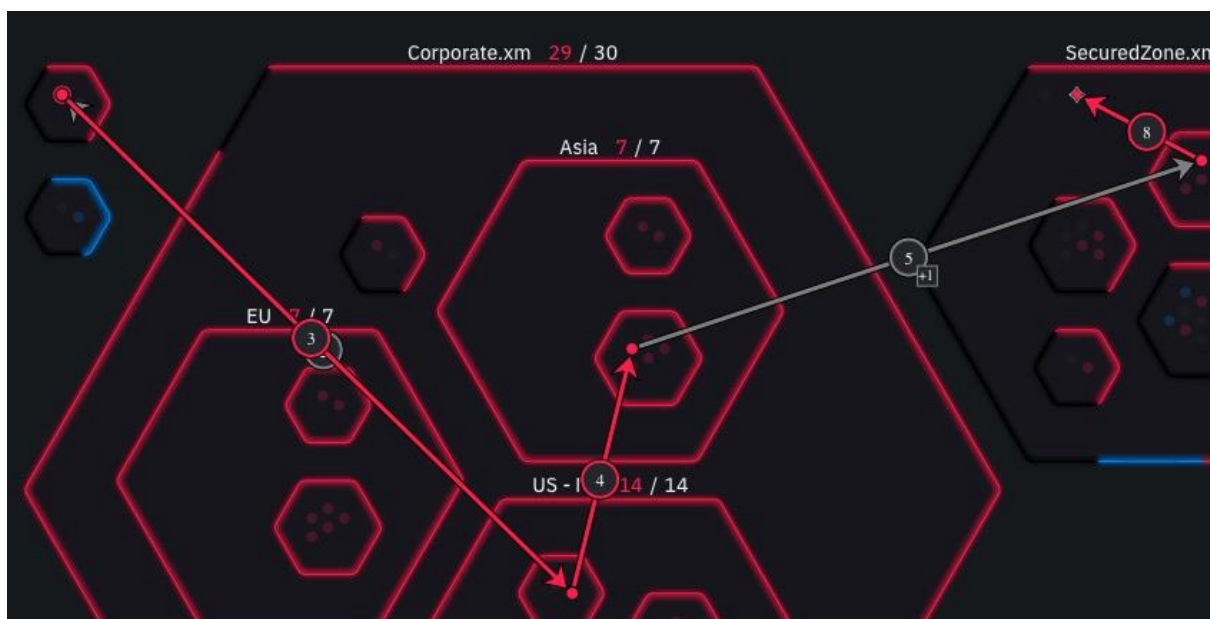


Timeline Control Bar

Button:	Function:
	Long Jump Backward
	Jump to Previous Event
	Play/Pause
	Jump to Next Event
	Long Jump Forward
	Current Speed; Increase/Decrease Speed

Timeline Control Buttons

The **Timeline** displays events as colored lines (red for compromised events, blue for reconnected). You can use the **Zoom** buttons on the right side of the **Timeline** to zoom in and out. When you zoom out to view only clusters, lines represent groups of events with the number of events displayed inside a circle on the line:



Cluster View with Numbers of Events Displayed inside Circles

Clicking on an event on the **Timeline** navigates to the device and the attack that compromised or reconnected the device on the **Battleground**. If the event represents a group of events, all events in that group are displayed.

You can also navigate the timeline by dragging the purple marker.

You can also move the marker by double clicking on any location on the **Timeline**; the marker jumps to the location selected.

As you move across the **Timeline**, the **Battleground** changes to display events that occurred at the specified time. By alternately using the **Zoom** and **Filter** buttons, you can gain an accurate picture of how the campaign progressed and identify how devices were compromised or reconnected.



Timeline
Marker

Color Key

The use of colors on the **Battleground** aids in understanding the campaign. Undiscovered devices appear in grey. A device turns color when compromised (red) or reconnected (blue). Events that triggered the change in status are displayed as red or blue arrows. The arrows originate from the device that caused the event to the device whose status was changed as a result. For example, a typical **Battleground** display looks like this



Battleground Display with different colored arrows

There are four arrows colors that correspond to different attack activities

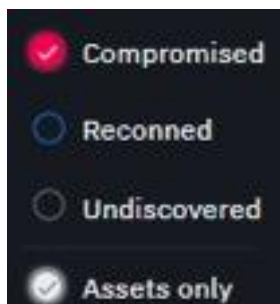
- Red Arrow – Compromise
- Blue Arrow – Recon
- Yellow arrow – Hacking
- Grey arrow – Environment activity
- Dotted yellow line – credential harvest from another source

Modifying the Display Using Filter Buttons

On the top right of the **Battleground** information panel are filter buttons that enable filtering the **Battleground** and display devices according to their status: compromised, reconnected, or undiscovered.

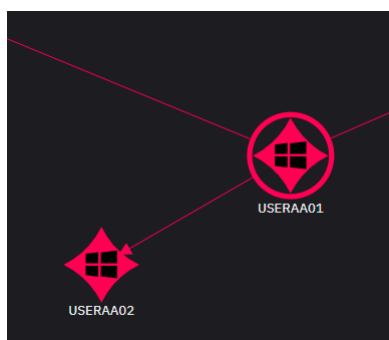


Filter Buttons



Filter Buttons Selected

Zooming in to this area displays additional detail for each node.



Zoomed-in Linux Device Asset

Moreover, you can restrict the display to assets only. For example, you can select the **Compromised** and **Assets** only buttons, resulting in a display showing only compromised assets (see below)



Filtered Display



Campaign Playback controls

Campaign Playback

The **Battleground** supports playback of previously run campaigns. When you open a pre-recorded campaign, **Playback Controls** will appear in the lower left-hand part of the **Campaign Visualization** pane. The buttons, left to right, control rewind, play, play to next log entry, fast-forward to end, and adjust playback speed pop-up menu (0.5X – 4X).

As you playback a campaign, the **Campaign Visualization** pane steps through the pre-recorded activities, reflected in the **Timeline** at the bottom of the display.


REPORTS

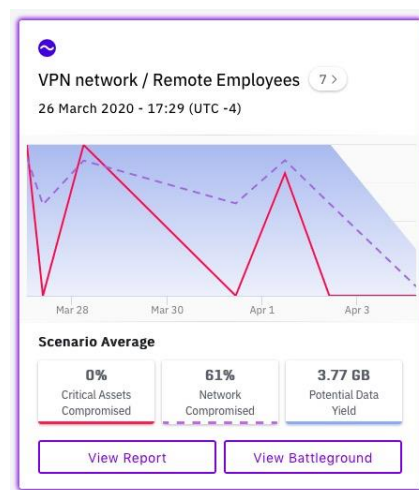
XM Cyber provides detailed reports on campaigns currently underway or already finished. Reports can be viewed on-screen or can be downloaded as PDF files. Reports provide useful summaries of scenarios, campaigns, technical details, and remediation advice.

How to Access Reports

Accessing Reports from the Scenario Hub


Scenario Reports

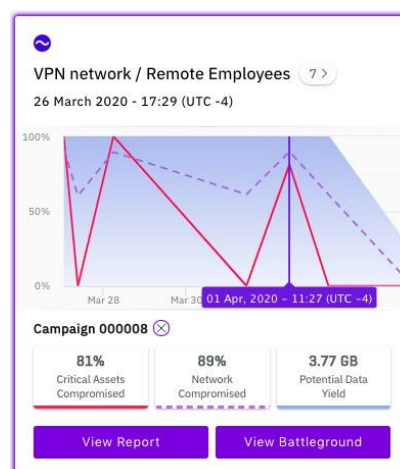
To view a scenario report, from the **Scenario Hub** screen, select a scenario card. Make sure you only click in the white space surrounding the scenario content. If you click on the scenario timeline graph, you will end up selecting a single campaign for that scenario. Once you have chosen a scenario, click the View Report button  (the button fill will be white).



Selecting a Scenario Report

Campaign Reports

To view a campaign report, from the **Scenario Hub** screen, select a scenario card. Move your mouse across the campaign timeline graphic in the middle of the card until you find your campaign of interest. Click in the white space surrounding the scenario content. If you click on the scenario graph, you will end up selecting a single campaign for that scenario. Once you have chosen a scenario, click the View Report button  (the button fill will be solid).

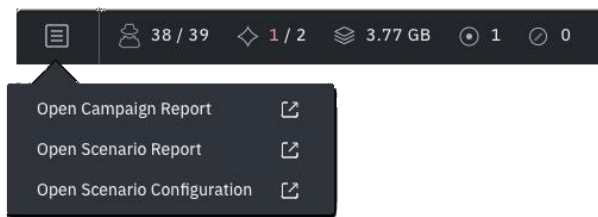


Selecting a Campaign Report

Note – once you have selected a campaign on a scenario timeline graph, you will only be able to select individual campaign reports from that scenario card using the graph. To view a full scenario report, you must reload the **Scenario Hub**.

Accessing Reports from the Battleground

You can access any campaign's report from the Battleground by clicking the Reports button on the **Battleground** ribbon and selecting **Open Campaign Report**. You can also view a report for the entire scenario by selecting **Open Scenario Report**. In either case, a new tab opens in your browser displaying the report.



Report / Configuration Pull-down

Report Navigation

Scenario Reports

Scenario Reports require that you specify start and end dates to view summarized campaign data > using the calendar tool at the top of the **View Report** screen.

You can scroll through the Scenario Report **Overview** to view the constituent Campaign Reports.

You can use the menu at the left of the report window to navigate to the type of Scenario Report information you want to view. See **Understanding Reports** below for a fuller explanation of the information in the report.



Scenario Report navigation menu

Campaign Reports

You can use the menu at the left of the report window to navigate to the type of Campaign Report information you want to view. See **Understanding Reports** below for a fuller explanation of the information in the report.

Note – the Campaign Report navigation menu contains the additional destination, **OS Summary**.

To download a Campaign Report as a PDF, click the **Export Report** pull down menu at the top right of the screen and specify the report items that you want to download. In addition, you can also download any section of the report as a .CSV file for use with Excel or other spreadsheet software by clicking the **Download** button at the far right, just below the **View Battleground** button.



Campaign Report navigation menu

Understanding Reports

Both Scenario Reports and Campaign Reports consist of the following sections:

- Critical Assets Findings
- Critical Assets
- All Findings
- All Devices
- Breach Points
- Scenario Configurations

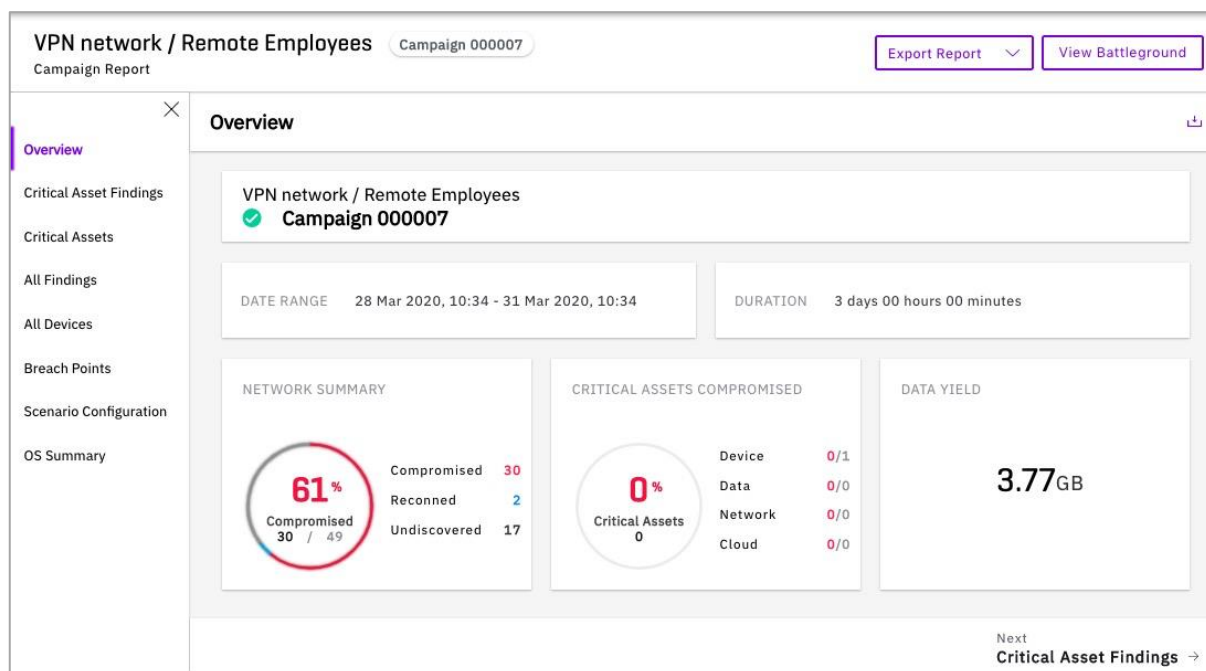
Campaign Reports have an additional section, OS Summary

The primary difference between Scenario and Campaign Reports is that while Scenario Reports summarize the data from all associated campaigns, Campaign Reports focus exclusively on a single campaign.

Overview

The Campaign Report **Overview** section displays the date, time, and duration of the campaign and provides a graphic overview of the number and percentage of compromised and reconned network devices and assets.

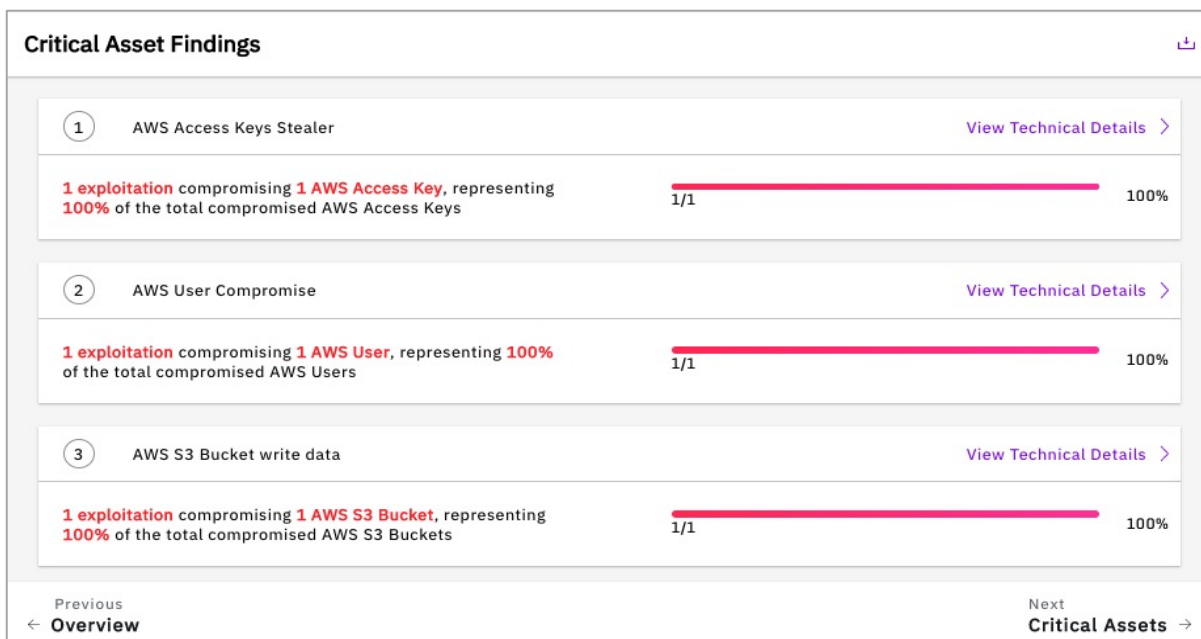
Note that in the following report extracts, the **Scenario** is named “VPN Network / Remote Employees” and the **Campaign** is 000007.



Campaign Report Overview Section

Critical Asset Findings

The **Critical Asset Findings** section highlights which assets were compromised in the campaign(s) and allows you to explore the particulars of each finding by clicking on the **View Technical Details** link.



The Critical Asset Findings display

Critical Assets

The **Critical Assets** section lists assets involved in the scenario or campaign.

Critical Assets

[All Critical Assets](#) [Critical Asset Rules](#)

Search Critical Assets [Show/Hide](#)

Name	Type	Affected Devices	Critical Assets At Risk	Cost of Exploitation	OS	IP	Status	Method	Cluster
customerda...	AWS S3 Bucket	N/A	N/A	10				AWS S3 Buc...	AWS/90852...
dc-custome...	Sensor	0	0	N/A	Linux cento...	172.0.201.11			SecuredZon...

Previous [Critical Asset Findings](#) Next [All Findings](#)

The Critical Assets display

For large asset inventories, you can Search through the listed assets. You can also hide the various columns in this report using the Show/Hide pull-down and selecting which columns to hide.

Asset / Entity Deep Dive

You can deep dive for additional asset and related entity information and learn about methods used to compromise that asset, by clicking on the asset names in a Campaign Report. Those links will bring you to the device and entity report screen and will show:

- Compromising Methods
- Critical Assets at Risk
- Affected Entities
- Outbound Attack Paths
- Hardening for that specific device

Mainframe-Ops

Campaign: 000008

Scenario: VPN network / Remote Employees

Cost of Exploitation: 8

Critical Assets at Risk: 2

spooler

rdp_server

Type: Sensor

OS: Windows 7 SP 1.0

Organizational Unit: SecuredZone.xmDallas

IP Address: 172.0.200.4

2 Compromising Methods

01

Group Policy Modification

50% - 1 Vectors out of 2

02

Domain Credentials

50% - 1 Vectors out of 2

Inbound Attack Path

BlueKeep (CVE-2019-0708)

John

Windows | 172.0.101.3

1

Mainframe-Ops

Windows | 172.0.200.4

20 May 2020 - 03:16:23 (UTC -4)

Asset / Entity Reporting Display

Outbound Attack Path

SSH Credentials Reuse

Data-Ops

Windows | 172.0.200.3

ControlTV

SECUREDZONE.XM\controltv\$

2

Credential Harvesting

SECUREDZONE.XM\controltv\$

3

Credential Reuse

SECUREDZONE.XM\controltv\$

4

dc-customers-db

Linux | 172.0.201.11

20 May 2020 - 03:17:04 (UTC -4)

Additional Asset /Entity Report display

Hardening

Apply Microsoft patches on the following machines:

Parameters: Mainframe-Ops: follow MSRC guidelines
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

Enable Network Level Authentication (NLA) on the following machines:

Parameters: Mainframe-Ops

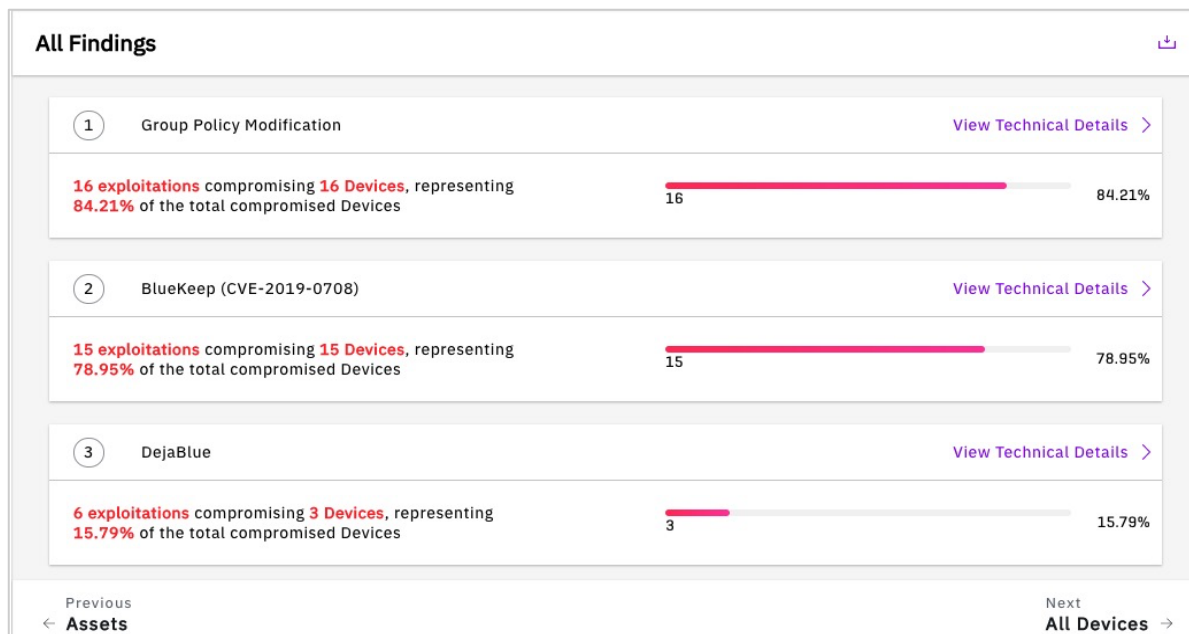
Disable Remote Desktop Service on the following machines:

Parameters: Mainframe-Ops

Hardening suggestions

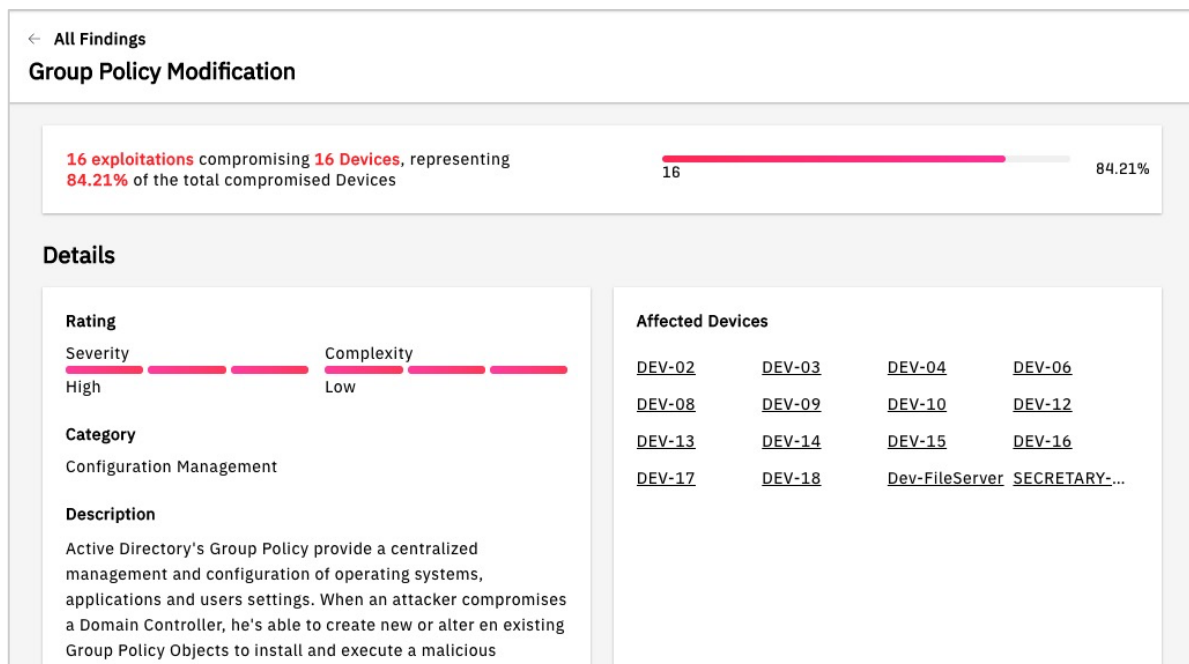
All Findings

The **All Findings** section of a Campaign Report lists the types of attacks that succeeded in compromising devices, the number of such devices, and the percentage of all compromised devices they represent.



All Findings Display

For each attack, you can click the **View Technical Details** link to display additional information, attack methods, and remediation advice.



View Technical Details display

Under **Affected Devices**, the first 40 affected devices are displayed by default; clicking **Show More**, displays a window with a scrollable list of all devices compromised by the attack. Clicking a device in the list displays a window with detailed information on the attack, including the time of the attack and the devices involved.

Group Policy Modification
DEV-09

Overview

TYPE
Device

STATUS
● Compromised

COMPROMISED TIME
07 March 2020
06:21:54 (UTC -5)

IP ADDRESSES
192.168.251.109

OPERATING SYSTEM
Windows 7 SP 1.0

OU
dev.model.demo > Workstations

ENTITY ID
12626999114036384033

RECONNED METHOD
Active Directory Computers Discovery

RECONNED TIME
07 March 2020 - 05:51:52 (UTC -5)

COMPROMISED METHOD
BlueKeep (CVE-2019-0708)

Findings

Affected Devices, Device Details display

All Devices

The **All Devices** section lists the devices participating in the campaign and provides information on Status (compromised or reconnected), Method, OS, IP, Cluster, User, and Source Device. You can deep dive for additional device information by clicking on the device names. For large device inventories, you can **Search** through the listed assets. You can also hide the various columns in this report using the **Show/Hide** pull-down and selecting which columns to hide.

VPN network / Remote Employees
7/7 Campaigns >
View Battleground
13/04/2020 > End Date
View Report

Overview
Critical Asset Findings
Critical Assets
All Findings
All Devices
Breach Points
Scenario Configuration

All Devices

Search Devices
Show/Hide

Name	Type	OS	IP
Jack	Sensor	Windows 7 SP 1.0	172.0.100.6
WinCC03	Sensor	Windows 7 SP 1.0	172.0.200.11
Steve	Sensor	Windows 7 SP 1.0	172.0.100.9
ny-jenkins-node	Sensor	Linux centos 7.5.1804 Workstation	172.0.201.7

Previous
All Findings

Next
Breach Points

Scenario Report All Devices Display

Breach Points

The **Breach Points** section of reports provides information on the breach points configured in the scenario or campaign.

Breach Points

All Breach Points

Breach Points Rules

Q

Search Breach Points

Download

Show/Hide

▼

Name	Type	OS	IP	Status	Cluster
DEV-07	Device	Windows 7 SP 1.0	192.168.251.107	<div></div>	dev.model.demo/Workst...

Previous

Next

← All Devices

Scenario Configuration →

Campaign Breach Points display

Clicking on a breach point provides additional detail about the device specified as a breach point.

Scenario Configuration

The Scenario Configuration section of both Scenario and Campaign reports provides comprehensive information on the selected scenario. See **Getting Started** for more information on scenarios and scenario configuration.

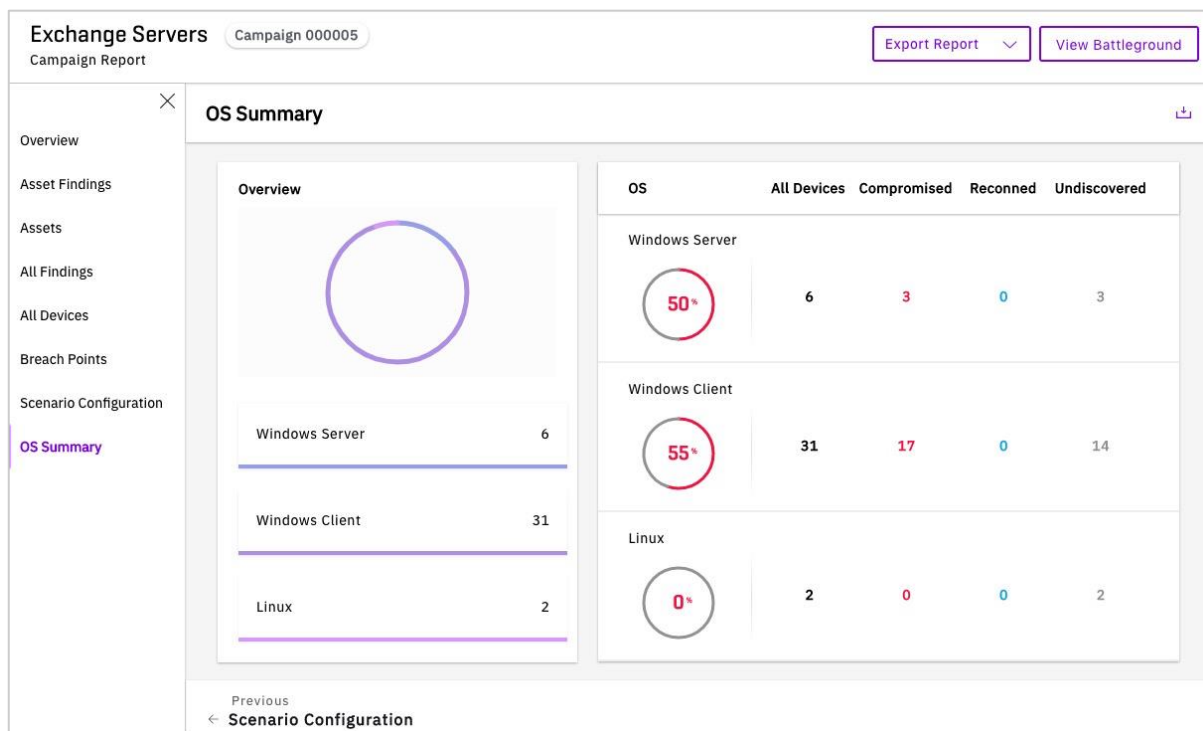
VPN network / Remote Employees		7/7 Campaigns >	View Battleground	13/04/2020 > End Date	View Report
Scenario Report					
<div> <div> Overview Critical Asset Findings Critical Assets All Findings All Devices Breach Points Scenario Configuration </div> <div> <div>Scenario Configuration</div> <div> Settings Scope Breach Points Critical Assets Exclusions </div> </div> </div>					
<div> <div>VPN network / Remote Employees</div> <div> <div> SCENARIO CREATED BY xm\gus DESCRIPTION </div> <div> MAXIMUM RUNNING CAMPAIGNS 1 </div> <div> CAMPAIGNS RUN FOR 03:00:00 </div> <div> CAMPAIGN GENERATED Manually </div> </div> </div>					
<div> <div>Previous</div> <div>Next</div> </div>					
← Breach Points					

Scenario Configuration Report

Click the tabs at the top of the section to display specific information, including Setting, Scope, Breach Points, Critical Assets and Exclusions. Not every scenario will have configuration data for all of these topics.

OS Summary

The **OS Summary** section (of Campaign Reports only) provides a graphic display showing a breakdown of the **Operating System** (Windows Server, Windows Client, Linux, MacOS) of compromised, reconnected, or undiscovered devices. The percentage represented by each of these platforms is indicated in the circle:



OS Summary Display in a Campaign Report

Aggregated Report

On the righthand side of the **Scenario Hub** are controls for generating an **Aggregated Report** for all scenarios across a specified range of dates.

Within the Aggregated Report itself, you can select which campaign scenarios to include in the report with the All Scenarios pull-down menu (see figure below)

8 Scenarios

67 Campaigns

Aggregated Report

Start Date:

21 / 09 / 2019

End Date:

No end date

View Report

Aggregated Report controls

All Scenarios

Start Date:

21 / 09 / 2019

End Date:

No end date

View Report

Select All

Customers Data

Network Superiority

IT to OT

Capture Corporate IP

3rd Party Supplier Exposure

Financial Servers Protection

Executive Protection

Ransomware Impact

View Technical Details

70.59%

View Technical Details

29.41%

View Technical Details

Selecting scenarios to include in an Aggregated Report

Other Reporting Capabilities

Throughout the XM Cyber user interface, tabular data can be exported and downloaded in CSV format (comma separated values) by clicking download icons () above the tables in question.



SYSTEM CONFIG

The **System Config** screen has six tabs, described in the following table.

Tab	Function
Health (default)	Displays CPU, Memory, and Disk Utilization for major parts of the XM system: Servers (Database, North, and South), and Sensors.
Sensors	Enables management of sensors including enabling, disabling, updating, and other tasks.
System Update	Displays the current XM Cyber version and provides an upload area for the latest system installation files.
Users	Enables XM Cyber user management. The tab displays user attributes such as Username, Role, etc. and enables creation and deletion of users and credentials management. It also supports configuration of the LDAP server connector and of OpenID service.
SIEM	Enables addition and management of one or more SIEMs (Security Information and Event Management) targets.
General Settings	Allows specification of a range of configuration options: DNS and Certificates, SMTP servers, API keys, cloud accounts and Email Security Validation.

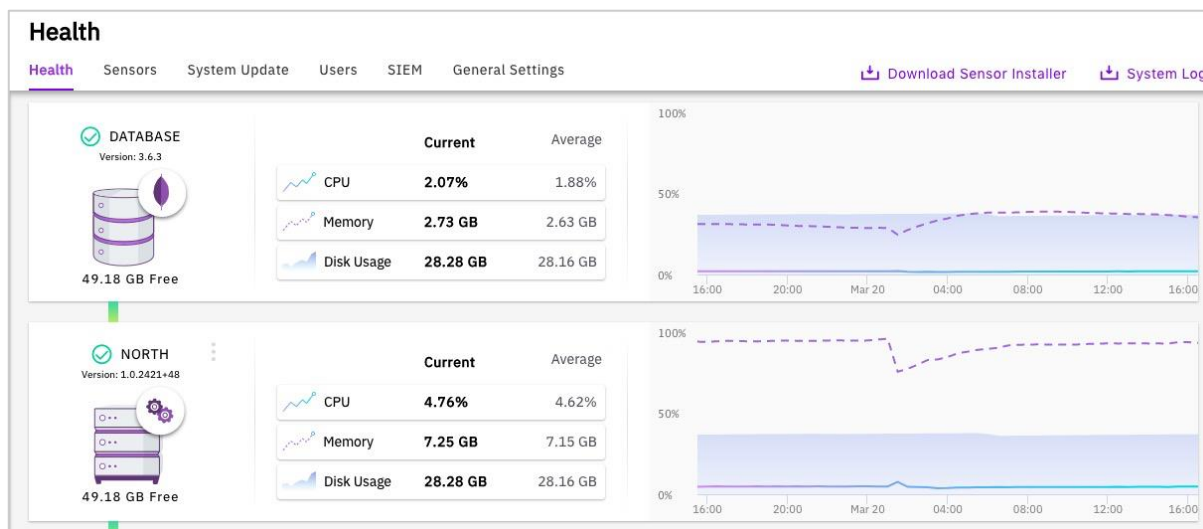
The following sections describe each of these tabs and their functions in detail.

System Config Tabs and Links

The System Config pane allows users to monitor the state of the system and set up and configure a range of functions. It also supports downloading the Sensor Installer (see Sensors below) and the System Log in CEF (Common Event Format). You may be asked to supply this file to XM Cyber for support and debugging purposes.

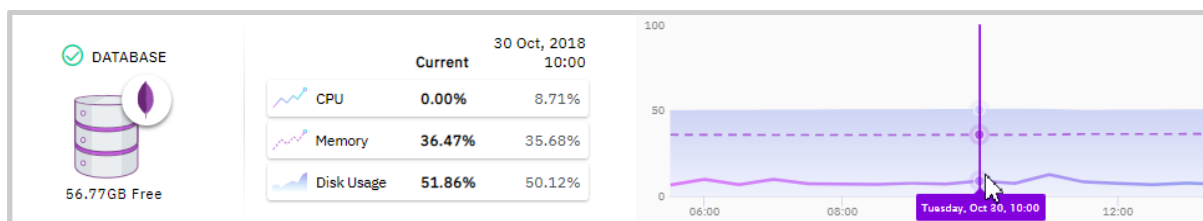
Health tab

The Health tab displays CPU, Memory, and Disk Utilization for each part of the XM Cyber system components (Database, North, South, and Sensors).

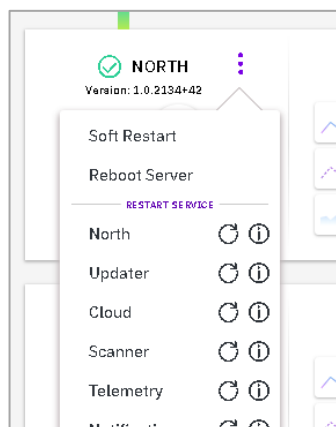


System Config Health Tab

A usage graph for each part of the system is displayed for both the current time and for a time period that you specify by sliding the time marker along the graph.



Using the Marker to Specify a Time on the Health Graph



Reboot / Restart pop-up

The **Health Tab** also includes display statistics for connected sensors, campaigns and utilization of campaigns across scenarios.

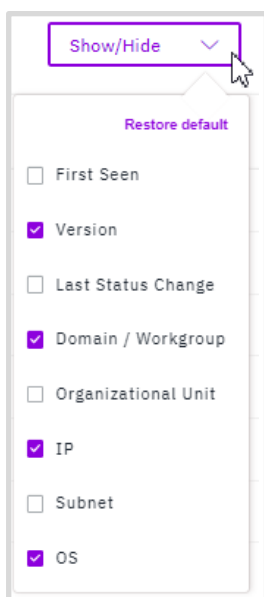
The **Health Tab** also offers a pop-up menu for rebooting services and restarting services, including assets and services hosted in the Cloud.

Sensors tab

The Sensors tab enables you to manage sensors, including enabling and disabling them, updating them, and other tasks, and looks like this:

Status	Sensor Name	Sensor ID	Version	Domain / Workgroup	IP	OS	Enabled
Connected	DEV-DC-01	15145668009214501546	1.3.740	dev.model.demo	192.168.251.1	Windows Server ...	Enabled
Connected	DEV-03	18440198360124938095	1.3.740	dev.model.demo	192.168.251.7	Windows 7 SP 1.0	Enabled
Connected	DEV-04	3851255405489920717	1.3.740	dev.model.demo	192.168.251.12	Windows 7 SP 1.0	Enabled
Connected	DEV-08	8910672088289132954	1.3.740	dev.model.demo	192.168.251.3	Windows 7 SP 1.0	Enabled
Connected	DEV-07	15498035859037701341	1.3.740	dev.model.demo	192.168.251.107	Windows 7 SP 1.0	Enabled
Connected	apache-tomcat	14364693442384536224	1.3.740	Linux	192.168.241.18	Linux centos 7.3....	Enabled

Sensors Tab

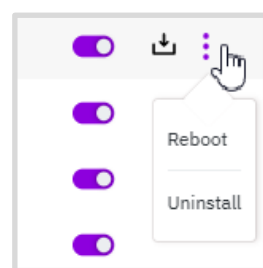


Show/Hide columns pull-down

For each sensor in the list, the following information is displayed: Status (green for enabled, red for disabled), Sensor Name (the name of the device on which the sensor is running), Sensor ID, Version, Domain/Workgroup, IP, OS, Enabled (move the slider to enable/disable the sensor).

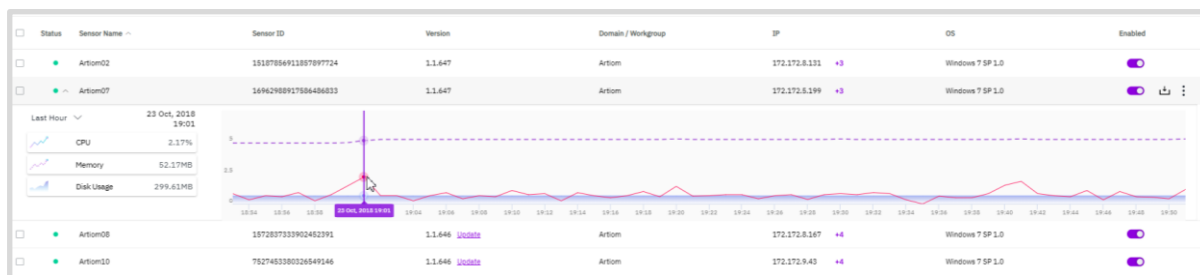
Clicking on the **Show/Hide** pull-down at the far right of the column headings displays the following column options:

For each sensor in the list, placing the cursor to the right of the **Enabled** button displays a **Download** button to download the sensor activity log, and a **More** button that provides two further options: Reboot and Uninstall.



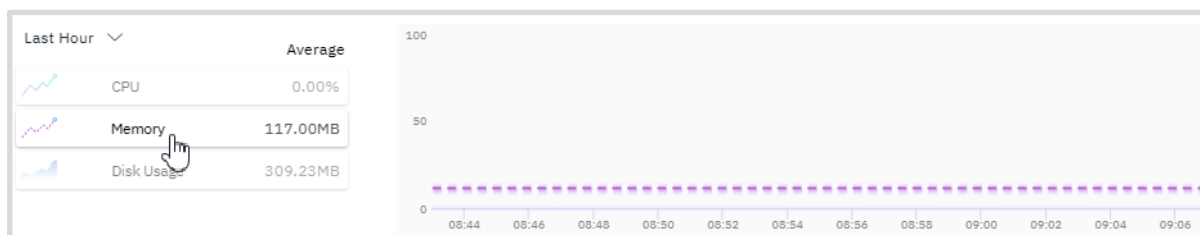
Sensor Log Download Button and Reboot and Uninstall Options

Clicking on the pull-down to the left of a sensor name displays information on CPU, Memory, and Disk Usage of the device running the sensor, including a usage graph for a specified time period. Use the purple marker to display usage for a specified time:



Information display for a device on which the sensor is located.

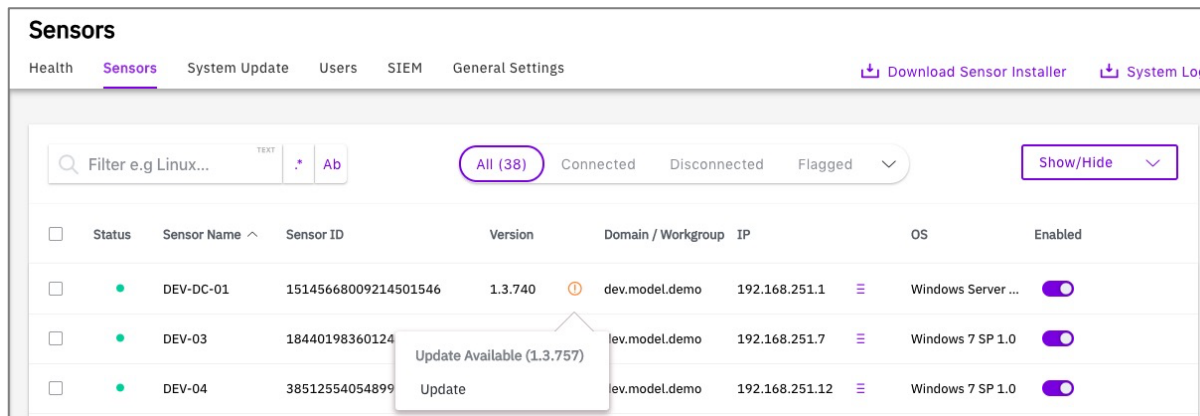
Hovering over an item (CPU, Memory or Disk Usage) displays the graph for that item:



Display for the memory information of a device hosting a sensor.

Updating Sensor Software

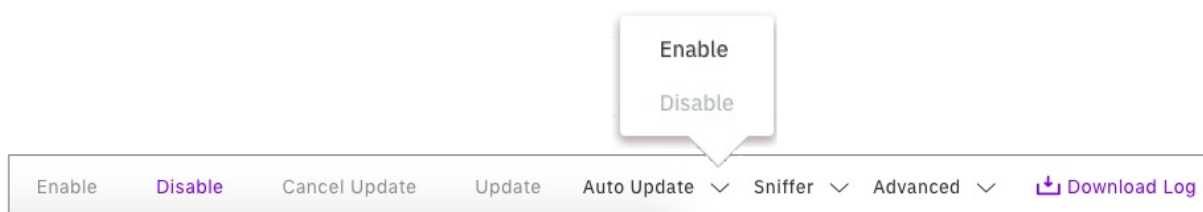
You can update the version of sensor software manually by clicking the update button to the right of the sensor version column.



Updating sensor software versions

Sensors also have the ability to update to new versions automatically. You can enable automatic update via the System Config **Sensors** tab as follows.

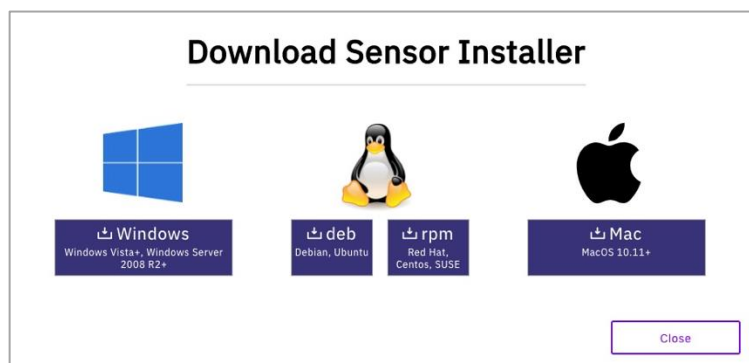
1. First, select one, multiple or all sensors using the checkbox(es) to the left of the Sensors pane. When you click any of the checkboxes, an options ribbon appears at the bottom of the Sensors pane.
2. To enable auto-update, click on the pop-up next to **Auto Update** and select Enable



Sensor configuration options ribbon with Auto Update pop-up

This screen also lets you download sensor software installation packages (depending on the host OS). When you click the Download Sensor Installer link at the top right of the screen, the following dialog appears with the option of downloading sensor software for Windows, Linux or MacOS.

Consult the *XM Cyber Sensor Installation Guide* and/or contact your system administrator for assistance.



Download Sensor Installation dialog

System Update tab

The System Update tab displays the current version number and date of the last update to the XM Cyber system as well as a listing of past updates. It also contains an upload area to enable for new versions of XM Cyber.

System Update


HealthSensorsSystem UpdateUsersSIEMGeneral Settings

Download Sensor InstallerSystem Log

Current Version 1.32.0.111
Last update was made 23 Jan, 2020 12:32 (UTC -5)

License Status
License valid until 30-12-2020 19:00:00

Check For Update



Drag & drop your latest update file here
or
Select File

Past updates

Version	Date & Time	Status
1.32.0.111	23 Jan, 2020 12:32 (UTC -5)	Successful
1.30.0.91	27 Nov, 2019 12:31 (UTC -5)	Successful

The System Update Tab

Users tab

The Users tab supports various types of user management and has three sub-tabs: **Users**, **LDAP Connector** and **OpenID Config**.


Users sub-tab


The Users sub-tab displays the XM Cyber user information, including Full Name, User Name, Realm Role (Admin, Security Analyst, Security Architect, SOC or user), Mail, and Last Login, and supports basic user administration.

Users					
Health	Sensors	System Update	Users	SIEM	General Settings
Download Sensor Installer System Log					
Add User Show/Hide					
Full Name	Username	Role Type	Mail	Enable Local	Last Login
Local User	local\user	Security Architect	user@local.com	<input checked="" type="checkbox"/>	Thursday 21 March 2019 ...
Local Admin	local\admin	Admin	admin@local.com	<input checked="" type="checkbox"/>	Saturday 28 March 2020 1...
xmtech	local\xmtech	Security Architect	xmtech@xmcyber.com	<input checked="" type="checkbox"/>	Sunday 14 July 2019 04:2...

Users tab

Creating a New User

To create a new user, click the **Add User** button  at the top of the tab and specify user attributes in the boxes that appear at the top of the user listing.

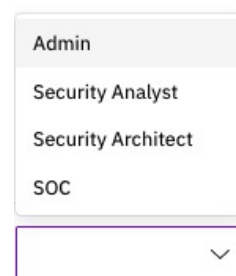
Full Name	Username	Role Type	Mail	Enable Local	Last Login
Full Name 	Username	<input type="text"/>	Mail	<input type="checkbox"/>	
Cancel Save					
Local User	local\user	Security Architect	user@local.com	<input checked="" type="checkbox"/>	Thursday 21 March 2019...
Local Admin	local\admin	Admin	admin@local.com	<input checked="" type="checkbox"/>	Saturday 28 March 2020 ...

Add New User dialog

For each new user created, you must supply their Full Name, a unique Username, an email address and a Role from the Role Type pull-down.

You can assign users one of four **Role Types**, with accompanying XM Cyber system privileges.

- **Admin** - full access to all XM Cyber system elements and configuration options, including user management
- **Security Analyst** – read-only access to scenarios and campaigns, without access to system configuration
- **Security Architect** – read write on scenarios and campaigns, without access to system configuration
- **SOC** – read-only access to the health of XM Cyber servers and system



Role Type pull-down menu

Editing User Attributes and Deleting Users

To delete a user or edit user attributes, click one of four buttons to the right of the user row on the Users tab.

	Prompts to delete the indicated user
	Enables changing a user password
	Edit the user details such as realm, username, role, full name or email
	When you are editing user attributes, the Enable Local switch (normally grayed out) lets you enable/disable users without actually deleting them.

LDAP Connector sub-tab

You can manage XM Cyber users via LDAP (Lightweight Directory Access Protocol) using the **LDAP Connector** tab.

LDAP Connector tab

The **LDAP connector** tab has the following fields, buttons and switches.

Disabled **Enabled** – the **Use LDAP Connector** switch determines whether to use the connector and is Disabled by default.

Domain and **URL** – these fields are required to establish a connection to an LDAP server

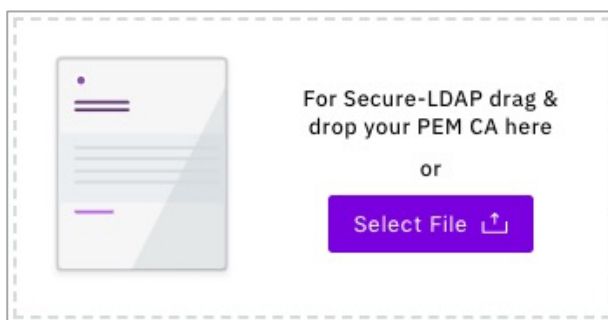
Username and **Password** – credentials required to access the LDAP server. Note that the Username must be entered in either UPN (User Principal Name) or DN (Distinguished Name) format. See the [XM Cyber Glossary](#) for additional information.

Base DN – the Base DN (Distinguished Name) is point in the LDAP directory tree where the server starts searches for usernames. You can test the validity of the Base DN with the accompanying Test button

+ Add Group - the **Add Group** button allows you to add existing LDAP groups to the XM Cyber user set. You will need to know the name of the group and will be permitted to assign one XM Cyber role to all members of that group.

Secure LDAP box – if you are using Secure LDAP, this box lets you drag-and-drop or select certificate files for upload containing a PEM CA (Privacy Enhanced Email Certificate of Authority).

Once you have edited the LDAP Connector settings, click **Apply Changes** to update or **Cancel** to revert.



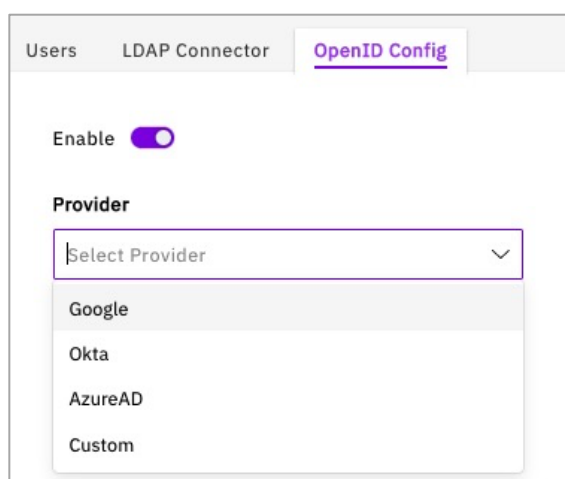
Secure LDAP certificate upload box

OpenID Config sub-tab

XM Cyber allows you to use the OpenID protocol for login authentication. Disabled by default, the Enable/Disable switch lets you enable the protocol and select an OpenID / SSO provider.

Most users will select a provider from the list – Google, Okta or AzureAD – which bring up the following authentication and configuration fields associated with that provider. These fields include

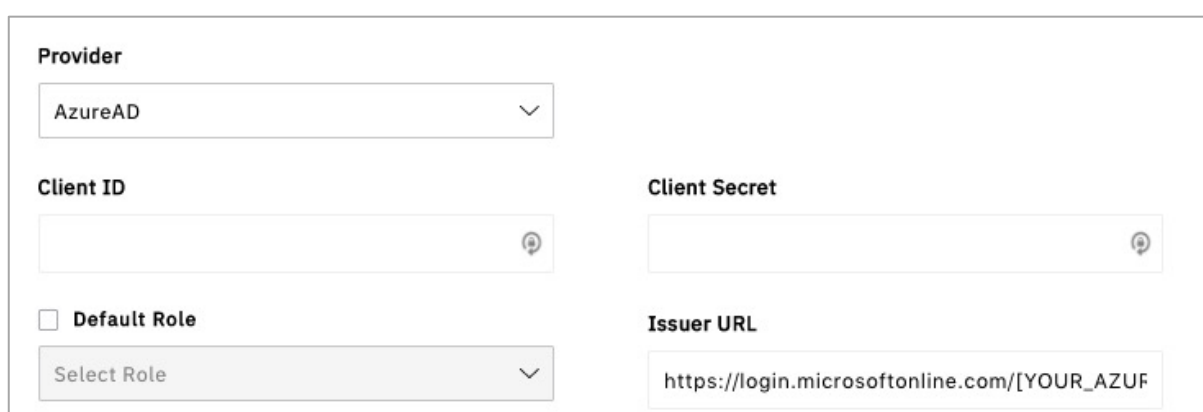
Client ID and **Client Secret** – authentication strings for the OpenID provider



OpenID Provider selection

Default Role – one of the four XM Cyber roles defined in the **Users sub-tab** above.

Issuer URL – the API URL associated with the OpenID provider. XM Cyber automatically provides a default value for this field.


 A screenshot of the OpenID configuration form for the AzureAD provider. The "Provider" dropdown is set to "AzureAD". Below it are two input fields: "Client ID" and "Client Secret", each with a help icon. There is a checkbox for "Default Role" and a "Select Role" dropdown. The "Issuer URL" field contains the text "https://login.microsoftonline.com/[YOUR_AZUF".

OpenID Config fields for AzureAD

Selecting a **Custom** provider brings up further fields as show below. Contact your OpenID administrator for the appropriate values to enter in those fields.



Provider <div>Custom</div>	Provider Name <div>Enter provider name</div>
Client ID <div></div>	Client Secret <div></div>
<input type="checkbox"/> Default Role <div>Select Role</div>	Issuer URL <div>https://sub.domain.com</div> <div>Discovery URL will populate both Authorization Endpoint URL and Token Endpoint URL</div>
Authorization Endpoint URL <div>https://sub.domain.com</div>	Token Endpoint URL <div>https://sub.domain.com</div>
JWKS URL <div>https://sub.domain.com</div>	

Custom OpenID provider fields

Once you have edited the OpenID Config settings, click **Apply Changes** to update or **Cancel** to revert.

Remember to set <https://demong.xmcyber.com/api/openId/loginSuccess> as an allowed callback when configuring your OpenID provider account.

SIEM tab

XM Cyber supports logging security events to one or more SIEM (Security Information and Event Management) servers and/or local files. The SIEM tab lets you specify the address of each and attributes of logging using the Add Server button **Add Server**.

The **New Logging Server** dialog box is used to configure logging settings. It includes a close button (X) in the top right corner.

Log Settings

- Siem target name:** A text input field with a placeholder "Enter display name" and a character count "0/50".
- Format:** A pull-down menu currently set to "plaintext".
- Enabled:** A toggle switch currently turned on.
- Local file / Remote server:** Two radio buttons. "Local file" is selected.
- Host:** A text input field with a placeholder "Enter Host" and a character count "0/50".
- Protocol:** A pull-down menu currently set to "UDP".
- Port:** A text input field containing "514".

Event Settings

- Scenarios:** ☒ (with a dropdown arrow)
- Campaigns:** ☒ (with a dropdown arrow)
- System Update:** ☒ (with a dropdown arrow)
- System Health:** ☒ (with a dropdown arrow)
- Sensors:** ☐ (with a dropdown arrow)

Add New button at the bottom right.

Logging Server dialog

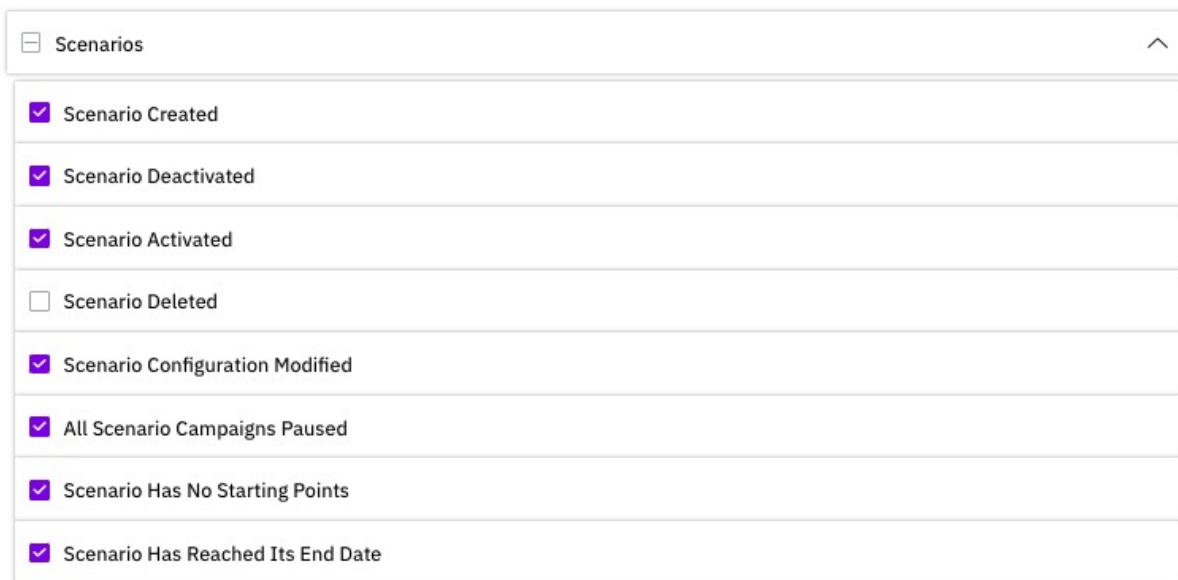
The New Logging Server dialog includes a number of fields, buttons and switches.

SIEM Target Name – this field allows you to specify a display name for the SIEM logging target, by default, a file on the system hosting XM Cyber. Using the Format pull-down, you can specify whether events are logged as plaintext or in CEF (Common Event Format).

The **Enabled** switch allows you to disable and re-enable logging to a given target.

☐ **Remote server** - the Remote server radio button lets you set up a remote SIEM server and requires that you supply a server address (as an FQDN), protocol (currently UDP only) and port number (default = 514).

Event Settings – this area includes checkboxes and pull-downs for logging major event types – Scenarios, Campaigns, System Updates, System Health and Sensors. Each pull-down includes checkboxes for sub-types, e.g., under Scenarios, there are checkboxes for Scenario Created, Scenario Deactivated, etc. Top-level checkboxes select all sub-types automatically, and you can select and delect sub-types using the individual pull-downs.

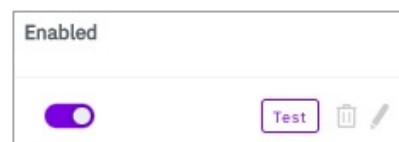


Event Settings pull-down


Once you have edited the **Logging Server** settings, click **Add New** or click the X at the top of the dialog to cancel.

Editing and Deleting Existing SIEM Servers.

You can disable/enable, test, modify or update SIEM server using the switch and buttons on the right-hand part of pane.




SIEM target controls

 **Enable** – this switch lets you disable/enable logging to a listed SIEM target

 **Test** – this button sends a test event to a logging file or server.

 **Trashcan** – lets you delete a listed SIEM target

 **Pen** – open a dialog comparable to the above New Logging Server dialog (above) to allow modification of SIEM target logging attributes.

General Settings tab

The General Settings tab has four sub-tabs with the following functions:

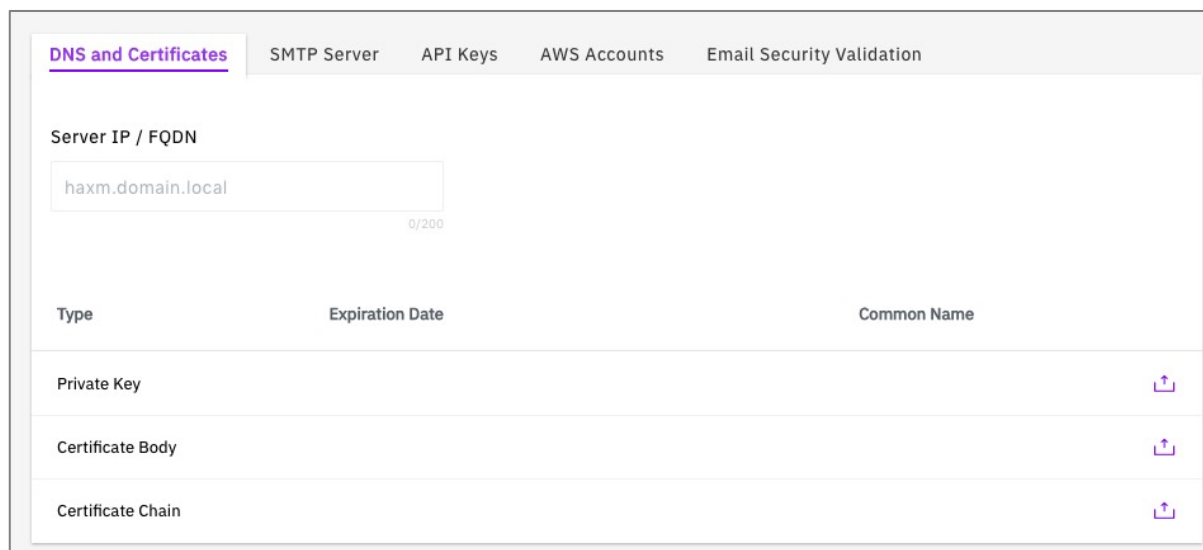
DNS and Certificates	Specifies the IP address / URL of the server hosting the XM Cyber application, keys and certificates to secure access to it.
SMTP Server	Email notifications from XM Cyber require specification of an SMTP (Simple Mail Transfer Protocol) server.
API Keys	Specifies API keys to use when accessing reports and other data outside of the XM Cyber application.
AWS Accounts	Configuration page to connect XM Cyber to AWS Accounts for attack simulations.

DNS and Certificates

This pane lets you specify the IP address or DNS URL of the server hosting the XM Cyber application, keys and certificates to secure access to it. The pane has the following fields and functions

Server IP / FQDN – enables specification of the XM Cyber server address either by IP address or using an FQDN (Fully Qualified Domain Name).

Certificate Information – while XM Cyber manages certificates for hosting of XM Cyber in the Cloud, on-premises users can upload keys and other certificate information here.



Default General Settings tab

SMTP Server

Email notifications from XM Cyber require specification of an SMTP (Simple Mail Transfer Protocol) server, in particular for password reset requests. The fields, buttons and menus of interest in this pane are

Type – allows you to specify whether the server requires authentication via simple login or with SMTP OAuth2.

Server IP / FQDN and **Port** – the address or URL of the SMTP server and port number, obtained from your service provider or from the configuration settings of your local email client.

☒ **Secure SMTP** – this checkbox indicates whether the server requires secure SMTP.

Username and **Password** – the login credentials for your SMTP server.

Username, **Refresh Token**, **Client ID** and **Client Secret** – these items apply only to OAuth2 configurations to support limited authorization access for sending emails. Contact your system administrator for appropriate values.

Send Test Email – this button allows you to test login or OAuth2 configurations. It will use the supplied email address (Username) to access the SMTP server. Check your email after using this test function.

Certificate Upload – the box in the upper right-hand part of the pane offers you the option of dragging/dropping or uploading a file containing an email server certificate (if required).

Apply Changes – click this button to commit any changes made to the SMTP Server configuration fields or click **Cancel** to exit without saving changes.

Authentication Type pull-down

SMTP Server Settings pane

API Keys

This pane lets you specify API keys to use when accessing XM Cyber reports and other data from outside of the XM Cyber application. XM Cyber APIs let users generate their own reports and extensions to XM Cyber analysis.

These keys are typically appended to the URL used to invoke the web APIs in question. The fields, buttons and menus in this pane include

Add API Key -- the **Add API Key** button lets you add new API keys to the set maintained by XM Cyber. Pressing this button brings up the **Create API Key** dialog. With successful API Key creation, a new entry will appear in the list shown in the pane.

The dialog box titled "Create API Key" contains two input fields: "NAME" with a text input labeled "App name", and "ROLE" with a dropdown menu labeled "Select...". A "Generate" button is located at the bottom right of the dialog.

The Create API Key dialogue

Name, **Key Prefix**, **Role**, etc. – fields reflecting the attributes of previously entered API keys. You can enable/disable the keys using the switch at the right of the row and delete keys with the dimmed trash icon at the far right.

– The **Show/Hide** pull-down lets you display or hide the various columns in the API Key listing.



DNS and Certificates SMTP Server API Keys AWS Accounts Email Security Validation						
Add API Key Show/Hide						
Name	Key Prefix	Role	Creation Date	Last Used	Last IP	Enabled
Splunk	f5861d9e	Security Architect	Tuesday 03 December 2...			
yohan	3692107a	Admin	Sunday 15 March 2020 1...			
dedup	1ddd6065	Admin	Wednesday 25 March 20...	Thursday 02 April 2020 ...	206.55.218.146	


API Keys configuration pane


AWS Accounts

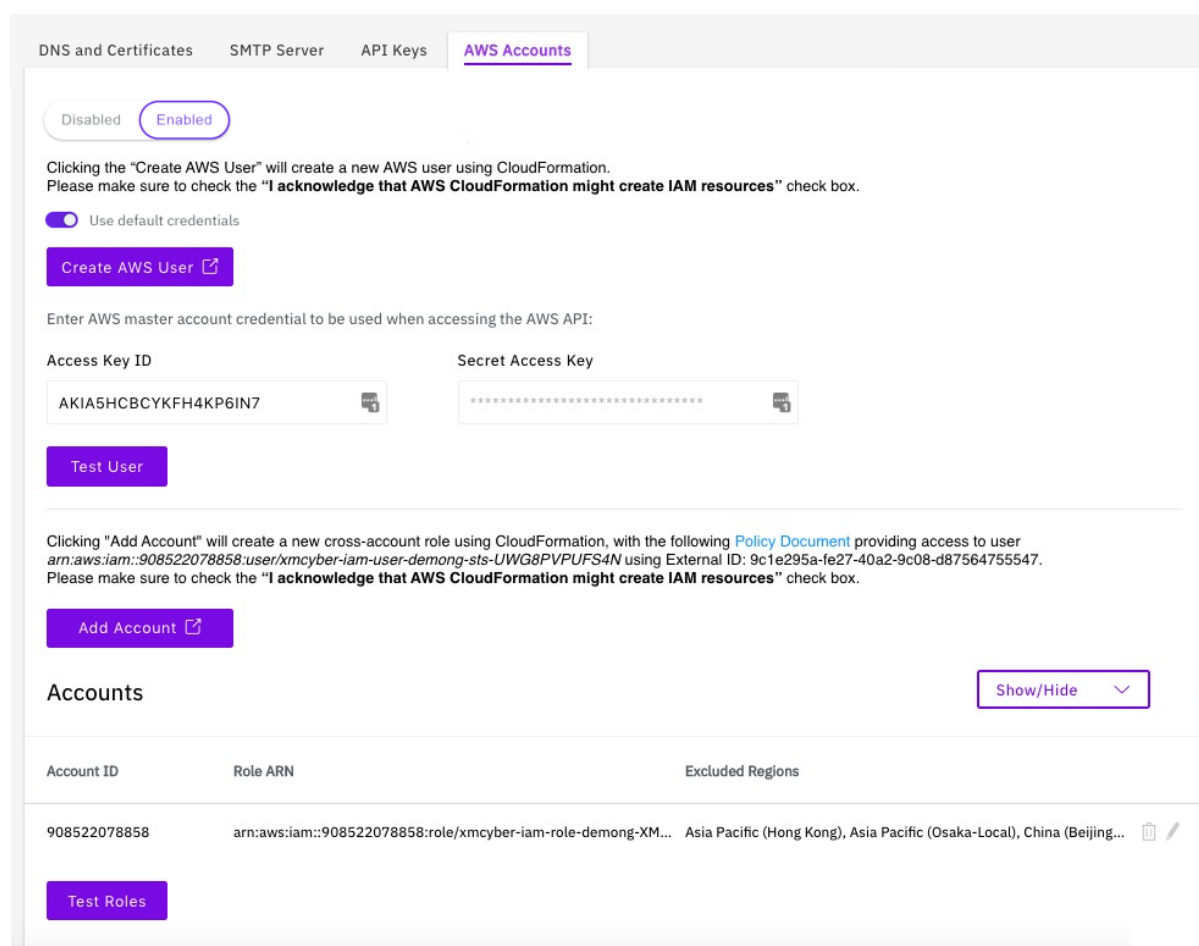
XM Cyber supports inclusion of assets and entities hosted on user private and public clouds. This page lets you configure the accounts and credentials needed to connect XM Cyber to AWS Accounts to facilitate attack simulations.

The fields, buttons, switches and menus on this pane include

  -- the **Disabled/Enabled** switch is enabled by default and should only be disabled for configurations not utilizing AWS (Amazon Web Services).

 Use default credentials - the **Use default credentials** switch is ON by default to support cloud users. When XM Cyber creates a customer cloud instance, an associated ARN (Amazon Resource Name) is created, and that ARN is then used with **Add Account** (see below).

 -- the **Create AWS User** button opens a new browser tab or window to login to your AWS account and create a new User. This step is not required for cloud configurations using credentials. Consult Amazon Web Services documentation for additional details.






The screenshot shows the 'AWS Accounts' configuration pane. At the top, there are tabs for 'DNS and Certificates', 'SMTP Server', 'API Keys', and 'AWS Accounts'. The 'AWS Accounts' tab is active. Below the tabs, there is a 'Disabled' button and an 'Enabled' button. A message states: 'Clicking the "Create AWS User" will create a new AWS user using CloudFormation. Please make sure to check the "I acknowledge that AWS CloudFormation might create IAM resources" check box.' Below this is a 'Use default credentials' switch, which is currently turned on. There is a 'Create AWS User' button. A label reads: 'Enter AWS master account credential to be used when accessing the AWS API:'. Below this are two input fields: 'Access Key ID' (containing 'AKIA5HCBCYKFH4KP6IN7') and 'Secret Access Key' (containing a masked string). There is a 'Test User' button. A message states: 'Clicking "Add Account" will create a new cross-account role using CloudFormation, with the following Policy Document providing access to user arn:aws:iam::908522078858:user/xmcyber-iam-user-demong-sts-UWG8PVPUS4N using External ID: 9c1e295a-fe27-40a2-9c08-d87564755547. Please make sure to check the "I acknowledge that AWS CloudFormation might create IAM resources" check box.' Below this is an 'Add Account' button. There is a section titled 'Accounts' with a 'Show/Hide' button. Below this is a table with columns 'Account ID', 'Role ARN', and 'Excluded Regions'. The table contains one row with the following data: Account ID: 908522078858, Role ARN: arn:aws:iam::908522078858:role/xmcyber-iam-role-demong-XM..., Excluded Regions: Asia Pacific (Hong Kong), Asia Pacific (Osaka-Local), China (Beijing...). There is a 'Test Roles' button.

AWS Accounts configuration pane

Access Key ID and **Secret Access Key** – these fields allow you to specify authentication credentials needed to access AWS APIs. Contact your cloud administrator or AWS support to obtain these credentials.

Test User – the **Test User** button tests the supplied AWS credentials and reports on success or failure. If unsuccessful, recheck your input of the credentials for typos.

Add Account  – the **Add Account** button opens a new browser tab or window and takes you to the AWS add account page. Upon returning to the XM Cyber screen, you will be prompted for an ARN (Amazon Resource Name) for the created role. Consult Amazon Web Services documentation for additional details.

Accounts – this listing summarizes all available AWS accounts and the fields specified in the **Show/Hide** pull-down. You can click the trashcan icon  to remove accounts and the pen icon  to edit account entries.

Test Roles – the **Test Roles** button uses the Accounts information to test specified roles. If unsuccessful, recheck your input of the account info for typos and/or the roles actually associated with the AWS account.

XM Cyber Terminology – Glossary

The following are important terms that should be understood when conducting a campaign.

APT Attack

An advanced persistent threat (APT) is an attack on the network that is undetected for a long period of time thereby enabling the attacker to exfiltrate data.

Asset

An entity in the tested network that has possible value to an attacker or the organization (which makes it a point of interest to an attacker). An asset can be one of the following:

- Device — endpoint in the network
- Data — file types found on any of the endpoints
- Network — a network-related entity, like a certain segment or subnet, etc.
- Cloud — there are multiple cloud entity types, such as S3, Lambda, roles, etc.

Blue Team

A dedicated internal security team that defends against attackers. If such a team does not exist in an organization, it may be specially set up in order to conduct a red team simulation.

Breach Point

Every campaign starts at a compromised endpoint called a breach point. A breach point may be an endpoint with a high probability to get infected, as the initial foothold of an attack. In XM Cyber you define breach points when setting up a scenario.

Campaign

An attack scenario executed by the virtual hacker. It contains the loaded APT capabilities (*methods*) and the current state of all sensors in the network — compromised, discovered, undiscovered or disabled. Every campaign runs with its configuration defined in its parent scenario.

Compromised Endpoint

An endpoint on which an attacker could potentially execute arbitrary code remotely.

CVE

Common Vulnerabilities and Exposures and/ Common Vulnerability Enumeration — the identification number and accompanying description (including public references) for known vulnerabilities as catalogued by [NIST](#) in the [National Vulnerability Database](#).

Data Yield

The amount of data in gigabytes potentially exfiltrated by an attacker as a result of a campaign. The measurement is based on files that the system has marked as important. Files that comprise the calculated data yield include databases, MS Office files, source code (e.g., Swift files), CAD files and other types.

Discovered/Undiscovered Endpoint

A discovered endpoint is an endpoint that a hacker has discovered, but not yet succeeded in compromising. A discovered endpoint is vulnerable as a hacker can then try various methods to gain access to the endpoint. An undiscovered endpoint is an endpoint in the organization that remains unknown to a hacker.

DN – Distinguished Name

A distinguished name (usually just shortened to “DN”) uniquely identifies an entry and describes its position in the LDAP Directory Information Table (DIT). DNs are comprised of comma-separated components called relative distinguished names, or RDNs. For example, the DN “uid=john.doe,ou=People,dc=example,dc=com” has four RDNs.

FQDN – Fully Qualified Domain Name

A complete domain name for a specific computer, or host, on the internet. An **FQDN** consists of two parts: a hostname and a domain name, e.g., an **FQDN** for a mail server might be *corpmail.somecompany.com*, where *corpmail* is the host and *somecompany.com* is the domain.

Method

This refers to one or more techniques used to compromise a computer system.

Network Superiority

Compromising more than 80% of the network is considered achieving superiority over the network.

Organizational Unit

A container within a Microsoft Active Directory domain which can hold users, groups, computers and other Organizational Units (OUs). An OU is the smallest unit to which an administrator can assign Group Policy settings or account permissions.

Purple Team

Enhances the effectiveness of campaigns conducted by red and blue teams by coordinating the campaigns and analyzing vulnerabilities found by the red team together with the defensive strategies and tactics of the blue team.



Recon

Refers to a key step in attacking a computer system: gathering information on potential victims. In XM Cyber, recon refers to discovering a victim which is the first step in conducting a successful hack.

Red Team

A team of cybersecurity analysts, IT and communication professionals, hackers, and others that conducts a comprehensive simulated campaign that tests how well an organization's personnel, network, and physical security withstand a real attack.

Rule

Rules are "If X then Y" assertions that provide guidance on how to act when those assertions are true. In XM Cyber rules determine which entities participate in scenarios, from which Breach Points attacks emanate, which assets are targeted, and which methods, pathnames, or credentials are excluded.

Scenario

A set of rules created by a XM Cyber user running a campaign. The rules determine such things as the scope of campaigns, breach points, the type of devices to be included, as well as campaign frequency and duration. XM Cyber assists users in creating scenarios.

Target

In XM Cyber this refers to a device that is attacked during a campaign. The device may represent an asset, or simply be part of a computer network.

UPN – User Principal Name

In Windows Active Directory, a User Principal Name (UPN) is the name of a system user in an email address format. A UPN (for example: john.doe@domain.com) consists of the username (logon name), separator (the @ symbol), and domain name (UPN suffix). A UPN is not the same as an email address.

User Manual and UI Conventions

This XM Cyber User manual and the User Interface it describes employ certain typographic and design conventions.

- **Bold Type** – Bold type in-line (not in section headers) refers to on-screen elements.
- **Purple UI Elements** – UI elements (text, buttons and switches) are colored purple when they are enabled and available for use.
- **Gray UI Elements** – UI elements (buttons, icons and switches) are grayed out either when disabled (buttons and switches) or when their use is restricted to certain roles (e.g., delete and edit icons).
- **Red Text** – XM Cyber issues warning text in red type, e.g., when elements are missing from fields in an input dialog.

Cybersixgill API

Reference Guide

April 2021

Contents

Scope.....	5
Generating API Credentials.....	6
Authenticating Requests.....	8
The Cybersixgill API Suite.....	12
Alerts API.....	13
actionable-alert (get).....	14
actionable-alert (delete).....	17
actionable-alert (patch).....	19
actionable_alert/stats (get).....	21
actionable_alert/count (get).....	23
actionable_alert/{actionable_alert_id} (get).....	24
actionable_alert/{actionable_alert_id} (delete).....	28
actionable_alert/{actionable_alert_id} (patch).....	30
actionable_alert_content/{actionable_alert_id} (get).....	32
CVE Enrichment API.....	36
cve/enrich (post).....	37
cve/{id} (get).....	41
cve/summary (get).....	44
cve/changes (get).....	46
CVE Feed API.....	48
ioc (CVE Feed).....	49
ioc/ack (CVE Feed).....	52
Dark Feed API.....	53
ioc (Dark Feed).....	54
ioc/ack (Dark Feed).....	56

Dark Feed Enrichment API.....	58
ioc/enrich (post).....	59
Intel Items API.....	62
aggs (post).....	63
intel_items (post).....	65
intel_items (get).....	69
intel_items/next.....	72
intel_items/{id}/thread.....	75
intel_items/thread/next.....	78
intel_items/{id}.....	80
histogram (post).....	83
Multi-Tenancy API.....	85
organization (post).....	87
organization (get).....	89
organization (delete).....	91
organization assets (post).....	92
organization assets (get).....	96
organization assets (put).....	99
organization/{organization_id}/user (get).....	103
organization/{organization_id}/user/{assigned_user_id} (post).....	104
organization/{organization_id}/user/{assigned_user_id} (get).....	106
organization/{organization_id}/user/{assigned_user_id} (put).....	107
organization/{organization_id}/user/{assigned_user_id} (delete).....	109

Scope

This document describes how to log in to the Cybersixgill Developer Portal and use Sixgill Ltd.'s APIs in your environment. It is a detailed reference with examples for the APIs endpoints.

The document contains the following sections:

- | [Generating API Credentials](#)
- | [Authenticating Requests](#)
- | [The Cybersixgill API Suite](#)

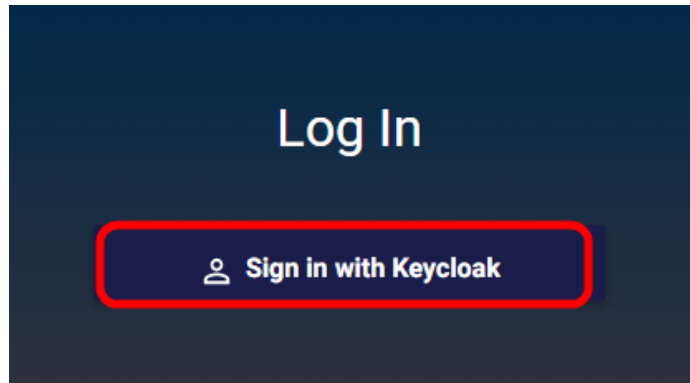
Generating API Credentials

Before you can use Cybersixgill's API, you must generate a client ID and secret by accessing the Developer Portal.

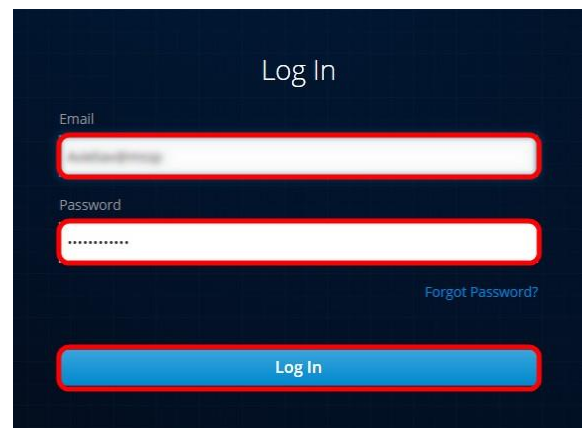
You will need your Cybersixgill credentials as defined when you registered with Cybersixgill.

To access Developer Portal:

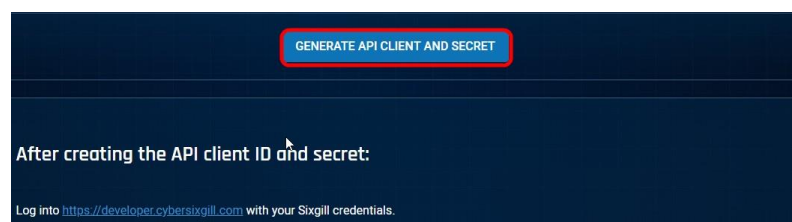
1. Open the following URL:
<https://developer.cybersixgill.com> and click Sign in with Keycloak.



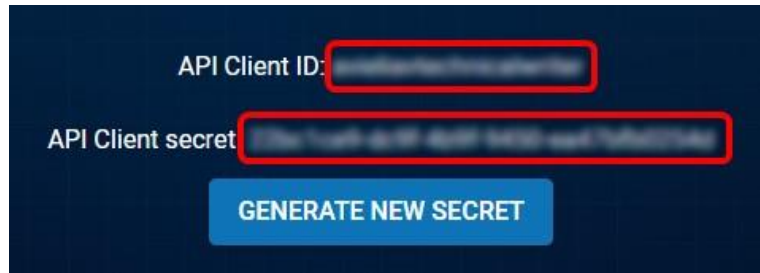
2. Enter your Cybersixgill credentials as defined when you registered with Cybersixgill and click Log In.



3. Click GENERATE API CLIENT AND SECRET.



4. Save the API Client ID and the API Client secret in a safe location. You will need it when using the API.



If you need to generate a new API client secret, click
GENERATE NEW SECRET.

You will need to apply the new secret to any application using the previous
secret.

Authenticating Requests

API authentication is performed via HTTP Basic Auth using the API Client and Secret you generated (see [Generating API Credentials](#)). The authentication method uses the bearer scheme and returns a token that you must use in your request headers.

All API requests must be made over HTTPS. Requests without authentication will fail.

General

Item	Details
URL	https://api.cybersixgill.com/auth/token
Description	Returns an authentication token for use in your API requests headers.
Method	POST

Parameters

Parameter	Required	Type	Description
client_id	Yes	string	Your API Client ID that you generated in the Sixgill Ltd. Onboarding Portal (see Generating API Credentials)
client_secret	Yes	string	Your API Client secret that you generated in the Sixgill Ltd. Onboarding Portal (see Generating API Credentials)
grant_type	Yes	string	Set value to: client_credentials

Request example

```
curl -L -X POST 'https://api.cybersixgill.com/auth/token' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'Cache-Control: no-cache' \
-H 'Content-Type: application/x-www-form-urlencoded' --data-
urlencode 'grant_type=client_credentials' --data-urlencode
'client_secret=<your client_secret>' --data-urlencode 'client_
id=<your client_id>'
```

Responses

Example: Response 200 - OK.



You will use access token value (between the " ") in the authorization header of your request.

```
{
  "access_token":
  "eyJhUxMiIsInR5cCIgOiAiSldUIiwCIwODY1lODI1LTRhNmEtYT
    ZiMCl1NDiNjA2MGM5YmIieHAiOjE1ODg4ODAxOTcsIm1hdCI6MTU4ODg1M
    TM5NyanRpIjoiYTc5NmEzNjctZjJmYi00NWl2LTljY2EtNTY0OThjODEiaH
    R0cH
    M69zZWN1cmVhY2Nlc3MuY3liZXJzaXhnaWxsLmNvbS9hdXR0L3JlYWxtcy9
    Ta
    XhnaWxsIiwiYXVkJoiYWNjb3
  .
  .
  .
  DdkYmU0ZjY50.8sE7RLeJlAUIICKAB8X3dKIOFFH18irHJrhol4luYNroNohmCy
  J674
  Fuk0g5YKhr36lGvAWUXEYY-Q",
  "expires_in": 28800,
  "refresh_expires_in": 86400,
  "refresh_token":
  "eyJhbGciOiJIInR5cCIgOiAiSldUIiwia2lkIiA6ICI4NzczMmU4ZS0
    U3LTRjMjEtODNiZS1hZWZhMzAzNMjYifQ.eE1ODg5Mzc3OTcsIm1hdCI6MT
    U
    4ODg1MTM5NywianRpIjoiYjlmM2RjZmEtNDEyNC00YjYxLWI3
  .
  .
  .
  naWxsLmwwic2Vzc2lrbzdGF0ZSI6QxNDk5OCIsInNjb3BlIjoiZW1haWwgcHJvZm
  lsZ
  SJ9.BtMN_31_fXhJl9MSEuvYU",
  "token_type": "bearer",
  "not-before-policy": 0,
  "session_state": "45fcc912-dde1-46a6-ba4c-2ae249d14998",
  "scope": "email profile"
}
```

Example: Response 400 - Bad parameters.

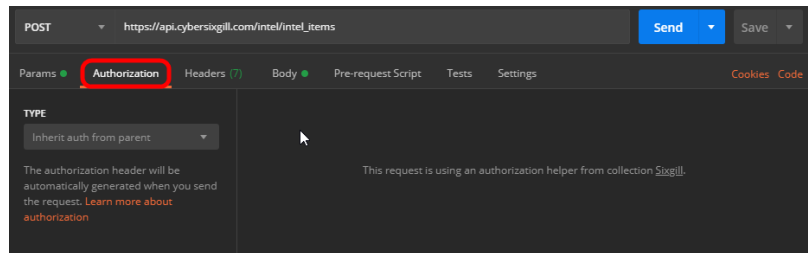
```
{
```


Example: Response 400 - Bad parameters.

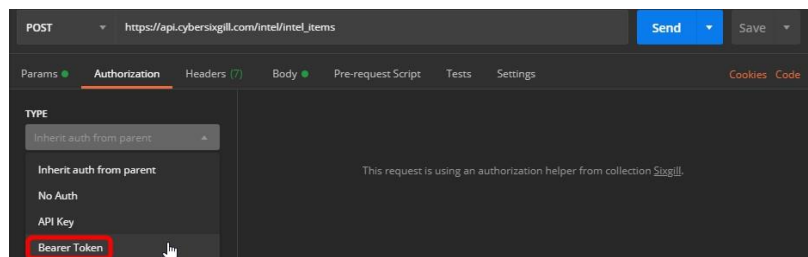
```
{
  "status_code": 400,
  "message": "Bad Parameters: query"
}
```

Example of Using Authentication in a Request in Postman

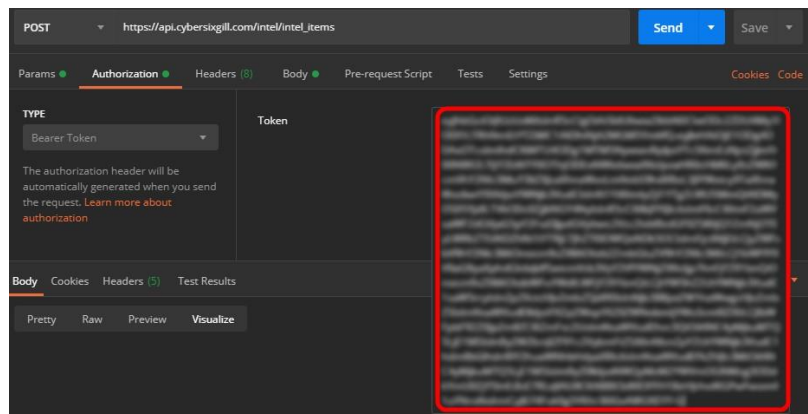
1. Click the Authorization tab.



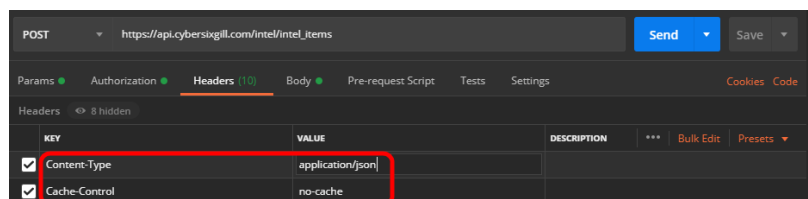
2. In the TYPE list, click Bearer Token.



3. In the Token box, paste the access_token value returned by the auth/token request.

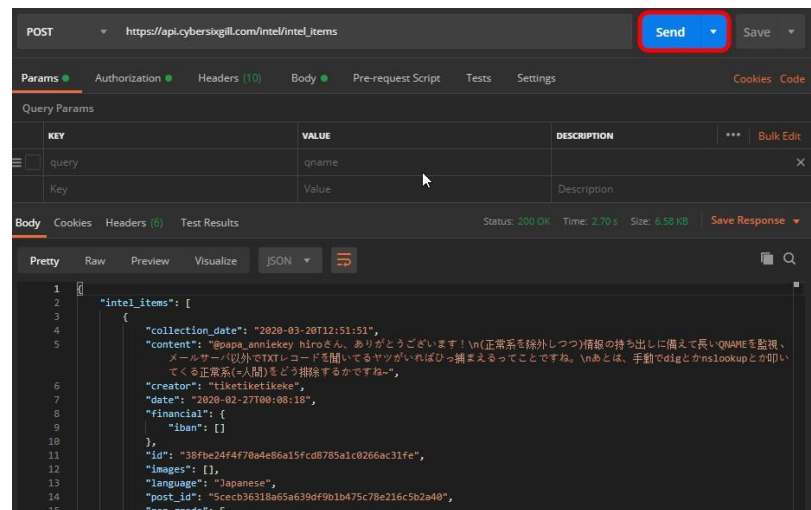


4. Click the Headers tab and add the following key values:



- Content-Type = application/json
- Cache-Control = no-cache

5. Set any parameters required for the request you are using and click Send. The response appears at the bottom of the window.



The Cybersixgill API Suite

Cybersixgill has created the following collection of APIs for use in your applications:



All data fetched by endpoints are returned as JSON files.

API	Description
Alerts API	Endpoints to manage actionable alerts.
CVE Enrichment API	Endpoints to enrich your CVEs with Cybersixgill's CVE dynamic rating.
CVE Feed API	Endpoints to manage CVE items.
Dark Feed API	Endpoints for Dark Feed IOC data.
Dark Feed Enrichment API	Endpoints for Dark Feed IOC enrichment data (service provided by Cybersixgill).
Intel Items API	Endpoints for obtaining detailed information on intel items, aggregations of intel items, and histograms based on a date range from the Cybersixgill system.
Multi-Tenancy API	Endpoints for use with the multi-tenant (MSSP) platform.

CVE Enrichment API

The CVE enrichment API allows you to request information about specific CVEs, and receive the current snapshot status of those CVEs (what is their rating, are they currently trending/not trending, etc.). The enrichment mode comes in STIX 2.0.

The API contains the following endpoints:

Group	Description	Endpoint	Method
CVE Enrichment API Calls	Enrich CVEs with Cybersixgill intelligence.	/cve/enrich (post)	POST
	Get data about a specific CVE.	/cve/{id} (get)	GET
	Get basic Cybersixgill Dynamic Rating data about a specific CVE.	/cve/summary (get)	GET
	Get CVEs whose score significantly changed within a specified date range.	/cve/changes (get)	GET

cve/enrich (post)

General

Item	Details
URL	https://api.cybersixgill.com/cve_enrich/cve/enrich
Description	Enrich CVEs with Cybersixgill intelligence.
Method	POST

Parameters

Parameter	Required	Type	Description
data	No	Object	See the request example below for the correct parameter format.

Request example

```
{
  "filters": {
    "query": "2020-0",
    "ids": [
      "CVE-2020-0674"
    ],
    "attributes": [
      "Has_POC_exploit_attribute"
    ],
    "sixgill_rating_range": {
      "from": 1,
      "to": 8
    },
    "nvd_rating_range": {
      "from": 1,
      "to": 8
    },
    "nvd_3_rating_range": {
      "from": 1,
      "to": 8
    },
    "nvd_modified_dates_range": {
      "from": "2020-02-18T00:00:00Z",
      "to": "2020-03-18T00:00:00Z"
    }
  }
}
```

```

    },
    "nvd_published_dates_range": {
      "from": "2020-02-18T00:00:00Z",
      "to": "2020-03-18T00:00:00Z"
    },
    "total_mention_counts_range": {
      "from": 1,
      "to": 8
    },
    "last_month_mention_counts_range": {
      "from": 1,
      "to": 8
    },
    "first_mention_dates_range": {
      "from": "2020-02-18T00:00:00Z",
      "to": "2020-03-18T00:00:00Z"
    },
    "last_mention_dates_range": {
      "from": "2020-02-18T00:00:00Z",
      "to": "2020-03-18T00:00:00Z"
    }
  },
  "results_size": 50,
  "from_index": 0
}

```

Responses

Example: Response 200 - The enriched CVE data.

```

{
  "id": "bundle--b56c1e2e-a40c-44ca-83dd-09e25936d273",
  "spec_version": "2.0",
  "x_bundle_size": 50,
  "x_total_matches": 100,
  "objects": [
    {
      "id": "vulnerability--c74d4bc9-d184-610a-7e81-66581422a535",

```

```

    "description": "A remote code execution vulnerability
exists in the way that the scripting engine handles objects in
memory in Internet Explorer, aka 'Scripting Engine Memory
Corruption Vulnerability'. This CVE ID is unique from CVE-2020-
0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-
0713, CVE-2020-0767.\n",
    "rating": {
      "sixgill": {
        "previouslyExploited": 5.26,
        "current": 8.4,
        "highest": {
          "value": 9.2,
          "date": "2020-02-18T00:00:00Z"
        }
      },
      "nvd": {
        "value": 7.6,
        "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-
0674",
        "severity": "HIGH",
        "publishDate": "2020-02-11T22:15Z",
        "modifyDate": "2020-02-12T17:53Z"
      }
    },
    "attributes": [
      {
        "name": "TrendingUnderground",
        "value": true,
        "description": "The CVE is trending on the
underground"
      }
    ],
    "mentions": {
      "mentions_total": 128,
      "first_mention": "2020-01-18T03:19:46Z",
      "last_mention": "2020-02-17T14:07:15Z"
    },
    "github": {
      "github_projects": 1,
      "watchersCount": 7,
      "forksCount": 2,
      "activity": {
        "first_date": "2020-01-23T12:30:51Z",
        "last_date": "2020-01-23T12:30:51Z"
      }
    },
    "topProjects": [

```

```

        {
          "link": "https://github.com/binaryfigments/CVE-
2020-0674",
          "name": "binaryfigments/CVE-2020-0674"
        }
      ],
    },
    "nvd": {
      "baseMetricV2": {},
      "baseMetricV3": {},
      "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-
0674",
      "publishDate": "2020-02-11T22:15Z",
      "modifyDate": "2020-02-12T17:53Z"
    }
  }
]
}

```

Example: Default response 200 - Any response other than the data.

```

{
  "detail": "The server encountered an internal error and was
unable to complete your request. Either the server is
overloaded or there is an error in the application.",
  "status": 500,
  "title": "Internal Server Error",
  "type": "about:blank"
}

```


cve/{id} (get)

General

Item	Details
URL	https://api.cybersixgill.com/cve_enrich/cve/{id}
Description	Get data about a specific CVE.
Method	GET

Parameters

Parameter	Required	Type	Description
id	Required	String	CVE ID to use as a filter.

Request Example

```
curl -X GET 'https://api.cybersixgill.com/cves/cve/CVE-2020-0796' \  
-H 'Content-Type: application/json' \  
-H 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \  
-H 'Authorization: Bearer [access_token value]' \  
--data-raw '  
'
```

Responses

Example: Response 200 - The requested CVE's data.

```
{  
  "id": "vulnerability--c74d4bc9-d184-610a-7e81-66581422a535",  
  "description": "A remote code execution vulnerability exists  
in the way that the scripting engine handles objects in memory  
in Internet Explorer, aka 'Scripting Engine Memory Corruption  
Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-  
2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-  
2020-0767.\n",  
  "rating": {  
    "sixgill": {  
      "previouslyExploited": 5.26,  
      "current": 8.4,  
      "highest": {
```

```

        "value": 9.2,
        "date": "2020-02-18T00:00:00Z"
    },
    {
        "nvd": {
            "value": 7.6,
            "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-0674",
            "severity": "HIGH",
            "publishDate": "2020-02-11T22:15Z",
            "modifyDate": "2020-02-12T17:53Z"
        }
    },
    "attributes": [
        {
            "name": "TrendingUnderground",
            "value": true,
            "description": "The CVE is trending on the underground"
        }
    ],
    "mentions": {
        "mentions_total": 128,
        "first_mention": "2020-01-18T03:19:46Z",
        "last_mention": "2020-02-17T14:07:15Z"
    },
    "github": {
        "github_projects": 1,
        "watchersCount": 7,
        "forksCount": 2,
        "activity": {
            "first_date": "2020-01-23T12:30:51Z",
            "last_date": "2020-01-23T12:30:51Z"
        }
    },
    "topProjects": [
        {
            "link": "https://github.com/binaryfigments/CVE-2020-0674",
            "name": "binaryfigments/CVE-2020-0674"
        }
    ],
    "nvd": {
        "baseMetricV2": {},
        "baseMetricV3": {},
        "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-0674",
        "publishDate": "2020-02-11T22:15Z",

```

```
    "modifyDate": "2020-02-12T17:53Z"  
  }  
}
```

Example: Default response 200 - Any response other than the data.

```
{  
  "detail": "The server encountered an internal error and was  
unable to complete your request. Either the server is  
overloaded or there is an error in the application.",  
  "status": 500,  
  "title": "Internal Server Error",  
  "type": "about:blank"  
}
```

cve/summary (get)

General

Item	Details
URL	https://api.cybersixgill.com/cve_enrich/cve/summary
Description	Get basic Cybersixgill Dynamic Rating data about a specific CVE.
Method	GET

Parameters

Parameter	Required	Type	Description
startDate	No	String	Start publish date, in format "YYYY-mm-DDTHH:MMZ".
endDate	No	String	End publish date, , in format "YYYY-mm-DDTHH:MMZ".

Request example

```
curl --location --request GET
'https://api.cybersixgill.com/cve_enrich/cve/summary' \
--header 'Authorization: Bearer <token>
```

Responses

Example: Response 200 - The list of CVEs published within the date range, with their scores.

```
{
  "info": {
    "totalCount": 23456,
    "maxCount": 1000,
    "sortBy": "Publish date, from newest to oldest"
  },
  "values": [
    {
      "id": "CVE-2020-0674",
      "rating": {
        "sixgill": {
          "previouslyExploited": 5.26,
```

```

        "current": 8.4,
        "highest": {
            "value": 9.2,
            "date": "2020-02-18T00:00:00Z"
        }
    },
    "nvd": {
        "value": 7.6,
        "link": "https://nvd.nist.gov/vuln/detail/CVE-2020-0674",
        "severity": "HIGH",
        "publishDate": "2020-02-11T22:15Z",
        "modifyDate": "2020-02-12T17:53Z"
    },
    "attributes": [
        {
            "name": "TrendingUnderground",
            "value": true,
            "description": "The CVE is trending on the underground"
        }
    ]
}

```

Example: Default response 200 - Any response other than the data.

```

{
    "detail": "The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.",
    "status": 500,
    "title": "Internal Server Error",
    "type": "about:blank"
}

```

cve/changes (get)

General

Item	Details
URL	https://api.cybersixgill.com/cve_enrich/cve/changes
Description	Get CVEs whose score significantly changed within a specified date range.
Method	GET

Parameters

Parameter	Required	Type	Description
startDate	No	String	Start publish date, , in format "YYYY-mm-DDTHH:MMZ".
endDate	No	String	End publish date, , in format "YYYY-mm-DDTHH:MMZ".

Request example using standard IOC enrichment

```
curl --location --request GET
'https://api.cybersixgill.com/cve_enrich/cve/changes' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <access token>'
```

Responses

Example: Response 200 - The list of CVEs that had significant changes in their scores during the specified time period. Returns the CVEs that experienced the significant changes, with only the specific fields/properties that experienced the change (i.e. not all fields are returned).

```
[
  {
    "id": "CVE-2020-0674",
    "score": {
```

```
    "sixgill": {  
      "highest": {  
        "value": 8.4  
      }  
    }  
  }  
}
```

Example: Default response 200 - Any response other than the data.

```
{  
  "detail": "The server encountered an internal error and was  
unable to complete your request. Either the server is  
overloaded or there is an error in the application.",  
  "status": 500,  
  "title": "Internal Server Error",  
  "type": "about:blank"  
}
```

CVE Feed API

The CVE Feed API provides an ongoing stream of CVE intelligence events, based on Cybersixgill's Dynamic CVE Rating. The feed comes in STIX 2.0 format for easy ingestion.

The API contains the following endpoints:

Group	Description	Endpoint	Method
Consume	Get bulk CVEs in bundle.	/ioc (CVE Feed)	GET
	Acknowledge consumed CVEs.	/ioc/ack (CVE Feed)	POST

ioc (CVE Feed)

General

Item	Details
URL	https://api.cybersixgill.com/cvefeed/ioc
Description	Get a bundle of CVEs in STIX2 format.
Method	GET

Parameters

Parameter	Required	Type	Description
limit	No	Integer	Amount of CVEs to consume. Default: 100
X-Channel-Id	Yes	String	Consumer channel of CVEs.

Request example

```
change endpoint
curl --location --request GET
'https://api.cybersixgill.com/cvefeed/ioc' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <access token>'
```

Responses

Example: Response 200 - Successfully fetched CVE bundle.

```
{
  "id": "bundle--c450c7de-808f-4027-bc2f-1ed088b7f075",
  "objects": [
    {
      "created": "2017-01-20T00:00:00.000Z",
      "definition": {
        "tlp": "amber"
      },
      "definition_type": "tlp",
    }
  ]
}
```

```

        "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
        "type": "marking-definition"
    },
    {
        "created": "2019-12-26T00:00:00Z",
        "definition": {
            "statement": "Copyright Sixgill 2020. All
rights reserved."
        },
        "definition_type": "statement",
        "id": "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
        "type": "marking-definition"
    },
    {
        "created": "2020-08-25T17:16:52.665Z",
        "external_references": [
            {
                "external_id": "CVE-2018-6789",
                "source_name": "cve"
            }
        ],
        "id": "cveevent--d048152f-f27a-4abf-8202-4bdb91a82e39",
        "modified": "2020-08-25T17:16:52.665Z",
        "object_marking_refs": [
            "marking-definition--41eaaf7c-0bc0-4c56-abdf-d89a7f096ac4",
            "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
        ],
        "spec_version": "2.0",
        "type": "x-cybersixgill-com-cve-event",
        "x_sixgill_info": {
            "event": {
                "_id": "5f454784ffebcfa91197cc04",
                "action": "modified",
                "description": "Sixgill Current score of
CVE-2018-6789 changed from Low to Medium.",
                "event_datetime": "2020-06-30T00:00Z",
                "level": "Medium",
                "name": "Sixgill_score_level_change",
                "prev_level": "prev_level",
                "type": "score_level"
            }
        },
    },

```

```

        "nvd": {
            "base_score_v3": 9.8,
            "base_severity_v3": "CRITICAL",
            "link":
"https://nvd.nist.gov/vuln/detail/CVE-2018-6789",
            "modified": "2019-03-06T20:27Z",
            "published": "2018-02-08T23:29Z",
            "score_2_0": 7.5,
            "severity_2_0": "HIGH",
            "vector_v2": "AV:N/AC:L/Au:N/C:P/I:P/A:P",
            "vector_v3":
"CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H"
        },
        "rating": {
            "current": 5.17,
            "highest": {
                "date": "2018-05-10T00:00Z",
                "value": 9.04
            },
            "previouslyExploited": 5.38
        }
    },
    "spec_version": "2.0",
    "type": "bundle"
}

```

Example: Response 403 - Request no authorized.

```

{
  "status_code": 403,
  "message": "Not authorized"
}

```

ioc/ack (CVE Feed)

General

Item	Details
URL	https://api.cybersixgill.com/cvefeed/ioc/ack
Description	Acknowledge consumed CVEs.
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	No	String	Consumer channel of CVEs.

Request Example

```
curl --location --request POST
'https://api.cybersixgill.com/cvefeed/ioc/ack' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <access token>'
```

Responses

Example: Response 200 - Number of successfully-acknowledged CVEs

```
3
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```

Dark Feed API

Darkfeed is a feed of malicious indicators of compromise, including domains, URLs, hashes, and IP addresses.



Please make sure to include the X-Channel-id:
d5cd46c205c20c87006b55a18b106428 as mentioned
below.

Group	Description	Endpoint	Method
IOC	Get a bundle of IOCs in STIX2 format.	/ioc (Dark Feed)	GET
	Acknowledge consumed IOCs.	/ioc/ack (Dark Feed)	POST

ioc (Dark Feed)

General

Item	Details
URL	https://api.cybersixgill.com/darkfeed/ioc
Description	Get a bundle of IOC items in STIX2 format.
Method	GET

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel. Use the following value: d5cd46c205c20c87006b55a18b106428
limit	No	integer	Amount of IOCs to consume. Default = 100



After each run of the ioc endpoint, run the [ioc/ack \(Dark Feed\)](#) endpoint to acknowledge you consumed a bundle (as set by the limit parameter) of IOC items. In this way, the next time you run the ioc endpoint, the next bundle of IOC items will be returned.

Request example

```
curl -X GET
'https://api.cybersixgill.com/darkfeed/ioc?limit=10' \
-H "Authorization: Bearer [access_token value]" \
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428"
```

Responses

Example: Response 200 - Successfully fetched IOC bundle.

```
{
  "id": "bundle--b56c1e2e-a40c-44ca-83dd-09e25936d273",
  "objects": [
```


```
{
  "created": "2019-05-01T06:13:14.000Z",
  "description": "this is the description",
  "id": "example--1",
  "modified": "2019-05-08T03:43:44.000Z",
  "name": "simple name",
  "type": "example",
  "additionalProp1": {}
}
],
"spec_version": "2.0",
"type": "bundle"
}
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```

ioc/ack (Dark Feed)

General

Item	Details
URL	https://api.cybersixgill.com/darkfeed/ioc/ack
Description	<p>Acknowledges that you consumed a bundle of IOC items after running the ioc (Dark Feed) endpoint.</p> <div> After each run of the ioc (Dark Feed) endpoint, run the ioc/ack endpoint to acknowledge you consumed a bundle (as set by the ioc endpoint limit parameter) of IOC items. In this way, the next time you run the ioc endpoint, the next bundle of IOC items will be returned.</div>
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel. Use the following value: d5cd46c205c20c87006b55a18b106428

Request example

```
curl -X POST 'https://api.cybersixgill.com/darkfeed/ioc/ack \
-H "Authorization: Bearer [access_token value]" \
-H "X-Channel-Id: d5cd46c205c20c87006b55a18b106428'
```

Responses

Example: Response 200 - Number of successfully acknowledged IOCs

```
2
```


Example: Response 403 - Request not authorized.

```
{  
  "status_code": 403,  
  "message": "Not authorized"  
}
```

Dark Feed Enrichment API

The Dark Feed Enrichment API provides endpoints for obtaining detailed information on IOCs (indicators of compromise).

The endpoint also allows you to enrich data based on two additional pivot points: actor name and post ID (i.e. getting all IOCs from a specific thread from an underground source).

The API contains the following endpoints:

Group	Description	Endpoint	Method
IOC Enrichment	Get items in STIX format related to the specified IOC.	/ioc/enrich (post)	POST

ioc/enrich (post)

General

Item	Details
URL	https://api.cybersixgill.com/ioc/enrich
Description	Get items in STIX format related to the specified IOC.
Method	POST

Parameters

Parameter	Required	Type	Description
X-Channel-Id	Yes	string	IOC consumer channel.

You can define the following optional parameters in the request:

Parameter	Type	Description
ioc_type	string	An array that can contain [ip, domain, url, hash]. Specify the value for these types in the sixgill_field_value parameter.
ioc_value	string	IOC items containing the value you specify here for the ioc_type parameter.
limit	integer	The number of IOC items to return. Default: 50 Minimum: 1
sixgill_field	string	Either of the following Cybersixgill fields: ▪ actor ▪ post_id Specify the value for this field in the sixgill_field_value parameter.

Parameter	Type	Description
sixgill_field_value	string	IOC items containing the value you specify here for the sixgill_field parameter.
skip	integer	Specifies how many IOC items to skip before displaying results. For example, skip: 200 displays the 201th item and forward (till the limit is reached). Default: 0 (displays from the first item)

Request example using IOC enrichment

```
curl --location --request POST
'https://api.cybersixgill.com/ioc/enrich' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: cea9a52effad4bc5e905a5a653f5cf9b' \
--header 'Authorization: <token>' \
--data-raw '{
  "ioc_type": "ip",
  "ioc_value": "190.2.31.172",
  "limit": 50,
  "skip": 0
}'
```

Request example using "sixgill_field"

```
curl --location --request POST
'https://api.cybersixgill.com/ioc/enrich' \
--header 'Content-Type: application/json' \
--header 'Cache-Control: no-cache' \
--header 'X-Channel-Id: d5cd46c205c20c87006b55a18b106428' \
--header 'Authorization: Bearer <token>' \
--data-raw '{
  "sixgill_field": "post_id",
  "sixgill_field_value":
"459ef8c762fa6c34e19031141642e9097f43a405",
  "limit": 50,
  "skip": 0
}'
```

Responses

Example: Response 200 - Number of successfully acknowledged IOCs.

```
{
  "items": [
    {
      "created": "2019-05-01T06:13:14.000Z",
      "description": "this is the description",
      "id": "example--1",
      "modified": "2019-05-08T03:43:44.000Z",
      "name": "simple name",
      "type": "example",
      "additionalProp1": {}
    }
  ],
  "total": 1
}
```

Example: Response 403 - Request not authorized.

```
{
  "status_code": 403,
  "message": "Not authorized"
}
```

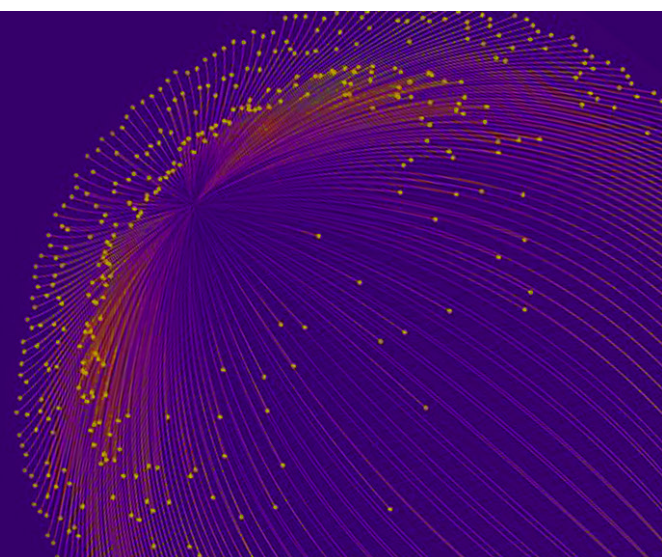
Example: Response 404 - Entered input is invalid.

```
{
  "message": "Invalid input",
  "status_code": 404
}
```


DARKFEED BY CYBERSIXGILL

Detect and obliterate threats and malicious IOCs

AUTOMATED | ACTIONABLE | COMPREHENSIVE | REAL-TIME



Darkfeed is an intelligence stream of indicators of compromise (IOCs), including malicious domains, URLs, IP addresses, and file hashes.

Darkfeed is automated, meaning that IOCs are extracted from Cybersixgill's deep, dark and surface web sources and delivered in real-time. It is actionable so you will be able to receive and preemptively block items that threaten your organization.

Darkfeed harnesses Cybersixgill's unmatched intelligence collection capabilities both in terms of breadth and quality. Darkfeed's contextual threat intelligence is highly accurate, comprehensive, covert and automated.

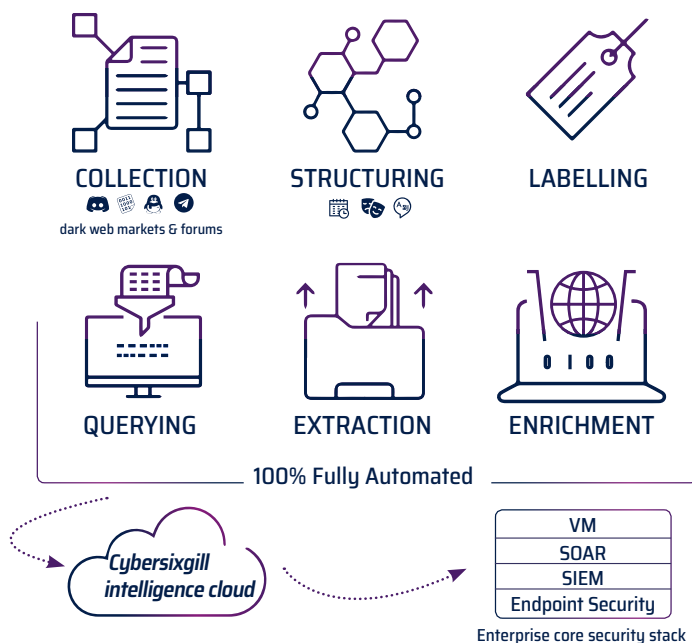
The feed is structured in the STIX format and shared via Cybersixgill's API, allowing customers to automatically consume and integrate it with their security solutions, whether SIEM, SOAR, vulnerability management tool, or any other platform.

ARCHITECTURE & INTEGRATION

Darkfeed is automated and transparent. It seamlessly integrates into your existing enterprise security stack and fits into the normal flow of your SOC without change or interruption. The feed is structured in the STIX format for automated parsing, custom properties (feed name, feed ID, post title, actor, source, etc.) for IOC enrichment and filtering, as well as external integrations for IOC enrichment (Mitre ATT&CK, VirusTotal, and more).

Benefits

- **Automatically integrate IOC** into your security stack (machine-to-machine)
- **Improve your SOAR, SIEM & Vulnerability Management System** with seamless integration of Cybersixgill's contextual data
- **Receive automated early warnings** of new malware threats
- **Get actionable insights** to effectively mitigate threats
- **Level up your threat hunting** for malicious IOCs in corporate networks
- **Better understand** malware TTPs and threats
- **Expandable and future-proof** with continuous additions and intel stream enrichment



Feed Content

Domains

- Compromised sites to which access is sold on the dark web
- Suspicious domains that are for sale on the dark web

Hashes

- Malware hashes
- Hashes of malware claimed to be undetected

IP addresses

- Command-and-control server IP addresses for most prevalent malware
- Command-and-control server IP addresses for servers involved in botnets, DDoS attacks, and proxy anonymization

URLs

- Links to malware files hosted on underground file-sharing sites

FUEL YOUR ANALYTICS

Use the data to track, trend and gain data-driven actionable insights to the IOCs collected by Darkfeed. Gain better understanding of malware TTPs and trends.

VISIBILITY INTO YOUR THREATSCAPE

Gain total visibility of the threatscape of your industry. Mitigate threats in advance, prevent incidents and minimize attack surface.



SECURITY We treat security of data with the highest standards. Cybersixgill's security-first approach leverages the best and most advanced technologies to make sure that your data stays safe and private. Our service undergoes rigorous audits and employs the latest best practices to ensure the integrity of the data as well as its authenticity, security and compliance.



Cybersixgill is a fully automated threat intelligence solution that helps organizations protect their critical assets, reduce fraud and data breaches, protect their brand and minimize attack surface. The portal empowers security teams with contextual and actionable alerts as well as the ability to conduct real-time investigations. Rich intelligence streams such as Darkfeed harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include global 2000 enterprises, financial services, MSSPs, government and law enforcement entities.



First draft version - Example

Physical Threat Intelligence tool



1. Overview
2. Anomaly detection
3. Event classification
4. Service invocation
5. Preliminary experiments of Spark-GHSOM
6. References

Overview

The objective of this manual is to describe the machine learning tasks performed by the big data analytics algorithms that are considered in the project. The tasks are *i)* anomaly detection and *ii)* event classification. The tasks are performed via data-driven approaches in order to construct models that will be capable to identify *i)* anomalies in the data distributions or *ii)* specific threats from the sensors data for the city of Padova and Oslo. In the following sections we define the machine learning tasks, the preliminary experiments conducted and the possibility to use the algorithm library in a stand-alone manner.

Anomaly detection

Anomaly detection is an unsupervised data-driven approach that aims to train a predictive model (henceforth *anomaly detector*) that is capable of catching anomalies from data. We identified three possible phases to train an accurate anomaly detector: the *i)* initial phase, *ii)* update phase, and *iii)* identification phase. At the initial phase, a weak predictive model is constructed that represents a “coin-flip” function with low predictive power that needs to be trained to improve the performance. To this aim, at this phase, a batch-learning approach is considered to overcome the weakness of the starting function. We say that the algorithm in this phase is at the “initial state”. After the first stage, the anomaly detector performs better than the previous starting function and it could be ready to take the sensor data as input to identify possible anomalies. However, since the distributions could vary also in normal cases (e.g. during the weekend CO₂ in the air could be lower than during working days) we proposed to introduce an additional update phase that aims to enable further training of the anomaly detector with the possibility to catch also non-anomalous variations in distributions. Furthermore, the update phase helps also to use a previous pre-trained model with possible reduction of the training time. The algorithm in this phase is at the “update state”. In the identification phase, the anomaly detector is ready to process sensor data to detect possible anomalies. At this phase, the anomaly detector could be placed in production to work actively with the real scenario data since it shows better performance. The algorithm in this phase is at the “identification state”. A general schema of the anomaly detection is showed in Figure 1.

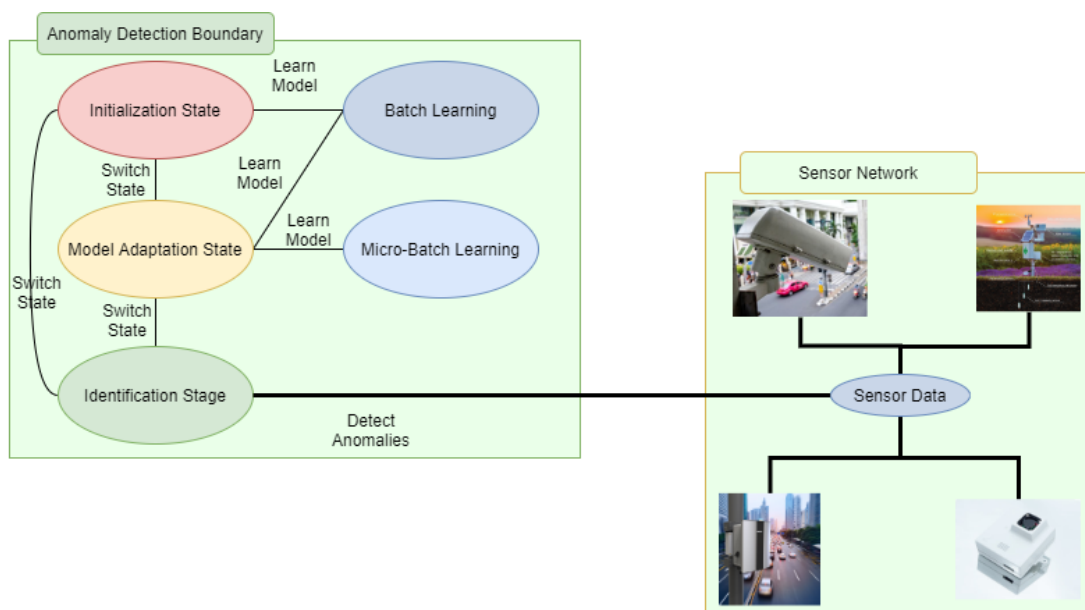


Figure 1. The anomaly detection for the identification of possible anomalies from sensor data

The anomaly detector can handle all the possible sensor data that presents spatial (e.g. GPS coordinates) and temporal information (e.g. timestamp) and a set of descriptive variables that are acquired by the specific sensor for the monitoring of the city. For instance, independently from the type of the sensor (e.g., traffic cameras, air pollution), the anomaly detector acts with the same approach. Indeed, the anomaly detector works with values usually indicating the level of something: pedestrians concentration, traffic level, temperature, humidity, level of PM2.5, level of CO2, and so forth that are automatically captured and transmitted by the sensor network. Therefore, in the real scenario, the anomaly detector will analyze the data coming from different sensors and it will be able to judge a data as normal or anomalous. The anomaly detector could produce different types of output depending on the level of detail. The simplest approach provides feedback for the current data in the form of a Boolean response. This kind of output could support to raise an alert if the response is equal to “anomaly” (see Figure 3 as an example).

✓	Timestamp	mean temperature	...	ambrosia	urticaceae
	2021-04-15 10:00	15.1	...	20.0	50.0
✗	Timestamp	mean temperature	...	ambrosia	urticaceae
	2021-04-16 11:00	15.1	...	30.0	52.0

**ALERT !
ANOMALOUS
INSTANCE
'2021-04-16 11:00'**

Figure 3. When an anomaly will be detected, the system will raise an alert indicating the timestamp and GPS coordinates.

This approach has the advantage that is really simple to handle and transmit as a binary variable (e.g. anomaly/normal, 0/1, true/false ...). However, the drawback of this approach is that it makes difficult for the final user interpreting the raised alert/anomaly. Therefore, a more informative approach could be considered by combining the previous one with a ranking of the variables with their importance indicating the contribution to catch the anomaly (see Figure 4).

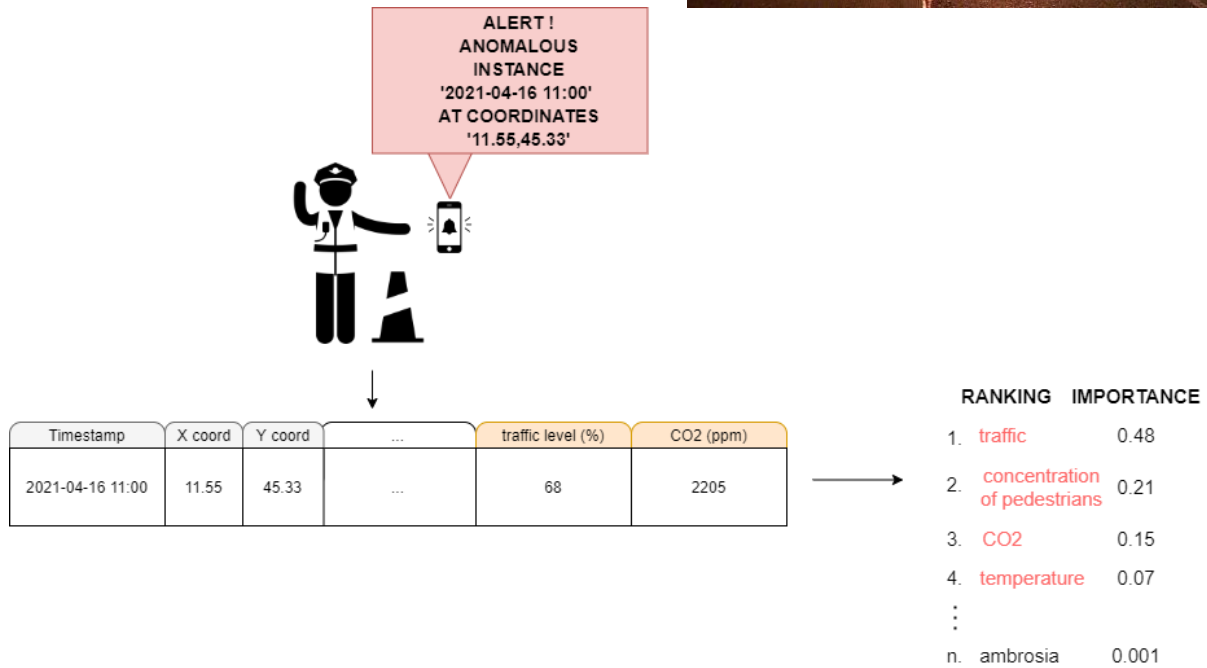


Figure 4. When an anomaly will be detected, the system will raise an alert and will provide a feature ranking according to the features importance in detecting the anomaly

The importance score is determined starting from a distance function between the current data under analysis and the anomaly detector model. The distance function is impacted by a predefined threshold (called *threshold factor*, that helps to control the sensibility of the algorithm). An anomaly will be detected if that distance is too high according to the previous data seen for training. A graphical example is showed in Figure 5. This approach helps to better understand if the set of current measurements represent an anomaly. In this way, the operator would be able to interpret if the current scenario is representing a threat.

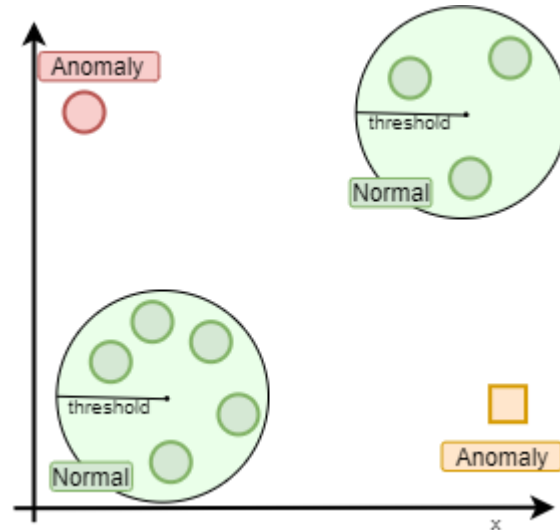


Figure 5. An example with two variables of analysis that correspond to two sensor measurements.

The anomaly detector considered for the preliminary experiments is called Spark-GHSOM [1] that enables the distributed computation performed by a Growing Hierarchical Self-Organizing Map (GHSOM). GHSOM is a dynamic variant of the SOM algorithm which generates a multi-level hierarchy of SOM maps based solely on input data (see Figure 6). However, in order to generate this multi-level structure, GHSOM requires multiple iterations over the input dataset, thus making it intractable on large datasets. Moreover, the conventional GHSOM algorithm is designed to handle datasets with numeric attributes only. This represents an important limitation as most modern real-world datasets are characterized by mixed attributes, numerical and categorical. Spark-GHSOM exploits the Spark platform to process massive datasets in a distributed manner.

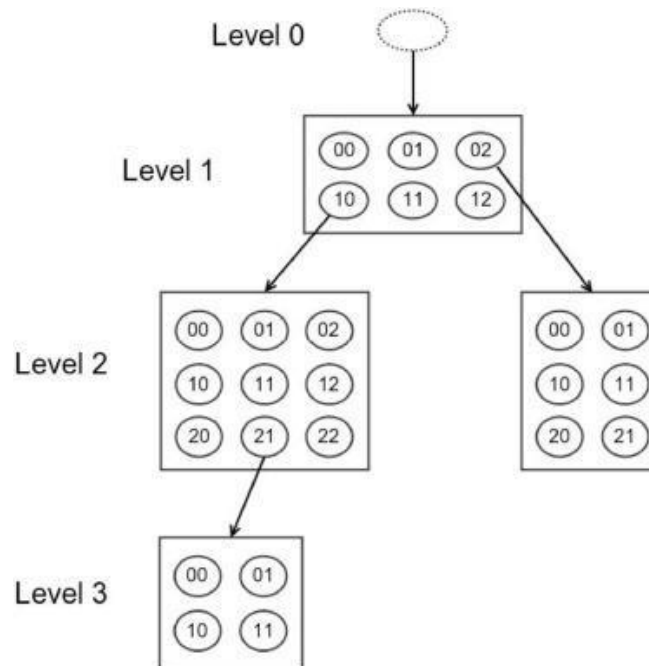


Figure 6. Image from [1] that shows the hierarchy of SOMs.

Summarizing, this approach for anomaly detection has different advantages: *i)* it is able to work with data from sensors independently from the type of the sensor; *ii)* it is able to work with the raw data by avoiding to convert from categorical to numerical data; *iii)* it is able to handle a huge amount of data since it is capable to exploit different computational nodes in a distributed fashion.

Event classification

Starting from a predefined set of threats (e.g. fire, car accident, attack with guns...), similarly to the anomaly detection task, the event classifier aims to classify the current unclassified sensor data under analysis as a particular threat or as a normal case. Therefore, in addition to the anomaly detector, the event classifier would be able to indicate also the type of the threat under analysis. For this task, similarly to the anomaly detection, a training phase and an event identification phase are foreseen. The main difference with the anomaly detection task is that usually the classification of an object/event/something is guided by the learning of a predictive model in a supervised manner. This means that the dataset used for the training of the model must be annotated by describing the possible threats for the real scenario. However, this could be demanding to obtain. To overcome this problem, unsupervised algorithms could be also considered for the classification task as for the anomaly detection. These algorithms are usually less accurate than the supervised ones since they exploit less informative data avoiding to consider predefined classes. The method proposed in [2], called DENCAST, could be used for the event classification since it is able to perform the unsupervised task of clustering also for the classification. It represents a novel distributed algorithm implemented in Apache Spark, which performs density-based clustering and exploits the identified clusters to solve both single- and multi-target regression tasks (and thus, solves complex tasks such as time series prediction). Contrary to existing distributed methods, it does not require a final merging step (usually performed on a single machine) and is able to handle large-scale, high-dimensional data by taking advantage of Locality Sensitive Hashing (LSH).

Service Invocation

The analytics tools can be invoked remotely prior to authentication and authorization via standard APIs.

More precisely the following API will be exposed:

- **Execution API:** This API will trigger the big data execution of the requested tool. It receives as input parameters specific for the tool execution and optional configurations. It will give as output the id of the analytics process activated. The outcome of the Execution can be either a machine learning model or prediction values. The API either receives from the caller information on where to store its output or returns to the caller the relative storing path/URI.
- **Stop API:** This API will stop the analytics process. It receives as input the id of the analytics process to be stopped. It will stop either the model creation process (ensuring a consistent status for the model) or the prediction analytics. It is useful to stop the model training or to stop predictions in order to change the model to a more updated one.

The system is capable to handle multiple parallel instances of tool executions.

Preliminary experiments of Spark-GHSOM

Data sources for the preliminary experiments are summarized in Table 1. The results of preliminary experiments for the data of Padova (ARPA Veneto, Open Section) are presented in Table 2.

Use case	Data sources
Padova	Air quality: <ul style="list-style-type: none"> • PM10 • PM2.5 • CO2 ... CCTV metadata: <ul style="list-style-type: none"> • Level of traffic • Concentration of pedestrians ... Meteorological: <ul style="list-style-type: none"> • Temperature • Humidity • Precipitation ...
	ARPA Veneto, Open Section: <ul style="list-style-type: none"> • https://www.arpa.veneto.it/dati-ambientali
Oslo	Air quality: <ul style="list-style-type: none"> • PM10 • PM2.5 • CO2 ... Public transport: <ul style="list-style-type: none"> • Number of pedestrians Traffic data: <ul style="list-style-type: none"> • Level of traffic • Concentration of pedestrians ...
	Air pollution: <ul style="list-style-type: none"> • Agency for Urban Environment - https://www.luftkvalitet.info Traffic data: <ul style="list-style-type: none"> • Statens Vegvesen - https://dataut.vegvesen.no Public transport: <ul style="list-style-type: none"> • ENTUR - https://developer.entur.org

Table 1. The data considered for the preliminary experiments.

tau 1	tau 2	training epochs	thresh. factor	update state	# of layers	true normal	false abnormal	false normal	true abnormal
0.7	1.0	10	6.0	no	1	371	21	2	1
0.7	1.0	10	5.5	no	1	369	23	1	2
0.7	1.0	10	5.0	no	1	363	29	1	2
0.7	1.0	10	4.5	no	1	355	37	0	3
0.7	1.0	10	4.0	no	1	342	50	0	3
0.7	1.0	10	3.5	no	1	322	70	0	3
0.7	1.0	15	6.0	no	9	385	7	3	0
0.7	1.0	15	5.5	no	9	384	8	1	2
0.7	1.0	15	5.0	no	9	378	14	1	2
0.7	1.0	15	4.5	no	9	374	18	0	3
0.7	1.0	15	4.0	no	9	364	28	0	3
0.7	1.0	15	3.5	no	9	352	40	0	3
0.7	1.0	10	6.0	yes	1	380	12	3	0
0.7	1.0	10	5.5	yes	1	377	15	3	0
0.7	1.0	10	5.0	yes	1	374	18	3	0
0.7	1.0	10	4.5	yes	1	371	21	2	1
0.7	1.0	10	4.0	yes	1	364	28	1	2
0.7	1.0	10	3.5	yes	1	355	37	0	3
0.7	1.0	15	6.0	yes	9	389	3	3	0
0.7	1.0	15	5.5	yes	9	387	5	3	0
0.7	1.0	15	5.0	yes	9	387	5	3	0
0.7	1.0	15	4.5	yes	9	386	6	2	1
0.7	1.0	15	4.0	yes	9	383	9	1	2
0.7	1.0	15	3.5	yes	9	376	16	0	3

Table 2. The results of the preliminary experiments using the data of Padova from ARPA Veneto. In green the best results that emphasize that the anomaly detector correctly identified the anomalies with acceptable error.

Table of general terms

Term	Definition	Values
instance	A specific sensor measurement	A vector of numerical and/or categorical values
dataset	A set of instances	A matrix of numerical and/or categorical values
class	A predefined set of threats or normal cases	A value (usually categorical, e.g., car accident, fire, toxic, normal...)
annotated instance	An instance with a class	A vector of numerical and/or categorical values that ends with a class value
annotated dataset	A set of annotated instances	A matrix of numerical and/or categorical values where the last column contains the values of the class

Table 3. The table of general terms and their definitions.

Table of Spark-GHSOM terms

Term	Definition	Values
winning neuron	A neuron that best matches the current instance under analysis	Contains real values
τ_1 (tau 1)	Parameter regulating the growth of a single SOM layer	A real value, ranging from 0 to 1
τ_2 (tau 2)	Parameter regulating the hierarchical growth	A real value, ranging from 0 to 1
threshold factor	Parameter regulating the sensitivity of the anomaly detector to catch the anomalies	A real value
epochs	number of reading iterations of the training dataset	An integer value
datasetPath	Dataset file path	A string value
update phase	Parameter indicating whether the updated phase is performed	A boolean value

Self-Organized Map (SOM)	A matrix of neurons fully connected with each other	Contains a matrix of values of the neurons
hierarchy	The set of SOMs connected in a hierarchical manner	Contains the whole model as a set of matrices of values
feature importance	The feature importance attributed by the selected neuron through a computation of geometrical distance between the feature and the neuron	A real value, ranging from 0 to 1
feature ranking	A ranking of features in a descending order with respect to their importance	A ranking of feature names with the corresponding importance value

Table 4. The table of Spark-GHSOM terms and their definitions.

Table of DENCAST terms

Term	Definition	Values
Locality Sensitive Hashing (LSH)	method for reducing the dimensionality of the vector space of a data set	NA
datasetPath	dataset file path	A string value
table name	name of the database table	A string value
LSH RDD partitions	RDD partitions used in LSH	An integer value
LSH dimensions	number of hyperplanes for LSH	An integer value
LSH num neighbors	number of nearest neighbors used in LSH	An integer value
LSH num permutations	number of random permutations used in LSH	An integer value
min cosine similarity	minimum number of neighboring objects for core objects	A real value
minPts	minimum number of neighboring objects for core objects	An integer value
core object	An object is a core object if it has at least minPts objects in its neighborhood	A vector representing an object
window size	spark-streaming batch and/or micro-batch size	An integer value

num targets	Number of target attributes	An integer value
-------------	-----------------------------	------------------

Table 5. The table of DENCAST terms and their definitions.

References

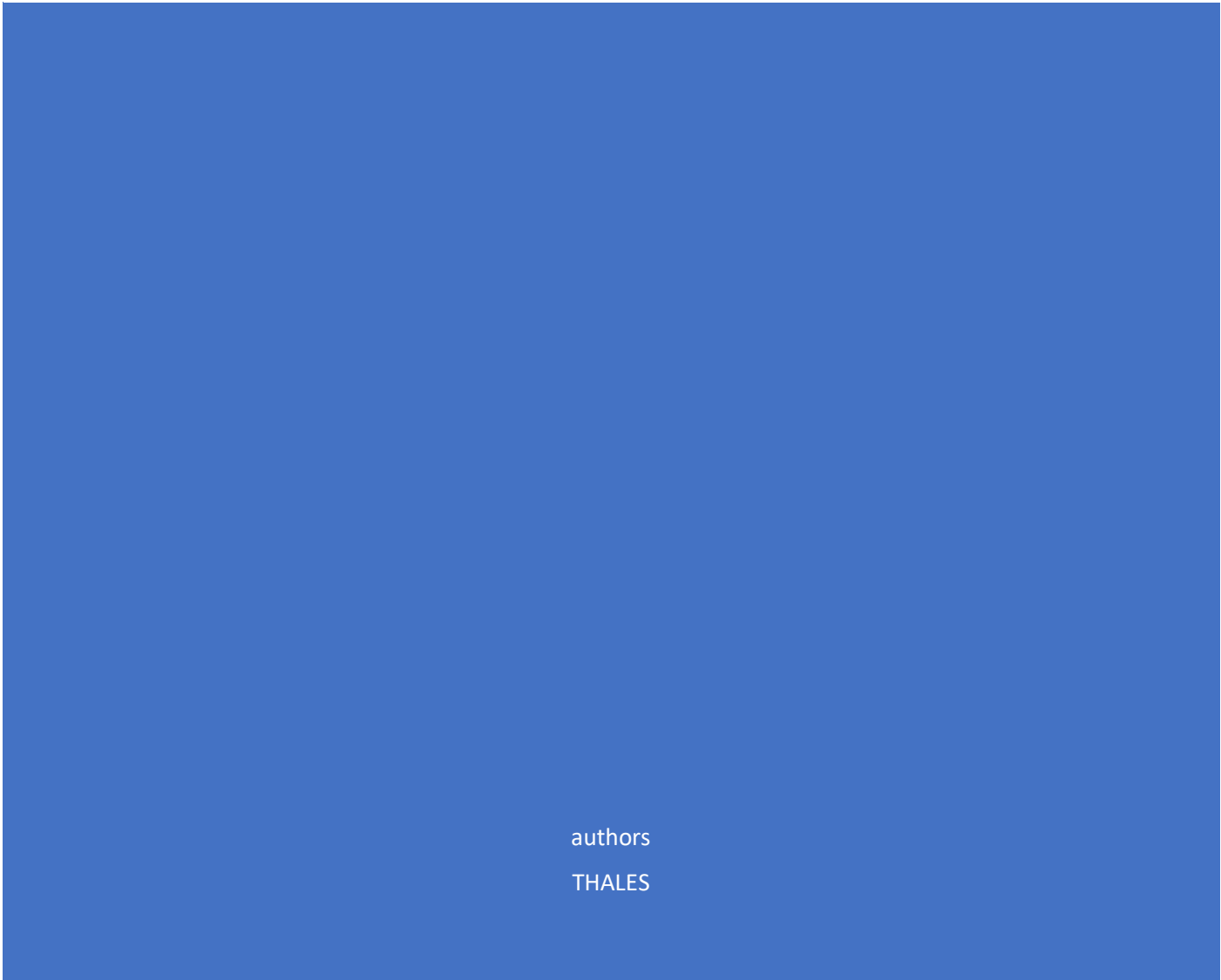
[1] Ameya Malondkar, Roberto Corizzo, Iluju Kiringa, Michelangelo Ceci, Nathalie Japkowicz, Spark-GHSOM: Growing Hierarchical Self-Organizing Map for large scale mixed attribute datasets, Information Sciences, Volume 496, 2019, Pages 572-591, ISSN 0020-0255, DOI: 10.1016/j.ins.2018.12.007.

[2] Roberto Corizzo, Gianvito Pio, Michelangelo Ceci, Donato Malerba, DENCAST: Distributed Density-Based Clustering for Multi-Target Regression, Journal of Big Data, 10.1186/s40537-019-0207-2



IMPETUS Human Interaction Tool

Draft User Manual



authors
THALES

Contents

Introduction	2
Human-Computer Interaction Tool	3
Use case City of Oslo	5
Use case City of Padova	5
HCI components	7
Sensor set	7
Data Acquisition Units	7
Secure USB drive	8
Server computer	8
Network	8
Overview	8
Graphical User Interface	10
Procedure	11
Protocols	11
COVID-19	11
Data management	12
Sensitive data	12
Appendix A: Forms	13
Appendix B: Sensors	15

Introduction

This document contains information about the “IMPETUS Human-Computer Interaction Tool”, its configuration and intended use during the Impetus project tests. Differences between the use cases for each partner city are due to the chosen setting and configuration of the sensors. In both cases, though, the Human Interaction Tool has the same generic purpose, setup and output, all of which are described in this document.

Human-Computer Interaction Tool

The purpose of the Human-Computer Interaction (HCI) Tool is to measure bio signals of the Human operators, who are interacting with their equipment and each other while performing their given tasks, and, using custom and personalized machine learning models, assess the operators' momentary mental workload and emotional stress levels. The output of the tool, which is this assessment, is then presented in (a graphic form) as feedback, to selected persons, depending on the end user preference.

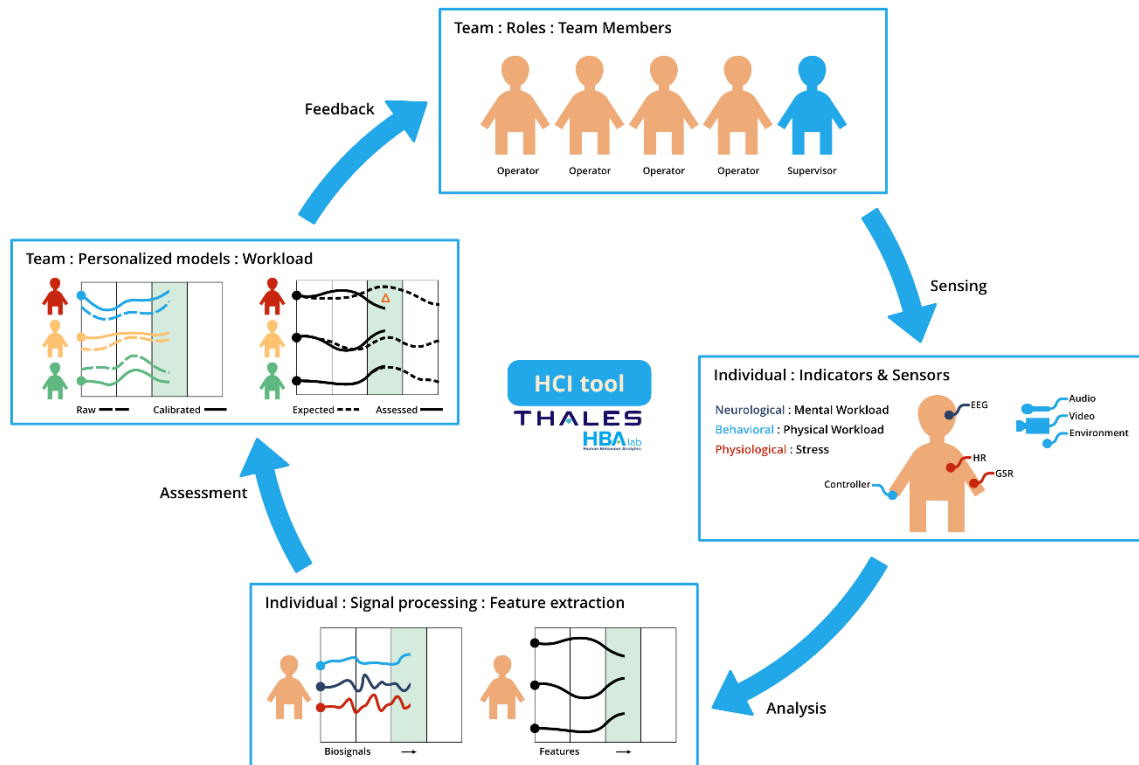
Measuring of the bio signals is done continuously, in real-time and as unobtrusively as possible. Specific configuration of the sensors used to perform this measurement will depend on the preference of the individuals and may include wearable sensors detecting brainwaves (using Electroencephalograms, or EEG), sweat (using Electrodermal Activity sensors or EDA), heartbeat activity (using Photoplethysmogram, or PPG) and physical activity (using software sensors capturing user input like keyboard or mouse). Additionally, environmental conditions like sound level and temperature can be recorded (using various sensors) in the room where the operators are at work.

The Human-Computer Interaction Tool processes these bio signal streams in real time and using (personalized) models, created prior to the use of the tool, produces an assessment of the mental, emotional and physical workloads of an individual operator as well as an indication of teamwork (where applicable). These assessments are updated each minute and produced continuously.

The assessment can be shown as feedback in configurable amount of detail, on individual and aggregated (team) levels, to person or persons of choosing, in the form of a (digital) dashboard. This feedback can also be used by other (digital) tools, developed by other partners in the Impetus project, in order to close the loop and adapt their interfaces or information they provide to the operators being assessed by the HCI Tool.

The end goal of the tool is to provide timely feedback and assure the operators can perform their tasks without being overloaded or overstressed which might impede their work and introduce unwanted fatigue, stress and reduced effectiveness of the operators.

The following graphic summarizes the steps of the continuous loop of the HCI tool: biosensing, analysis, assessment and feedback.



Schematic representation of the HCI tool

Use case City of Oslo

SOC: Agency for Fire and Emergency.

The team consists of 1 supervisor and 4 operators. Specifics are still being established in cooperation with the city of Oslo.

The HCI tool will be deployed on premises.

Use case City of Padova

SOC: Local Police City of Padova

The team consists of 1 supervisor/commander and 4 operators. Each operator has 3-4 screens, phone and all share a video-wall showing images from the cameras in the city.

Operators provide support to citizens. Calls come in that need to be handled.

Issues related to the calls vary in terms of scope:

- Lowest level (“business as usual”): minor incidents, handled by individual operators
- Next few levels require alignment with supervisor and other stakeholders
- Top ‘disaster’ level goes up to alignment with the prefect, national level

Operators work individually and follow the manual. The need to cooperate is not explicitly stated in the manual. However, in practice, operators help each other out and discuss issues when they sense the need (actual way of working).

Workload / stress levels monitored by the supervisor / commander. Typical intervention is task load management.

Commitment from SOC Local Police as well as willingness to participate by operators has been confirmed.

Note: stress levels at this SOC have not caused issues. Other (related) SOC's might provide situations where workload/stress has more impact on operator (teaming) performances.

The HCI tool will be deployed on premises.



Example of a SOC

HCI components

The HCI Tool consists of the following components:

Sensor set

A sensor set usually consisting of a Shimmer and a Muse sensor. This sensor set can be altered depending on the operator's tasks and or needs. The Sensor set will be connected wirelessly via Bluetooth to a dedicated Data Acquisition Unit (DAU). Each workstation (operator) will have a sensor set (up to four sensor sets in total).

More information on the sensors can be found in Appendix B.



Photos of the Shimmer (left) and the Muse (right) sensors.

Data Acquisition Units



The DAU on each workstation will handle (bio) data acquisition, feature extraction and workload assessment for the operator. The DAUs will also send alerts based on personal settings to the IMPETUS platform. These alerts will be based on Signal Quality or the Assessment outcome.

Secure USB drive

On the secure USB drive will be used by each operator to store his or hers personalized workload model and alert settings. The USB drive has to be inserted into the DAU in order for the system to be able to make assessments. This ensures protection of personal data.



Server computer

The server collects data from all DAUs and checks the HCI system status. Based on the status, alerts can be sent to the IMPETUS platform.

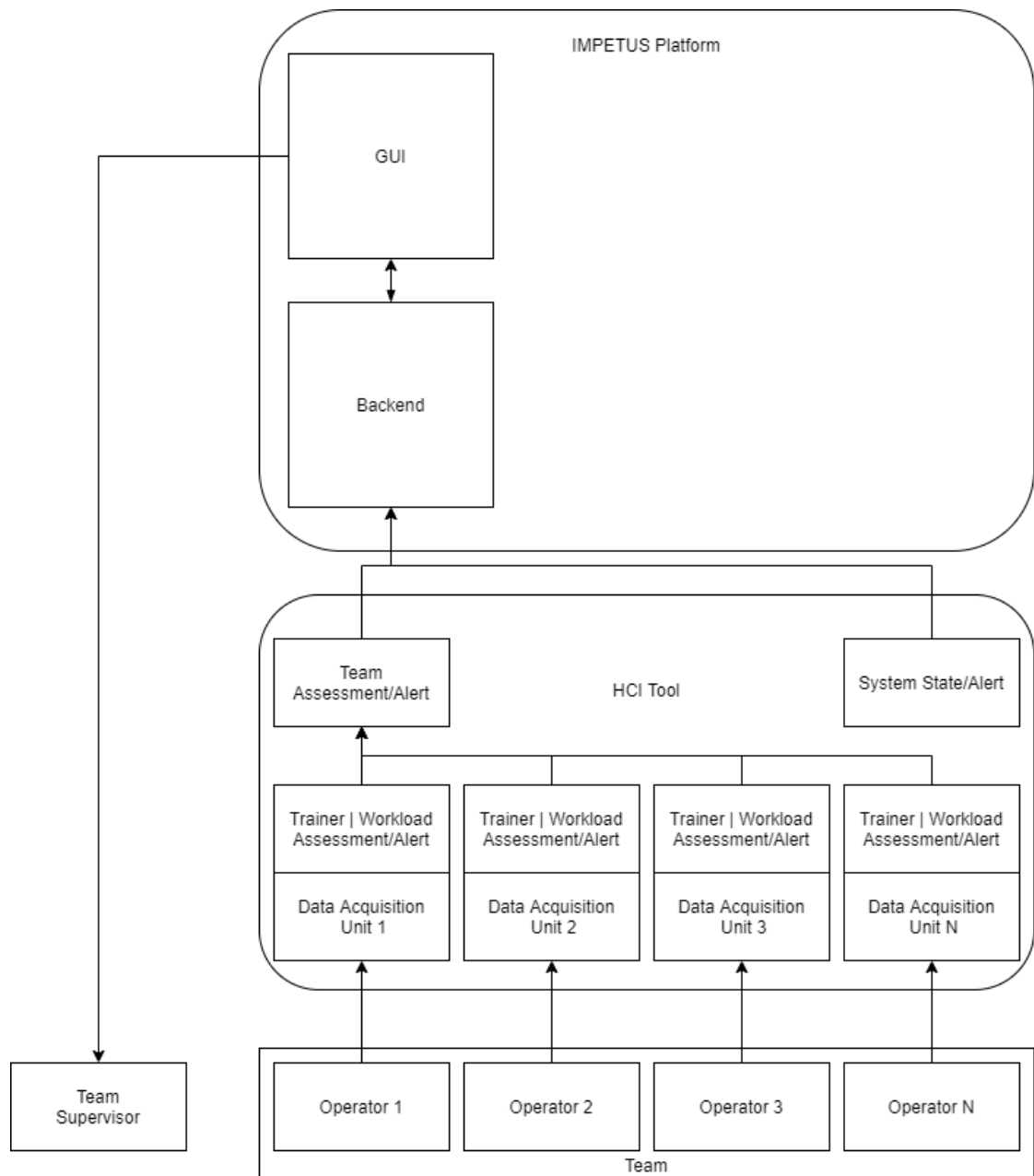
When multiple operators are connected to the server, the server can also assess the level of teamwork between the operators.

Network

A local LAN is needed to connect the DAUs and the server. This can be done on the already present network infrastructure, but for the tests we will create a new dedicated Ethernet LAN.

Overview

This schematic gives an overview of the HCI tool components described above and the communication between them.



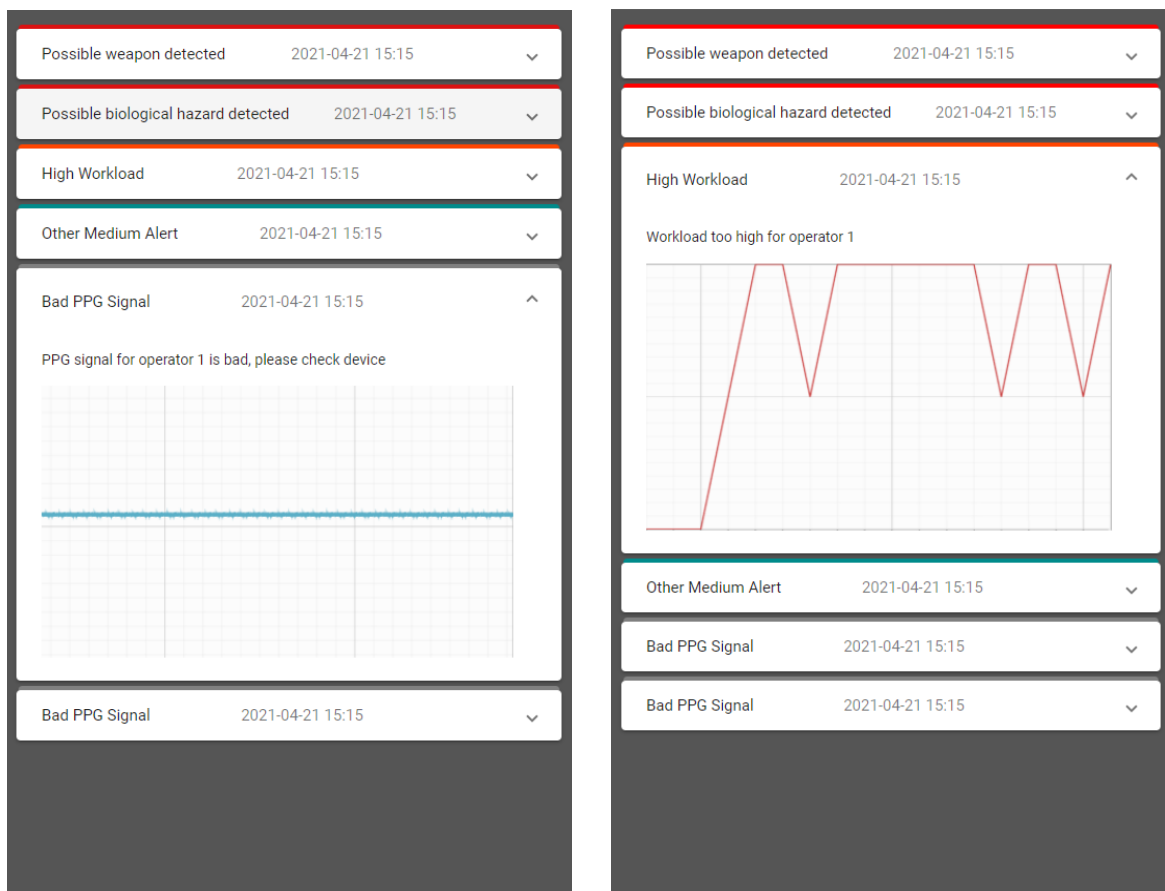
HCI tool hardware overview schematic

Graphical User Interface

The HCI Graphical tool Graphical User Interface (GUI) consists of an interface on the Data Acquisition Units (DAU) and a common GUI on the IMPETUS platform.



The GUI on the DAU is there as an interface to the HCI sensor set status. The common GUI is there to alert the user of alerts generated by the IMPETUS Tools.



Common GUI mock-ups

Procedure

Protocols

For the operators participating in the Impetus tool tests, custom made machine learning (ML) models will be used to assess their mental state (workload). To create these models, the participants will be asked to perform a series of short generic “calibration” tasks (2 to 3 hours, including preparation). Detailed instructions for these tasks will be explained beforehand. During these tasks, the participants will also be asked to fill in a short questionnaire about their mental state. Prior to these tasks, informed consent will be asked of the participants and a brief demographics and basic health check questionnaire will have to be filled in, to make sure no unnecessary risks are taken during the experiment. All these forms are appended below.

Note: the informed consent form will be customised and will contain mention of all the biosensors the participants agreed to prior to participation.

Once the calibration tasks are performed and the custom personalized models are built, the Human-Computer Interaction tool will be ready for (repeated) use in the actual Impetus pilot evaluations, where the tools developed in Impetus will be used in (simulated) exercises. In these pilots, each participant will wear the same biosensors they agreed to and have worn during the calibration tasks. The decision about which sensors will be used by whom, will be taken in advance, and a specific questionnaire about them has (by the time of this writing) been distributed among the operators participating in the Impetus partner cities Oslo and Padova.

Both the calibration tasks and the pilots will be performed locally, in the setting where the operator perform their daily tasks.

COVID-19

In order to perform all tasks described in this document safely and with minimal risks, given the COVID-19 threat (and as long as it continues), the following measures are incorporated in all the procedures:

- Before any experiment / test, a “viral health safety checklist” will be filled in (and signed) by all people present, to ascertain everyone is free of COVID-19 symptoms and has taken the required precautions.
- A minimum of 1,5 meters interpersonal distance will be observed by all participating Thales staff.
- All Thales staff will wear face masks during the calibration tasks and further experiments.
- Participants will be instructed (and verbally assisted) in how to put on and take off all the wearable biosensors by themselves, to minimize any close contact.
- All equipment used will be sanitised before and after each use, by the Thales staff.

In case there are other or additional rules that apply locally, these will of course be observed and incorporated in the workflow.

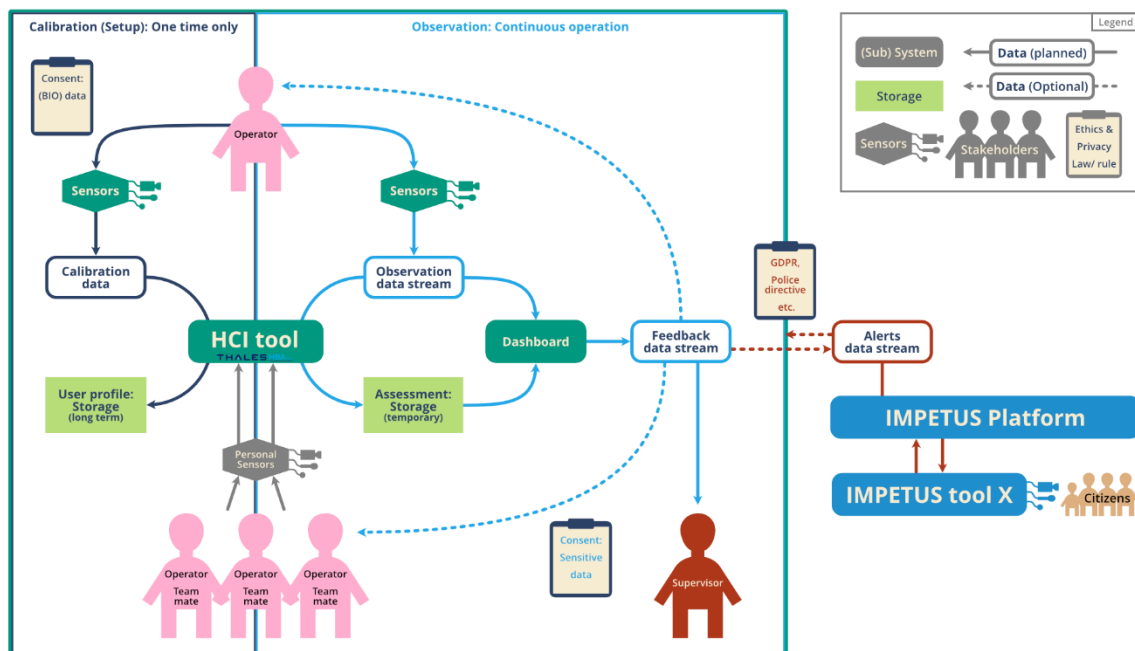
Data management

Sensitive data

Biosensor data and some personal health information will be collected in the course of the Impetus project in order to enable the use of the Human Interaction Tool. The use of this data will be strictly limited to the Impetus project and access to this data limited to a limited number of Thales personnel participating in the Impetus project. Informed consent forms will be securely stored digitally and kept for future reference. All other sensitive data will be destroyed after the end of Impetus project. No communication of the biodata collected (streamed) during the use of the Human Interaction Tool is necessary, as the system is a stand-alone solution and does not require external (internet) connections.

Any communication between the Tool and other Impetus tools provided by Impetus partners, will only exchange the processed result (i.e., the assessment) and no other sensitive data.

Specific data management plan will be provided on a case-by-case basis. Local rules and regulations will be taken into account.



Graphical summary of data flow of the HCI tool. Dashboard refers to the DAU GUI.

Appendix A: Forms

Participant demographic and health questionnaire.

This form will have to be filled in on the day of the experiment, but please read it now. If you have any objections and wish not to consent to the rules described here, please let us know ahead of time, so we can reschedule the experiment with another participant. Thank you.

General information

1. What is your name?
.....
2. What is your age?
.....
3. What is your gender?
 - ☐ Female
 - ☐ Male
 - ☐ I'd rather not say
4. How good are you at English?
 - ☐ Beginner
 - ☐ Intermediate
 - ☐ Advanced
 - ☐ Native speaker
5. You are:
 - ☐ Right-handed
 - ☐ Left-handed
 - ☐ Ambidextrous

Health related information

1. Do you have or have you had a neurologic condition (like Epilepsy) or a heart condition (like a pacemaker)?
 - ☐ No
 - ☐ Yes. Please specify:
2. Do you have any diagnosed psychiatric disorder(s)?
 - ☐ No
 - ☐ Yes
3. Have you had any major head trauma?
 - ☐ No
 - ☐ Yes
4. During last two weeks, have you consumed any drugs that affect the Central Nervous System (like benzodiazepines, antidepressants, anticonvulsants or narcotics)?
 - ☐ No
 - ☐ Yes
5. Have you consumed any alcohol in the last 24 hours?
 - ☐ No
 - ☐ Yes
6. Are you or do you think you are pregnant at this moment?
 - ☐ No
 - ☐ Yes

.....
Name of participant (printed),

.....
Signature,

.....
Date

Informed Consent Form

YOU WILL BE GIVEN A (DIGITAL) COPY OF THIS INFORMED CONSENT FORM

Please tick the appropriate boxes

Yes No

Taking part in the pilot

I have read and understood the pilot information sheet, or it has been read to me. I have been able to ask questions about the pilot and my questions have been answered to my satisfaction. ☐ Yes ☐ No

I consent voluntarily to be a participant in this pilot and understand that I can refuse to answer questions and I can withdraw from the pilot at any time, without having to give a reason. ☐ Yes ☐ No

I understand that taking part in the pilot involves collecting my behavioural, physiological and neurological data using wearable sensors, a webcam and a questionnaire I will have to fill in. I further understand how the recorded data will be stored and processed, as described in the information sheet. ☐ Yes ☐ No

Use of the information in the pilot

I understand that information I provide will be used for internal evaluation and validation of algorithms by the Thales/HBA-Lab researchers and only anonymised data will be stored and possibly used in further research or shared with other researchers. ☐ Yes ☐ No

I understand that personal information collected about me that can identify me, such as my name, will not be shared beyond the pilot team. ☐ Yes ☐ No

Consent to be audio/video recorded or photographed (optional)

I agree to be audio/video recorded during the pilot, for documentation purposes. ☐ Yes ☐ No

Signatures

Name of participant (printed)

Signature

Date

I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

Researcher name (printed)

Signature

Date

Appendix B: Sensors

The various (wearable) biosensors used for the workload assessment are described and depicted here.

(1) EEG (brain waves) sensor headband. Worn on your head, rests over/behind your ears. This sensor can be worn in combination with glasses.



(2, 3) PPG (heart pulse) and EDA (sweat) sensors. These two sensors are combined in one lightweight casing (2a) which can be worn on the wrist forearm. It is secured by an adjustable elastic band, so can be easily worn over any clothing.



The two sweat-sensing electrodes (2b) are secured to the skin by Velcro tape and are worn usually on two digits of the hand, for an optimal signal quality. Alternative locations are possible if required (like around the ankle), depending on user preference.

The pulse sensor measuring the heartbeat (3) can either be attached to the top of a finger or to the earlobe, like a clip, placing it conveniently out of the way.

Other sensors not depicted here are optional and may be used in later studies / tests during the Impetus project.

One such sensor is an eye tracker, which can be either a small bar attached to the monitor, or built in special goggles, which can be worn over normal glasses in most cases.

Another sensor is the fNIR, which measures blood flow in the brain. This sensor can vary in size and complexity and can be built in a flexible head band.

In addition to the (wearable) biosensors, the so called ambient sensors can be used. These are housed in a small package and contain temperature and noise level sensors, measuring these in the room where the operators are working.



IMPETUS

[draft version]

Prelude-ELK - User Manual



Institut Mines-Télécom

General Information	2
Overview	2
What is a SIEM?	2
What is Prelude?	2
What is ELK?	3
Collection and analysis of data	3
Correlation of alerts	3
Installation of the Prelude-ELK demonstrator	4
Prewikka Dashboards	6
Overview	6
Content of the dashboards	8
Menu bar alerts	8
Menu bar admin	8
General - Alerts	9
Content - Alerts details	11
General - Threats	11
Content - Threat details	13
General - Heartbeats	14
Content - Heartbeat details	14
General - Agents	15
General - Aggregated alerts	17
General - Aggregated threats	18
General - Aggregated heartbeats	19
Content - Heartbeats analysis	20
Kibana Dashboards	20
Overview	21
Content of the dashboards	22
Menu bar	22
General - Table of logs	22
General - Discover dashboard	24
Content - Goal graphic of logs	25
Conclusion	29

General Information

Overview

The objective of this manual is to show the main capabilities of the Prelude-ELK SIEM in the following two use cases:

- Monitoring an organization network to detect attacks and incidents in order to alert the cybersecurity experts of Padova and Oslo cities.

Data sources in these use cases are:

Use case	Data sources
Padova	Simulated network system
	Network system
Oslo	Simulated network system
	Network system

What is a SIEM?

A Security Information and Event Management (SIEM) system is composed of monitoring software for the analysis and management of events created by cybersecurity tools (e.g., log events created from antivirus tools, network firewalls and intrusion detection systems). The processed events are stored and managed as cybersecurity alerts.

What is Prelude?

Prelude is a SIEM that collects and centralizes the security information of an organization to offer a central point of control. It provides analysis and correlation of cybersecurity logs and triggers alerts about cyberattack attempts in real-time. Under the scope of the IMPETUS project, we will use the open-source (freeware) version of the Prelude SIEM, Prelude OSS, available at <https://www.prelude-siem.org/> (GPLv2 version of <https://www.prelude-siem.com/>). Hereinafter, we will refer to Prelude OSS as Prelude, for simplicity reasons.

What is ELK?

Under the scope of the IMPETUS project, we will use a version of Prelude extended with ELK, which is an abbreviation for three open source projects, namely Elasticsearch, Logstash et Kibana. Hereinafter, we will refer to Prelude-ELK to Prelude+ELK, for simplicity reasons.

Elasticsearch allows indexing and processing unstructured data. It provides a distributed web interface to access the resulting information. Logstash is the parsing engine associated with Elasticsearch for collecting, analyzing, and storing logs. It can integrate many sources simultaneously. Finally, Kibana is a data visualization platform that provides visualization functionalities on indexed content in Elasticsearch. Users can create dashboards with charts and maps of large volumes of data.

Collection and analysis of data

The addition of ELK into Prelude allows the injection and visualization of third party logs, received from both system and network components, via TCP/IP messages.

The collection of data can still be combined with the traditional collection and visualization tools of Prelude. For instance, we can keep using Prelude's LML (Log Monitoring Lackey) and third party sensors, in order to monitor and process syslog messages generated from different hosts on heterogeneous platforms. LML has two main operation modes:

- Watching log files on the host where it is running (e.g., Syslog data feeds).
- Receiving UDP Syslog messages from other hosts on the network.

In addition, any other third party sensors (e.g., Suricata and Snort) can still be registered into Prelude-ELK, following the steps below:

1. Allocating a unique identity for the sensor.
2. Creating a directory to be used by the sensor.
3. Registering to a remote manager, e.g., via signed X509 certificates (to allow secure communication between sensors and managers).

The agent registration process is directed by a single tool, prelude-admin, using the following command-line steps:

```
$ prelude-admin register <profile name> <requested permission> <manager address> --uid  
<uid> --gid <gid>
```

Correlation of alerts

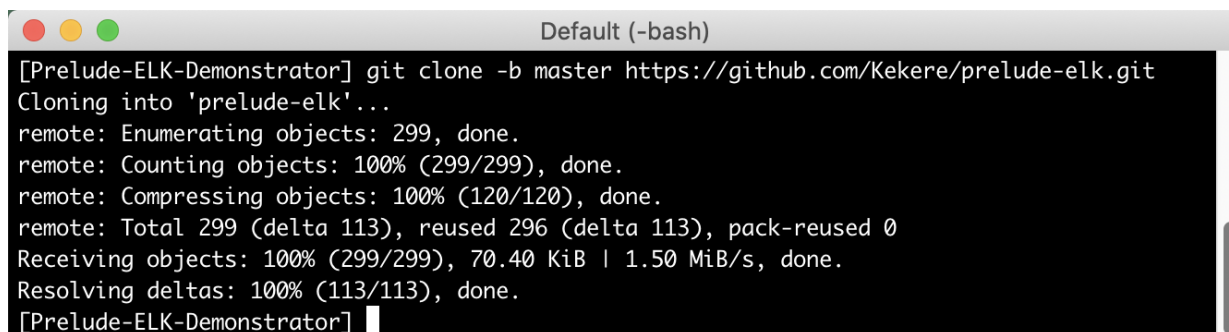
The configuration of LML and third-party sensors allows Prelude-ELK to generate alerts reporting the exploitation of vulnerabilities. Later on, a Python script (named prelude-correlator) provides Prelude-ELK with a rule-based correlation engine that connects and fetches alerts from other sensors or managers, providing new alerts (with a higher degree of information, i.e., with information about coordination attacks).

Installation of the Prelude-ELK demonstrator

We show next the installation of a dockerized version of Prelude-ELK.

1. Clone the repository using the following command-line step:

```
$ git clone -b master https://github.com/Kekere/prelude-elk.git
```



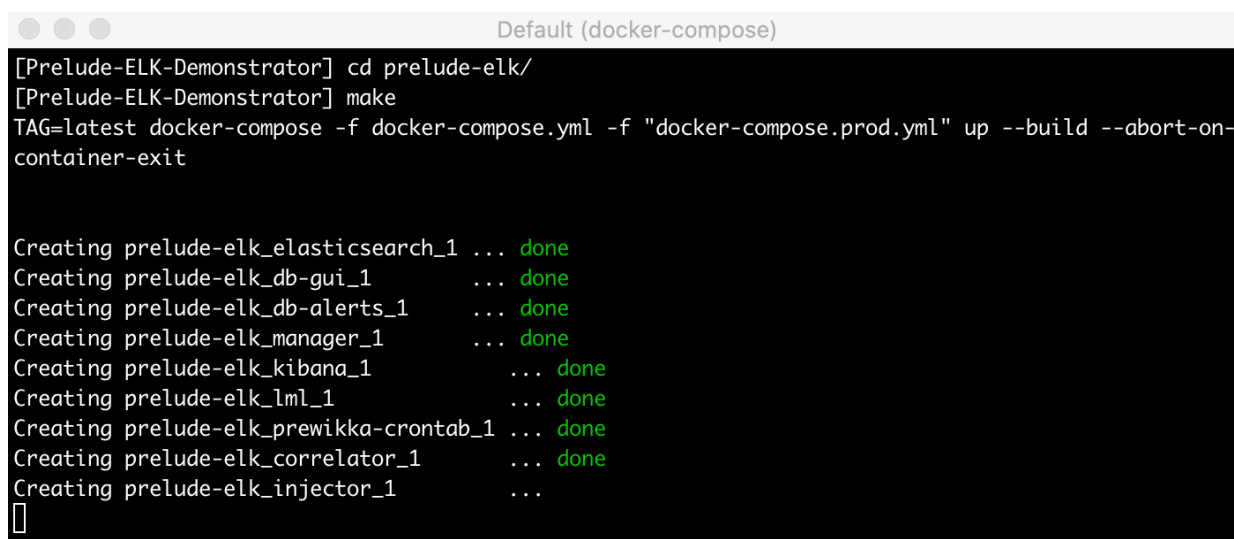
```

Default (-bash)
[Prelude-ELK-Demonstrator] git clone -b master https://github.com/Kekere/prelude-elk.git
Cloning into 'prelude-elk'...
remote: Enumerating objects: 299, done.
remote: Counting objects: 100% (299/299), done.
remote: Compressing objects: 100% (120/120), done.
remote: Total 299 (delta 113), reused 296 (delta 113), pack-reused 0
Receiving objects: 100% (299/299), 70.40 KiB | 1.50 MiB/s, done.
Resolving deltas: 100% (113/113), done.
[Prelude-ELK-Demonstrator]

```

2. Go to the newly created folder and type “make” to build the demonstrator:

```
$ cd prelude-elk/; make
```



```

Default (docker-compose)
[Prelude-ELK-Demonstrator] cd prelude-elk/
[Prelude-ELK-Demonstrator] make
TAG=latest docker-compose -f docker-compose.yml -f "docker-compose.prod.yml" up --build --abort-on-container-exit

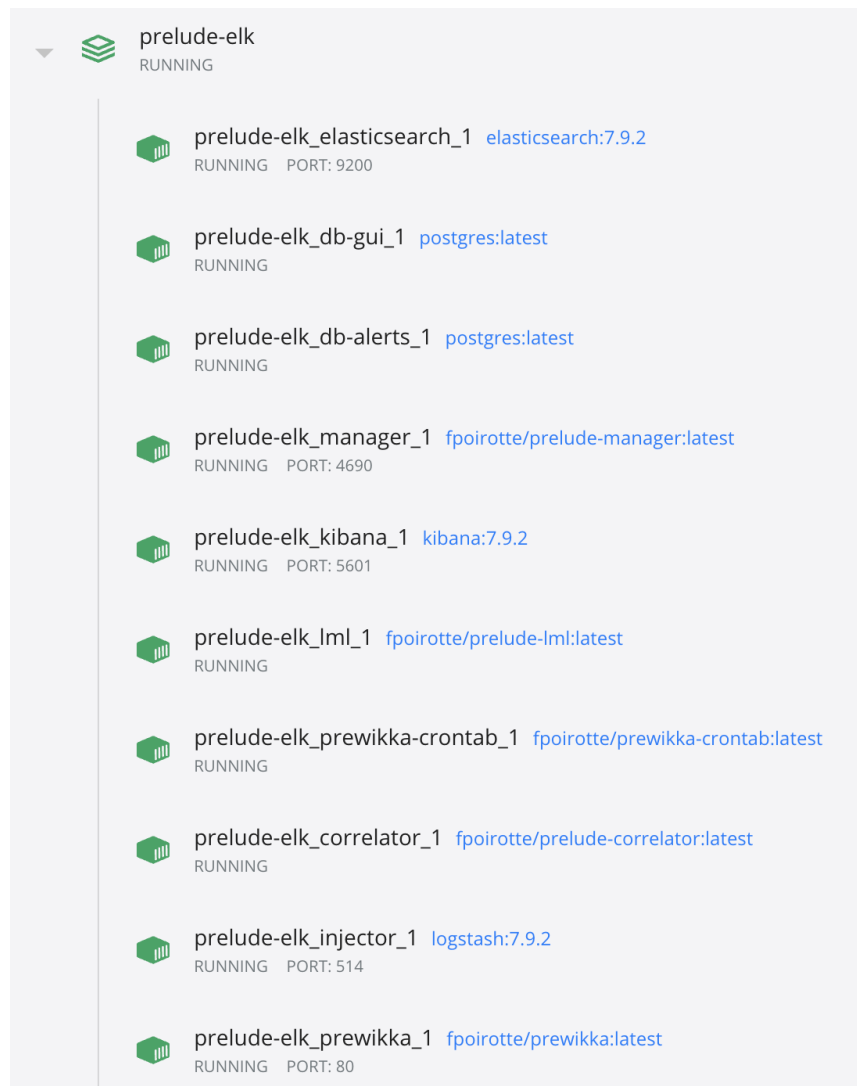
Creating prelude-elk_elasticsearch_1 ... done
Creating prelude-elk_db-gui_1 ... done
Creating prelude-elk_db-alerts_1 ... done
Creating prelude-elk_manager_1 ... done
Creating prelude-elk_kibana_1 ... done
Creating prelude-elk_lml_1 ... done
Creating prelude-elk_prewikka-crontab_1 ... done
Creating prelude-elk_correlator_1 ... done
Creating prelude-elk_injector_1 ...

```

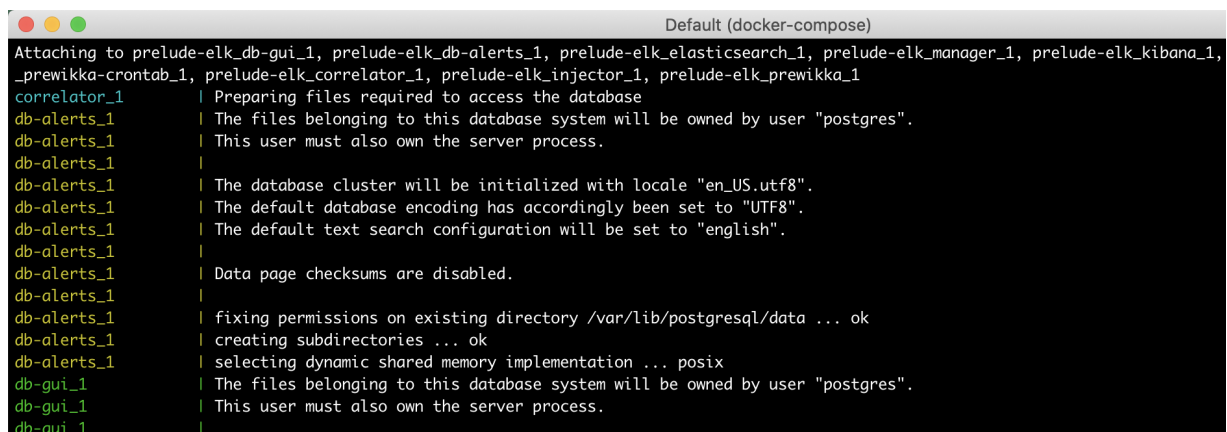
The following containers are created during the installation process:

- prewikka: Prelude's web user interface
- prewikka-crontab: periodic scheduler used by prewikka
- manager: Prelude's manager
- kibana: ELK's data visualization
- elasticsearch: ELK's log storage
- correlator: alert correlator
- injector: entrypoint for logs
- lml: Prelude's log management servant
- db-alerts: database server for Prelude's alerts
- db-gui: database server for Prewikka

The containers can be displayed and managed using graphical user interfaces such as Docker Desktop for Windows or macOS, as shown next:



The following two screenshots illustrate the startup process of the dockerized version of Prelude-ELK on macOS:



```
Default (docker-compose)
tified by the Kibana UUID: 422264b7-f04e-4537-87bf-00eb98ab671d"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["info","plugins","watcher"],"pid":9,"message":"Your basic license does not support w
atcher. Please upgrade your license."}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["info","plugins","crossClusterReplication"],"pid":9,"message":"Your basic license do
es not support crossClusterReplication. Please upgrade your license."}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["info","plugins","monitoring","monitoring","kibana-monitoring"],"pid":9,"message":"S
tarting monitoring stats collection"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:kibana@7.9.2","info"],"pid":9,"state":"green","message":"Status cha
nged from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:elasticsearch@7.9.2","info"],"pid":9,"state":"yellow","message":"St
atus changed from uninitialized to yellow - Waiting for Elasticsearch","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:elasticsearch@7.9.2","info"],"pid":9,"state":"green","message":"Sta
tus changed from yellow to green - Ready","prevState":"yellow","prevMsg":"Waiting for Elasticsearch"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:xpack_main@7.9.2","info"],"pid":9,"state":"green","message":"Status
changed from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:monitoring@7.9.2","info"],"pid":9,"state":"green","message":"Status
changed from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:spaces@7.9.2","info"],"pid":9,"state":"green","message":"Status cha
nged from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:security@7.9.2","info"],"pid":9,"state":"green","message":"Status c
hanged from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:beats_management@7.9.2","info"],"pid":9,"state":"green","message":"
Status changed from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:apm_oss@7.9.2","info"],"pid":9,"state":"green","message":"Status ch
anged from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["status","plugin:console_legacy@7.9.2","info"],"pid":9,"state":"green","message":"St
atus changed from uninitialized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:40Z","tags":["listening","info"],"pid":9,"message":"Server running at http://0:5601"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:41Z","tags":["info","http","server","Kibana"],"pid":9,"message":"http server running at http://0:
5601"}
elasticsearch_1 | {"type":"server","timestamp":"2021-04-22T12:43:41.455Z","level":"INFO","component":"o.e.c.m.MetadataIndexTemplateService","cluster.nam
e":"docker-cluster","node.name":"6a1ffccdd4cd","message":"adding template [.management-beats] for index patterns [.management-beats]","cluster.uuid":"6cd5UEf
YS0eywfdelxIlog","node.id":"Vjr4QT8nTDqP4m_BWvP6A"}
kibana_1 | {"type":"log","@timestamp":"2021-04-22T12:43:41Z","tags":["warning","plugins","reporting"],"pid":9,"message":"Enabling the Chromium sandbox pr
ovides an additional layer of protection."}
```

Prewikka Dashboards

Prewikka is the official Graphical User Interface (GUI) of Prelude, for the visualization and management of the alerts. Next, we show some representative information, using a Web browser pointing out to the <http://localhost> url (i.e., prelude-elk_prewikka_1, port 80).

Overview

Alerts timeline	General	Time distribution of alerts.
	Raw data	Chart bar of alerts based on time distribution.
Threats timeline	General	Time distribution of threats.
	Raw data	Chart bar of threats based on time distribution.
Aggregated alerts	General	Alerts group by selected criteria.
	Raw data	Chart bar of alerts based on selected criteria.
Aggregated threats	General	Threats group by selected criteria.
	Raw data	Chart bar of threats based on the selected criteria;


Alerts table	Date	Time when the alert was generated.
	Classification	Type and description of the attack.
	Sources	Information about the attacker machine.
	Target	Information about the target machine.
	Analyzer	Information about the analyzer that detects the attack.
Threats table	Date	Time when the threat was detected.
	Classification	Type of the threat.
	Sources	Information about the attacker machine.
	Target	Information about the target machine.
	Program	Name of the program.
Heartbeats timeline	General	Time distribution of the heartbeats.
	Raw data	Chart bar of heartbeats based on time distribution.
Heartbeats table	Date	Time when the heartbeat is registered.
	Agent	Agents that register the heartbeat.
	Node address	Ip address of the agent;
	Node name	Identification of the heartbeat.
	Model	Name of the agent;
Agents	Alert listing	Timeline chart bar for the alerts and table listing alerts for the agent.
	Heartbeat listing	Timeline chart bar for the heartbeats and table listing heartbeats for the agent.
	Heartbeat analysis	Heartbeats information for the alerts.

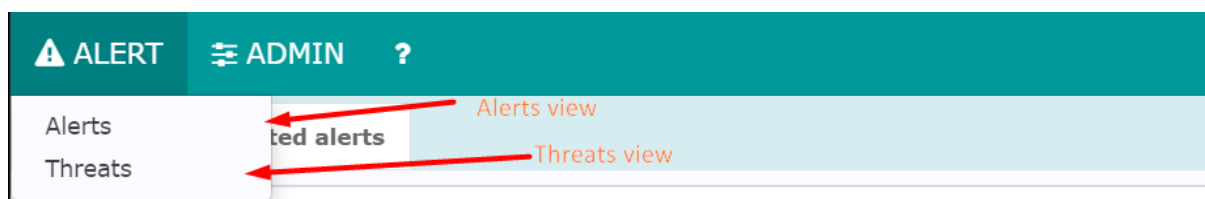
All alerts are shown in the same dashboard for the sake of simplicity including the option to group them by criteria or to search specific alerts by keywords. All threats are shown in the same dashboard for the sake of simplicity including the option to group them by criteria or to search specific alerts by keywords. All heartbeats are shown in the same dashboard for the sake of simplicity including the option to group them by criteria or to search specific alerts by keywords. All agents are shown in the same dashboard with the possibility to see the list of alerts for each agent and the heartbeats of the agents too.

Content of the dashboards

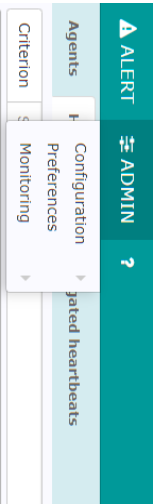
In this section we show some representative dashboards and menu options of prewikka.

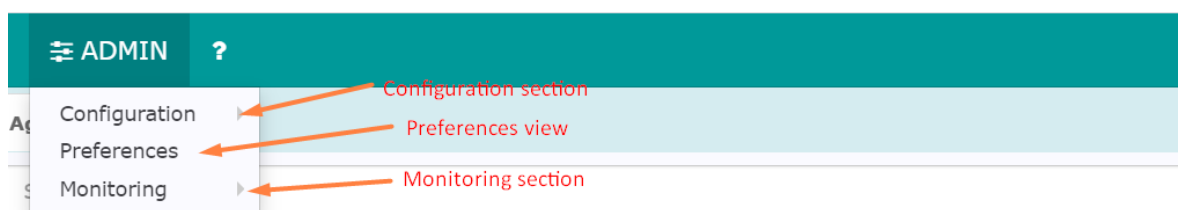
Menu bar alerts

Graph	Content	Capabilities
	Alert options	Select if you want to see the alerts dashboard or the threats dashboard.



Menu bar admin

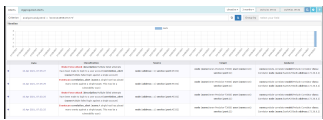
Graph	Content	Capabilities
	Admin options	<ul style="list-style-type: none"> In the configuration section, we can schedule alerts. In the preferences section, we can save a name and an email. In the monitoring section, we can access the agents dashboard, heartbeats dashboard or aggregated heartbeats dashboard.



General - Alerts

This page contains all the alerts generated on the network, in a table format. A chronologic distribution of the alerts is also shown.

It is useful for searching and filtering across all the information collected and showing them in a table format.

Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify criterion for displaying alerts table Selection area to select option to group alerts by Chart bar to visualize alerts distribution on the time Alerts table 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Alert fields (classification, source, target, analyzer)

Non sécurisé | 157.159.68.66/alerts/forensic

Applications Gmail YouTube Maps ecampus: Accueil Enriched Generatio... Adobe creative des... jgalfaro/sandbox-a...

ALERT **ADMIN** ?

Alerts Aggregated alerts 3 months 19/01/21 12:17

Criterion !source.node.name && analyzer.analyzerid = '2886253996640989' && classification.text = 'Credentials Change'

Timeline

Write criterion for listing alerts

Also include inactive alerts

Select time range for displaying alerts

Alerts


Alerts timeline based on criterion

Table of alerts based on criterion

Date	Classification	Source	Target	
22 Feb 2021, 11:44:10	Credentials Change (description:User tried to authenticate as etudiant and failed)	user (number:1000)	node (name:PCdebian) user (name:etudiant)	name:PAM
22 Feb 2021, 11:27:28	Credentials Change (description:User tried to authenticate as etudiant and failed)	user (number:1000)	node (name:PCdebian) user (name:etudiant)	name:PAM
22 Feb 2021, 10:49:45	Credentials Change (description:User tried to authenticate as etudiant and failed)	user (number:1000)	node (name:PCdebian) user (name:etudiant)	name:PAM

Content - Alerts details

Drop down section that contains detailed information about a specific alert.

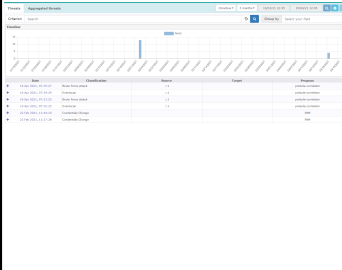
Graph	Content	Capabilities
	Detailed information about a specific alert	Additional information that does not appear in the table is shown.
Hints	Discover all details about an alert	Deploy the plus icon before the date column.

Deploy to see details of an alert

Date	Classification	Source
16 Apr 2021, 07:35:27	Brute Force attack (description:Multiple failed attempts have been made to login to a user account) correlation_alert (name:Multiple failed login against a single account)	node (address:::1) service (port:45332)
additional_data(0).data	BruteForcePlugin	
additional_data(0).meaning	Rule ID	
additional_data(0).type	string	
analyzer(0).analyzerid	2886253996640989	
analyzer(0).class	Concentrator	

General - Threats

Page contains all the threats generated on the network, in a table format. A chronologic distribution of the threats is also shown. It is useful for searching and filtering across all the information collected and showing them in a table format.

Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify criterion for displaying threats table Selection area to select option to group threats by Chart bar to visualize threats distribution on the time Threats table 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Alert fields (classification, source, target, analyzer)

ecampus: Accueil | Zimbra: Réception | User manual PRELUDE+ELK | User manual PRELUDE+ELK | Prelude - Threats | Zone étu

Non sécurisé | 157.159.68.66/threats/forensic

Applications | Gmail | YouTube | Maps | ecampus: Accueil | Enriched Generatio... | Adobe creative des... | jgalfaro/sandbox-a...

ALERT **ADMIN** ?

Threats **Aggregated threats** Also show inactive threats ☐ Inactive 3 months

Criterion: classification.text = 'Credentials Change' Show threats for this time period

Timeline

Write criterion for listing threats

Timeline threats based on criterion

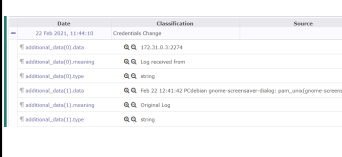
Alerts

Date	Classification	Source	Target
22 Feb 2021, 11:44:10	Credentials Change		
22 Feb 2021, 11:27:28	Credentials Change		
22 Feb 2021, 10:49:45	Credentials Change		
22 Feb 2021, 10:49:40	Credentials Change		
22 Feb 2021, 10:49:37	Credentials Change		
22 Feb 2021, 10:48:33	Credentials Change		

Table of threats based on criterion

Content - Threats details

Drop down section that contains detailed information about a specific threat.


Graph	Content	Capabilities
	Detailed information about a specific threat.	Additional information that does not appear in the table is shown.
Hints	Discover all details about a threat.	Deploy the plus icon before the date column.

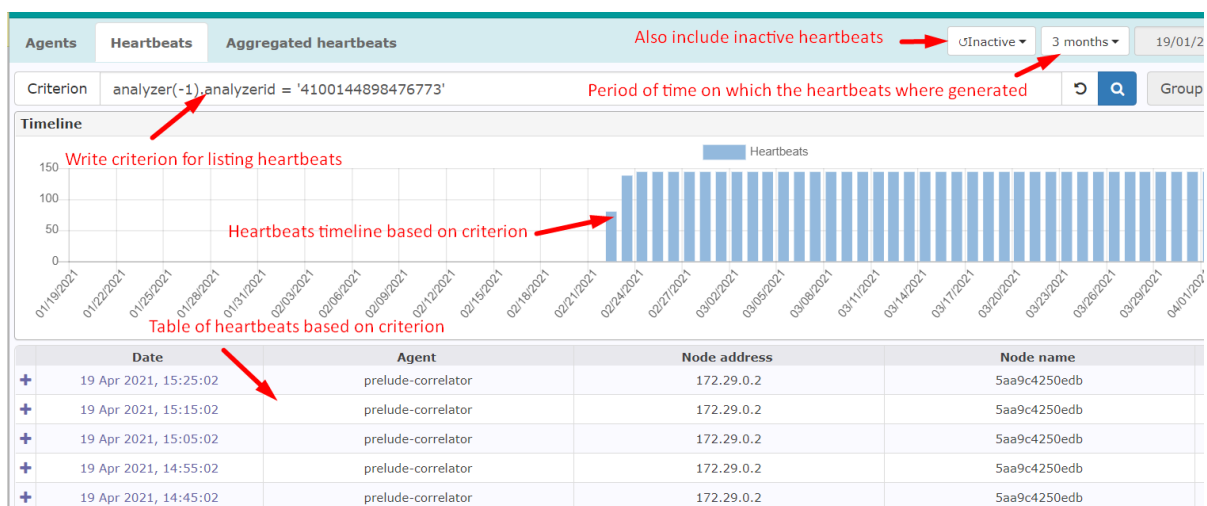
Deploy to show threat details			
	Date	Classification	
+	16 Apr 2021, 07:33:25	Brute Force attack	
-	16 Apr 2021, 07:32:25	Eventscan	
	additional_data(0).data	EventScanPlugin	
	additional_data(0).meaning	Rule ID	
	additional_data(0).type	string	
	analyzer(0).analyzerid	2886253996640989	
	analyzer(0).class	Concentrator	
	analyzer(0).manufacturer	http://www.prelude-siem.com	

General - Heartbeats

Page contains all the heartbeats generated by the agents, in a table format. A chronologic distribution of the heartbeats is also shown.

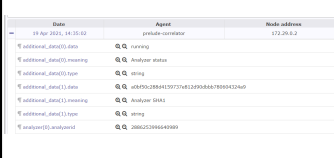
It is useful for searching and filtering across all the information collected and showing them in a table format.

Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify criterion for displaying heartbeats table Selection area to select option to group heartbeats by Chart bar to visualize heartbeats distribution on the time Heartbeats table 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Alert fields (create_time, heartbeat_interval, additional_data, messageid, analyzer)



Content - Heartbeats details

Drop down section that contains detailed information about a specific heartbeat.

Graph	Content	Capabilities
	Detailed information about a specific Heartbeat.	Additional information that does not appear in the table is shown.
Hints	Discover all details about a heartbeat.	Deploy the plus icon before the date column..

Deploy to show details of the heartbeat

Date	Agent	Node address
19 Apr 2021, 14:35:02	prelude-correlator	172.29.0.2

- additional_data(0).data: running
- additional_data(0).meaning: Analyzer status
- additional_data(0).type: string
- additional_data(1).data: a0bf50c288d4159737e812d90dbbb780604324a9
- additional_data(1).meaning: Analyzer SHA1
- additional_data(1).type: string
- analyzer(0).analyzerid: 2886253996640989

General - Agents

Raw data page contains information about the agents, in a table format.

Graph	Content	Capabilities
	Table with the alerts listed	We have the possibility to list the alerts and heartbeats for each agent. We can also visualize an analysis of heartbeat for each agent.

Hints	Discover alerts list group by agent.	Click on the agent name and click on Alerts listing option
	Discover heartbeats list group by agent.	Click on the agent name and click on Heartbeats listing option.
	Discover heartbeat analysis.	Click on the agent name and click on Heartbeat analysis.

Agents

Heartbeats

Aggregated heartbeats

0Inactive

3 months

19/01/21 15:36

19/04/21 15:36

Q

⚙

?

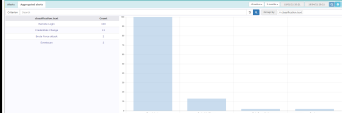
Show/Hide all

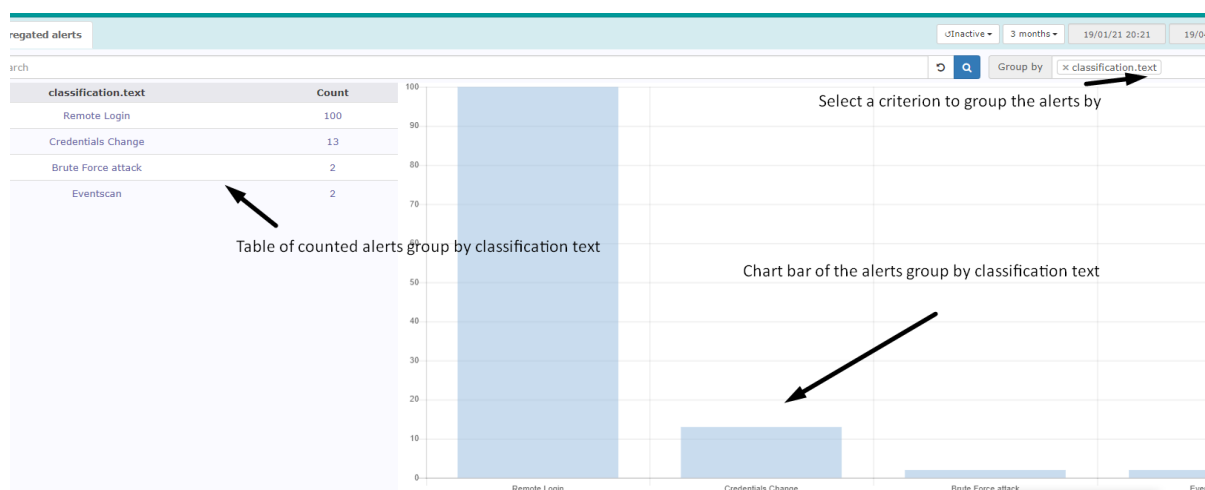
Table of agents Specify keywords for listing agents Search

<input type="checkbox"/>	Name	Model	Version	Class	Latest heartbeat	Status
Node location n/a (3 agent(s))						
0d67421333f6 - Linux 5.4.0-65-generic (1 agent(s))						
<input type="checkbox"/>	prelude-lml	Prelude LML	5.1.0	Log Analyzer	2 minutes ago	Online
26f67f3c7bfe - Linux 5.4.0-65-generic (1 agent(s))						
<input type="checkbox"/>	prelude-manager	Prelude Manager	5.1.0	Concentrator	1 minute ago	Online
5aa9c4250edb - Linux 5.4.0-65-generic (1 agent(s))						
<input type="checkbox"/>	prelude-correlator	Prelude Correlator	5.1.0	Correlator	1 minute ago	Online

General - Aggregated alerts


This page contains a table and a chart bar of the alerts counted, group by the selected option.

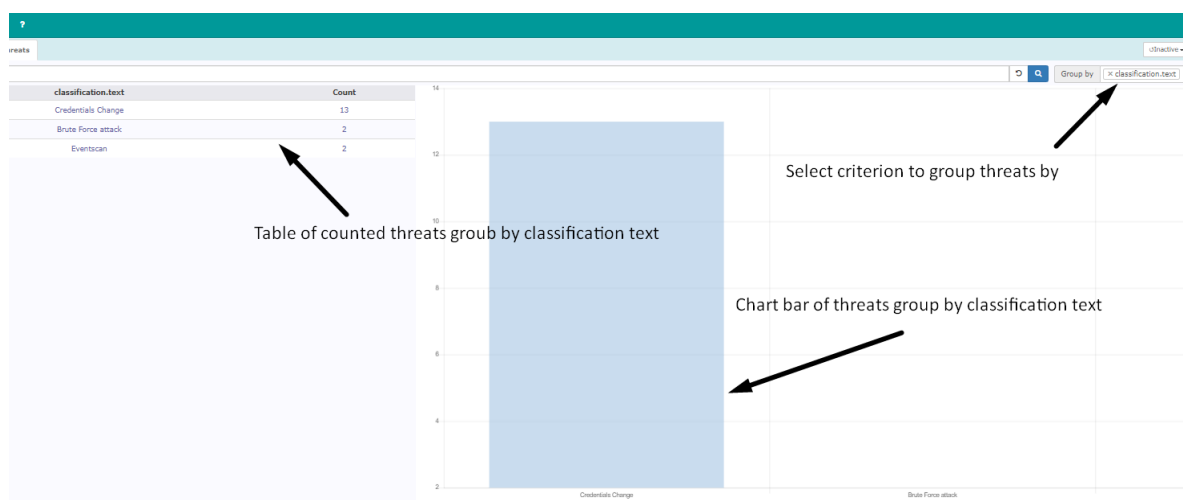
Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify filter for displaying chart bar. Selection area to select criterion to group alerts by Table with counted alerts group by filter. Chart bar of alerts grouped by criterion or filtered alerts 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Alert fields (classification, source, target, analyzer)



General - Aggregated threats

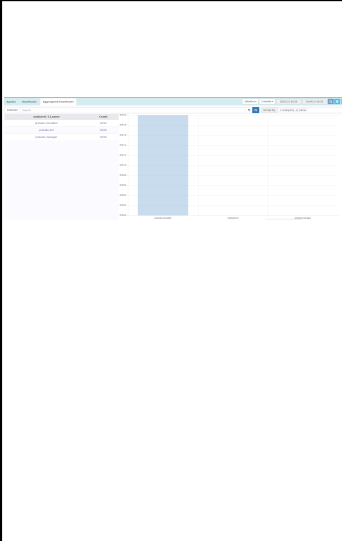
This page contains a table and a chart bar of the threats counted, group by the selected option.

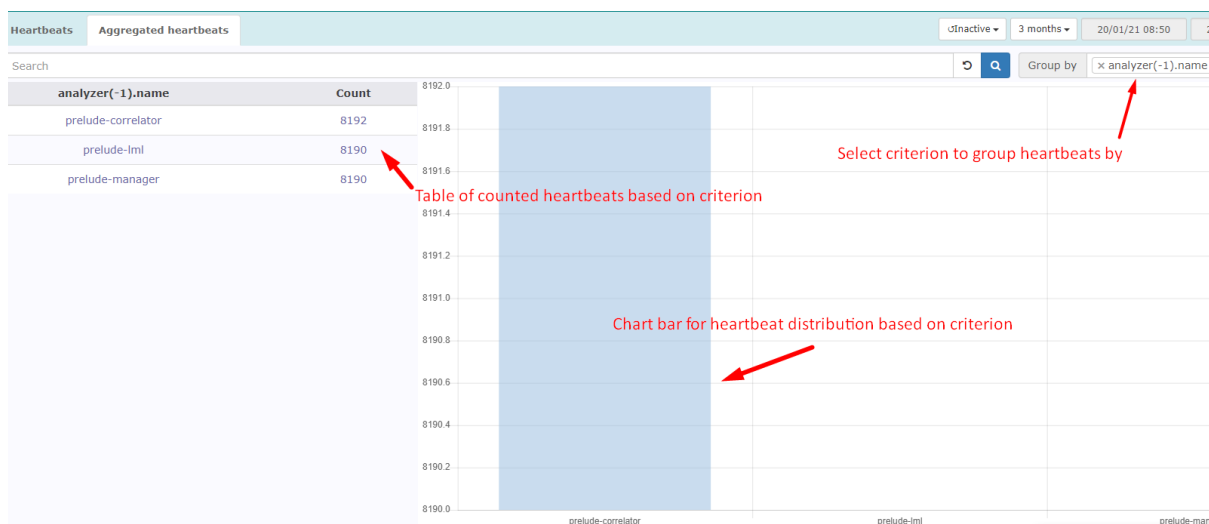
Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify filter for displaying chart bar. Selection area to select criterion to group threats by Table with counted threats group by filter. Chart bar of threats grouped by criterion or filtered threats 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Threat fields (classification, source, target, analyzer)



General - Aggregated heartbeats

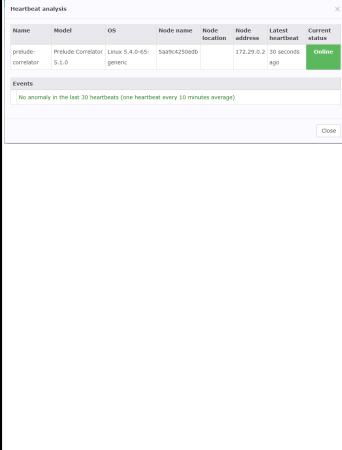
This page contains a table and a chart bar of the heartbeats counted, group by the selected option.

Graph	Content	Capabilities
	<ul style="list-style-type: none"> Search area to specify filter for displaying chart bar. Selection area to select criterion to group heartbeats by Table with counted heartbeats group by filter. Chart bar of alerts grouped by criterion or filtered heartbeats 	<p>Group by:</p> <ul style="list-style-type: none"> Time values (minute, hour, day, month, year) Heartbeat fields (classification, source, target, analyzer)



Content - Heartbeats analysis

A modal window contains an analysis of the heartbeats.

Graph	Content	Capabilities
	<ul style="list-style-type: none"> • Search area to specify filter for displaying chart bar. • Selection area to select criterion to group heartbeats by • Table with counted heartbeats group by filter. • Chart bar of alerts grouped by criterion or filtered heartbeats 	<p>Group by:</p> <ul style="list-style-type: none"> • Time values (minute, hour, day, month, year) • Heartbeat fields (classification, source, target, analyzer)

Heartbeat analysis							
Table contening information about heartbeat analysis							
Name	Model	OS	Node name	Node location	Node address	Latest heartbeat	Current status
prelude-correlator	Prelude Correlator 5.1.0	Linux 5.4.0-65-generic	5aa9c4250edb		172.29.0.2	30 seconds ago	Online
Events							
No anomaly in the last 30 heartbeats (one heartbeat every 10 minutes average)							
Close							

Kibana Dashboards

Kibana is the official Graphical User Interface (GUI) of the ELK stack, for the visualization and management of the Elasticsearch indexes. Next, we show some representative information, using a Web browser pointing out to the <http://localhost:5601> url (i.e., prelude-elk_kibana_1, port 5601).

Overview

Table of logs	Name	Name field
	Type	Type of data
	Format	Format data (it is empty)
	Searchable	Indicate if the field is searchable.
	Aggregatable	Indicate if the field is aggregatable.
	Excluded	Indicate if the field is excluded.
Discover dashboard	Chart bar	Chart of the logs counted ,group by the time metric specified in the select area.
	Table of logs	Table with all the logs.
	Filter areas	Filter by: <ul style="list-style-type: none"> • message • received_at • received_from • syslog_message • etc
Goal visualization of logs	Filter areas	Filter by: <ul style="list-style-type: none"> • message • received_at • received_from • syslog_message • etc
	Goal graphic	Visualize logs counted in a goal graphic format.
	Graphic functionalities options	The style of the graphic can be changed. The metric can also be changed; count can be changed for average.

Content of the dashboards

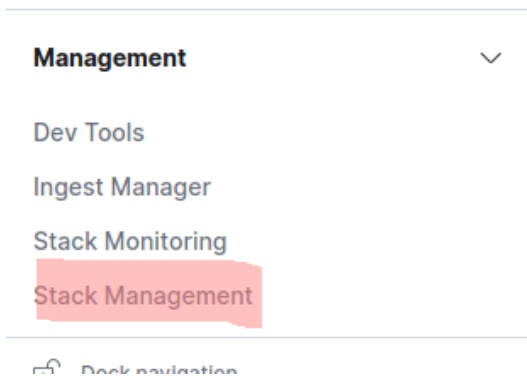
Menu bar

Click on the deployment icon to deploy the menu.

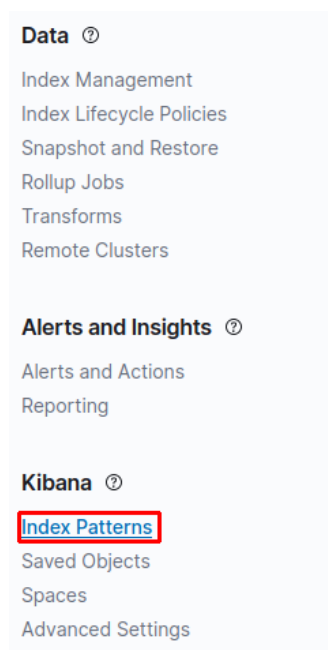


General - Table of logs

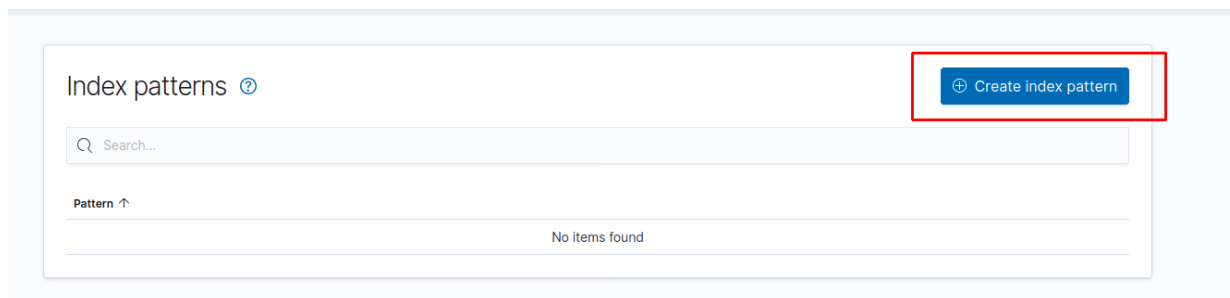
Click on the Stack Management subsection in the Management section to have access to the management menu.



Click on the Index Patterns subsection in the Kibana section to have access to the list of index patterns and to create new index patterns.



Click on the blue button to create a new index pattern.



Index patterns ?

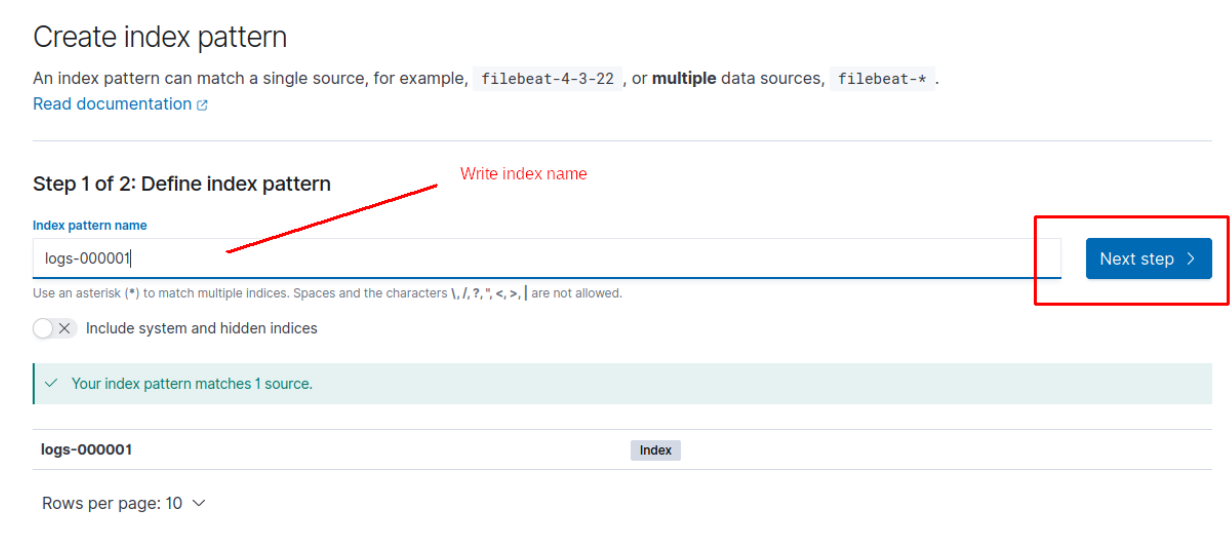
Search...

Pattern ↑

No items found

Create index pattern

If the index exists in Elasticsearch, click on the blue button to go to the next step.



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 1 of 2: Define index pattern

Write index name

Index pattern name

logs-000001

Use an asterisk (*) to match multiple indices. Spaces and the characters `\,/,?,",<,>|` are not allowed.

☒ Include system and hidden indices

✓ Your index pattern matches 1 source.

logs-000001	Index

Rows per page: 10

Next step >

Choose a time field in the select area as the primary time field.



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 2 of 2: Configure settings

logs-000001

Select a primary time field for use with the global time filter.

Choose time field

Time field

Refresh

> Show advanced options

< Back Create index pattern

A table will be shown with the name fields and their characteristics.

★ logs-000001 ★ 🔄 🗑️

Time Filter field name: 'received_at' Default

This page lists every field in the **logs-000001** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#).

[Fields \(29\)](#) [Scripted fields \(0\)](#) [Source filters \(0\)](#)

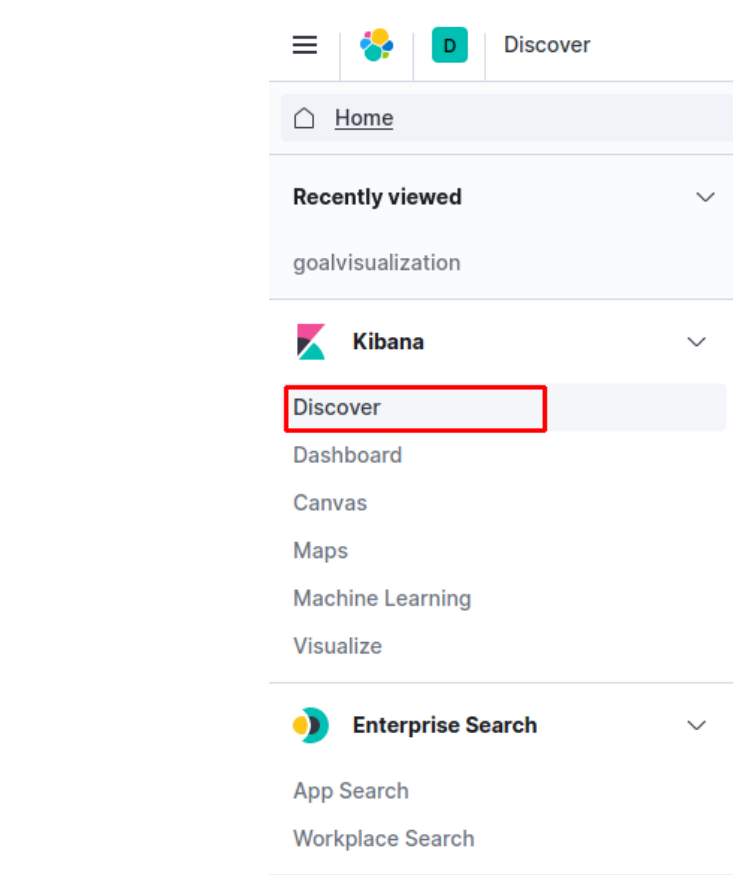
🔍 Search All field types ▾

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	
@version	string		•	•	
_id	string		•	•	
_index	string		•	•	
_score	number				
_source	_source				
_type	string		•	•	
geoip.ip	ip		•	•	
geoip.latitude	number		•	•	
geoip.location	geo_point		•	•	

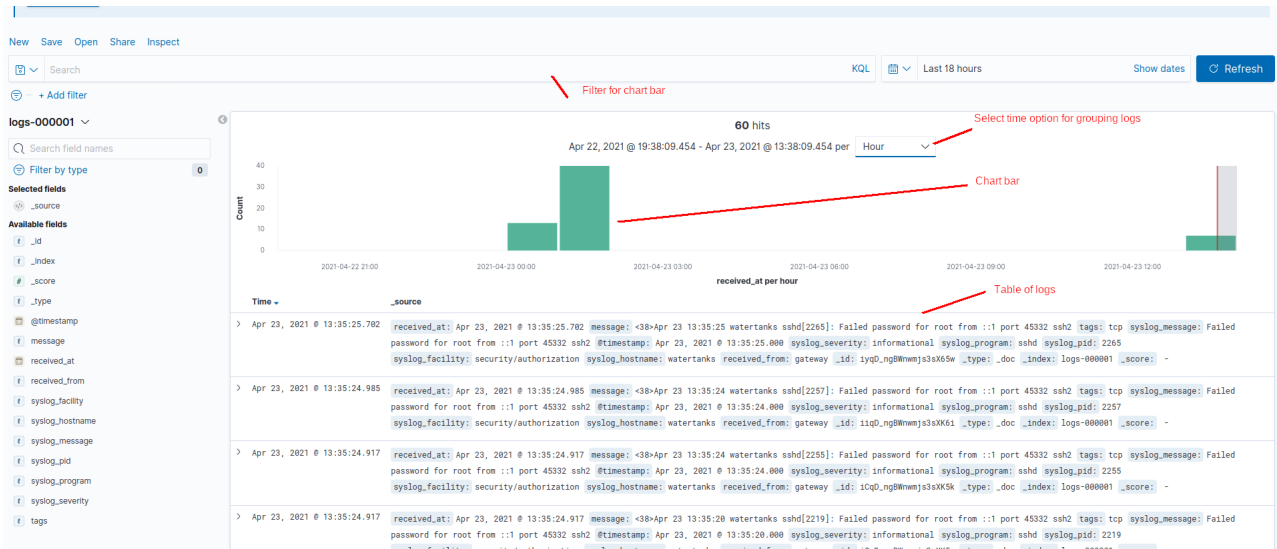
Rows per page: 10 ▾ < 1 2 3 >

General - Discover dashboard

Click on the Discover subsection in the Kibana section.

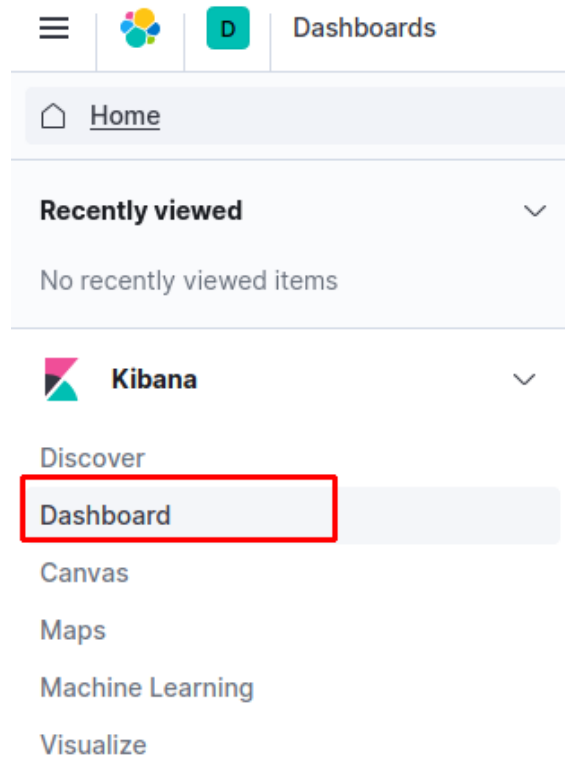


In the Discover dashboard, a chart bar of the counted logs group by the time metric selected is shown. A table with all the details of the logs is also shown. There are filter areas to search for specific logs. The available fields are listed in the left.

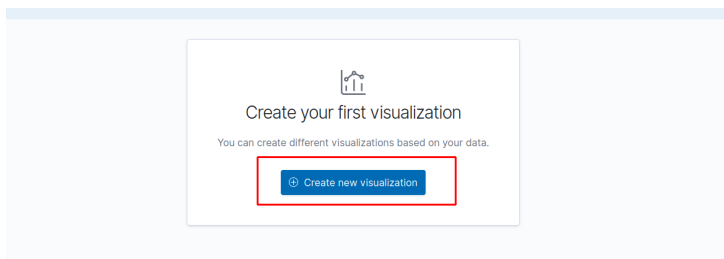


General - Goal graphic of logs

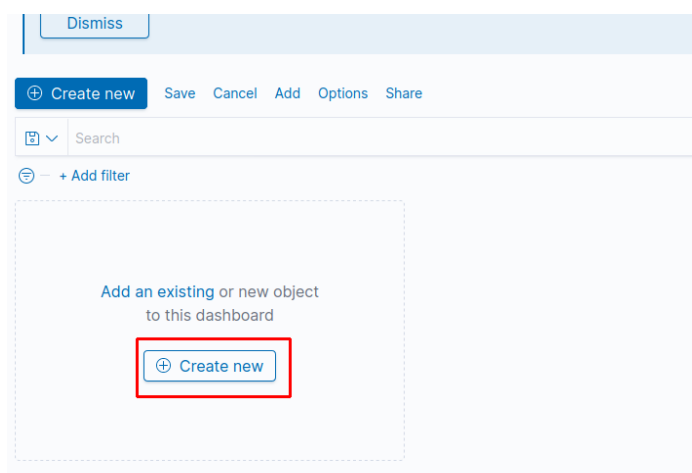
Click on the Dashboard subsection in the Kibana section.



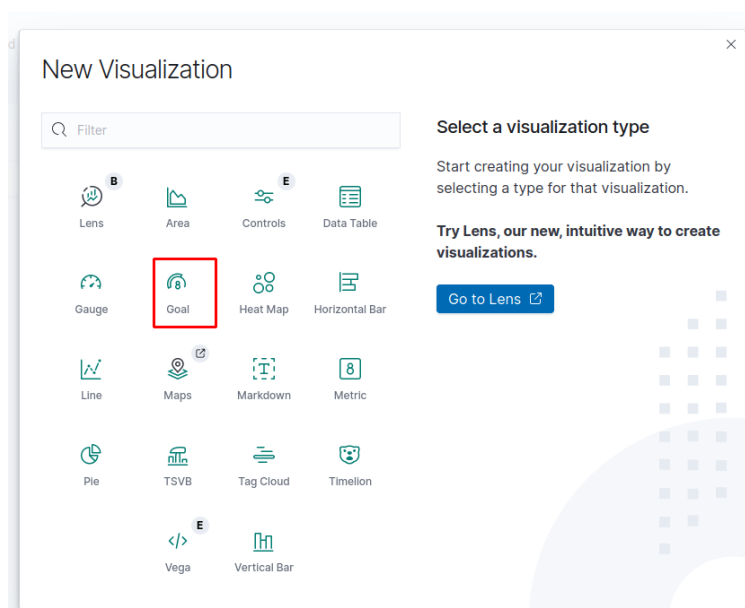
Click on the blue button to create a new visualization.



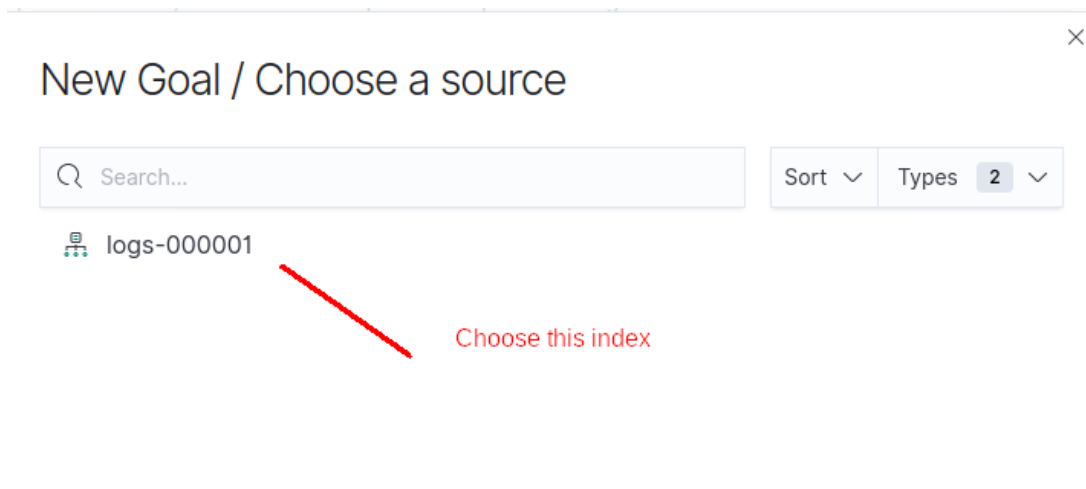
If you have already saved a visualization, you can click on Add an existing, if not click on the create new button to create a new one.



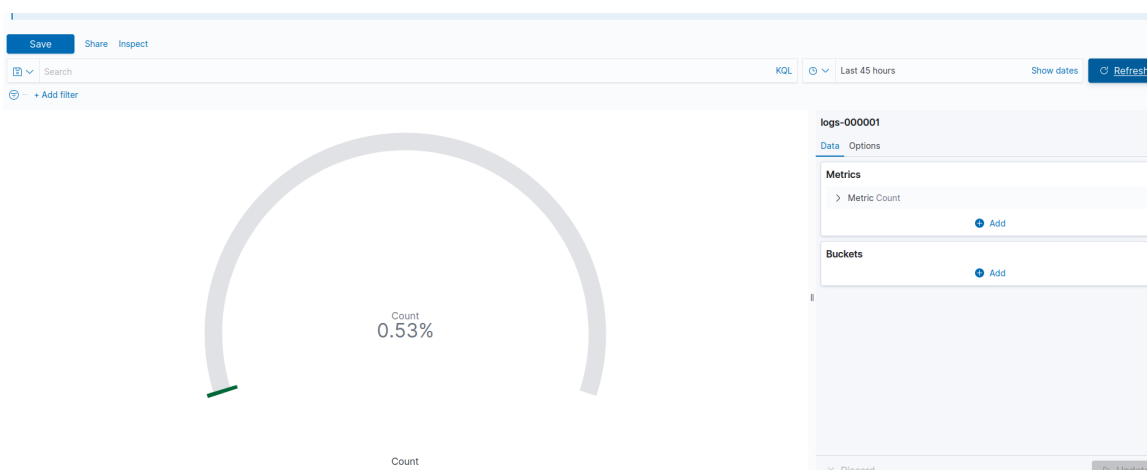
Choose the type of visualization.



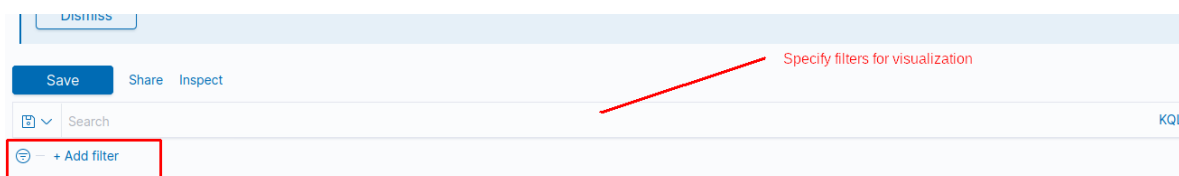
Choose an index to create visualization on.



The dashboard is created, some options are available to customize it.



You can select filters to visualize the graphic only for a category of logs.



Select the time interval in which the logs that will be represented were generated.

Select time interval of the logs

⌚

Last 45 hours

Show dates

Refresh

Select the metric for the graphic representation of the logs.

Metrics

▼ Metric

Aggregation Count help

Count | ▼

Metric Aggregations

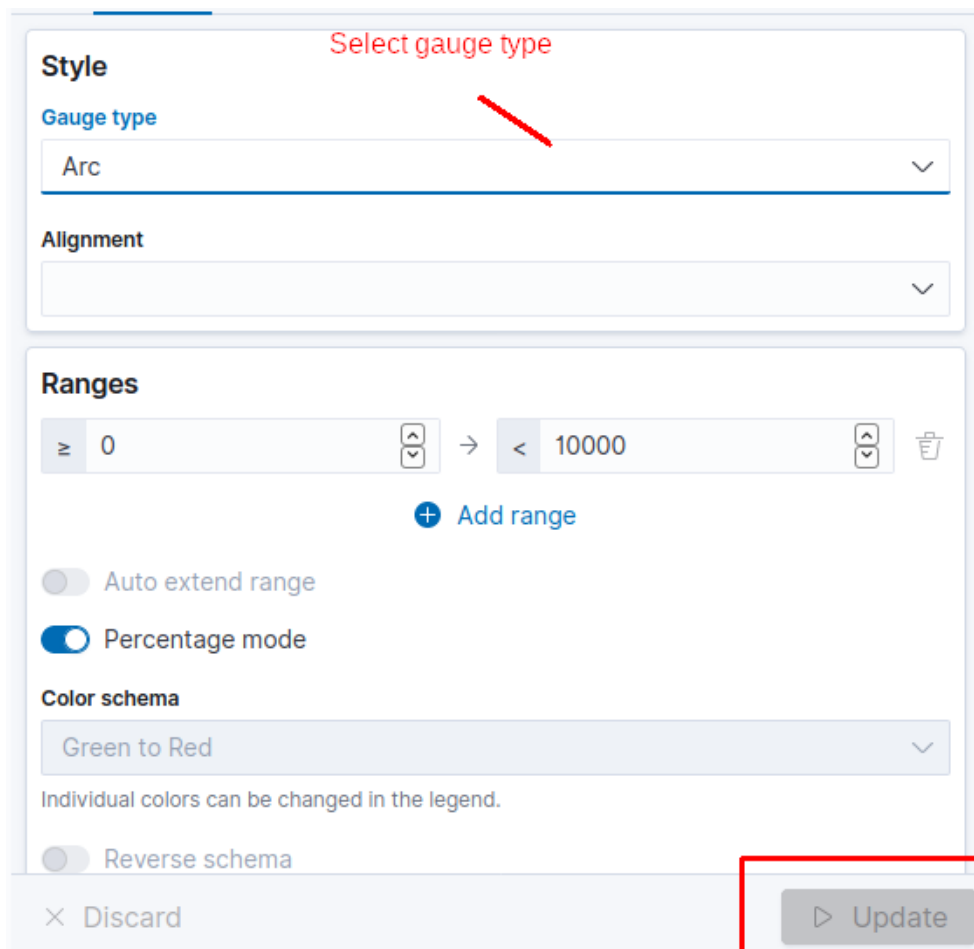
- Average
- ✓ Count
- Max
- Median
- Min
- Sum

Buckets

+ Add

× Discard Update

Select the style for the goal graphic representation of the logs.



Style

Select gauge type

Gauge type

Arc

Alignment

Ranges

≥ 0 → < 10000

+ Add range

☐ Auto extend range

☒ Percentage mode

Color schema

Green to Red

Individual colors can be changed in the legend.

☐ Reverse schema

× Discard Update

Conclusion

Prelude is used to generate alerts with the logs received from components of the organization's network. A graphical representation of the distribution of logs is possible on Prewikka, the graphic interface of Prelude. Correlation of alerts is also possible with Prelude. They can also be displayed graphically using Prewikka. In addition, the ELK stack allows Prelude to create additional dashboards for deeper analysis of threats and countermeasures.