Artificial Intelligence Threat Reporting and Incident Response System

D6.1 APIs and data models for the integration of smart city's infrastructure with the IRIS platform

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	D6.1
Deliverable Due Date:	31/10/2023
Deliverable Submission Date:	31/10/2023
Deliverable Version:	1.0
Main author(s) and Organisation:	Vasiliki-Georgia (Giovana) Bilali, Eustratios Magklaris, Lazaros Karagiannidis, Athanasios Douklias, Eleftherios Ouzounoglou (ICCS) Dimitrios Skias, Sophia Tsekeridou (INTRA) Bruno Vidalenc (THALES) Susana Gonzalez Zarsoza (ATOS) Xavier Azemar (CISCO)

	Nathan Hue, Irene Karapistoli, Shenba Gomathi (CLS) Theocharis Saoulidis, Zisis Batzos (SID) Bardin Sebastien (CEA) Eleni Darra, Angelos Papoutsis, Dimitris Kavallieros, Thodora Tsikrika (CERTH) Andrew James Roberts (TALTECH), René Serral (UPC), (IMI BCN), Nikita Akmaikin (FVH)
Work Package:	WP6 IRIS Platform Integration and Testing
Task:	Task 6.1 APIs for integration with the smart city's IoT- and AI-enabled infrastructures
Dissemination Level:	PU: Public

Quality Control

	Name	Organisation	Date
Editor	Vasiliki-Georgia Bilali, Eustratios Magklaris	ICCS	26/10/2023
Peer Review 1	Theocharis Saoulidis, Zisis Batzos	SID	16/10/2023
Peer Review 2	Roland Kromes	TUD	16/10/2023
Submitted by (Project Coordinator)	Gonçalo Cadete	INOV	31/10/2023

Contributors

Organization
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)
INTRASOFT INTERNATIONAL SA (INTRA)
THALES SIX GTS FRANCE SAS (THALES)
ATOS IT SOLUTIONS AND SERVICES IBERIA SL (ATOS)
CISCO SYSTEMS SPAIN S.L. (CISCO SPAIN)
CYBERLENS B.V. (CLS)
SIDROCO HOLDINGS LIMITED (SID)
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH)
TALLINNA TEHNIKAÜLIKOOL (TALTECH)
UNIVERSITAT POLITECNICA DE CATALUNYA (UPC)
INSTITUT MUNICIPAL D'INFORMATICA DE BARCELONA (IMI BCN)
FORUM VIRIUM HELSINKI OY (FVH)

Document History

Version	Date	Modification	Partner
V.01	01/02/2023	Creation of ToC	ICCS
V.02	15/03/2023	Receive input for Section 2, 4 and Annex	ATA owners, PUC leaders
V.03	11/4/2023	Initial input in Section 1, 2, 3, 4, 5	ICCS
V.04	20/4/2023	Request for feedback and input in Section 2, 4, 6	All
V.05	1/6/2023	Compilation of partners input/feedback in Section 1, 2, 4,6	ICCS
V.06	14/9/2023	Consolidation of partners input, in Section 3, 4	ICCS, ATA owners, PUC leaders
V0.7	16/10/2023	Peer Review	SID, TUD
V0.8	26/10/2023	Further alignment of context with comments and consolidation of input	ICCS
V.09	26/10/2023	Consolidation of peer review comments	ICCS
V1.0	31/10/2023	Final deliverable submission	INOV

Legal Disclaimer

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
ATA	Automated Threat Analytics
ATIO	Advanced Threat Intelligence Orchestrator
CERTs	Computer emergency response teams
CACAO	Collaborative Automated Course of Action Operations
COA	Course of Action
CSIRTs	Computer security incident response teams
CTI	Collaborative Threat Intelligence
DB	Database
DPA	Data Protection and Accountability
HP	Hyperledger Fabric
IDS	Intrusion Detection System
IoT	Internet of Things
JSON	JavaScript Object Notation
MISP	Malware Information Sharing Platform
OAuth AAA	Open Authentication Authentication, Authorisation and Accounting
PUC	Pilot Use Case
RRR	Risk-based Response and Self-Recovery
SAML AAA	Security Assertion Markup Language Authentication, Authorisation and Accounting
SCO	STIX Cyber-observable Object
SDO	STIX Domain Object
SRO	STIX Relationship Object
SOAR	Security Orchestration Automation Recovery
SOC	Security Operations Centres
STIX	Structured Threat Information eXpression
T	Task
VCR	Virtual Cyber Range
VDM	Vulnerability Discovery Manager
UI	User Interface
WP	Work Package
UOP	Urban Open Platform

Executive Summary

This deliverable D6.1 "APIs and data models for the integration of smart city's infrastructure with the IRIS platform" was conducted under task T6.1 and contains information on the specification and analysis of data and logs produced by IoT and AI-enabled Systems and existing monitoring and protection tools. Moreover, it includes the design and development of APIs for the integration of ATA solutions to infrastructure. The respective APIs adapted to an OpenAPI framework. Finally, is stating the potential responses, either applied directly to the infrastructure or indirectly and the respective processes.

1 INTRODUCTION

1.1 Deliverable Purpose

The purpose of this deliverable is to present the OpenAPI framework that was developed around the Advanced Threat Intelligence Orchestrator (ATIO), the data model for the integration of smart city's infrastructure with the IRIS platform and the potential produced responses sent to infrastructure.

1.2 Relation to other Tasks and Deliverables

This deliverable is rigidly connected to tasks both within and outside of WP6. Task T6.1 under WP6 collaborated closely with WP3 and Task 4.3, to develop a set of APIs and identify data models for integrating ATA solutions with the smart city's IoT and AI-enabled infrastructures. Also, specific information from IRIS tools (WP3, WP4) and PUCs (WP7) are presented.

1.3 Data models and APIs in IRIS architecture

The data model refers to an abstract model that organises elements of data received from the infrastructures (or ATA monitoring tools deployed there) towards components in the ATA module. In addition to the data model and ATIO OPENAPIs presented in Section 3 and Section 5, which is under the purpose of the deliverable, initial information about the sharing and recovery data models and APIs of the platform will be presented in Section 6. More specifically, is referred to the connection and the data transfer of ATIO towards IRIS Enhanced Melicertes Ecosystem (EME) interfaces, such as Malware Information Sharing Platform (MISP), Data Protection Accountability module (DPA) and EME Dashboard.

Additionally, the APIs for transferring response actions from the infrastructure to the ATA tools are shown.

1.4 Document Organization

Section 2 details on the data transfer of information from infrastructure to ATA tools.

Section 3 presents the data model of IRIS identification event report in STIX2.1 and the relations among objects.

Section 4 is referred to the data transfer of PUCs and the infrastructure responses processes for each PUC and possible interventions.

Section 5 is referred to the OpenAPIs adaptation of ATIO (Advanced Threat Intelligence Orchestrator) APIs.

Section 6 highlights the additional Interfaces that corresponding to recovery, sharing and visualisation and threat management.

2 DATA TRANSFER FROM INFRASTRUCTURE TOOLS TO AUTOMATED THREAT ANALYTICS TOOLS (ATA)

2.1 Data Transfer from Infrastructure tools connected to automated threat analytics tools (ATA)

When it comes to data transfer in IRIS we have two types of communication between infrastructure and ATA tools: passive communication that occurs through sensor data transfer and active communication that occurs via APIs (mostly REST-APIs). A schematic depiction can be found in Figure 5, Figure 6, Figure 7. The work below is complementary with the D4.3 *(1)* work carried out and follows the architectural flows of D2.6 *(2)*.

2.1.1 APIs for VDM

#	Type of API	Data Transfer	Data From:	Data To:
1	REST API	Inventory of devices.	Cybervision	VDM
2	syslog	New device detected in the infrastructure (it will trigger a scan process).	Cybervision	VDM

Table 1: Execution request of Vulnerability Discovery Manager -PUC1

The Vulnerability Discovery Manager performs a dynamic vulnerability assessment of the devices participating in the different Pilot Use Cases. In the case of PUC2 and PUC3, the IP addresses to be scanned will be known in advance and provided to the tool through the configuration. In the case of PUC1 the IP addresses will be provided by the infrastructure through one of these ways:

- Syslog messages sent from Cybervision to a Syslog Server deployed together with the VDM to notify a new device has been detected in the infrastructure. These logs are sent using the standard Syslog message format as described in Cisco CyberVision documentation[1].

[1] https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/syslog/b_Cisco_Cyber_Vision_Syslog_notification_format_Configuration_Guide/m_annex_syslog.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

In particular, VDM processes only syslog messages related to the category "Inventory Events" concerning new components detected on the network, which include a field "IP" with the ip address of the device that should be scanned. If it is provided in the syslog message the field "MAC", it will be also used by the VDM to be included in the vulnerability report with the information about the asset scanned. In Figure 1, it is included an example of these syslog messages:

```
local3 info 84.88.40.110 cybervision 1  May 17 11:41:14 type="Classification" seve
rity="High" category="Inventory Events" family="Component" description="New compon
ent detected on the network: IP 173.38.220.59, MAC 80:6a:00:85:52:a5, vendor " com
ponent-id="b92e5336-ac7f-5845-942b-20d724ee3912" flow-properties="EventType=\"new_
component\", component.id=\"b92e5336-ac7f-5845-942b-20d724ee3912\", sensor.id=\"b0
c5fa14-ffb6-4cce-895b-db68dc232bd5\""
```

Figure 1: Cybervision Syslog Message example (PUC1)

- Requests to the asset inventory sent by VDM to Cybervision REST API. Details about this API can be found in the Cisco Cybervision documentation[2]. From the JSON received, the IP address of the device is retrieved, that will be used to launch a scanning process against it, and additionally if available, the MAC and the description of the device. This information will be added to the vulnerability report generated by VDM.
- Providing directly the list of IP addresses to be scanned in the scanning requests done to VDM from the ATIO.

2.1.2 APIs for NightWatch

#	Type of API	Data Transfer	Data From:	Data To:
1	REST API	Network traffic data	NightWatch Probe	NightWatch Cortex

Table 2: Data transfer of NIGHTWATCH tool (PUC1 and PUC2)

To gather data from CISCO's IoT infrastructure (PUC1) and Tallin's AI-provisioned infrastructure (PUC2), the NightWatch Probe needs to be connected to the switch tasked with collecting network traffic from the targeted infrastructure and the configuration of the switch should be such that it forwards port communication towards the Probe. After deployment, the data from the NightWatch Probe is communicated to the NightWatch Cortex by sending HTTP requests via the API web framework FastAPI using Keycloak as authentication provider.

Regarding the data logs, the NightWatch Probe utilizes several network traffic analysers such as TShark, Zeek, and p0f to generate logs that contain information about the collected network data. These logs include details such as timestamps, source/destination

[2] https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_REST-API_User_Guide_Release_3_1_0.pdf

IP addresses, port numbers, packet sizes, protocols used, and other relevant metadata associated with the network traffic.

The Nightwatch Probe also integrates a python 'FileMonitoring' class which processes the aforementioned logs files. In essence, the newly added entries are pre-processed, filtered, aggregated, and securely encrypted via TLS, and are cached at a very high speed to a Redis broker. This data is then permanently stored to a QuestDB, an open-source SQL database that performs complex queries on the historical data and processes large time series data with low latency, and is then being transferred at a high rate from the Probe to the processing unit of NightWatch, namely the Cortex.

Cortex's detection mechanism analyses the logs to detect threat indicators. Upon detection of threat incidents, the Cortex pushes threat alerts to the ATIO in the form of STIX-formatted JSON reports. The threat reports can then be forwarded to the CTI component of the IRIS platform and to the EME dashboard to become visible to the end-users.

2.1.3 APIs for BINSEC

#	Type of API	Data Transfer	Data From:	Data To:
1	REST API	POST Infrastructure Executable file	CTI operator (through cloud)	BINSEC (through ATIO)

Table 3: Execution requests of BINSEC tool

BINSEC communicates via REST API. It takes as Input the binary code to be analyzed, an analysis setup (architecture, entry point in case it is not the normal one, initial state, etc.) and an optional initial test suite to start from. It then output a report in the form of a STIX-formatted JSON report.

2.1.4 APIs for SiHoneypot

#	Type of API	Data Transfer	Data From:	Data To:
1	Kafka topic	Telemetry data	Honeypot	SiHoneypot core
2	Kafka topic	Stream of sensor-like data	SiHoneypot core	Honeypot

Table 4: Data transfer of SiHoneypot core component PUC 2

#	Type of API	Data Transfer	Data From:	Data To:
1	TCP sockets	Telemetry data	Server Honeypot	Client Honeypot

Table 5: Data transfer of SiHoneypot core component PUC 3

In PUC 2, the SiHoneypot communicates with the honeypot deployed in the infrastructure via Kafka topics. The deployed honeypot collects telemetry data regarding the intruder's behaviour and actions and shares this information with the core SiHoneyPot (Digital Twin).

Sensor-like data in a continuous dataflow is streamed from the SiHoneyPot to the deployed honeypot. This streaming process requires an open channel of communication which is implemented utilizing a Kafka topic.

In PUC 3, the client and server MODBUS honeypots communicating by Modbus/TCP requests via TCP sockets.

More information about SiHoneypot's communication protocols and APIs will be provided to the corresponding deliverable, D3.4.

2.1.5 APIs for SiVi

#	Type of API	Data Transfer	Data From:	Data To:
1	Beats protocol	Network traffic anomalies	SiVi Sensor	Sivi Core

Table 6: Execution requests of SiVi core component

The deployed SiVi sensor communicates with the SiVi core component using Beats protocol. Beats communication protocol is a lightweight and efficient protocol designed for sending data between various components of a distributed system, particularly in the context of data processing and analytics, developed by Elastic. Beats is valuable because it offers an efficient, scalable, modular, and secure solution for collecting and transporting data that facilitates real-time analytics, monitoring and log processing, all needed for SiVi's robust functionality.

2.1.6 APIs for MAI-GUARD

#	Type of API	Data Transfer	Data From:	Data To:
1	REST API	Last image captured by AV Shuttle vision system	Autonomous AV Shuttle	MAI-GUARD (through EME Dashboard/ ATIO)

Table 7: *Execution requests of MAI-GUARD tool- PUC2*

MAI-GUARD communicates via REST API. It takes as Input the last image captured by the vehicle vision system (PUC2). It then output a report in the form of a STIX-formatted JSON report. The report contains whether or not the image has been modified via an adversarial example attack.

3 IRIS DATA MODEL

Data model presented in Section 3.3, is referred to the information communicated between Infrastructure and automated threat analytics tools (ATA) in STIX2.1 format (3).

3.1 Design Process of IRIS Data Model in STIX2.1

Rather than the creation of the actual data model by itself a major effort was given from ATA tool owners to the design and the translation to STIX2.1 format output from conventional tools (see Annex 8.1.1.2, Annex 8.1.1.3). Then, all the information of the standardized model's objects, relations and extensions consolidated to the final data model.

The design steps are mentioned below:

Step 1 is to analyse the information output of the Analysis tool and see their commonalities and differences. Also, to check the output formats (either STIX2.1 or customized format) and then check the compliance with STIX2.1 format.

Step 2 is to verify the json outputs to a STIX 2.1 verificator, in order to see if they met all the standardized requirements,

Step 3 is to investigate thoroughly to the abstract connection schema of the architectural design and provide the proper STIX2.1 relation.

3.2 STIX 2.1 Documentation

IRIS data model will follow, STIX 2.1 standardised language.

STIX2.1 terminology will be explained based on **[STIX-v2.1]** (4) enabling the thorough understanding of the STIX2.1 compatible IRIS data model.

3.2.1 STIX Objects

STIX 2.1 has entities that enable the communication of the high-level information of the threat landscape.

STIX Bundle Objects STIX bundle objects can aggregate in a specialised format any information including either STIX Core Objects or/ and STIX Meta Objects.

STIX Core Objects are STIX Domain Objects (SDO), STIX Cyber-observable Objects (SCO), or STIX Relationship Objects (SRO).

STIX Domain Objects (SDOs) define a set of 18 high level Intelligence Objects representing behaviours describing in parallel the whole threat landscape. Those SDOs are namely: Attack Pattern, Campaign, Course of Action, Grouping, Identity, Indicator, Infrastructure, Intrusion Set, Location, Malware, Malware Analysis, Note, Observed Data, Opinion, Report, Threat Actor, Tool, and Vulnerability.

STIX Cyber-observable Objects (SCOs) represent a set of observables for characterizing host-based and network-based information. SCOs are used by various STIX Domain Objects (SDOs) to provide supporting context. The Observed Data SDO, for example, indicates that the raw data was observed at a particular time.

STIX Relationship Objects (SROs) connect STIX Domain Objects together, STIX Cyber-observable Objects together, and connect STIX Domain Objects and STIX Cyber-observable Objects together.

STIX Meta Objects A STIX Object that provides the necessary glue and associated metadata to enrich STIX Core Objects to support user and system workflows.

3.2.2 STIX2.1 Extension Definition

STIX 2.1 has the capability to include custom objects, extensions, and properties. More specifically, threat intelligence experts can develop new STIX domain, cyber observable, or relationship objects using the framework provided by STIX 2.1's STIX object (Extension Definition object) [stix-v2.1_extension]. Any additional properties and objects that the extension defines are described in detail in the Extension Definition object. The schema property (see Figure 4) is a URL linking to a JSON schema and refers to the extension's normative definition**.**

Figure 2: Inclusion process of STIX extension to STIX object

3.3 Data model between Infrastructure and ATA module

Herein this document, the data model is referred to an abstract model that organises elements of data received from multiple tools and sources and structures them to a unique format in order to be digested from the system, produces event response and finally sends all information to be communicated through a Report object to EME Unified Dashboard. The data model is showcased to the Figure 3.

3.3.1 IRIS identification event report Data Model

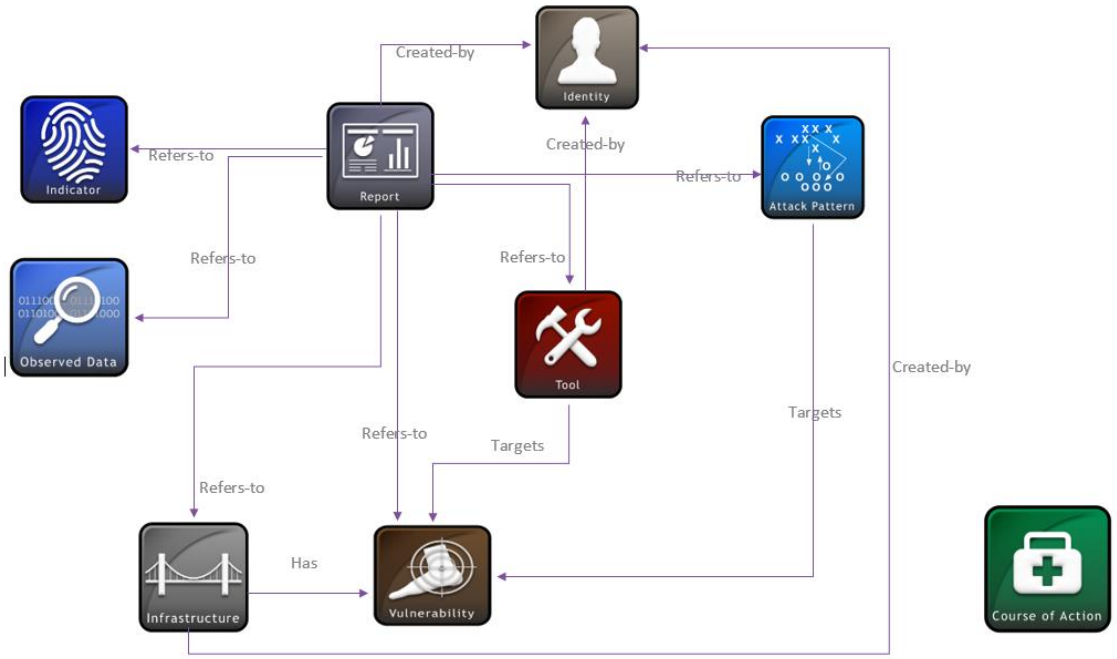


Figure 3: Data model of IRIS identification event report from infrastructure.

The common object of all the STIX2.1 (4) produced output is the *Report* that relates all the objects with each other.

Indicator object corresponds to some suspicious or malicious cyber activity detected by Threat Detection ATA tools of IRIS architecture.

Vulnerability object refers to a weakness or defect identified in the infrastructure by the tools of IRIS architecture for identifying either network or software vulnerabilities.

Tool object corresponds to the ATA tools of IRIS architecture. More specifically, VDM, BINSEC, Sivi, NIGHTWATCH, MAI-GUARD.

Identity object represents either to the tool organisation or to the infrastructure entity.

Infrastructure object corresponds to PUC1, PUC2, PUC3.

Attack pattern object is used to categorize a potential attack that could be performed taking advantage of some of the vulnerabilities identified in the infrastructure.

Observed data object corresponds to raw information (e.g. an IP address, URLs, domain names, email addresses, network activity evidence, files, registry keys, etc.) that has been observed by some of the ATA tools of IRIS architecture, but without any context.

Finally, the *course of action* information corresponds to the proposed mitigation response actions of IRIS.

Because they adhere to distinct formats (*Course of action* follows STIX-CACAO format and *Report* STIX 2.1 format, and they are internally associated by an "IRIS id"), IRIS *course of action* object and *Report* object do not have relationships in the IRIS data model.

3.3.2 Data Model Objects

In this data model (5) a set of 9 STIX Domain Objects (SDOs) exist: *Indicator, Observed Data, Report, Identity, Infrastructure, Vulnerability, Tool, Attack-pattern, Course of Action (COA)*. The mandatory and optional properties of the objects are mentioned in the table below.

It is observed that there are some properties that are marked neither as required nor as optional but as reserved. This means that the action property of the course of action is under actively research and has been reserved for being defined in future versions of STIX 2.1 documentations.

SDOs	Required Common Properties	Optional Common Properties
Report	type, spec_version, id, created, modified, name	description, report_type, published, objects_refs
Identity	type, spec_version, id, created, modified, name	description, roles, identity_class, sectors, contact_information
Observed Data	type, spec_version, id, created, modified, first_observed, last_observed, number_observed	objects, objects_refs
Indicator	type, spec_version, id, created, modified, pattern, pattern_type, valid_from,	name, description, indicator_types, pattern_version, valid until, kill_chain_phases
Infrastructure	type, spec_version, id, created, modified, name	description, infrastructure types, aliases, kill_chain_phases first_seen), last_seen
Tool	type, spec_version, id, created, modified, name	description, tool_types, aliases, kill_chain_phases, tool_version
Vulnerability	type, spec_version, id, created, modified, name	description, external_references
Attack Pattern	type, spec_version, id, created, modified, name	external_references, description, aliases,kill_chain_phases
Course of Action	type, spec_version, id, created, modified, name	Description, action (reserved)

Table 8: STIX Domain Objects (SDOs) properties of IRIS event identification report data model enabling for, sharing and response

3.3.3 Data Model Relationships

The STIX Domain Objects (SDOs) (5) are tied with 4 relations: refers-to, created-by, has, targets.

Source	Relationship Type	Target	Description
Report	Refers-to	Indicator, Observed Data, Infrastructure, Vulnerability, Tool, Attack-pattern.	This relationship indicates that the Report includes information about related Indicator (referred to threat detection), Observed Data, Infrastructure, Vulnerability, Tool and Attack patterns.
Report	Created-by	Identity	This relationship describes that the Report can be created by Identity (tool owners' organisation)
Infrastructure	Has	Vulnerability	This Relationship describes that this specific Infrastructure has this specific Vulnerability.
Infrastructure	Created-by	Identity	This Relationship describes that this specific piece of information from Infrastructure (e.g. executable file, image) created by identity

			(infrastructure entity).
Tool	Targets	Vulnerability	This relationship indicates that the respective tool targeted vulnerabilities.
Tool	Created-by	Identity	This relationship indicates that each tool created by each organisation
Attack-pattern	Targets	Vulnerability	This Relationship describes that this Attack Pattern is used to deliver this malware instance (or family).

Table 9: Object Relationships within IRIS data model

3.3.3.1 Extension properties connected to Report

Herein is presented the extension property of Report object. The below image is referred to 1 of the ATA tools, indicatively to NIGHTWATCH.

{

"extension_type":"property-extension",

"organisation":"Org1",

"source":"Nightwatch",

"status":"Open",

"threat_description":"unknown",

"detection_summary":"192.168.2.200 was observed making many unique ICMP connections to host 192.168.2.103 within a 10 minutes period.",

"actor":"192.168.2.200",

"target":"192.168.2.103",

"dst_port":"unknown",

"duration":0.61,

"severity":"Medium",

"risk_score":59,
"confidence":0.999721,
"service_indicator":"ICMP",
"mitre_attack":{"Inhibit Response Function":{"Denial of Service":"T0814"}}
}

Figure 4: Extension json example

4 INFRASTRUCTURE RESPONSES FROM IRIS ADVANCED THREAT INTELLIGENCE PLATFORM

4.1 Description of Infrastructure Assets' Connections within IRIS

The IRIS pilot use cases are based on actual scenarios taking into consideration infrastructure assets and networks, both of which are split in distinct regions. There are multiple devices coexisting in each scenario. Data shared between devices may come from several locations, providing knowledge about the infrastructure which ought to be safeguarded. With the exception of the sensors that belong to the IRIS ATA tools, the information leaves the infrastructure through a single server. However, when response information is returned, it enters through a device, designating a single access point per PUC, increasing technical simplicity while also boosting security by reducing sites of intrusion. This means that only one device in each infrastructure perceives the API from the EME trusted environment (via ATIO) with a standard message. Each infrastructure handles this message while adhering to its individual corporate guidelines and law regulations.

4.1.1 PUC1

In Pilot Use Case Scenario 1, the devices are placed in three (3) locations (see Annex 8.1.1.1):

- Devices at Datacenter located at Ca l'Alier
- Devices at tram station – Pledger devices
- Other Devices at IRIS Sandbox at Cisco

The proposed responses produced by the Risk-based Response and Self-Recovery (RRR) are sent to the firewall. More information about the particular response process in Section 4.2.

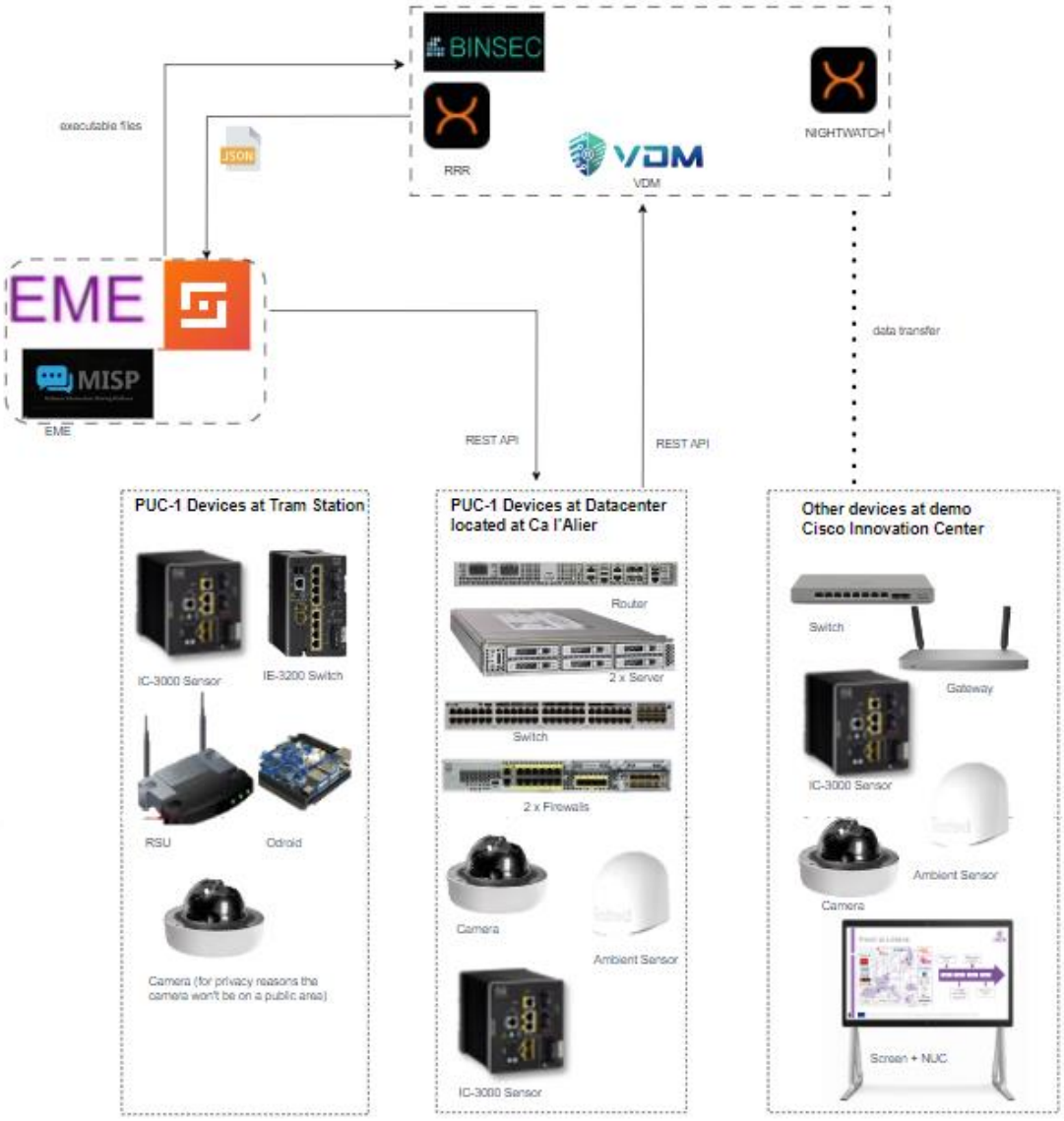


Figure 5: Interconnectivities of PUC1- INFRASTRUCTURE integrated with IRIS platform

In order to secure the physical infrastructure, we have deployed a physical firewall (Firewall IMI). Due to current legislation, external entities cannot interact with this firewall (Firewall IMI) that protects a municipality network; so, for the purposes of the demonstration and the pilots, a second firewall (Firewall IRIS) has been then installed in PUC1. A third-party orchestrator (IRIS) will interact with the second firewall (Firewall IRIS) through Firepower Threat Defense REpresentational State Transfer (REST) Application Programming Interface (API), over HTTPS.

#	Type of API	Supported HTTP Methods	Data From:	Data To:
1	REST API	GET, POST, PUT DELETE	Third-party orchestrator (IRIS)	Firewall IRIS

Table 10: Execution requests of ATIO-PUC1

The REST API uses JavaScript Object Notation (JSON) format to represent objects. Here you can find information about the REST API (6) & (7).

4.1.2 PUC2

The devices in Pilot Use Case Scenario 2, are divided into two distinct areas (see Annex 8.1.1.1):

- Urban Operating Platform
- Digital Twin HoneyPot of the Autonomous AV SHUTTLE

The proposed responses produced by the Risk-based Response and Self-Recovery (RRR) were sent to the Digital Twin HoneyPot produced by SiDRocco and the Digital Twin of the AV Shuttle produced for the ML Evasion attack scenario. The Digital Twin Honeypot is a replication of data of the LiDAR sensor of the Autonomous Vehicle. The Digital Twin of the AV Shuttle is the training data used for object detection of traffic lights. More information about the particular response process in Section 4.2.

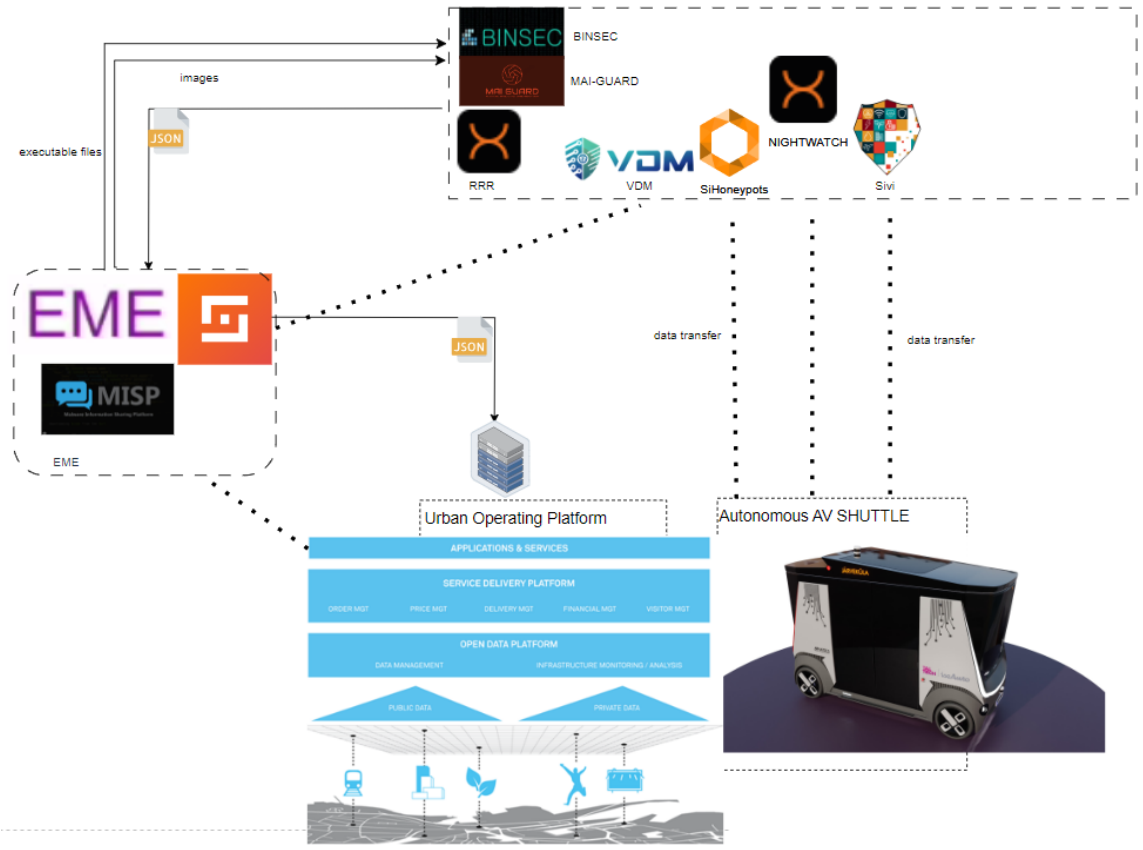


Figure 6: Interconnectivities of PUC2- INFRASTRUCTURE integrated with IRIS platform

#	Type of API	Execution Request	Data From:	Data To:
1	REST API	POST response	EME Dashboard (through ATIO)	Urban Open Platform

Table 11: Execution requests of ATIO-PUC2

The Urban Open Platform (UOP) is equipped to receive data through a REST API endpoint via a POST request. Subsequently, this data is seamlessly relayed to various UOP components for subsequent processing, storage, and further actions.

4.1.3 PUC3

In Pilot Use Case Scenario 3, the devices are divided to three (3) categories (see Annex 8.1.1.1):

- Simulated devices of Residential Building Infrastructure and Substation Infrastructure
- Physical devices available (already installed) as part of the residential building infrastructure
- Physical devices available as part of the substation infrastructure

The proposed responses produced by the Risk-based Response and Self-Recovery (RRR) tool sent to the Urban Open Platform (UoP) API automatically. More information about the particular response process in Section 4.2

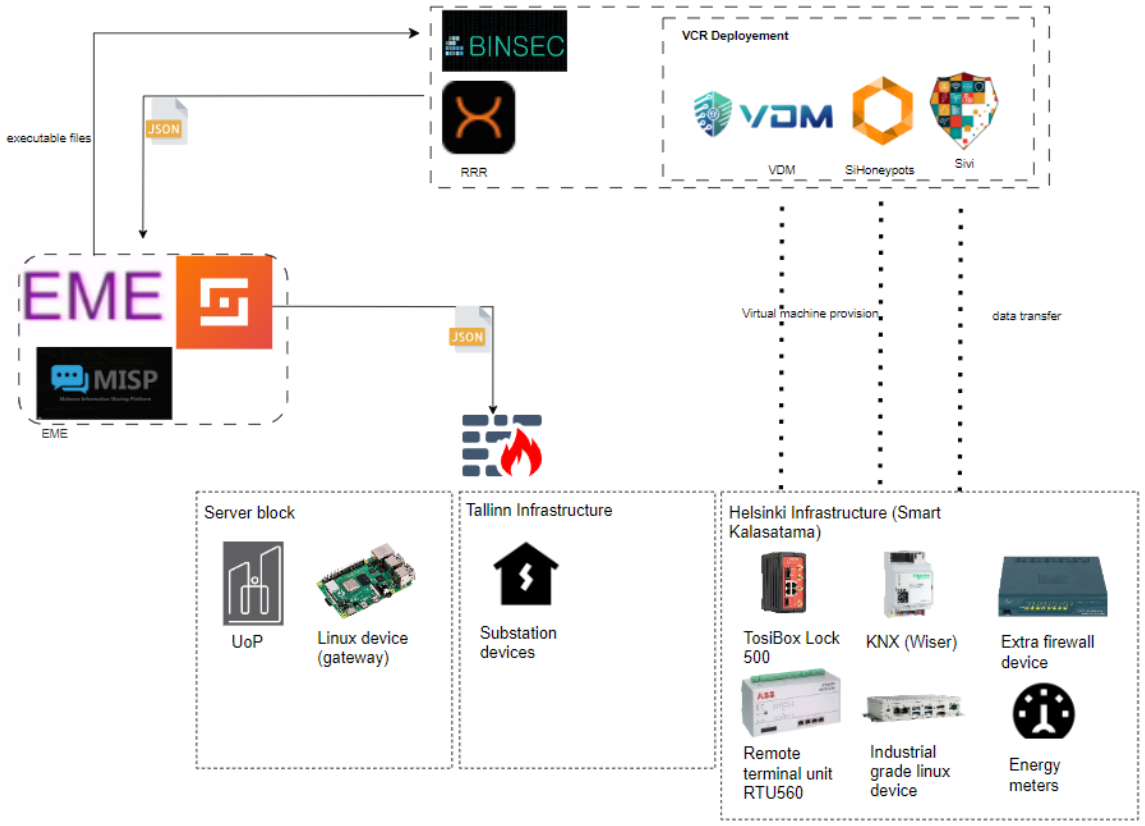


Figure 7: Interconnectivities of PUC3- VCR integrated with IRIS platform

#	Type of API	Execution Request	Data From:	Data To:
1	REST API	POST response	EME Dashboard (through ATIO)	Urban Open Platform

Table 12: Execution requests of ATIO-PUC3

The Urban Open Platform (UOP) is equipped to receive data through a REST API endpoint via a POST request. Subsequently, this data is seamlessly relayed to various UOP components for subsequent processing, storage, and further actions.

4.2 Response Architectural Flows

PUC	Direct Response Apply	Human Execution Response Apply
PUC1	X	X
PUC2		X
PUC3		X

Table 13: Response executions for each PUC

The Response actions will be sent through the Advanced Threat Intelligence Orchestrator (ATIO) to the infrastructure either in STIX-CACAO format or through an infrastructure compliant standardised message.

The responses can be sent to the released REST-API and applied either directly to the threat actor IP or will be executed by the corresponding security expert of the infrastructure.

4.3 Response Actions

The Risk-based Response and Self-Recovery module (RRR) of the IRIS platform generates responses which are sent to the smart city's infrastructure through the Advanced Threat Intelligence Orchestrator (ATIO). To provide optimized response recommendations for each organization and detected incident (vulnerability or threat), the RRR module must first identify the available response actions. A dictionary is being created with three (3) keys ("**contain**", "**harden**", and "**recover**") that represents different phases of the cyber incident response process[3].

Contain

{"id":1, "detection_actor": "10.0.1.1", "action": "Do not contain", "description": "At this time, no containment action is recommended","execution_api": "", "action_impact": 0}

{"id":2, "detection_actor": "10.0.1.1", "action": "Isolate Host", "description": "It is recommended that the host is isolated from

[3] a structured process organization use to identify and deal with cybersecurity incidents.

the network to prevent further compromise and impact.", "execution_api": "", "action_impact": 10}

{"id":3, "detection_actor": "10.0.1.1", "action": "Block Host Service", "description": "It is recommended that the affected service is blocked on the host", "execution_api": "", "action_impact": 5}

{"id":4, "detection_actor": "10.0.1.1", "action": "Shutdown host", "description": "It is recommended that the host is shutdown", "execution_api": "", "action_impact": 5}

Harden

{"id":5, "detection_actor": "10.0.1.1", "action": "Do not harden", "description": "At this time, no harden action is recommended", "execution_api": "", "action_impact": 0"}

{"id":6, "detection_actor": "10.0.1.1", "action": "Install software patches.", "description": "It is recommended that software patches are issued to the affected host as soon as they become available and it is safe to do so.", "execution_api": "software_patch()", "action_impact": 5}

{"id":7, "detection_actor": "10.0.1.1", "action": "Disable services", "description": "It is recommended that affected remote services are disabled on the affected system(s)", "execution_api": "disable_hosted_services()", "action_impact": 5}

{"id":8, "detection_actor": "10.0.1.1","action": "Implement access control", "description": "It is recommended that network segmentation and access controls are implemented to limit unauthorised connectivity to and from the affected host.", "execution_api": "disable_hosted_services()", "action_impact": 5}

Recover

{"id":9, "detection_actor": "10.0.1.1", "action": "Do not recover", "description": "At this time, no recovery action is recommended", "execution_api": "", "action_impact": 0"}

{"id":10, "detection_actor": "10.0.1.1", "action": "System Restore", "description": "It is recommended that the system should be restored to a last known good configuration state.", "execution_api": "system_restore()"}

{"id":11, "detection_actor": "10.0.1.1","action": "System Reconfiguration", "description": ”It is recommended that the system should be reconfigure to a safe operational state.", "execution_api": "system_reconfig()"}

As it can be seen, each response sub-action in the dictionary contains information such as:

- ID: A unique identifier for the response sub-action.
- Detection Actor: The host or system impacted by the incident.
- Action: The recommended response action to be implemented.
- Description: Further details regarding the action and its potential impact.

- Execution API: A code function or script that enables the automated execution of the action.

This information is used by RRR's optimisation model to determine the best response action and corresponding sub-actions for a specific incident. With the purpose of standardizing the way IRIS creates, documents, and shares commands and playbooks that are both human-understandable and machine-executable, these optimal response actions are converted into a STIX/CACAO (8) format prior to being sent to the ATIO.

Further insights into the execution of the selected actions within the pilot infrastructures of the IRIS project will be included in the deliverables D7.2-D7.4. These deliverables will also provide an overview of the availability of a given response action for execution in a target system of the pilot infrastructure, providing a better understanding of the responses that can be executed in each specific pilot scenario.

5 OPENAPI ADAPTION

In IRIS architecture three kinds (3) of API schemas will be defined towards the integration with the smart city's IoT- and AI-enabled infrastructures.

- APIs of vulnerability and threat detection from the infrastructure following STIX2.1 format.
- APIs for SiHoneypots following STIX2.1 format.
- APIs to send responses to the infrastructure following STIX - CACAO format

Also, there are three (3) additional APIs towards external interfaces such as

- APIs for DPA module following a customised format.
- APIs for MISP, following STIX2.1 format
- APIs for EME, following STIX2.1 format

For the APIs definition, the OpenAPI specification will be adopted.

5.1 API SCHEMA for vulnerability and threat detection

In IRIS architecture, the IoT infrastructure is covered by a number of defensive modules that are able to detect threats and vulnerabilities in real time. These versatile tools are producing event reports constantly, which in turn are sent towards the Enhanced Melicertes Ecosystem to be stored and analysed.

Advanced Threat Intelligence Orchestrator (ATIO) has been incorporated inside the IRIS architecture assisting IRIS tools performing json and formats' modifications and providing efficient end-to-end communication and data transfer through automatic step execution.

The API of the Advanced Threat Intelligence Orchestrator endpoints tries to generally support and not to interrupt the communication between the other modules. In this spirit, the Orchestrator employs a transparent nature of operation, in the sense of trying to not alter the information passing through, where ever this is possible. In particular, the API is comprised of a single "webhook" endpoint for each module that needs to push data towards the EME. Each webhook is designated by a unique UUID, that is only known to the respective detection module. The detection is then validated, analyzed and accordingly routed, using the mechanisms that rely internally in the ATIO, namely Workflow Execution Engine, Workflow Combination Engine, Data Exchange Framework, Command Execution Requests Framework.

This "push-based" architecture adds to the efficiency of the whole process, as in the case of an incident, the number of emitting detection events may suddenly rise steeply.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

5.2 OpenAPI description

The OpenAPI is a specification for a machine-readable interface definition language for describing, producing, consuming and visualizing web services. Previously part of the Swagger framework, it became a separate project in 2016, overseen by the OpenAPI Initiative, an open-source collaboration project of the Linux Foundation.

By taking as input OpenAPI Specification compliant files, swagger and some other tools can generate code, documentation, and test cases for a web service or API.

5.2.1 YAML description

OpenAPI specrification is expressed in YAML (Yet Another Markup Language) format. YAML is closely related to the JSON format, as it follows the same principles and structure, but at the same time it removes unnecessary Markup syntax, such as the weary curly braces, or the mandatory indentation conformation for better readability purposes.

5.2.2 OpenAPI usages

OpenAPI standard helps programmers as well as machines to define the structure of an API, its requirements and usages, and at the same time it provides an easy way to share API configuration among machines, in a machine-readable format. Using the OpenAPI standard in IRIS architecture, allows fast and reliable redeployment of APIs, as well as a user-friendly way to describe, share among humans, or create automatic tests.

Below is the OpenAPI specification of the Advanced Threat Intelligence Orchestrator endpoints that listen for detection events:

5.3 IRIS Orchestrator Endpoints

```
openapi: 3.0.0

info:
  title:             Iris             Orchestrator             API
  description:                                                  |
    Workflows for the IRIS platform orchestration.

servers:
  - url: https://iris.iccs.gr

tags:

paths:
  /api/v1/hooks/webhook_945aa821-55ad-4b02-8b01-76900386e978:
    post:
      summary: "[VDM] Get a vulnerability report generated by the
VDM                                                             tool"
      description:                                              |
        **This   is   the   endpoint   for   the   VDM   workflow.**
      operationId:
      tags:
```

```
      requestBody:
        $ref:       "#/components/requestBodies/VDM_JSON_Request"
      responses:
        "200":
          $ref: "#/components/responses/GenericResponse"

paths:

  /api/v1/hooks/webhook_16e4606f-2a5f-498d-97e6-be28392a20cf:
    post:
      summary: "[NightWatch] Get a threat detection report
generated by the NightWatch tool"

NIGHTWATCH
      description: |
        **This is the endpoint for the NightWatch workflow.**
      operationId:
      tags:
      requestBody:
        $ref:
"#/components/requestBodies/NightWatch_JSON_Request"
      responses:
        "200":
          $ref: "#/components/responses/GenericResponse"

paths:

/api/v1/hooks/webhook_2c07a519-a230-448c-8d0c-0440a05e0ee8:
    post:

      summary: "[SiVi] Get a threat detection report generated by
the SiVi tool"
```

```
SiVi
      description: |
        **This is the endpoint for the SiVi workflow.**
      operationId:
      tags:
      requestBody:
        $ref:

"#/components/requestBodies/SiVi_JSON_Request"
      responses:
        "200":
$ref: "#/components/responses/GenericResponse"

paths:

/api/v1/hooks/webhook_2c07a519-a230-448c-8d0c-0440a05e0ee8:
    post:
      summary: "[SiVi] Get a threat detection report generated by
the SiVi tool"
```

```
SiHoneyPot


      description: |
        **This is the endpoint for the SiHoneypot workflow.**
      operationId:
      tags:
      requestBody:
        $ref:
"#/components/requestBodies/SiHoneypot_JSON_Request"
      responses:
        "200":
          $ref: "#/components/responses/GenericResponse"

paths:

  /api/v1/hooks/webhook_cc575211-1877-4864-bc08-10849c0c5822:
    post:
      summary: "[SiHoneypot] Retrive telemetry data generated by
the SiHoneypot module"
```

```
BINSEC

      description: |
        **This is the endpoint for the BinSec workflow.**
      operationId:
      tags:
      requestBody:
        $ref: "#/components/requestBodies/BinSec_JSON_Request"
      responses:
        "200":
          $ref: "#/components/responses/GenericResponse"

paths:


  /api/v1/hooks/webhook_55dbd167-5cee-4009-8cdc-9b7e0cfc0844:
    post:
      summary: "[BinSec] Retrive results generated by the BinSec
module"
```

```
components:
  schemas:

  parameters:

  securitySchemes:
    ApiKeyAuth:
      type: apiKey
```

```
      in: header
      name: Authorization
      description:
            Authorization: YOUR_API_KEY

  requestBodies:


    VDM_JSON_Request:
      content:
        application/json:
          schema:
            type: object
            properties:
    NightWatch_JSON_Request:
      content:
        application/json:
          schema:
            type: object
            properties:

    SiVi_JSON_Request:
      content:
        application/json:
          schema:
            type:object
            properties:

    SiHoneypot_JSON_Request:
      content:
        application/json:
          schema:
            type:object
            properties:

    BinSec_JSON_Request:
      content:
        application/json:
          schema:
            type:object
            properties:


responses:
    GenericResponse:

    content:

        application/json:

          schema:

            type: object
```

```
          properties:


headers:

security:
  - ApiKeyAuth: []
```

6 ADDITIONAL INTERFACES

6.1 API SCHEMA for EME: STIX

For the API definition of the MISP instance inside the Enhanced Melicertes Ecosystem, the OpenAPI specification of the official MISP documentation will be used.

MISP API allows you to query, create, modify data models, such as Events, Objects, Attributes. It also lets you perform administrative tasks such as creating users, organisations, altering MISP settings, and much more. In order to use the API, an API key is required for authentication purposes. There is also a need to specify the `Accept` and `Content-type` headers for the POST HTTP request. For example:

```
curl      --header      "Authorization:      YOUR_API_KEY"      \
      --header         "Accept:         application/json"         \
   --header "Content-Type: application/json" https://<misp url>/
```

PyMISP is a Python library to access MISP platforms via their REST API. It allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

6.1.1 MISP-STIX translation

Natively, MISP stores event information in a specified format, other than STIX2.1.

In fact, MISP event format is not very different from STIX2.1 format, as is also used to describe and share threat intelligence information (CTI). Advantages of each of these cases are perhaps out of the scope of this document, but the main advantage of STIX2.1 is maybe the universally unique identification of CTI, across any system.

Both formats, MISP and STIX, are created by the same community of security experts, and thus share many ideas. After all, the information to be shared is still the same, it is only the representation that differs.

In IRIS, as CTI is transferred among the different modules in STIX2.1 format, it needs to be translated into MISP format before being able to be imported into the MISP database. To that end, the IRIS ATIO has implemented a custom solution application that translates CTI from STIX2.1 to MISP format and back. This solution is based on PyMISP library, as well as an open-source effort called “misp-stix”, found on Github.com.

The event information is translated in real-time at the time of arrival on the ATIO API. As the two formats are slightly different, many fields and pieces of information of minor importance are dropped, and only the common fields are preserved.

Below, you can see a screenshot of an actual ATIO flow implementing the above idea:

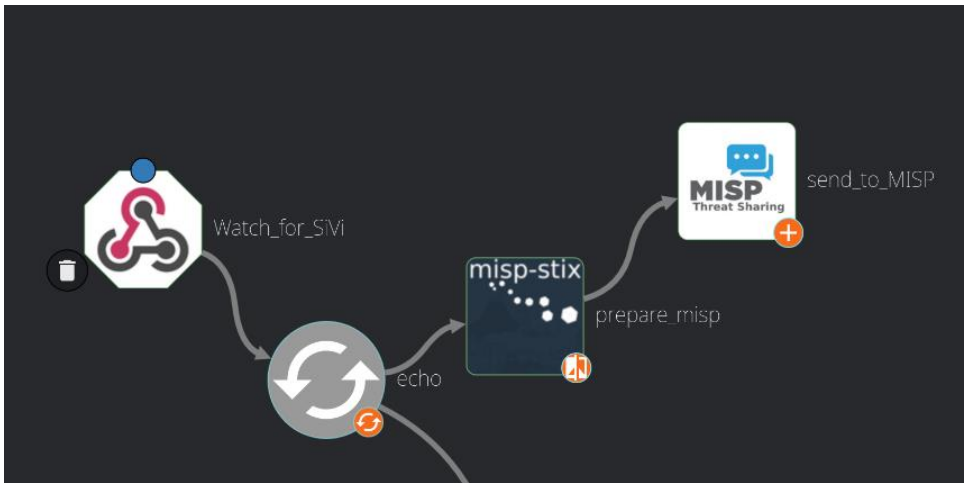


Figure 8: *Retranslation from STIX to MISP captured from SHUFFLE visual environment*

The complete OpenAPI specification of MISP can be found in the following link on https://raw.githubusercontent.com/MISP/MISP/develop/app/webroot/doc/openapi.yaml

6.2 DPA API Specification

The DPA's access point is a REST API Server. A DPA REST API Server is either an auditing or logging interface, and can be accessed with the credentials of a user properly registered in the DPA.

6.2.1 POST Requests:

Audit data is written in the DPA via POST requests. If the DPA user identity credentials provided in the request do not correspond to a user with *logging* (WRITER) permissions, the POST request will fail.
The following is a sample *curl* POST request, to a DPA REST API Server deployed in the IRIS Integration Infrastructure:

```
curl --request POST \
       --url 'https://dpa-api-server-dpa-channel-logger.platform.iris-
h2020.eu:5000/WriteAuditData' \
       --header 'content-type: multipart/form-data' \
       -F 'auditData=@audit-data.json' \
       -F 'auditMetadata=@audit-metadata.json' \
       --cert 'public.crt' \
       --key 'private.key' \
       --cacert 'ca.crt'
```

The following inputs are necessary to perform the POST request:

- ***Audit Data***:
  - The JSON file containing the audit log.
- ***Audit Metadata***:
  - The JSON file containing the metadata that identifies the *audit data*.
- ***API Client Public and Private Keys***:

    - The credentials to authenticate the DPA user identity.
- ***TLS CA Certificate***:
    - The CA certificate to validate the REST API Server identity.

6.2.2 GET Requests:

Audit data is read from the DPA via GET requests. If the DPA user identity credentials provided in the request do not correspond to a user with *auditing* (READER) permissions, the GET request will fail.
The following is a sample *curl* GET request, to a REST API Server deployed in the IRIS Integration Infrastructure:

```
curl --request GET \
       --url 'https://dpa-api-server-dpa-channel-auditor.platform.iris-
h2020.eu:5000/ReadAuditData?query=\{"selector":\{"systemID":"CERT-
PT"\}\}' \
       --cert 'public.crt' \
       --key 'private.key' \
       --cacert 'ca.crt'
```

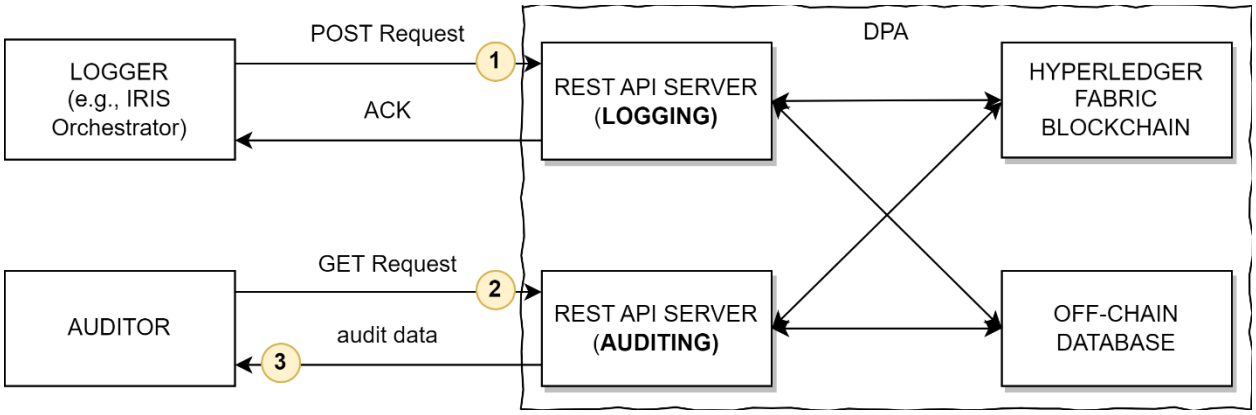
The following inputs are necessary to perform the GET request:

- ***Query***:
    - A query following the structure of an Hyperledger Fabric rich query.
- ***API Client Public and Private Keys***:
    - The credentials to authenticate the DPA user identity.
- ***TLS CA Certificate***:
    - The CA certificate to validate the REST API Server identity.

6.2.3 DPA Data Model

This section provides insight into the structure of the input and output data to and from the DPA through its external interfaces. Therefore, the following data model is relevant to the integration of external components (e.g., the IRIS Orchestrator) with the DPA.

The following figure illustrates where the relevant data structures materialize in the DPA architecture (1, 2 and 3):



- ❶ ***POST Request Input Data***:

  In a POST request to write audit data, two JSON files are provided - one containing the audit log (the DPA is oblivious to the structure of this file), and another containing the structured metadata that will identify that audit log in the DPA.

  The structured metadata should be provided as follows:

```
{
  "systemID": "...",
  "orchestratorID": "...",
  "correlationID": "...",
  "collaborationID": "...",
  "userID": "...",
  "orchestratorTimestamp": "..."
}
```

- ❷ ***GET Request Query***:

  In a GET request, the desirable query should be provided in a format compatible with Hyperledger Fabric rich queries:

```
{
  "selector": {
    "systemID": "..."
    "orchestratorID": "..."
    ...
  },
}
```

- ❸ ***GET Request Response***:

  The response to a GET request is a string containing all audit data, in its original JSON format, that has been found in the DPA and that corresponds to the specified query (the identifying ID is generated internally):

```
Audit Log # 960579994

{
   ...
}

Audit Log # 872687323

{
   ...
}

Audit Log # 438745448

{
   ...
}

...
```

6.3 EME DASHBOARD

The IRIS-Enhanced MeliCERTes ecosystem (EME) will incorporate the majority of the technical developments that concern the CTI sharing in IRIS and act as a CTI sharing and collaboration interface towards the envisaged users of the IRIS platform. EME will act as a distributed and customized solution, and provide for secure and trusted online communication, collaboration and information sharing among CI operators and CERTs/CSIRTs allowing them to interact with the IRIS platform through a unified customizable dashboard.

EME dashboard is the main user interface for the IRIS project stakeholders namely, Critical Infrastructure operators and CERT/CSIRT operators. The EME dashboard receives the CTI events information that are captured by the IRIS platform through the ATA deployed tools by the ATIO module. EME dashboard functionalities are supported by a REST API server (back-end) which also incorporates a REST API. Among others ME dashboard API is responsible for collecting the CTI data received. In the section below, we present the particular endpoint that has been implemented.

6.3.1 EME DASHBOARD API

EME dashboard collects the CTI events through the following POST endpoint.

URL	https://EME-api.platform.iris-h2020.eu/CTI_event/
Method	POST
Headers	Content-Type: application/json

Request body	RRR JSON (see below)
Response body	N/A
Response codes	201 – Reported accepted CTI event. 400 – Provided data is invalid or malformed 405 – This type of method is not allowed for this endpoint 500 – Internal server error

6.3.2 EME DASHBOARD JSON

The CTI information that is collected by the EME back-end follows a JSON structure. It contains information regarding the ATA tool that detected the event, details on the specific threat that was detected (attack or vulnerability) including event criticality and impact details and the suggested mitigation actions that are proposed to the EME CI operator which are generated by the RR component. The structure of this document is presented below.

```
{
  "type": "bundle",
  "id": "….",
  "objects": [
    {
      "type": "extension-definition",
      "spec_version": "2.1",
      "id": "….",
      "created_by_ref": "…..",
      "created": "…",
      "modified": "…",
      "name": "Response action definition",
      "description": "Additional properties defined for the
execution of response actions",
      "schema": "https://.......",
      "version": "1.0",
      "extension_types": [
        "property-extension"
      ],
      "detection": {
        "organisation": "…",
        "detection_name": "…",
        "detection_summary": "…",
        "source": "…",
        "classification": "…",
        "first_seen": "…",
        "last_seen": "…",
        "actor": "…",
        "confidence": "…",
```

```
      "risk_score": "…",
      "threat": "…",
      "iris_id": 012
    },
    "policies": {
      "organisation": "…",
      "action_policy": {
        "contain": {
          "isolate": "enabled",
          "block_service": "enabled",
          "shutdown": "enabled"
        },
        "harden": {
          "install_patches": "enabled",
          "disable_service": "enabled",
          "implement_access_control": "enabled"
        },
        "recover": {
          "restore": "enabled",
          "reconfigure": "enabled"
        }
      }
    },
    "criticalities": {
      "organisation": "…",
      "asset_ip": "…",
      "asset_device": "…",
      "criticality": "1"
    },
    "playbook_actions": {
      "type": "playbook",
      "playbook_id": "",
      "spec_version": "cacao-2.0",
      "playbook_standard": "CACAO",
      "name": "playbook name",
      "created_by": "RRR",
      "created": "…-06-14T14:29:22.24089Z",
      "modified": "…",
      "playbook_valid_from": "…",
      "playbook_valid_until": "…",
      "organization_type": "…",
      "asset": "…",
      "risk_score": "…",
      "playbook_impact": "…",
      "playbook_severity": "…",
      "playbook_priority": "…",
      "playbook_type": "…",
      "workflow_start": "3",
      "workflow": [
        {
          "id": 2,
          "impacted_actor": "…",
          "action": "Isolate Host",
```

```
            "description": "It is recommended that the host is
isolated from the network to prevent further compromise and impact
.",
            "execution_api": "",
            "action_impact": 10
          },
          {
            "id": 3,
            "impacted_actor": "…",
            "action": "Block Host Service",
            "description": "It is recommended that the affected
service is blocked  on the host",
            "execution_api": "",
            "action_impact": 5
          },
          {
            "id": 4,
            "impacted_actor": "…",
            "action": "Shutdown host",
            "description": "It is recommended that the host is
shutdown ",
            "execution_api": "",
            "action_impact": 10
          }
        ]
      }
    }
  ]
}
```

7 CONCLUSIONS

This deliverable includes data for nine (9) requests for data transfers from the Infrastructure to the ATA module, which are indicated by the ATA tools VDM, BINSEC, Sivi, NIGHTWATCH, SiHoneypot, and MAI-GUARD. The data model for the IRIS event identification report is supplied in STIX2.1 format, allowing the IRIS integrated platform to use this information for dissemination, enrichment, and the production of STIX-CACAO potential mitigation measures. Furthermore, the intervention architectural flows of each pilot case were built, and the potential mitigation actions in total were listed. In addition, OpenAPI designed around ATIO in order to interface with ATA tools is described in this deliverable.

8 REFERENCES

1. **Consortium, IRIS.** *D4.3 APIs for advanced threat intelligence orchestration.* 2022.

2. —. *D2.6 IRIS platform and reference architecture -final version.* 2023.

3. **Czekster, Ricardo M, Metere, Roberto and Morisset, Charles.** Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings. *Applied Sciences* . 12, 2022 , Vol. 5005.

4. **OASIS Committee Specification 01.** STIX™ Version 2.1. [Online] Edited by Bret Jordan, Rich Piazza, and Trey Darley. 20 March 2020. https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html. Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1..

5. **Organization for the Advancement of Structured Information Standards (OASIS).** STIX™ Version 2.1, Commitee Specification 0.1 . [Online] March 2020. https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html#_1j0vun2r7rgb .

6. **CISCO.** Introduction to Firepower Threat Defense REST API. *Cisco Developer.* [Online] Cisco systems. https://developer.cisco.com/docs/ftd-api-reference/latest/.

7. —. Secure Firewall Threat Defense (FTD) API. *Cisco Developer.* [Online] CISCO systems. https://developer.cisco.com/secure-firewall/.

8. **OASISS OPEN.** CACAO Security Playbooks Version 2.0. [Online] 2023. https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd01/security-playbooks-v2.0-csd01.html.

8.1.1.1 ANNEX DETAILS on Infrastructure

PUC1 devices

Devices at Datacenter located at Ca l'Alier	Devices at tram station – Pledger devices	Other Devices at IRIS Sandbox at Cisco
Cisco Switch Catalyst 9300	Cisco Switch Catalyst IE3200 (to be deployed)	Cisco Gateway (MX68CW-WW) (VPN to DC ca lAlier)
Cisco Firewall Firepower	Cisco sensor IC3000 (to be deployed)	Switch Cisco (MS120-8FP)
Cisco UCS Server with ESXI containing.	Pledger device - Odroid-H2+ [4]	Cisco Sensor IC-3000 [5]
Cisco Cyber Vision: • Cybervision provides syslog messages to ATOS syslog about events detected an asset inventory throught REST API • Kali Server used to simulate attacks • NIGHTWATCH Probe sensor	Pledger device - Radio Node device[6]	IP Camera MV12WE[7]

4 https://www.odroid.co.uk/ODroid-H2
5 https://www.cisco.com/c/en/us/products/collateral/routers/3000-series-industrial-compute-gateways/datasheet-c78-741204.html
6 Gateworks Newport https://www.gateworks.com/products/industrial-single-board-computers/octeon-tx-single-board-computers-gateworks-newport/gw6400-single-board-computer/
7 https://meraki.cisco.com/products/smart-cameras/models/

Air Quality Sensor from Bettair[8]	N/A	Cisco IP Camera 8000 [9]
IP Camera MV22X[10]	N/A	Air Quality Sensor from Bettair[11]
N/A	N/A	IP Camera MV12WE [12]

PUC2 devices

Simulated devices of Autonomous Vehicle Infrastructure	Physical devices available (already installed) as part of the Autonomous Vehicle Infrastructure	Physical devices available as part of the infrastructure:
SIVI sensor	LiDAR Sensor (Used on the vehicle is the Velodyne VLP-16) – Digital Twin of the physical device	To be decided
Urban Operating Platform	API platform for smart city data collection and visualisation	To be decided

PUC3 devices

Simulated devices of Residential Building Infra and Substation Infrastructure	Physical devices available (already installed) as part of the residential building infrastructure:	Physical devices available as part of the substation infrastructure:
SIVI sensor	Remote terminal unit – RTU560 CMG	To be decided
Residential device (SiHoneyPot)	Logic controller Wiser (KNX) LSS100100 https://thebluenx.store/products/wiser-for-knx	To be decided
Virtual Digital twin gateway	Remote terminal units I/O – RTU560 I/O	To be decided
N/A	Apartment KNX/IP modules	To be decided
N/A	Access to the internal network – Tosibox Lock 500 https://www.tosibox.com/for-sites-tosibox-lock-500	To be decided

[8] https://bettaircities.com/
[9] https://www.cisco.com/c/en/us/products/collateral/connected-safety-security/video-surveillance-8000-series-ip-cameras/datasheet-c78-739216.html
[10] https://meraki.cisco.com/products/smart-cameras/models/
[11] https://bettaircities.com/
[12] https://meraki.cisco.com/products/smart-cameras/models/

N/A	Extra firewall device – Cisco AS5505	To be decided
N/A	Industrial grade Linux device – Advantech UNO2372G https://www.advantech.com/en-eu/products/1-2mlj9a/uno-2372g/mod_f4ff5680-f016-44bd-bff0-e5eddfd82237	To be decided

Due to the requirement of the VCR to have infrastructure components (devices) running on the virtual machine, some devices will be simulated in the VCR environment's VM running sending/receiving scripts (HTTPs push messages sending JSON payload), acting as real infrastructure devices. Such scripts, simulating both residential and substation infrastructure devices will be sending real device's data repeatedly. Data consistency and format will be provided as is.

8.1.1.2 ANNEX JSON FILES

VDM


```
{
   "type": "bundle",
   "id": "bundle--ccc3ed11-31f1-4219-8354-612e4f60650f",
   "objects": [
      {
         "type": "vulnerability",
         "spec_version": "2.1",
         "id": "vulnerability--3448b69e-01fc-445c-9730-78388d2ec9cd",
         "created": "2023-06-21T08:39:33.975624Z",
         "modified": "2023-06-21T08:39:33.975624Z",
         "name": "SSL/TLS: Certificate Expired",
         "description": "The remote server's SSL/TLS certificate has already expired.",
         "labels": [
            "SSL and TLS"
         ]
```

```
    },
    {
        "type": "vulnerability",
        "spec_version": "2.1",
        "id": "vulnerability--5277a548-edb2-4d8f-bfa0-e89ab42645c3",
        "created": "2023-06-21T08:39:34.199215Z",
        "modified": "2023-06-21T08:39:34.199215Z",
        "name": "SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection",
        "description": "It was possible to detect the usage of the deprecated TLSv1.0\n and/or TLSv1.1 protocol on this system.",
        "labels": [
            "SSL and TLS"
        ],
        "confidence": 98,
        "external_references": [
            {
                "source_name": "cve",
                "url": "https://ssl-config.mozilla.org/",
                "hashes": {
                    "SHA-256":
"529b0eabe2ed573a1f35015cc3b4647df981372aa1f46e83026c31643c59a610"
                },
                "external_id": "CVE-2015-0204"
            },
            {
                "source_name": "cve",
                "url": "https://bettercrypto.org/",
                "hashes": {
                    "SHA-256":
"edc4688ae3c5afc26bb95dcc4ada115d45f0c6d541884150552dccb8d1deaf09"
```

```
            },
            "external_id": "CVE-2015-0204"
        },
        {
            "source_name": "cve",
            "url": "https://datatracker.ietf.org/doc/rfc8996/",
            "hashes": {
                "SHA-256":
"40559e823485685d334bcb2ab1161459e9a273d2dd94a5b0ebf482c4c7f32394"
            },
            "external_id": "CVE-2015-0204"
        },
        {
            "source_name": "cve",
            "url": "https://vnhacker.blogspot.com/2011/09/beast.html",
            "hashes": {
                "SHA-256":
"5bbfb1bf0ca5ebf87729969e57c26b8f8ec6a580e1dea33d0c6531a1664a2517"
            },
            "external_id": "CVE-2015-0204"
        },
        {
            "source_name": "cve",
            "url":
"https://web.archive.org/web/20201108095603/https://censys.io/blog/freak",
            "hashes": {
                "SHA-256":
"87e630bee3c6b9ff53c33bb4816b576fee38ff04020060f0d37a15574ced4f42"
            },
            "external_id": "CVE-2015-0204"
```

```
            },
            {
                "source_name": "cve",
                "url":     "https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014",
                "hashes": {
                    "SHA-256": "9fdcaff4c36b68db83c01395a139c29208972f1910d90be15bbc075972dc3f88"
                },
                "external_id": "CVE-2015-0204"
            },
            {
                "source_name": "cwe",
                "url": "https://cwe.mitre.org/data/definitions/310.html",
                "hashes": {
                    "SHA-256": "057ae8243238bb29aa57c2257c6901cc2253b16f0ceac479c3781767d3a37ff6"
                },
                "external_id": "CWE-310"
            }
        ]
    },
    {
        "type": "attack-pattern",
        "spec_version": "2.1",
        "id": "attack-pattern--f5ab1c61-523f-4da4-bd0a-c8e76814405b",
        "created": "2023-06-21T08:39:34.201263Z",
        "modified": "2023-06-21T08:39:34.201263Z",
        "name": "CAPEC-485",
```

```
        "description": "An attacker obtains an authoritative or reputable signer's private signature key by exploiting a cryptographic weakness in the signature algorithm or pseudorandom number generation and then uses this key to forge signatures from the original signer to mislead a victim into performing actions that benefit the attacker.",
        "external_references": [
          {
            "source_name": "capec",
            "url": "https://capec.mitre.org/data/definitions/485.html",
            "hashes": {
              "SHA-256": "2b9ca752b021acc9ab204879696f69a51719aee9ba46c84021b82d567eed968a"
            },
            "external_id": "CAPEC-485"
          }
        ]
      },
      {
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--9371e03b-4828-423d-a7fa-cdcad63bb49c",
        "created": "2023-06-21T08:39:37.44812Z",
        "modified": "2023-06-21T08:39:37.44812Z",
        "relationship_type": "targets",
        "source_ref": "attack-pattern--f5ab1c61-523f-4da4-bd0a-c8e76814405b",
        "target_ref": "vulnerability--5277a548-edb2-4d8f-bfa0-e89ab42645c3"
      },
      {
        "type": "identity",
        "spec_version": "2.1",
        "id": "identity--b62a8c47-dba3-496f-9db2-0880895cb417",
```

```
        "created": "2023-06-21T08:39:37.449488Z",
        "modified": "2023-06-21T08:39:37.449488Z",
        "name": "VDM",
        "identity_class": "system"
    },
    {
        "type": "identity",
        "spec_version": "2.1",
        "id": "identity--08d80953-8682-4d26-9ba6-4c327737ad3e",
        "created": "2023-06-21T08:39:37.449806Z",
        "modified": "2023-06-21T08:39:37.449806Z",
        "name": "org1",
        "identity_class": "organization"
    },
    {
        "type": "observed-data",
        "spec_version": "2.1",
        "id": "observed-data--5105d564-dee8-4249-bf63-371e42bfd724",
        "created": "2023-06-21T08:39:37.450823Z",
        "modified": "2023-06-21T08:39:37.450823Z",
        "first_observed": "2023-06-21T08:39:28.888Z",
        "last_observed": "2023-06-21T08:39:33.949832Z",
        "number_observed": 1,
        "objects": {
            "1": {
                "type": "ipv4-addr",
                "spec_version": "2.1",
                "id": "ipv4-addr--977fff1a-da35-5e82-8534-551137fd0ddb",
```

```
                "value": "10.0.2.4"
            }
        }
    },
    {
        "type": "report",
        "spec_version": "2.1",
        "id": "report--47081722-ac7b-4be8-9aae-85372fbeb776",
        "created_by_ref": "identity--b62a8c47-dba3-496f-9db2-0880895cb417",
        "created": "2023-06-21T08:39:37.451757Z",
        "modified": "2023-06-21T08:39:37.451757Z",
        "name": "VDM Report",
        "description": "Vulnerability report generated by Vulnerability Discovery Manager",
        "report_types": [
            "vulnerability"
        ],
        "published": "2023-06-21T08:39:37.451745Z",
        "object_refs": [
            "vulnerability--3448b69e-01fc-445c-9730-78388d2ec9cd",
            "vulnerability--5277a548-edb2-4d8f-bfa0-e89ab42645c3",
            "attack-pattern--f5ab1c61-523f-4da4-bd0a-c8e76814405b",
            "relationship--9371e03b-4828-423d-a7fa-cdcad63bb49c"
        ]
    }
  ],
  "created_by_ref": "identity--08d80953-8682-4d26-9ba6-4c327737ad3e"
}
```

BINSEC


```
{
   "type": "bundle",
   "id": "bundle--2ac7882f-76a3-4a9b-97b3-811b3af1c7c0",
   "objects": [
      {
         "type": "identity",
         "spec_version": "2.1",
         "id": "identity--sabr-cea-list",
         "created": "2015-02-24T15:50:10.564Z",
         "modified": "2015-02-24T15:50:10.564Z",
         "name": "SABR Team, CEA List",
         "roles": [
            "Cyber Security"
         ],
         "identity_class": "organization",
         "sectors": [
            "technology"
         ],
         "contact_information": "sebastien.bardin@cea.fr"
      },
      {
         "type": "tool",
         "spec_version": "2.1",
         "id": "tool--binsec",
         "created_by_ref": "identity--sabr-cea-list",
         "created": "2016-04-06T20:03:48.000Z",
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

```
    "modified": "2016-04-06T20:03:48.000Z",
    "tool_types": ["vulnerability-scanning"],
    "name": "Binsec"
},
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--puc-xxx",
    "created": "2015-02-24T15:50:10.564Z",
    "modified": "2015-02-24T15:50:10.564Z",
    "name": "PUC provider XXX",
    "roles": [
        "Smart city"
    ],
    "identity_class": "organization",
    "sectors": [
        "technology","government-local"
    ],
    "contact_information": "john.smith@pucXXX.fr"
},
{
    "type":"infrastructure",
    "spec_version": "2.1",
    "id":"infrastructure--binary-xxx-zzzzzz",
    "created_by_ref": "identity--puc-xxx",
    "created":"2016-05-07T11:22:30.000Z",
    "modified":"2016-05-07T11:22:30.000Z",
    "name":"Binary File ZZZZZZ",
```

```
    "infrastructure_types": ["undefined"]
  },
  {
    "type": "report",
    "spec_version": "2.1",
    "id": "report--binsec-analysis-of-binary-xxx-zzzzzz",
    "created_by_ref": "identity--sabr-cea-list",
    "created": "2017-12-21T19:59:11.000Z",
    "modified": "2017-12-21T19:59:11.000Z",
    "name": "Binsec analysis of YYYYYY binary from XXX",
    "published": "2017-01-20T17:00:00.000Z",
    "report_types": ["vulnerability"],
    "object_refs": [
      "tool--binsec",
      "infrastructure--binary-xxx-zzzzzz",
      "vulnerability--invalid-memory-access-binary-xxx-zzzzzz-loc-4525",
      "relationship--binsec-targets-invalid-memory-access-XXX-YYYYYY-4525",
      "relationship--binary-XXX-YYYYYY-has-invalid-memory-access-at-loc-4525"
    ]
  },
  {
    "type": "vulnerability",
    "spec_version": "2.1",
    "id": "vulnerability--invalid-memory-access-binary-xxx-zzzzzz-loc-4525",
    "created": "2017-12-21T19:59:11.000Z",
    "modified": "2017-12-21T19:59:11.000Z",
    "created_by_ref": "identity--sabr-cea-list",
    "name": "Invalid memory access in ZZZZZZ binary from XXX at line 4525",
```


```
      "external_references": [
       {
        "source_name": "Binsec",
        "description": "Binsec-specific data about found vulnerability"
       }
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--binsec-targets-invalid-memory-access-XXX-YYYYYY-4525",
      "created": "2017-12-21T19:59:11.000Z",
      "modified": "2017-12-21T19:59:11.000Z",
      "relationship_type": "targets",
      "source_ref": "tool--binsec",
      "target_ref": "vulnerability--invalid-memory-access-binary-xxx-zzzzzz-loc-4525"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--binary-XXX-YYYYYY-has-invalid-memory-access-at-loc-4525",
      "created": "2017-12-21T19:59:11.000Z",
      "modified": "2017-12-21T19:59:11.000Z",
      "relationship_type": "has",
      "source_ref": "infrastructure--binary-xxx-zzzzzz",
      "target_ref": "vulnerability--invalid-memory-access-binary-xxx-zzzzzz-loc-4525"
    }
]
```

```
}
```


NIGHTWATCH


```
{
    "type": "bundle",
    "id": "bundle--2955987b-3a0c-4b0b-9036-2419fd176f71",
    "objects": [
        {
            "type": "report",
            "spec_version": "2.1",
            "id": "report--395846ee-d6b5-493a-a86c-774b19233287",
            "created_by_ref": "identity--4606ab85-e3f2-4326-8332-7e1ee8137f27",
            "created": "2023-06-14T14:29:46.722594Z",
            "modified": "2023-06-14T14:29:46.722594Z",
            "name": "Suspicious number of failed  SSH login / authentication attempts in small time window",
            "description": " Internal host 192.168.2.200 has generated a high rate of failed SSH authentication / login attempts to 192.168.2.103 in a small amount of time. ",
            "report_types": [
                "threat-report"
            ],
            "published": "2023-06-14T14:29:46.722Z",
            "object_refs": [
                "indicator--bee4622b-8b0f-406d-ac11-cf167dc6e90b",
                "indicator--2329e690-52fa-438e-af35-8853f1415f9c"
            ],
            "extensions": {
                "extension-definition--23948758-742a-45fe-9b94-1737110549ab": {
                    "extension_type": "property-extension",
```

```
                "organisation": "Org1",
                "source": "Nightwatch",
                "status": "Open",
                "threat_description": "unknown",
                "detection_summary": " Internal host 192.168.2.200 has generated a high rate of failed SSH authentication / login attempts to 192.168.2.103 in a small amount of time. ",
                "actor": "192.168.2.200",
                "target": "192.168.2.103",
                "dst_port": 22,
                "duration": 327.29,
                "severity": "High",
                "risk_score": 79,
                "confidence": 0.999992,
                "service_indicator": "SSH",
                "mitre_attack": {
                    "Lateral Movement": {
                        "Remote Services": "T0866"
                    }
                }
            }
        }
    },
    {
        "type": "identity",
        "spec_version": "2.1",
        "id": "identity--4606ab85-e3f2-4326-8332-7e1ee8137f27",
        "created": "2023-06-14T14:29:46.71583Z",
        "modified": "2023-06-14T14:29:46.71583Z",
```

```
        "name": "CLS-NightWatch",
        "identity_class": "organization",
        "lang": "en"
    },
    {
        "type": "extension-definition",
        "spec_version": "2.1",
        "id": "extension-definition--23948758-742a-45fe-9b94-1737110549ab",
        "created_by_ref": "identity--4606ab85-e3f2-4326-8332-7e1ee8137f27",
        "created": "2023-06-14T14:29:46.71583Z",
        "modified": "2023-06-14T14:29:46.71583Z",
        "name": "Detection properties extension",
        "description": "Additional properties observed by the Threat Intelligence identity",
        "schema": "https://www.fsisac.com/stixtaxii/schemas/ctix-vuln/v1/",
        "version": "1.0",
        "extension_types": [
            "property-extension"
        ]
    },
    {
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--bee4622b-8b0f-406d-ac11-cf167dc6e90b",
        "created": "2023-03-10T10:24:16.000Z",
        "modified": "2023-03-10T10:29:43.000Z",
        "name": "Step 0 - Indicator 1",
        "description": " 81 failed successive SSH login / auth attempts in 5 minutes,27.293
seconds",
        "indicator_types": [
```

```
            "malicious-activity"
        ],
        "pattern": "[ipv4-addr:value ='192.168.2.200']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-03-10T10:24:16Z",
        "kill_chain_phases": [
            {
                "kill_chain_name": "lockheed-martin-cyber-kill-chain",
                "phase_name": "lateral-movement"
            }
        ]
    },
    {
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--2329e690-52fa-438e-af35-8853f1415f9c",
        "created": "2023-03-10T10:24:16.000Z",
        "modified": "2023-03-10T10:29:43.000Z",
        "name": "Step 1 - Indicator 1",
        "description": "Rare SSH client fingerprint for SSH authentication attempt",
        "indicator_types": [
            "malicious-activity"
        ],
        "pattern": "[ipv4-addr:value ='192.168.2.200']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-03-10T10:24:16Z",
```

```
        "kill_chain_phases": [
          {
            "kill_chain_name": "lockheed-martin-cyber-kill-chain",
            "phase_name": "lateral-movement"
          }
        ]
      }
   ]
}
```


Sivi


```
{
        "type": "bundle",
        "id": "bundle--8f682731-48d9-4e5c-b96d-7890627dd1c8",
        "objects": [
                {
                        "type": "report",
                        "spec_version": "2.1",
                        "id": "report--39997819-1240-4419-a5f9-4abba057a3b2",
                        "created_by_ref": "identity--f7e220eb-ebf7-4c59-bfde-3931487c63fc",
                        "created": "2023-07-13T13:59:05.559002Z",
                        "modified": "2023-07-13T13:59:05.559002Z",
                        "name": "Suspicious number of connections / attempts in small time window",
                        "description": "A possible DDoS Attack was detected on host 192.168.16.7 from 192.168.16.3",
                        "report_types": [
                                "threat-report"
                        ],
```

```
                "published": "2022-06-29T16:35:31.531Z",
                "object_refs": [
                        "indicator--a92d24d6-ef54-41d1-8707-67e320651782"
                ],
                "extensions": {
                        "extension-definition--099e52c5-d6c1-4599-9868-
d34f2b917add": {
                                "extension_type": "property-extension",
                                "organisation": "Org1",
                                "source": "Sivi",
                                "status": "Open",
                                "threat_description": "DDoS Attack",
                                "detection_summary": "A possible DDoS Attack was
detected on host 192.168.16.7 from 192.168.16.3 in a small ammount of time",
                                "actor": "192.168.16.3",
                                "target": "192.168.16.7",
                                "dst_port": "9001",
                                "severity": "High",
                                "risk_score": 80,
                                "confidence": 0.999999
                        }
                }
        },
        {
                "type": "identity",
                "spec_version": "2.1",
                "id": "identity--f7e220eb-ebf7-4c59-bfde-3931487c63fc",
                "created": "2023-07-13T13:59:05.557001Z",
                "modified": "2023-07-13T13:59:05.557001Z",
```

```
                "name": "Sidroco",
                "identity_class": "organization",
                "lang": "en"
        },
        {
                "type": "indicator",
                "spec_version": "2.1",
                "id": "indicator--a92d24d6-ef54-41d1-8707-67e320651782",
                "created": "2023-07-13T13:59:05.518996Z",
                "modified": "2023-07-13T13:59:05.518996Z",
                "name": "Cyberattack on host 192.168.16.7",
                "description": "A cyberattack was detected on host 192.168.16.7 from 192.168.16.3",
                "pattern": "[network-traffic:x_destination_port = '9001' AND network-traffic:x_destination_ip = '192.168.16.7']",
                "pattern_type": "stix",
                "pattern_version": "2.1",
                "valid_from": "2023-07-13T13:59:05.518996Z",
                "labels": [
                        "malicious-activity"
                ]
        },
        {
                "type": "ipv4-addr",
                "spec_version": "2.1",
                "id": "ipv4-addr--15cd3d64-9eae-5071-a67f-b5673381f2be",
                "value": "192.168.16.3"
        },
        {
```

```
                        "type": "ipv4-addr",
                        "spec_version": "2.1",
                        "id": "ipv4-addr--1418c268-b05b-5fab-8856-c6149a68f31a",
                        "value": "192.168.16.7"
                },
                {
                        "type": "observed-data",
                        "spec_version": "2.1",
                        "id": "observed-data--7f612d7b-9cf4-42e8-9915-f2cf5f58f585",
                        "created": "2023-07-13T13:59:05.561Z",
                        "modified": "2023-07-13T13:59:05.561Z",
                        "first_observed": "2022-06-29T16:35:31.531Z",
                        "last_observed": "2022-06-29T16:35:31.531Z",
                        "number_observed": 1,
                        "object_refs": [
                                "ipv4-addr--15cd3d64-9eae-5071-a67f-b5673381f2be",
                                "ipv4-addr--1418c268-b05b-5fab-8856-c6149a68f31a"
                        ]
                }
        ]
}
```


SiHoneypots


```
{
   "type" : "bundle",
   "id" : "bundle--111fd7e6-5f88-4bdc-a115-e34854e76427",
   "objects" : [
```

```
    {
        "type": "infrastructure",
        "name": "Honeypot-X",
        "id": "infrastructure--8ac90ff3-ecf8-4835-95b8-6aea6a623df5",
        "spec_version": "2.1",
        "created" : "2023-06-26T12:05:25",
        "modified" : "2023-06-26T12:05:25",
        "description" : "Host X contacted honeypot. Data request: {011DA2F86}. Data reply: {0B4022FF}",
        "infrastructure_type" : "honeypot"
    },
    {
        "type": "attack-pattern",
        "name": "DoS attack on IoT device",
        "id": "attack-pattern--8ac90ff3-ecf8-4835-95b8-6aea6a623df5",
        "spec_version": "2.1",
        "created": "2023-06-26T12:05:25",
        "modified": "2023-06-26T12:05:25",
        "external_refernces": [
            {
                "source_name": "Excavation",
                "description": "An adversary actively probes the target in a manner that is designed to solicit information that could be leveraged for malicious purposes.",
                "url": "https://capec.mitre.org/data/definitions/116.html",
                "external_id": "CAPEC-116"
            }
        ]
    },
    {
```

```
            "type" : "threat-actor",
            "spec_version" : "2.1",
            "id" : "intrusion-set--ed69460a-f067-ba6y-9ba2-c4616b9a6713",
            "name" : "Attacker-IP-1.2.3.4",
            "created" : "2023-06-26T12:05:25",
            "modified" : "2023-06-26T12:05:25",
            "description" : "IP 1.2.3.4 has communicated with the honeypot XXXX. This device may be compromised"
        }
    ]
}
```


MAI-GUARD


```
{
    "type": "bundle",
    "id": "bundle--2ac7882f-76a3-4a9b-97b3-811b3af1c7c0",
    "objects": [
        {
            "type": "identity",
            "spec_version": "2.1",
            "id": "identity--b7a579a2-d4af-4a32-b3b6-ea29e5a2f743",
            "created": "2020-02-02T15:50:10.564Z",
            "modified": "2020-02-02T15:50:10.564Z",
            "name": "INUM Team, CEA CTReg DSUD",
            "roles": [
                "Embed Artificial Intelligence"
            ],
            "identity_class": "organization",
            "sectors": [
```

```
            "technology"
        ],
        "contact_information": "javier.gil-quijano@cea.fr"
    },
    {
        "type": "tool",
        "spec_version": "1.3",
        "id": "tool--789e2a3f-bc5a-4d2f-a0c6-f7a4e0435f3a",
        "created_by_ref": "identity--b7a579a2-d4af-4a32-b3b6-ea29e5a2f743",
        "created": "2022-01-10T10:05:30.000Z",
        "modified": "2023-07-06T18:08:52.000Z",
        "tool_types": ["adversarial-examples-detection"],
        "name": "MAI-GUARD"
    },
    {
        "type": "identity",
        "spec_version": "2.1",
        "id": "identity--d2a2e2f6-4d99-4f8b-8f50-4f8ed3178427",
        "created": "2023-03-30T15:50:10.564Z",
        "modified": "2023-03-30T15:50:10.564Z",
        "name": "PUC provider 2",
        "roles": [
            "Public transportation"
        ],
        "identity_class": "organization",
        "sectors": [
            "technology",
            "government-local"
```

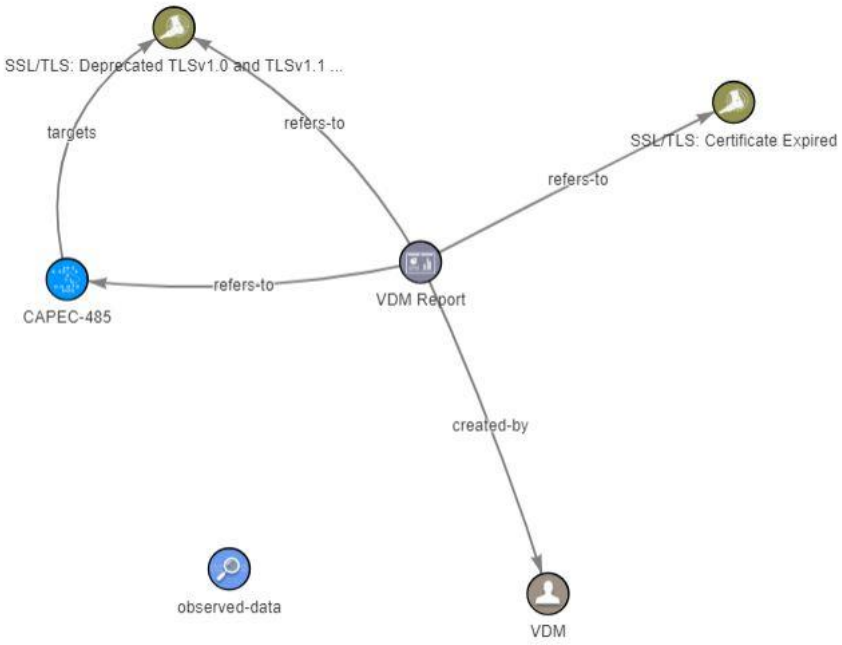
```
        ],
        "contact_information": "john.smith@puc2.com"
    },
    {
        "type": "x-attack-target",
        "spec_version": "2.1",
        "id": "x-attack-target--76d3a6c9-efba-40e3-98b7-e1fca4dfe1c4",
        "created": "2023-07-13T14:12:05.559002Z",
        "modified": "2023-07-13T14:12:05.559002Z",
        "name": "AUV Camera System",
        "description": "Camera on a given AUV that is susceptible to adversarial attacks.",
        "object_id": "AUV-XXX-CAM-XXX"
    },
    {
        "type": "report",
        "spec_version": "2.1",
        "id": "report--39997820-1240-4419-a5f9-4abba057a3c3",
        "created_by_ref": "identity--f7e220ec-ebf7-4c59-bfde-3931487c64fd",
        "created": "2023-07-13T14:10:05.559002Z",
        "modified": "2023-07-13T14:10:05.559002Z",
        "name": "Misclassification of traffic sign",
        "description": "A possible adversarial attack was detected on an autonomous vehicle's vision system.",
        "report_types": [
            "threat-report"
        ],
        "published": "2023-07-13T14:10:05.559002Z",
        "object_refs": [
            "indicator--a92d24d7-ef54-41d1-8707-67e320651783"
```

```
        ],
        "extensions": {
            "extension-definition--099e52c6-d6c1-4599-9868-d34f2b917add": {
                "extension_type": "property-extension",
                "organisation": "identity--d2a2e2f6-4d99-4f8b-8f50-4f8ed3178427",
                "target": " x-attack-target--76d3a6c9-efba-40e3-98b7-e1fca4dfe1c4",
                "status": "Open",
                "threat_description": "Adversarial Attack on Vision System",
                "detection_summary": "A manipulated image was processed leading to a misclassification of a traffic sign.",
                "severity": "Medium",
                "risk_score": 70,
                "confidence": 0.85
            }
        }
    },
    {
        "type": "identity",
        "spec_version": "2.1",
        "id": "identity--f7e220ec-ebf7-4c59-bfde-3931487c64fd",
        "created": "2023-07-13T14:10:05.557001Z",
        "modified": "2023-07-13T14:10:05.557001Z",
        "name": "PUC Incident Response",
        "identity_class": "organization",
        "lang": "en"
    },
    {
        "type": "indicator",
        "spec_version": "2.1",
```

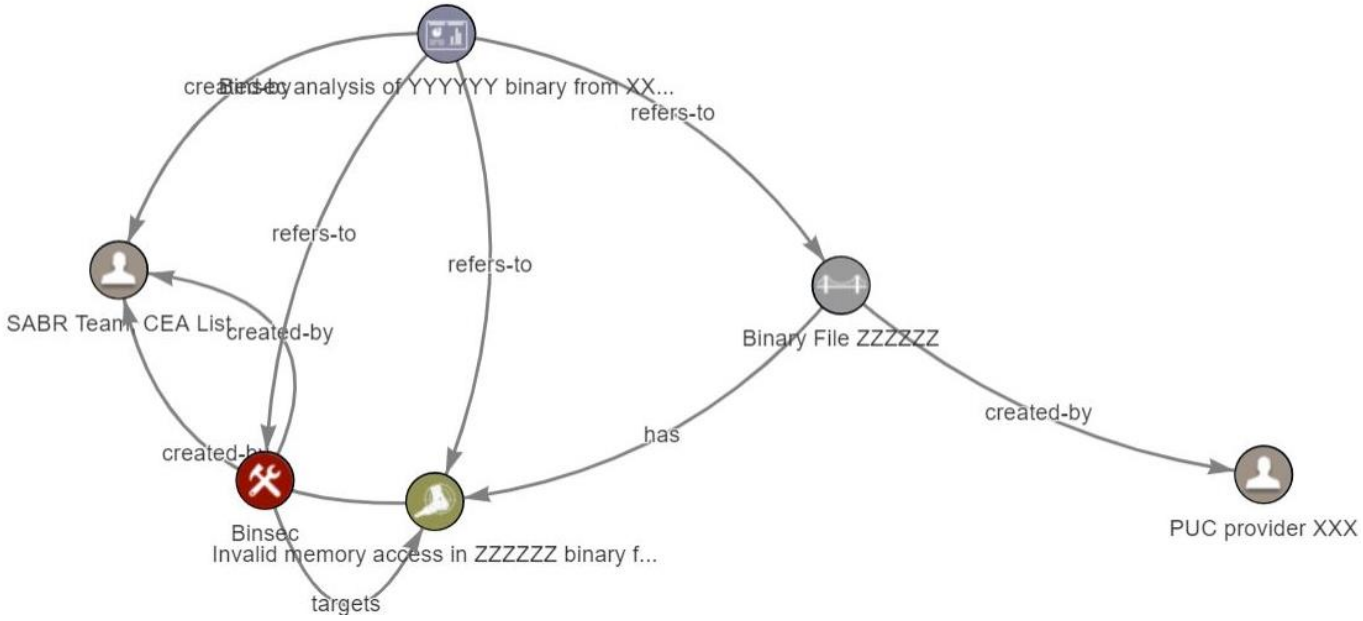
```
        "id": "indicator--a92d24d7-ef54-41d1-8707-67e320651783",
        "created": "2023-07-13T14:10:05.518996Z",
        "modified": "2023-07-13T14:10:05.518996Z",
        "name": "Adversarial manipulation of image",
        "description": "The vision system processed an image that was potentially manipulated to mislead detection.",
        "pattern": "[file:image_hash = 'abc123def456' AND file:name = 'adversarial_image.png']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-07-13T14:10:05.518996Z",
        "labels": [
          "malicious-manipulation"
        ]
      }
  ]
}
```


8.1.1.3 ANNEX ATA Modules STIX2.1 Data models

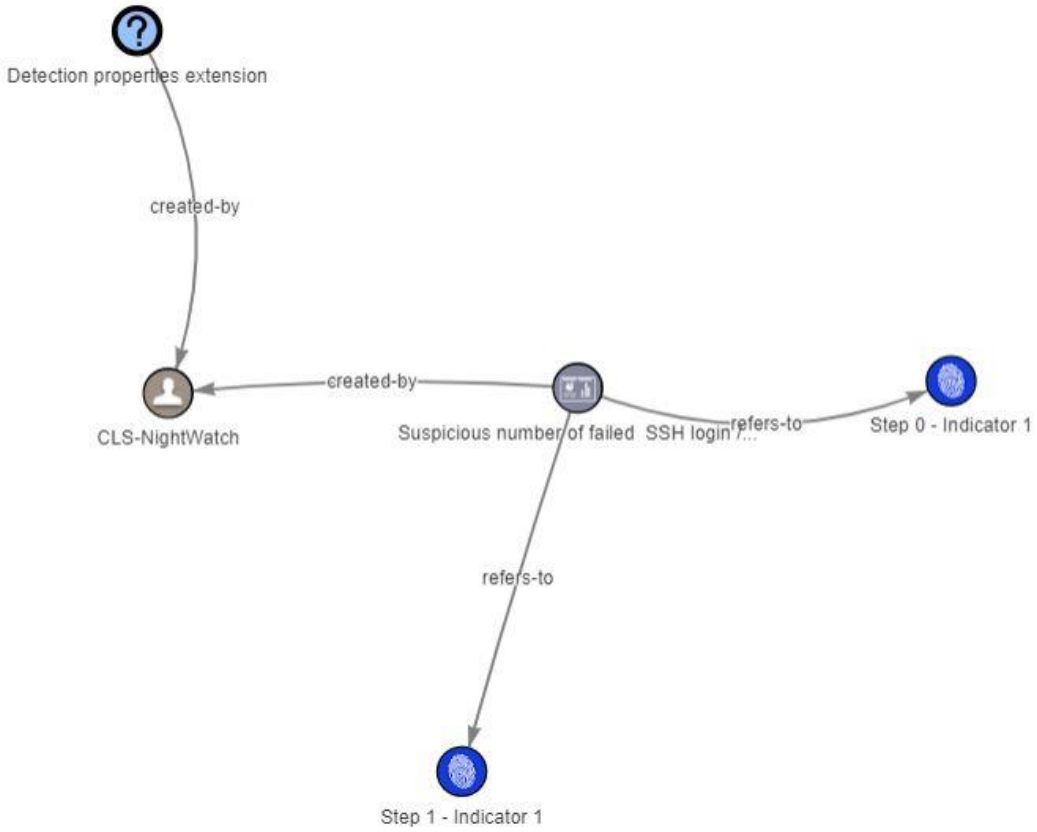
VDM


SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 ...
targets
refers-to
SSL/TLS: Certificate Expired
refers-to
CAPEC-485
refers-to
VDM Report
created-by
observed-data
VDM

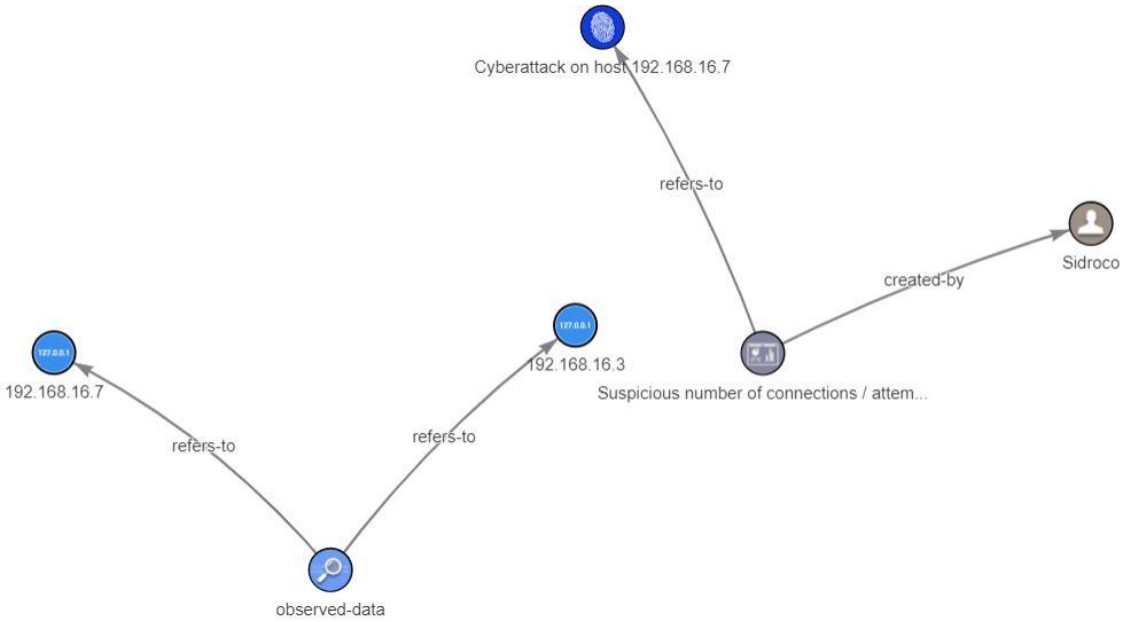
BINSEC


created-by
Binsec analysis of YYYYYY binary from XX...
refers-to
refers-to
refers-to
SABR Team, CEA List
created-by
Binary File ZZZZZZ
created-by
has
created-by
Binsec
Invalid memory access in ZZZZZZ binary f...
PUC provider XXX
targets

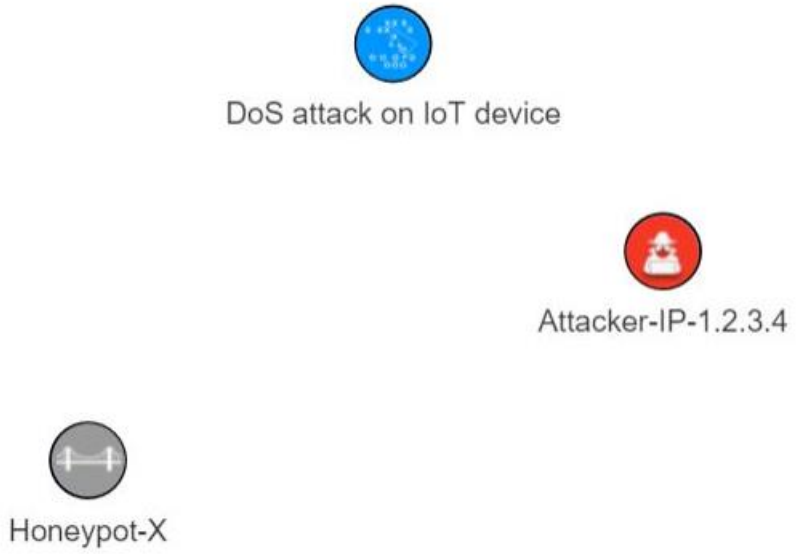
NIGHTWATCH



SIVI



SIHONEYPOTS



MAI-GUARD