E-CORRIDOR
Edge Enabled Privacy & Security Platform
For Multi Modal Transport

D 4.2

ISAC Pilot Architecture

WP4 – ISAC Pilot

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 31/05/2021
Actual submission date: 31/05/2021

Responsible partner: MISE

Editor: Sandro Mari

E-mail address: sandro.mari@mise.gov.it

31/05/2021

Version 1.0

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Authors: **Giacomo Giorgi (CNR), Andrea Saracino (CNR), Sandro Mari (MISE)**

Approved by: **Stefano Sebastio (UTRC), Riccardo Orizio (UTRC)**

Revision History

Version	**Date**	**Name**	**Partner**	**Sections Affected / Comments**
0.1	01-Mar-2021	G. Giorgi, A. Saracino S. Mari	CNR, MISE	Initial ToC
0.2	07- Apr-2021	G. Giorgi	CNR	Revision architecture components
0.3	21-Apr-2021	G. Giorgi A. Saracino	CNR	Architecture components description Analytic description
0.4	26-Apr-2021	G. Giorgi A. Saracino	CNR	Data model, security model, deploying model.
0.5	30-Apr-2021	G. Giorgi A. Saracino	CNR	Contribution towards E-CORRIDOR objective, conclusion
0.6	12-May-2021	R. Orizio S. Sebastio	UTRC	Revision
1.0	25-May-2021	G. Giorgi A. Saracino	CNR	Added interconnection with other pilot section, revised figures, table of content, bibliography and glossary.
1.0	28-May-2021	G. Giorgi A. Saracino S. Mari	CNR MISE	Final revision

Executive Summary

This deliverable presents the first version of the ISAC pilot architecture. Building on the results of Deliverable D4.1 [1], in this deliverable it will be shown how the ISAC architecture will match the pilot requirements, presenting both a high level and detailed view of the architectural component. The ISAC pilot is general and imposes noticeable challenges, since, differently from other pilots, it has to be ready to receive and handle any possible type of CTI information, managing data with different format and semantic from other pilots. After presenting the architectural model, the relevant Use Cases presented in Deliverable D4.1 [1] are addressed by new architecture diagrams that will be used to guide the implementation phase, in particular those for data collection, dispatching and visualization. Afterward, the deliverable will delve in the data which will be used for analysis, their format, and desired analysis. The deliverable will close with considerations on security, deploying model, contributions to the E-CORRIDOR objectives, requirements matching and plan of future work.

The content of the deliverable has been built in collaboration with E-CORRIDOR partners, taking into consideration that the ISAC pilot is in part dependant from the results of the other Pilots (WP2, WP3, WP7).

1. Introduction

1.1. Overview

The goal of the ISAC pilot is to provide analysis on cyber data collected from public sources and private stakeholders related to different transportation sectors. The analysis is oriented to aggregate different cyber knowledge to detect, anticipate, or mitigate cyber-security threats through the information dispatching or the security report presentation. In the following we will provide the description of the ISAC pilot architecture, mapping the E-CORRIDOR components in the specific pilot implementation. Furthermore, a description of the pilot specific analytics will be provided.

1.2. Structure of the Deliverable

The document is structured as follow:

Section 2 provides an overview of the ISAC pilot. Section 3 describes the system architecture. Section 4 describes in depth each architecture component, showing the interaction with the E-CORRIDOR framework. In addition, the behaviour of each architecture component is shown for each use cases presented in Deliverable D4.1 [1]. To the end of Section 4, the ISAC analytics and the corresponding data format used is described. Section 5 deals with the security model of the pilot focusing in particular on authentication and authorization. Section 6 presents the main technical requirements for the deployment of the pilot. Section 7 depicts the relation between the architecture diagrams and the user stories and use cases presented in Deliverable D4.1 [1]. Section 8 describes the contribution of the pilot towards the E- CORRIDOR framework. Finally, Section 9 concludes the deliverable and presents the future work.

2. System Overview

Interconnected Transportation Systems (automotive, aviation, railway) produce and consume a large amount of data. These pieces of information concerns both the operative side of the transports and of their users. Being a critical sector, motivation of attackers in targeting this is rising for several reasons, such as accessing private user information, causing denial of service with the intention of tampering reputation of rival companies, or even attempt to perform terrorist actions [1,2,3]. To prevent such attacks, it is required to have systems that can timely notify known vulnerabilities and strategies to address them, while keeping the privacy/control of shared information. If ones share the information on a 0-day vulnerability or an attack it might either compromise the reputation of a company or expose involuntarily a company to attacks due to disclosure of an existing vulnerability [4]. To this end the Information Sharing and Analysis Center (ISAC) can help critical transportation infrastructure owners and operators to protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyse and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. The ISAC can involve multiple transportation sector in the sharing and analysing process to the end to increase the overall picture of vulnerabilities and attacks of the whole transportation ecosystem and provide a notification system to timely react to possible cyber-attacks.

Through the E-CORRIDOR framework it is easier to gather and share data in a controlled manner, by leveraging purpose-specific Data Sharing Agreements, as specified in deliverable D6.1, and thus possibly control the analytics functions that can be applied on the shared data to discover possible cyber threats or anomaly events. This will allow transport services and infrastructures to exchange, retrieve and analyse in a privacy preserving manner information on vulnerabilities, attacks, safety issues, incident reports and other relevant data.

Through the ISAC, the interested stakeholder can receive information on course of actions to fix vulnerabilities, to mitigate or to stop ongoing attacks and/or to recover the system functionalities, after a successful attack. The ISAC can receive information from different stakeholders, which are aggregated in a collaborative manner and gives a global view of the whole multi-modal transport system. The correlated information will eventually provide a complete and timely view of the systems that might be affected by a vulnerability, or potential victim of a threat. Then, the interested stakeholders are immediately notified, while maintaining the privacy, if desired, of the initial provider of information. Figure 1 shows the main idea of the ISAC multimodal transportation (ISAC-MMT). It can collect heterogeneous information related to cyber-threat from different sources, i.e., (i) external ISACs, (ii) transportation sector organizations (automotive, railway, aviation companies), (iii) transportation edge devices (In-Vehicle Infotainment system, smartphones, cameras), (iv) cyber-thread public sources (vulnerabilities, exploits databases). Simultaneously the ISAC-MMT can manipulate and analyse and aggregate data collected to extract new cyber-threat knowledge. The main objective of the ISAC-MMT process is to dispatch the analysed knowledge to (i) the Small and Medium Enterprises (SMEs) that often struggle due to a lack of awareness, expertise, and resources to manage cyber-threats and, (ii) the transportation sector companies that have been shared its local information.

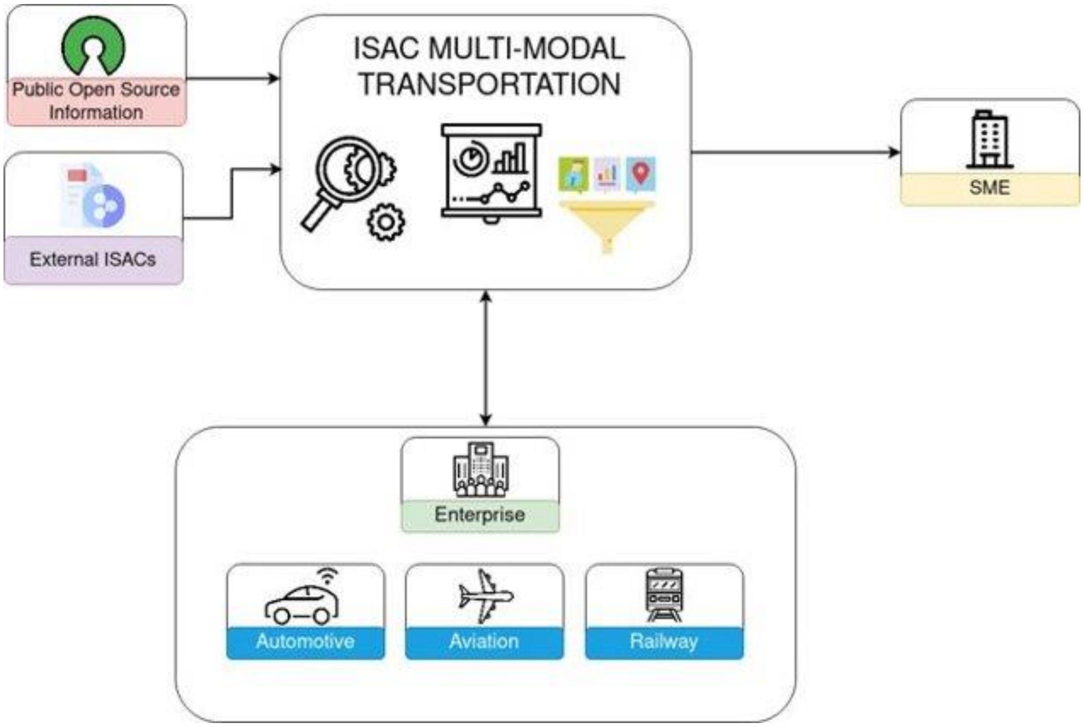

Public Open Source Information
External ISACs
ISAC MULTI-MODAL TRANSPORTATION
SME
Enterprise
Automotive
Aviation
Railway

Figure 1: ISAC overview

Summarizing, the main contributions offered by the ISAC pilot are:

- Collecting cyber-threat information
- Analysing data
- Dispatching information
- Presenting analysis

3. System Architecture

The ISAC pilot follows the mixed distributed architecture of the E- CORRIDOR framework showed in Figure 2 and defined in Deliverable D5.2 [6]. The Information Sharing Infrastructure (ISI) can be deployed both on the edge, i.e., in the local edge devices of the prosumer environment, and in the centralised ISAC infrastructure. Considering this approach, a locally instantiated ISI allows a producer to apply Data Sharing Agreement (DSA) policies locally in order to define some Data Manipulation Objects (DMOs) like data anonymisation before sharing its data with the centralised ISI infrastructure located in the ISAC premise. Like the ISI, the Information Analytic Infrastructure (IAI) can be instantiated on the edge to perform local analysis, or each prosumer can interact with the ISAC centralised IAI for the analytic services.

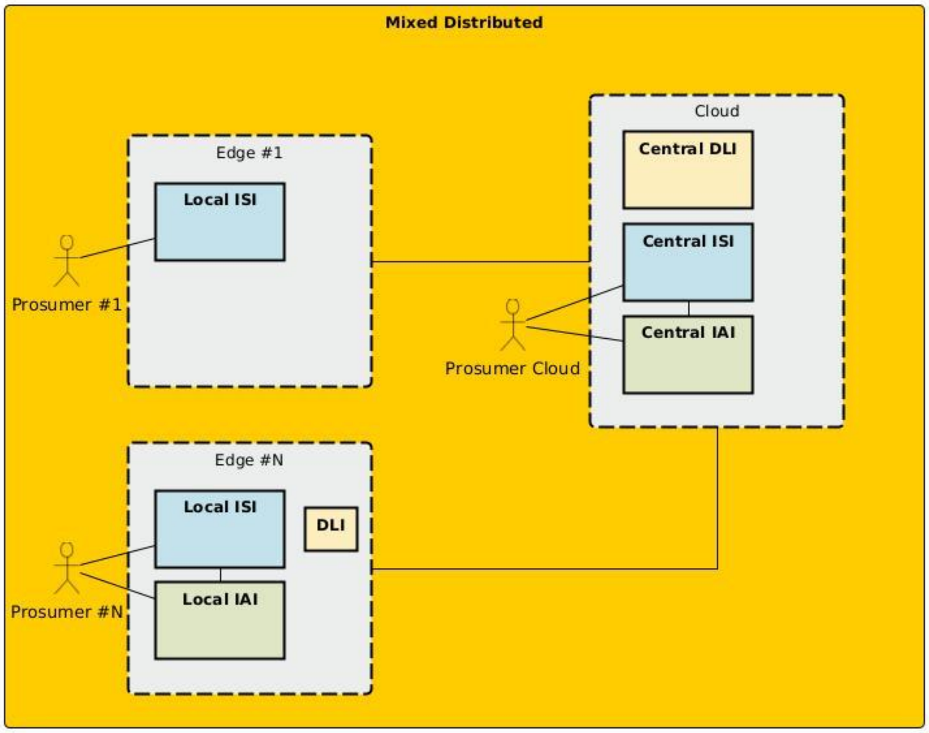


Figure 2: Mixed distributed architecture

An in-depth representation of the architecture is showed in Figure 3. In the architecture are defined different types of providers that are the representation of the stakeholders described in Section 2. As discussed, the data provider can interact with the ISAC premise in three different ways. A *passive provider* premise does not store neither the ISI nor the IAI in local, but it interacts directly with the ISI API exposed by the ISAC premise following the DSA defined in the Data Sharing Agreement (DSA) Lifecycle Infrastructure (DLI) of the ISAC premise. An *active provider* premise stores an instance of the ISI and DSA manager locally. The local DLI is used to define policies for the shared data before sharing them with the centralized ISI located in the ISAC premise. In such

way part of the policies will be enforced by the local ISI, and additional policies will be enforced by the remote ISI through the centralized DLI. Finally, an *active provider with analytics capabilities* premise stores locally both the ISI and the IAI instance. As the active provider, it can enforce policy on its data locally, before sharing with the ISAC, and in addition can run local analysis exploiting its IAI component. In such way, it can choose to share, with the ISAC, both its local collected data and the analytic results obtained by the local IAI. In both cases the data can be preliminarily manipulated according to the local ISI.
The ISAC premise is composed of the remote ISI through which it can enforce policies on the shared data, in particular the one related to data analysis obtained through the remote IAI and to result redistribution. The remote DSA manager is mainly used to define policies related to data storage and maintenance. The remote IAI has the function to perform collaborative analysis on the shared data and are invoked by the consumer request or directly by the ISAC itself.

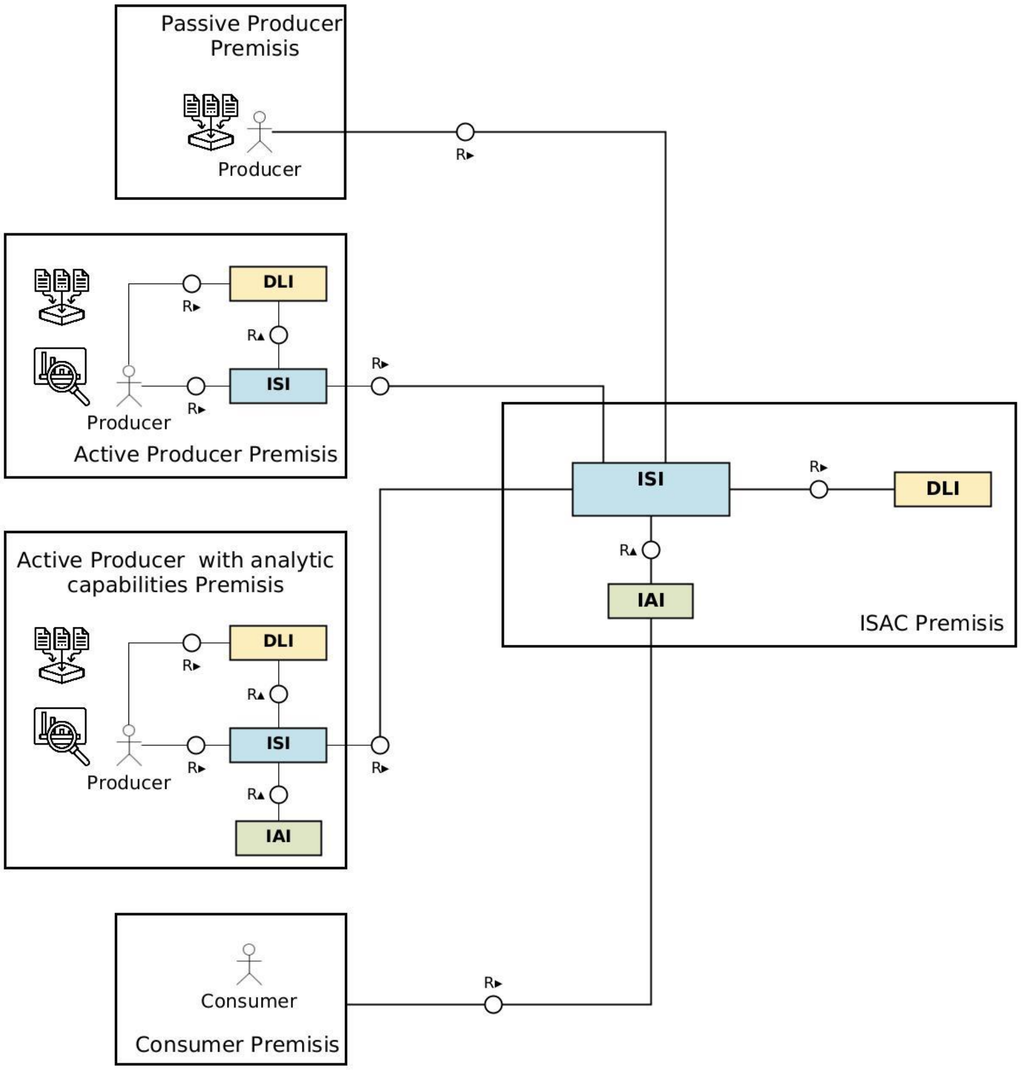


Figure 3: ISAC high level architecture

4. Component Architecture

This section reports the details of the ISAC architecture, describing the main components and their interactions with the E-CORRIDOR framework and the external components. The overall view of the ISAC is depicted in Figure 4. As explained in Section 3, the ISAC premise contains a remote ISI, IAI and DLI. These components interact with the four main ISAC components exploited to implement the ISAC functionalities: the *ISAC collector, the ISAC dispatcher, the ISAC portal and the ISAC analytics toolbox.* These are used to interact with the data producer and the consumers to: (i) collect information (raw data or analytic results), (ii) notify the consumer about the analytic results, (iii) provide an interactive tool to show the aggregating cyber-threat analytic results performed by the ISAC analytics toolbox.

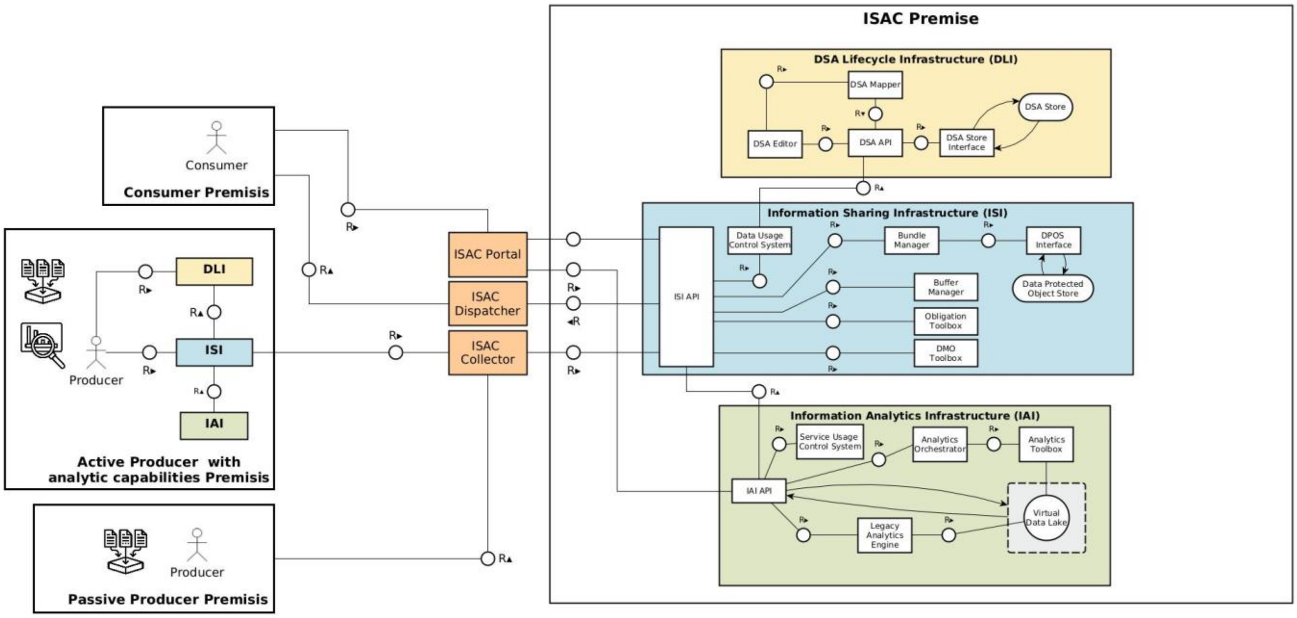


Figure 4: ISAC architecture

In the following sections are reported the details of the internal ISAC components and how they interact with the E-CORRIDOR framework and the external entities.

4.1. ISAC portal

The portal is the main ISAC component that acts as interconnection between the consumer/provider and the ISAC itself. The two main goals of this component are related to the management of the requests provided by the external entities (consumer/provider) related to the information sharing or the analytics running, and provides an interactive visualization tool able to present the analytic results performed by the ISAC analytics.

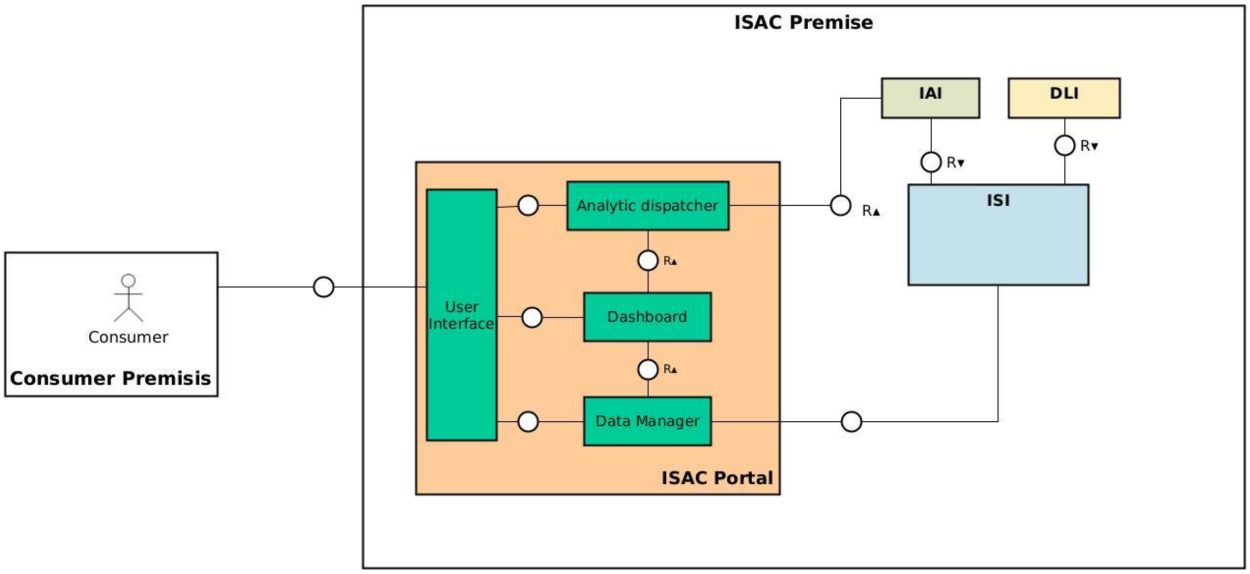


Figure 5: ISAC portal architecture

As showed in Figure 5, the ISAC portal is composed of four main sub-components. The u*ser interface* interacts externally with the providers and consumers and allows the user to perform requests about (i) sharing the private information, (ii) running the ISAC analytics, (iii) visualizing the analytics results or (iv) visualizing the report of the general analysis performed by the ISAC analytics on the public data. To manage the above requests the user interface component interacts with three other components: the *analytic dispatcher* used to issue the analytic operations, either when receiving requests from consumer, or during the internal analytics invocation, generally to infer information of public interest and present them to the dashboard. The *dashboard* is the visualization component that receive the request from the user interface and reads the data from the ISI to provide a user-friendly data representation of the analytics results. Finally, the last portal component is the *data manager* whose main goal is to interact with the ISI to store the data coming from the providers and read the data stored into the ISI to be sent to the dashboard.

4.2. ISAC collector

The ISAC collector aims to gather data from the private or public sources and interact with the ISI to store data with the appropriate DSA. It is composed by four sub-components. The *gathering component* is used to collect data from public sources. It interacts with open sources databases, like NIST database[1], to update the ISAC knowledge about cyber-threats. In addition, such component can perform a web scraping on trusted security website in order to extract useful information to the ISAC knowledge. The collected information is passed to the *filtering component* that acts on the data to remove meaningless information, like redundant or malformed data, then the *data adapter* is invoked to adapt the data format to be consistent with the ISI format. The pre-

[1] https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

processed data are then passed to the sharing component that acts as the interaction component with the ISI and the DLI to store or move the data on the virtual data lake. In Figure 6 is reported the architectural description of the ISAC collector.

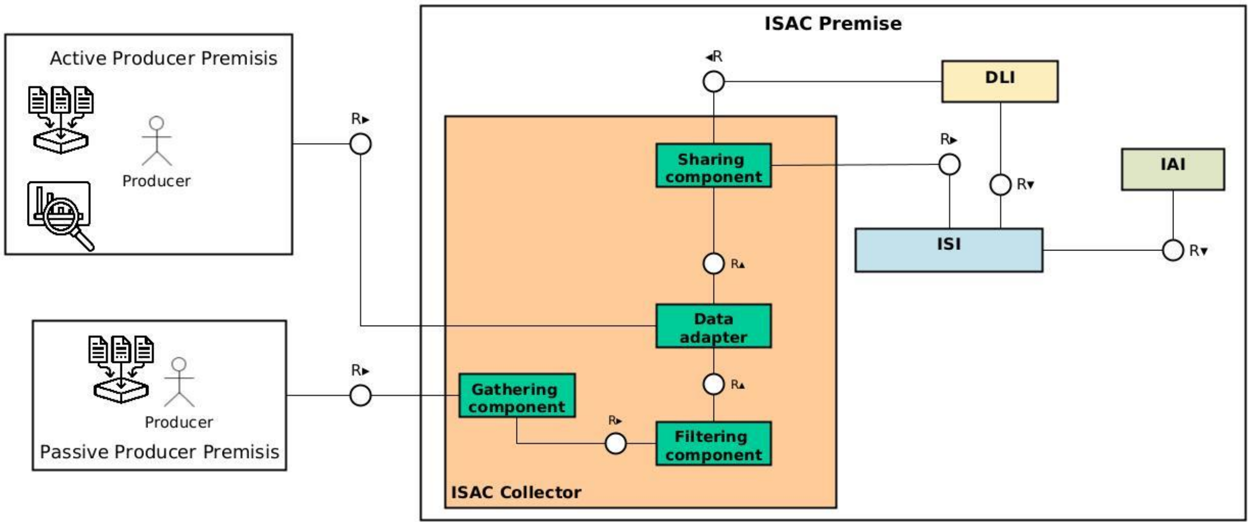


Figure 6: ISAC collector architecture

4.3. ISAC dispatcher

The ISAC dispatcher is the component used to notify the end-user about new threats and vulnerability discovered by the ISAC and every cyber-threat information related to a subscribed topic. It interacts with the ISAC portal to receive the subscription request issued by a consumer and stores them in a subscription list. It interacts with the ISI for receiving the analytic results produced by the IAI, and after a matching between the labelled result and the subscription list, it sends the information to the subscriber. Such a process is done automatically, providing results coming from ISAC analysis without explicit user analysis request. The only user request is the initial subscription to a specific security topic. In Figure 7 is showed the architectural connection of the ISAC dispatcher.

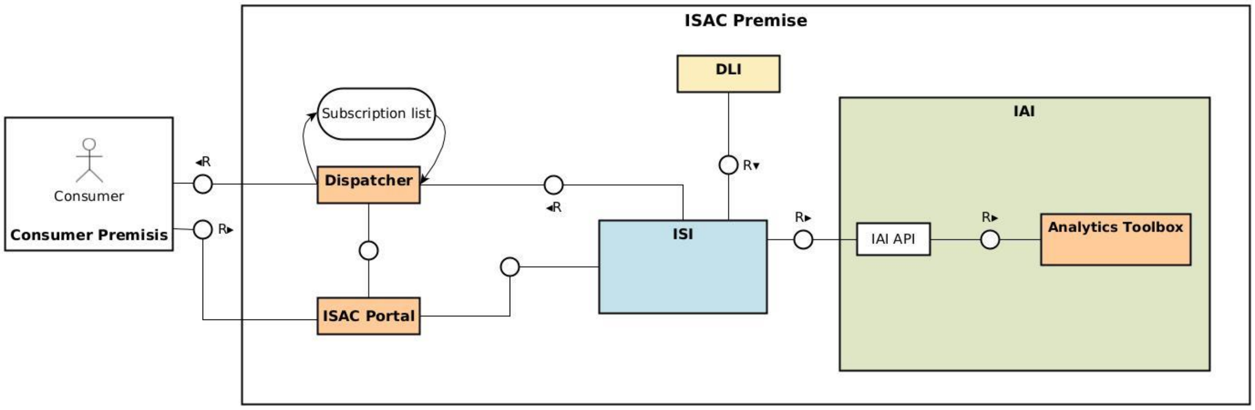


Figure 7: ISAC dispatcher architecture

4.4. ISAC analytics toolbox

The ISAC analytic toolbox, Figure 8, is the component that implements the pilot specific analytics. It is contained in the IAI infrastructure and the analytic consumer interact with them using the IAI API. In particular the consumer sends the request through the portal for the execution of the data analysis on a particular data shared with the ISAC. The data are taken through the ISI and the analytic is invoked only after the invocation of the Service Usage Control System used to enforce policies on it. The details of each analytics are given in Section 4.6. **Analytics**

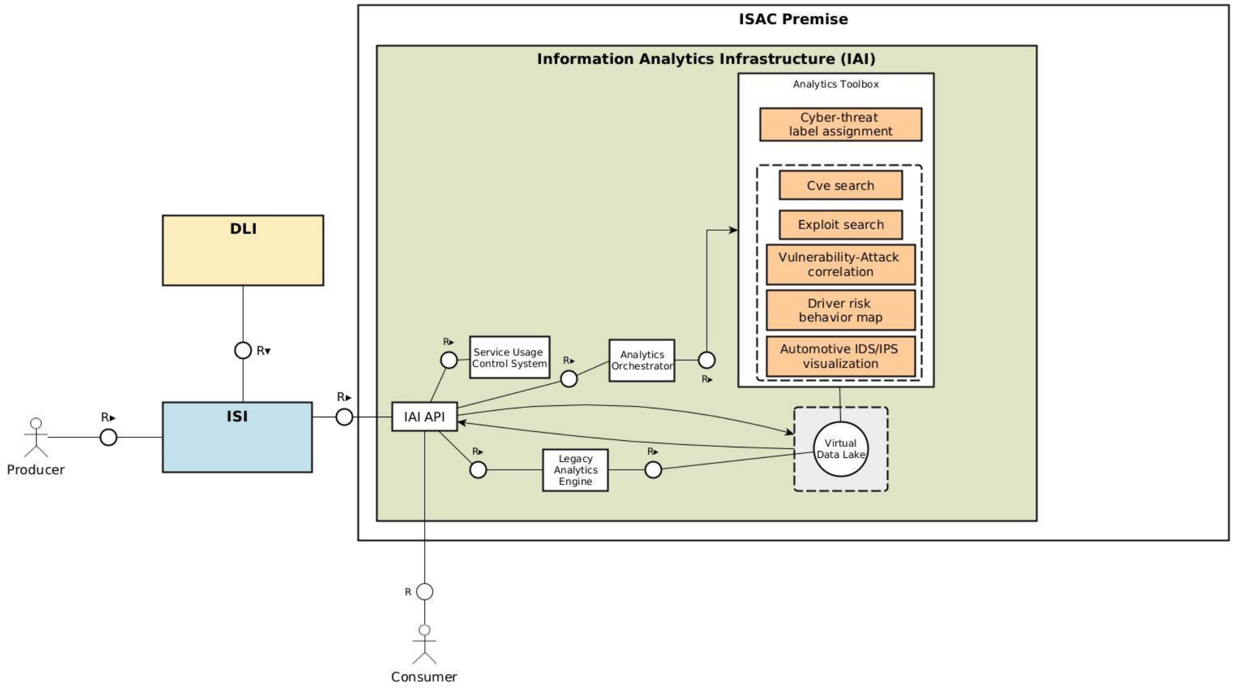


Figure 8: ISAC analytics toolbox

4.5. Block Design

This section aims to provide details of high-level subsystems identified in the previous section reporting the behaviour of each component in the use cases defined in the E-CORRIDOR project deliverable 4.1 [1].

4.5.1 ISAC-BD-01: Block diagram for ISAC-UC-01: Collecting public data

The ISAC-UC-01 aims to collect cyber-threat information from public sources. In such context the data provider is passive, i.e., the provider does not contain any sharing infrastructure components. To store data on the ISAC premise, the ISAC collector has to inquiry different public sources to collect and update the ISAC information. Figure 9 shows the Fundamental Modelling Concepts (FMC) (FMC) block diagram of this use case.

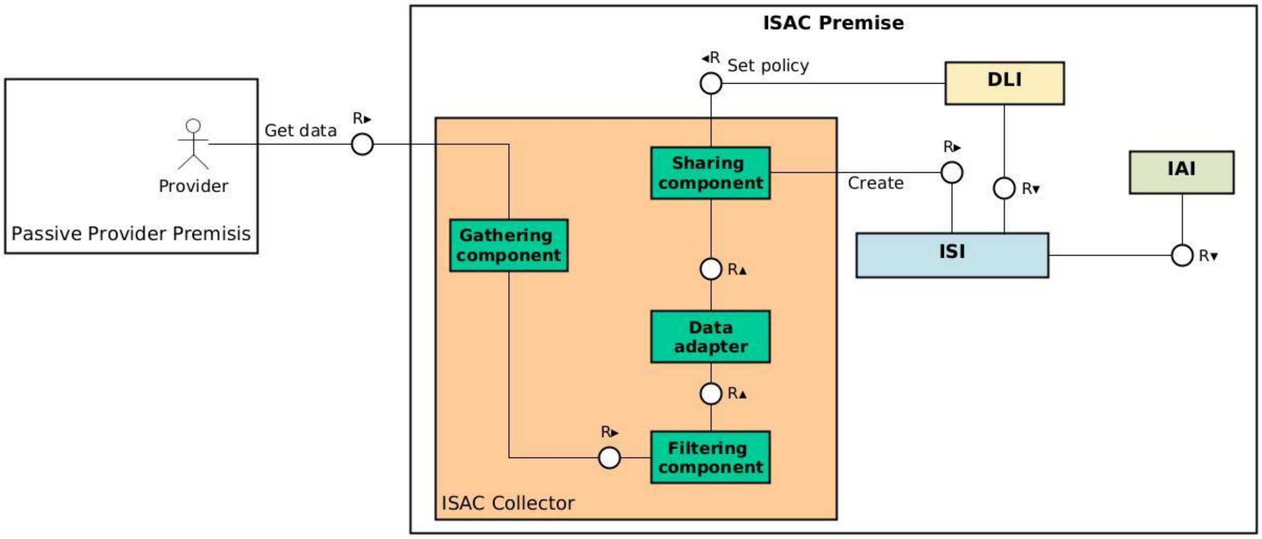


Figure 9: ISAC-BD-01 - Collecting public data

The *gathering component* of the ISAC collector aims to periodically get information from public cyber-threat databases (common vulnerability enumeration, exploit, attack pattern), scraping data from websites and getting news from RSS feeds. The gathered information is forwarded to the *filtering component* with the aim to pre-process the data removing the meaningful information. Then the result is passed to the *data adapter component* which convert, if necessary, the data format to make them suitable for the ISI. After the conversion, the *sharing component* is responsible to set the DSA on the collected data and call the create ISI API to store it.

4.5.2. ISAC-BD-02: Block diagram for ISAC-UC-06 – ISAC-UC-02 - ISAC-UC-03: Collecting private data

The main purpose of the ISAC-UC-02, ISAC-UC-03 and ISAC-UC-06 is to collect data from the private transportation sector that wants to share information (data locally collected or analytic results) to the ISAC. Specifically, the ISAC-UC-02 and ISAC-UC-03 are provider side use cases through which a specific transportation entity, e.g., car, train, organization, defines a DSA on a certain information and share them on the ISAC premise. The ISAC-UC-06 is specific for the ISAC data collection through which the data are collected from the private transportation sector, converted in a standard format and stored. Figure 10 describes the FMC block diagram of this use cases.

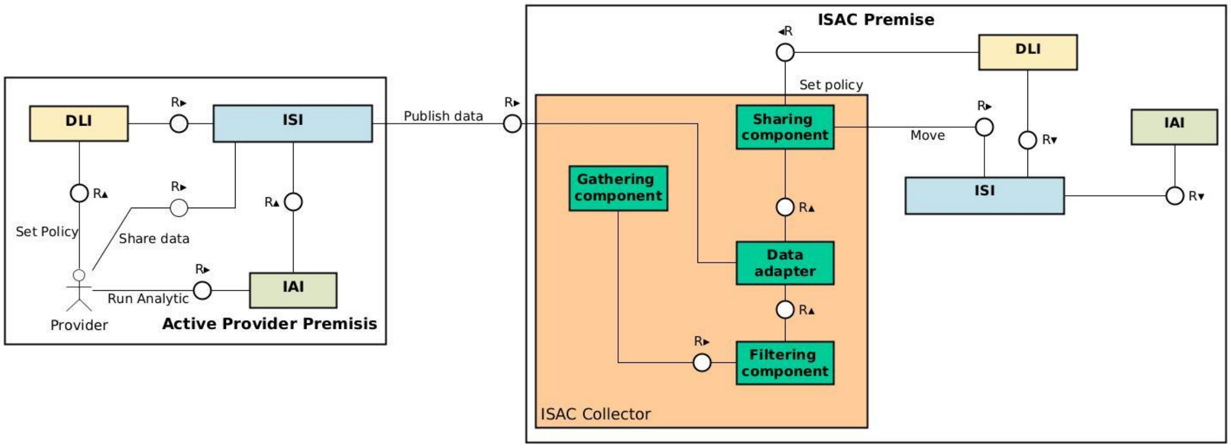


Figure 10: ISAC-BD-02 - Collecting private data

The active or semi-active data provider that store locally the ISI, DLI and IAI instances, can decide to share its own information with the ISAC in order to add cyber-threat knowledge at global level. The provider can share either its raw collected information or directly its analytic results (only in the active provider premise). Hence the provider can share its information on the local ISI after having set the DSA using the local DLI. In addition, it can perform analytics using the local IAI on the data created on the local ISI. To share the information on the ISAC premise, the provider contacts the ISAC collector, which directly interacts with the ISI API, managing thus the data storage operations acting as interconnection between the Local and Remote ISI. Before sharing the data are passed to the data adapter component to ensure the data format is suitable to be stored in the remote ISI. The result of the data adapter is forwarded to the *sharing component* that can set additional DSA before calling the data creation on the ISI.

4.5.3. ISAC-BD-03: Block diagram for ISAC-UC-04, ISAC-UC-08: Running analytics and visualization

The following section describes the block diagram for the ISAC-UC-04 and ISAC-UC-08, respectively related to the ISAC analytic results visualization and the execution of a remote analytic. The main ISAC components involved in such scenario are the ISAC portal and the ISAC analytics contained into the IAI analytic toolbox. Figure 11 shows the interaction between the consumer, who wants to analyse and to visualise the data, and the ISAC premise internal component.

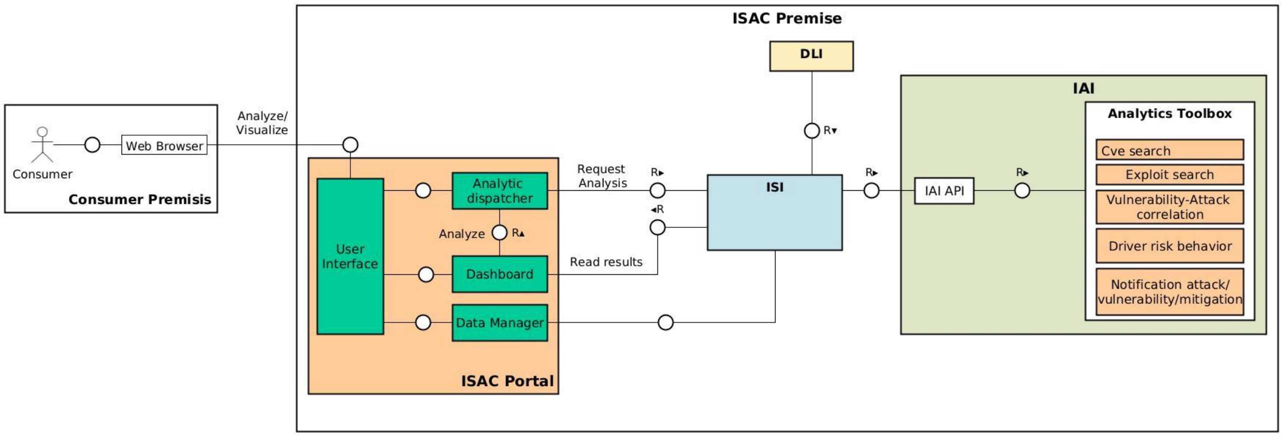


Figure 11: ISAC-BD-03 - Running analytics and visualization

The consumer, through a web browser, logs in to the ISAC portal which provides the main user an interface to access different components, i.e., Dashboard, Analytic services and DLI. The analytic dispatcher component is responsible to forward the analytic request to the ISI which consequently invoke the analytic function in the IAI if the DSA applied on data and on the analytic are respected. The analytic results are directly stored by the analytic interacting with the ISI. The dashboard component aims to make the analytic results in a readable format, reporting both a customized view of multiple security analytics run by a consumer and a global statistical view of the security metrics extracted from the analysis done or collected from the public sources.

4.5.4. ISAC-BD-04: Block diagram for ISAC-UC-05: Cyber-threat notification

The ISAC-UC-05 aims to inform a subscriber about new threats, vulnerabilities and mitigations discovered by the ISAC collaborative analysis. The main ISAC component involved in this scenario is the ISAC dispatcher, shown in Figure 12. The consumer, interacting with the ISAC portal through the web browser, sends a request of subscription to the ISAC notification service providing a list of security topics of which he/she wants to be notified as soon as new information are discovered. As example of topics the user can specify a transportation sector (e.g., aviation, railway, automotive), a list of software/hardware (Gateway ECU, Oracle Mysql) or specific keywords selected by a predefined list (Cryptolocker, Stuxnet, DoSStet). The request is sent to the analytic dispatcher which invokes the dispatcher. At first the dispatcher stores the user and its subscription information into the subscription list, then sends back the request to the analytic dispatcher to activate the notification service on the new topics. The dispatcher keeps inquiring the ISI to get the analytic results (the information contained in the ISAC knowledge related to the specified topic) and to check whether the results are within the users' subscription list, in which case notifications are sent. The new information checking is done periodically (e.g., 1 time per day) to maintain the subscriber as up to date as possible.

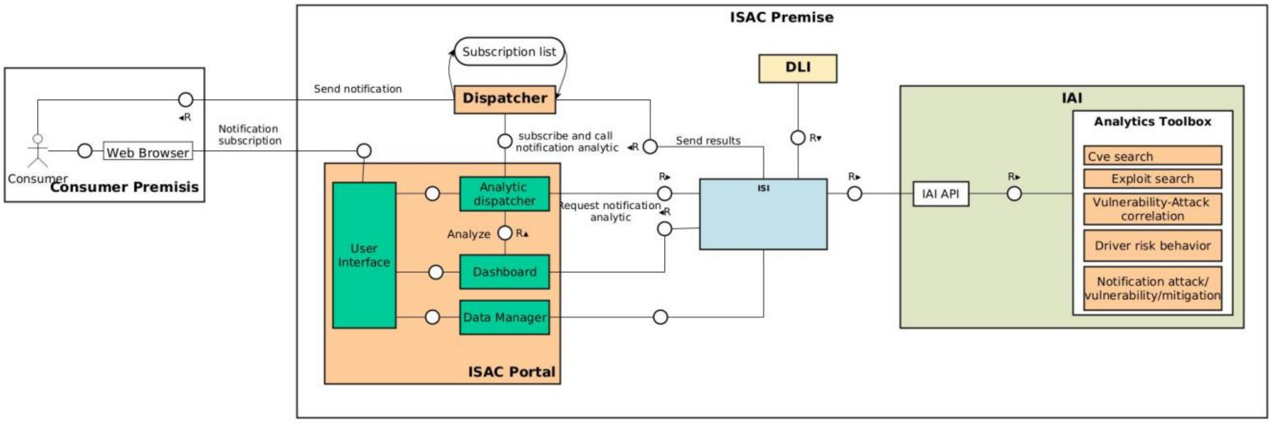


Figure 12: ISAC-BD-04 - Cyber-threat notification

4.6. Analytics

The ISAC provides pilot-specific analytics performed on data collected from public sources and the analytic results shared by the stakeholders. The aim of the ISAC analysis is to aggregate the collected information in order to increase the cyber-threat knowledge and provide an easy and intuitive visualization of the huge amount of data gathered. To this end, the analytic toolbox contained in the ISAC IAI component is composed of two types of analytics: the *cyber data label assignment* and the *cyber data visualization tool.*

4.6.1. ISAC-AF-01: Cyber data label assignment

This analytic is exploited as main element for the notification workflow discussed in Section 4. The ISAC is, in fact, bound to collect a huge amount of information from various providers and at the same time it must redistribute the collected data timely to interested stakeholders. Selecting the right information to be sent to the right partner is of high importance. In fact, on one hand, failing in providing information on a relevant vulnerability, might increase the exposure time of stakeholders to the identified cyber-attacks. On the other hand, flooding the stakeholder with non-relevant information increases the processing times and might result in a lowered attention to actual security threats.

This analytic, represented in Figure 13, exploits text analysis and clustering methodologies to separate the information in different *topics* (e.g., “vulnerabilities in aircraft systems”) to which the stakeholders can subscribe to. In such a way, the stakeholders will be automatically notified about the information that are relevant to them. The analytic also considers the possibility that some information may come already labelled. In this case, the label is semantically analysed to identify possible similarities with a set of already known topics. Such analysis can be conducted exploiting machine learning algorithms with training strategy supervised (multi-class classifier customized to recognize a set of predefined topics) or unsupervised (clustering algorithms that aggregate textual information basing on the semantic and syntactic similarity). If the information belongs to a topic that has not been identified yet, a new topic is created, notifying the consumers about the possibility of receiving information related to this new topic. If a label is not provided, the topic is identified by semantic text analysis, by identifying the keywords and computing their probability of belonging to an existing topic. The information that cannot be automatically categorized can be manually analysed and classified by the data collector.

The huge amount of information collected by the ISAC have an unstructured representation difficult to analyse. The analytic applies Natural Language Processing (NLP) techniques able to transform unstructured natural language text into structured information [5,6]. The objective is to apply machine-learning algorithms that determines textual information relevant for cybersecurity, then extract textual entities to determine and cluster the text in a particular topic, e.g., vulnerabilities, malware, threat and, if present, the corresponding transportation sector.

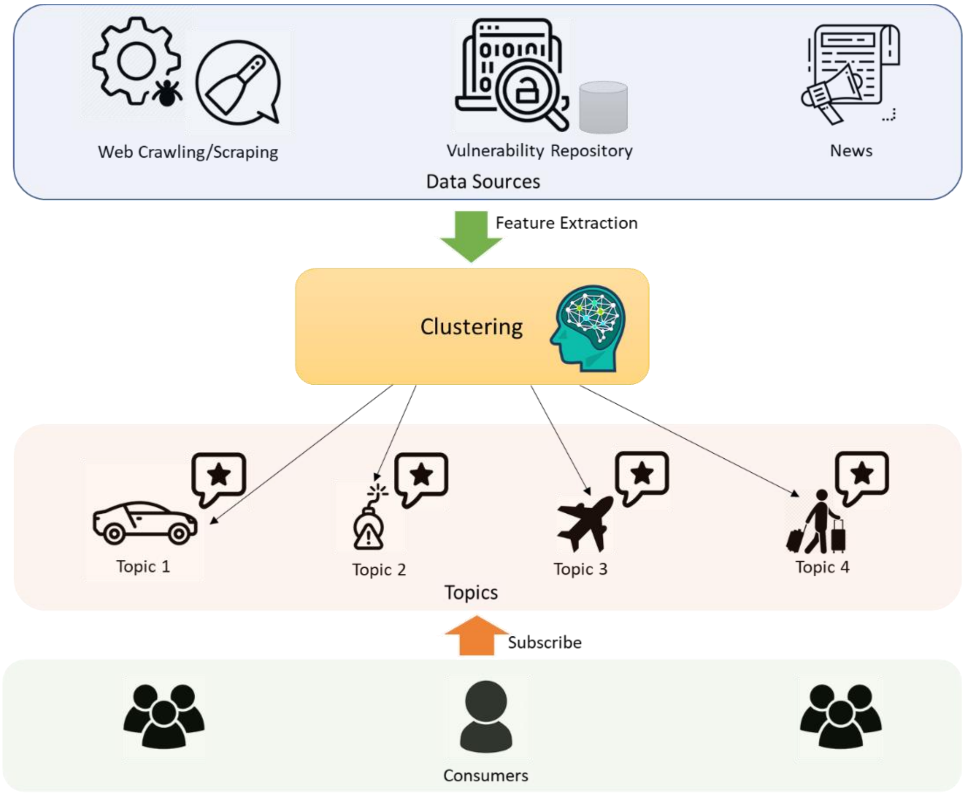


Figure 13: Cyber-data label assignment analytic

The granularity of the clustering algorithm can be regulated by the consumer to increase or decrease the specificity of each considered topic, allowing subscribers to select between large sets of interesting information or their subsets (e.g., Automotive, network attacks, DoS, ECU CAN bus).

4.6.2. ISAC-AF-02: Cyber data visualization

This analytic is used to provide stakeholders with an organized and aggregated representation of data collected and analysed by the ISAC related to specific topics. It is a macro analytics used to present and speed up the information retrieval process. It is composed of a set of visualization analytics provided through the dashboard of the ISAC portal. An in-depth explanation is given in the following.

4.6.2.1 Security report

The security report is a set of statistical analysis extracted from the overall data collected and processed by the ISAC. It is regularly updated every time new cyber data is collected, and it is offered to the consumer to increase awareness in the cyber-threat field. The list of the reporting data is described in Table 1 security report dashboard is presented in Figure Figure 14.

Data	Description	Visualization tool
Vulnerabilities	Distribution of the number of CVE in the last 10 years.	Histogram
	Distribution of the degree of danger (CVSS) of all CVEs discovered.	Pie chart
	Distribution of the number of CVEs concerning the most used transportation software/hardware.	Histogram
	Distribution of the degree of hazard of the CVE discovered in the current year.	Histogram
	Latest CVE discovered	Table
Exploit	Distribution of the number of exploit types in the last 10 years.	Line graph
	Distribution of the number of exploits discovered in the last 10 years.	Histogram
	Distribution of the number of exploits related to the most common transportation software.	Line graph
	Latest exploits discovered	Table

Table 1: Security report description

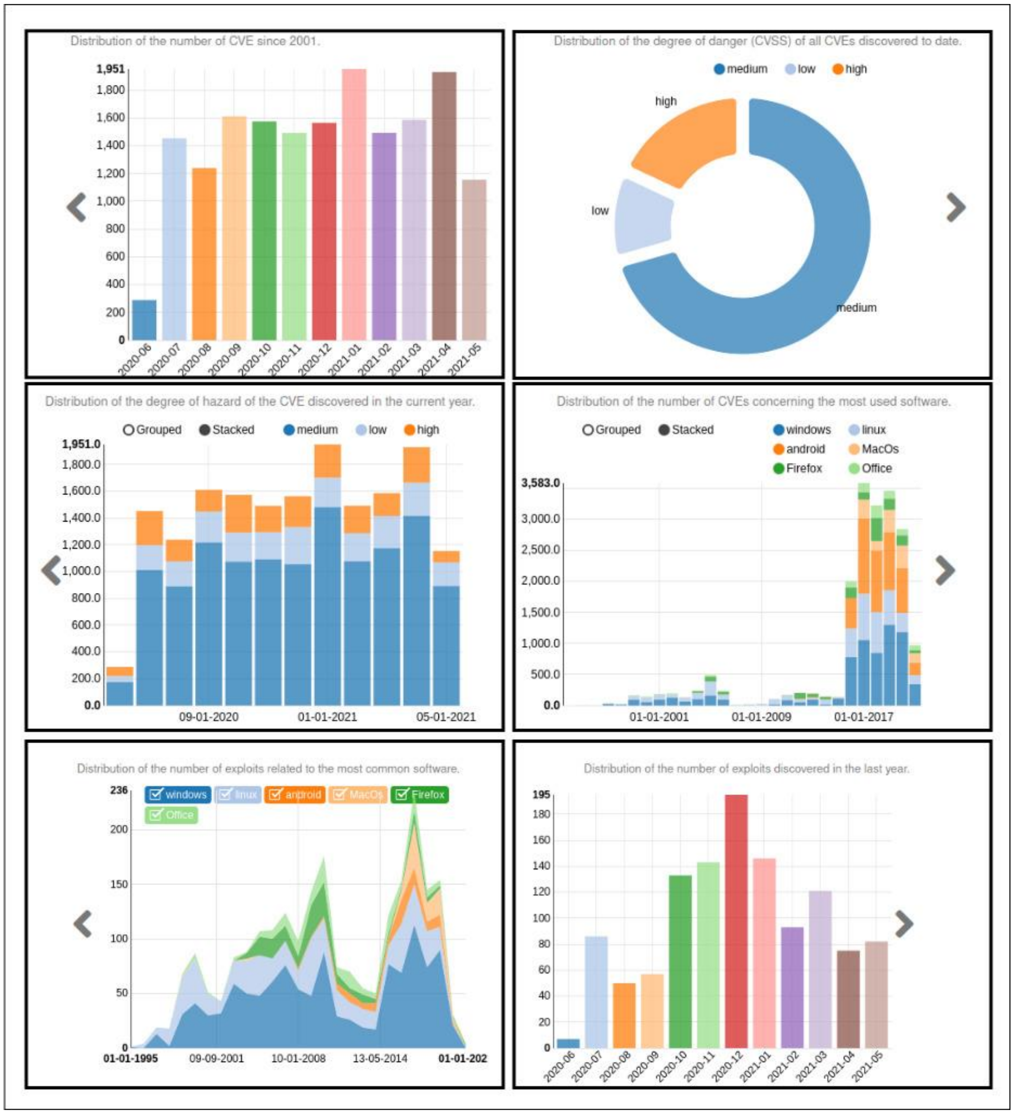
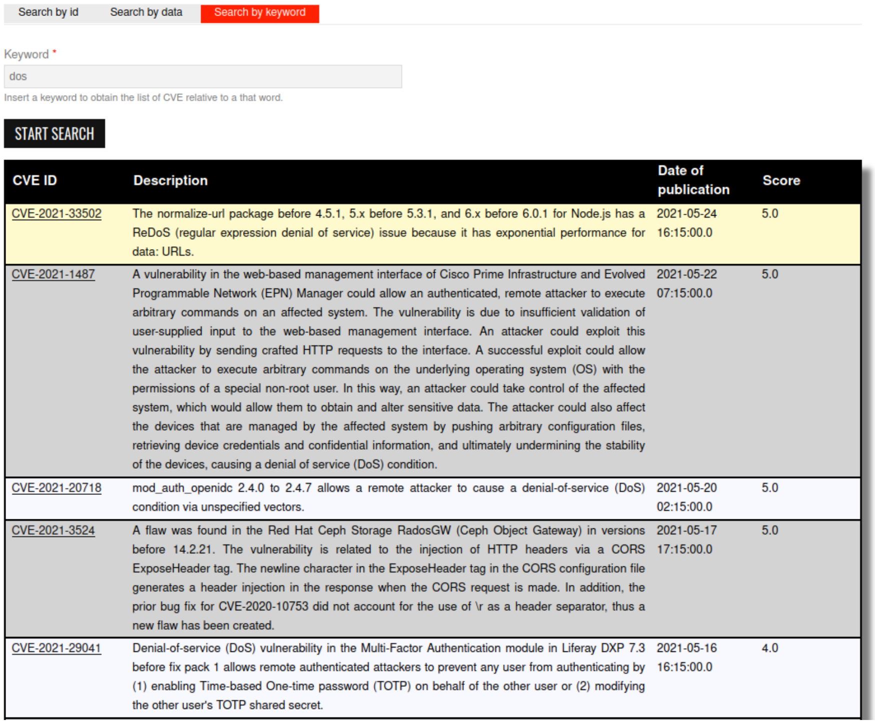


Figure 14:Security report dashboard

4.6.2.2 CVE search

This service offers the possibility of searching public domain information related to known security hardware and software vulnerabilities. This service provides a general description of the vulnerabilities reporting the publishing date, a short description, and the CVE score. The consumer can research the vulnerabilities specifying an interval time or a specific keyword. Figure 15 shows an example of a vulnerabilities searching interface and the presentation of the results.



Keyword *

dos

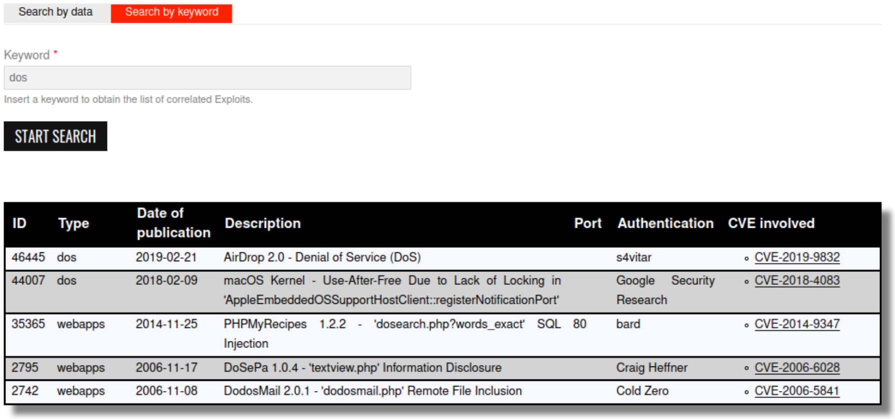
Insert a keyword to obtain the list of CVE relative to a that word.

CVE ID	Description	Date of publication	Score
CVE-2021-33502	The normalize-url package before 4.5.1, 5.x before 5.3.1, and 6.x before 6.0.1 for Node.js has a ReDoS (regular expression denial of service) issue because it has exponential performance for data: URLs.	2021-05-24 16:15:00.0	5.0
CVE-2021-1487	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition.	2021-05-22 07:15:00.0	5.0
CVE-2021-20718	mod_auth_openidc 2.4.0 to 2.4.7 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vectors.	2021-05-20 02:15:00.0	5.0
CVE-2021-3524	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created.	2021-05-17 17:15:00.0	5.0
CVE-2021-29041	Denial-of-service (DoS) vulnerability in the Multi-Factor Authentication module in Liferay DXP 7.3 before fix pack 1 allows remote authenticated attackers to prevent any user from authenticating by (1) enabling Time-based One-time password (TOTP) on behalf of the other user or (2) modifying the other user's TOTP shared secret.	2021-05-16 16:15:00.0	4.0

Figure 15: Vulnerability searching interface

4.6.2.3 Exploit search

This analytic offers the possibility of searching information related to exploits by date or keyword. This analytic shows the date, description, and the specific platform on which the exploit is effective. Figure 16 shows an example of a exploits searching interface and the presentation of the results.



Keyword *

dos

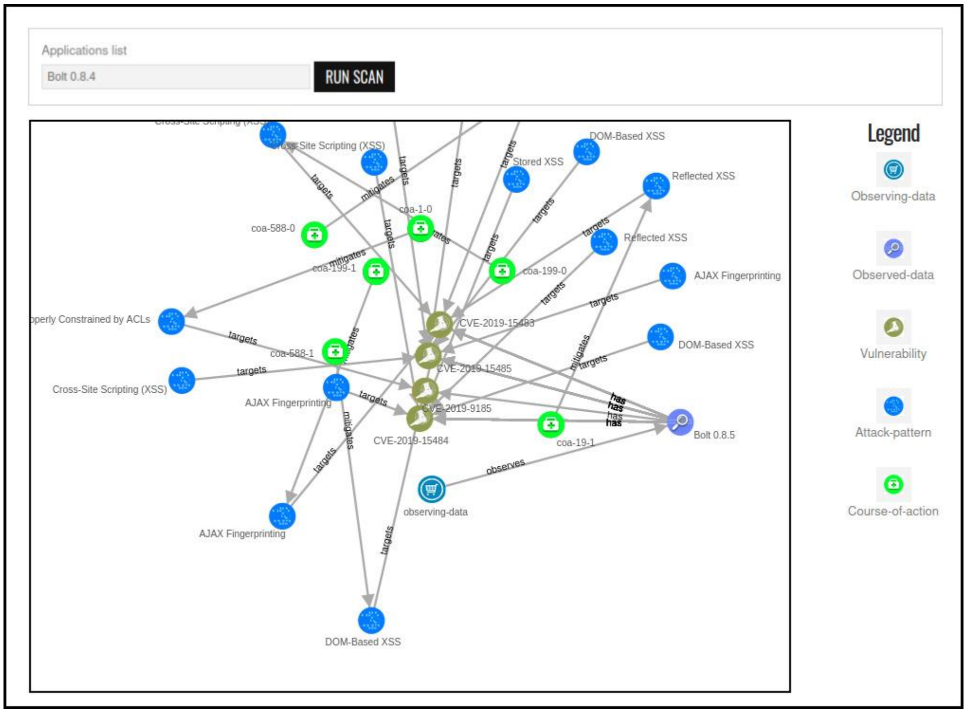
Insert a keyword to obtain the list of correlated Exploits.

ID	Type	Date of publication	Description	Port	Authentication	CVE involved
46445	dos	2019-02-21	AirDrop 2.0 - Denial of Service (DoS)		s4vitar	◦ CVE-2019-9832
44007	dos	2018-02-09	macOS Kernel - Use-After-Free Due to Lack of Locking in 'AppleEmbeddedOSSupportHostClient::registerNotificationPort'		Google Security Research	◦ CVE-2018-4083
35365	webapps	2014-11-25	PHPMyRecipes 1.2.2 - 'dosearch.php?words_exact' SQL Injection	80	bard	◦ CVE-2014-9347
2795	webapps	2006-11-17	DoSePa 1.0.4 - 'textview.php' Information Disclosure		Craig Heffner	◦ CVE-2006-6028
2742	webapps	2006-11-08	DodosMail 2.0.1 - 'dodosmail.php' Remote File Inclusion		Cold Zero	◦ CVE-2006-5841

Figure 16:Exploit searching interface

4.6.2.4 Vulnerability attack correlation

This analysis allows the consumer to explore the interconnection between the vulnerabilities and attack patterns of specific known software or hardware. Additionally, the analytic provides recommendations for attacks and vulnerability mitigation. The visualization tool permits to the consumer to specify a software or hardware contained in a predefined list, and return a graphic representation of the interconnection between the vulnerabilities, the attacks and the mitigation between the applications selected. Figure 17 shows a graphical interface example of the vulnerability attack correlation analytic and its result presentation.



Applications list: Bolt 0.8.4

Figure 17: Vulnerability attack correlation analytic interface

4.6.2.5 Automotive intrusion detection/prevention visualization

This analytic is based on the automotive intrusion detection system analysis results explained in Deliverable D7.1. The produced result is the classification of the CAN bus messages and the potential detection of an anomaly within the vehicle's data. Such information shared by multiple vehicles with the ISAC is exploited to create a graphic visualization of the intrusion information, incident, related types, and incident classes of a single vehicle. In addition, there is the possibility to visualize the correlation of the intrusion detected in different vehicles.

4.6.2.6 Driver risk behavior

The analytic exploits the data provided by the results of the Driver DNA analytics. As explained in Deliverable D7.1, the analytic provides the driver risk profile, e.g., more aggressive, speeding more frequently. Correlating these results with the geo-localization of the vehicles, the ISAC analytics can produce a map of the city reporting the average driver behavior in each road section.

In such a way, it is possible to highlight the most dangerous section of the city and increase the drivers' awareness.

4.7. Data model

This section introduces the data model that defines a first structure of the data collected by the ISAC. In particular, this section will provide a first overview of the data model considering each analytic and functionality discussed in Section 4.6. **Analytics**

4.7.1. ISAC-AF-01: Data schema

The ISAC-AF-01 is based on the analysis of textual information collected from public sources (vulnerabilities and exploits databases) and information scraped from trusted security websites. Such data are mainly provided by the ISAC data collector that performs a data adaptation before storing them into the ISI. The data adapter contained into the ISAC collector, converts the gathered data, in some cases unstructured, in a JSON format, providing a structure to the data collected and allowing the analytic to extract useful information. The data format of the data scraped from the web and the data collected from public databases are showed in the following sections.

4.7.1.1. Expected data format

The input data of the ISAC-AF-01 is represented by all the textual information extracted from the data scraped from the web (trusted security blogs) and the textual information contained into the public security databases (vulnerabilities, exploits).

Public data scraped from web

The data scraped from security websites is represented through a JSON file. Each element is composed by an *id* that identifies the information, the *author*, the scraped *date*, the *image path* of the scraped information and the *textual* information, the *title* of the post and the referring *website*. Figure 18: Security data scraped from web shows an example of information scraped from two different blogs before passing them to the filtering and data adapter component.

```
[{
   "_id":"https://thehackernews.com/2021/04/critical-rce-bug-found-in-
homebrew.html",
   "author":"Ravie Lakshmanan",
   "date":"2021-04-24",
   "image":"https://thehackernews.com/images/-
Rbma_7ItY9E/YIRuyaBP1MI/AAAAAAAACW8/j8FmgzPFpbY0rUZFxfEMON5JGWtvdBDrgCLcBGAsYHQ/s728
-e1000/homebrew-package-manager.jpg",
   "text":[

   ],
   "title":"Critical RCE Bug Found in Homebrew Package Manager for macOS and Linux",
   "website":"The Hacker News"
},

{
   "_id":"https://www.wired.com/story/signal-cellebrite-hack-app-store-scams-
security-news/",
   "author":null,
   "date":"04.24.2021 09:00 AM",
   "image":null,
   "text":"Brian BarrettSecurity04.24.2021 09:00 AMSecurity News This Week: Signal’s
Founder Hacked a Notorious Phone-Cracking DevicePlus: App Store scams, an anti-
surveillance bill, and more of the week’s top security news. The incident is notable
because it involves Apple—and the reease of confidential schematics—but also because
it represents an intersection from multiple disturbing trends in digital
extortion.In other Apple-adjacent hackig news, Facebook researchers found that a
Palestine-linked group had built custm malware to attack iOS, ...",
   "title":null,
   "website":"Security | WIRED"
}]
```

Figure 18: Security data scraped from web

Public data collected from public security databases

The data collected from public security databases are related to vulnerabilities and exploits.

The vulnerabilities information is collected from the National Vulnerability Database provided by the NIST, and readapted by the data collector following the JSON schema reported in Figure 19. It contains the CVE identifier, the referring link to the vulnerability, the list of platforms that contain the vulnerability, the published date, the last modification, the CVSS score and the summary of the vulnerability, which is the textual information used in the ISAC-AF-01. In addition, the vulnerability entry has extra information regarding how it is accessed, its complexity and the consequent impact[2].

```
{
   "_id":{
      "$oid":"5b19633fc17e0b400317e033"
   },
   "id":"CVE-1999-0008",
   "references":[
      "http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll\u0026doc=secbull/170"
   ],
   "vulnerable_configuration":[
      "cpe:2.3:o:hp:hp-ux:10.34",
      "cpe:2.3:o:hp:hp-ux:11.00",
      "cpe:2.3:o:sun:solaris:2.3",
      "cpe:2.3:o:sun:solaris:2.4",
      "cpe:2.3:o:sun:solaris:2.5",
      "cpe:2.3:o:sun:solaris:2.5.1",
      "cpe:2.3:o:sun:solaris:2.6"
   ],
   "vulnerable_configuration_cpe_2_2":[
      "cpe:/o:hp:hp-ux:10.34",
      "cpe:/o:hp:hp-ux:11.00",
      "cpe:/o:sun:solaris:2.3",
      "cpe:/o:sun:solaris:2.4",
      "cpe:/o:sun:solaris:2.5",
      "cpe:/o:sun:solaris:2.5.1",
      "cpe:/o:sun:solaris:2.6"
   ],
   "Published":{
      "$date":"1998-06-08T00:00:00.000Z"
   },
   "Modified":{
      "$date":"2008-09-09T08:33:31.320Z"
   },
   "cvss":10.0,
   "access":{
      "vector":"NETWORK",
```

[2] https://www.first.org/cvss/v2/guide

```
      "complexity":"LOW",
      "authentication":"NONE"
   },
   "impact":{
      "confidentiality":"COMPLETE",
      "integrity":"COMPLETE",
      "availability":"COMPLETE"
   },
   "cvss_time":{
      "$date":"2004-01-01T00:00:00.000Z"
   },
   "summary":"Buffer overflow in NIS+, in Sun's rpc.nisd program."
}
```

Figure 19: vulnerability information collected from NVD database

The exploit information is collected from the exploit-db project[3]. The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed to be used by penetration testers and vulnerability researchers. The collection of exploits is gathered through direct submissions, mailing lists, as well as other public sources, and presented in a freely-available and easy-to-navigate database. Figure 20 shows the JSON representation of the information contained in the exploit. It contains the description, which is the textual information used by the ISAC-AF-01, the author, the port involved, the publishing date, the platform, the path of the exploit source, the type of exploit and the identifier.

```
{
   "description":"Inteno\u2019s IOPSYS - (Authenticated) Local Privilege Escalation",
   "author":"neonsea",
   "port":"",
   "date_published":"2018-07-21",
   "platform":"linux",
   "file":"exploits/linux/local/45089.py",
   "type":"local",
   "id":"45089"
}
```

Figure 20: Exploit information collected from exploit-db

4.7.2. ISAC-AF-02: Data schema

The ISAC-AF-02 aims to present a synthesis of the information gathered and elaborated by the analytics. The input data of the analytics are the vulnerabilities and exploits information presented in Section 4.7.1. **ISAC-AF-01: Data schema** and the information shared by the automotive intrusion detection and prevention system explained in D7.1.

Automotive intrusion detection and prevention visualization

The automotive intrusion detection and prevention analytics, presented in Deliverable D7.1, provides to the ISAC the analytic results represented in STIX format. The results are shared with the ISAC by the automotive security system or directly by the automotive company. An example of STIX object shared by the automotive Intrusion Detection System (IDS) is shown in figure in Figure 21. The STIX object contains as relevant information the detected attack pattern, the description of the attack, the creation date, the type of activity detected and information related to the observed object. Similarly, the Intrusion Prevention STIX object contains the description

[3] https://www.exploit-db.com

of the malicious activity, the confidence percentage, the percentage of failed challenges reported by the Intrusion Prevention analytic, the observation time-window of the frame received and the number of challenges done.

```
{
   "id":"bundle--c6d5ea7d-2594-47cc-b3e9-8a0e1e8d7420",
   "objects":[
      {
         "confidence":83,
         "created":"2020-01-26T17:55:10.442Z",
         "description":"For CAN ID 768 values can range from 0 to 255",
         "id":"indicator--9299f726-ce06-492e-8472-2b52ccb53191",
         "indicator_types":[
            "malicious-activity"
         ],
         "modified":"2020-01-26T17:55:10.442Z",
         "name":"Invalid CAN Payload",
         "pattern":"[x-can:id = 768 AND x-can:value >= 0 AND x-can:value <= 255]",
         "pattern_type":"stix",
         "pattern_version":"2.1",
         "spec_version":"2.1",
         "type":"indicator",
         "valid_from":"2021-02-25T10:31:20.588827Z"
      },
      {
         "created":"2020-01-26T17:55:10.442Z",
         "id":"identity--5206ba14-478f-4b0b-9a48-395f690c20a2",
         "identity_class":"system",
         "modified":"2020-01-26T17:55:10.442Z",
         "name":"CAN bus IDS",
         "roles":[
            "Cyber Security"
         ],
         "sectors":[
            "technology"
         ],
         "spec_version":"2.1",
         "type":"identity"
      },
      {
         "count":1,
         "created":"2020-01-26T17:55:10.442Z",
         "created_by_ref":"identity--5206ba14-478f-4b0b-9a48-395f690c20a2",
         "id":"sighting--8356e820-8080-4692-aa91-ecbe94006833",
         "modified":"2020-01-26T17:55:10.442Z",
         "observed_data_refs":[
            "observed-data--5046dbb6-0e6a-44bd-8b23-34ce41fae19e"
         ],
         "sighting_of_ref":"indicator--9299f726-ce06-492e-8472-2b52ccb53191",
         "spec_version":"2.1",
         "type":"sighting",
         "where_sighted_refs":[
            "identity--5206ba14-478f-4b0b-9a48-395f690c20a2"
         ]
      },
      {
         "type":"observed-data",
         "spec_version":"2.1",
         "id":"observed-data--5046dbb6-0e6a-44bd-8b23-34ce41fae19e",
         "created_by_ref":"identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
         "created":"2020-01-26T17:55:10.442Z",
         "modified":"2020-01-26T17:55:10.442Z",
         "first_observed":"2020-01-26T17:50:04.432Z",
         "last_observed":"2020-01-26T17:55:10.442Z",
         "number_observed":42,
         "object_refs":[
            "artifact--ecdbbb47-8db2-47b3-ab81-edc4bfaa71bc"
         ]
      },
      {
         "type":"artifact",
         "spec_version":"2.1",
         "id":"artifact--ecdbbb47-8db2-47b3-ab81-edc4bfaa71bc",
         "mime_type":"text/plain",
         "payload_bin":"<put messages here>"
      }
   ],
   "type":"bundle"
}
```

Figure 21: Automotive intrusion detection system result in STIX format

5. Security Model

The security model of the ISAC pilot regards the adoption of authentication and authorization mechanisms to protect user data when they are interacting with the ISAC portal. The portal provides different information depending on the user that interact with it. Hence, the data are made available only to the authorized users and therefore an authentication mechanism is required.

5.1. Authentication and Authorization

As discussed in Section 4.1. **ISAC portal** the portal is accessible through a web browser. The portal contains a private part, accessible only through authentication, and a public part, accessible to any user. In addition, specific authorizations will be assigned to each user that require access to specific content and functionalities.

For the *authentication* to the portal an HTTP Basic Auth will be implemented with the communication encrypted through SSL.

The *authorization* is managed by the ISI through the DLI and the Service Usage Control System as better detailed in Deliverables D6.1 and D5.2 [6]. Using these components, the information is accessed only by the authorized parties. When the user enters to the ISAC portal, its authorizations are verified and the relative functionalities are shown. Furthermore, the DSA associated to the data is also checked to ensure that only the authorized users can properly access and manipulate it.

6. Deploying Model

In the following section, the hardware and software requirements needed to ensure an efficient and effective running of the ISAC pilot are presented.

It is expected that the ISAC continuously runs a gathering process to collect large amount of information and performs analytics on such data. In addition, it also provides a portal component, and its user interface, to the users. To this end, a presentation layer (front-end) and a data access and processing layer (back-end) are considered to be deployed.

6.1. Hardware requirements

6.1.1. Front-end hardware requirements

- Processors: 4 Intel/AMD 64-bit (8 cores, if provided as Virtual Core)
- Minimum RAM: 4GB
- Hard Disk: 500 GB

6.1.2. Back-end hardware requirements

- Processors: 4 Intel/AMD 64-bit (8 cores, if provided as Virtual Core)
- Minimum RAM: 16 GB
- Hard Disk: 2 TB

6.2. Software requirements

6.2.1. Front end software requirements

- Operating system: Linux
- Database: MySql
- Other software: Apache Tomcat, Kibana

6.2.2. Back-end software requirements

- Operating system: Linux
- Database: Apache Drill [4]and MySql
- Other software: Apache Tomcat[5], ElasticSearch[6], Kibana[7], Flask[8].

[4] https://drill.apache.org/

[5] http://tomcat.apache.org/

[6] https://www.elastic.co/

[7] https://www.elastic.co/kibana

[8] https://flask.palletsprojects.com/en/1.1.x/

7. Requirements Matrix

The requirements matrix, presented in Table 2: Mapping Use Cases and User Stories to architecture diagrams, summarises how the Use Cases (and the associated User Stories) presented in Deliverable 4.1 [1] can be implemented adopting the ISAC design described in the previous sections.

Use case	User Story	Block diagram	Description
ISAC-UC-01	ISAC-US-01	ISAC-BD-01	It refers to the possibility to collect public cyber-threat information from public sources.
ISAC-UC-02	ISAC-US-07 ISAC-US-09 ISAC-US-10	ISAC-BD-02	It refers to the possibility to collect cyber-threat information from the sharing process performed by providers.
ISAC-UC-03	ISAC-US-07 ISAC-US-09 ISAC-US-10	ISAC-BD-02	It refers to the possibility to set a DSA on the cyber-threat information shared by the providers.
ISAC-UC-04	ISAC-US-03	ISAC-BD-03	It refers to the possibility run an ISAC security analytic.
ISAC-UC-05	ISAC-US-04	ISAC-BD-04	It refers to the possibility to notify the subscription consumer about new cyber-threat information discovered by the ISAC analytics and its topics of interest.
ISAC-UC-06	ISAC-US-02	ISAC-BD-02	It refers to the possibility to collect cyber-threat information from the sharing process performed by providers.
ISAC-UC-07	ISAC-US-06 ISAC-US-08	ISAC-BD-04	It refers to the possibility to collect the provider local analytic results through the sharing process.
ISAC-UC-08	ISAC-US-05	ISAC-BD-03	It refers to the possibility show and present the ISAC analytic results in a user-Friedly way to the data consumer.

Table 2: Mapping Use Cases and User Stories to architecture diagrams

8. Contribute towards the E-CORRIDOR

8.1. E-CORRIDOR Objectives

The objectives of the ISAC pilot are to produce a prototype implementation of a managed security analytics platform integrating the E-CORRIDOR technology to allow controlled sharing/pooling of security data belonging to different providers (private transportation sector providers or public providers). By using this prototype platform, it would be possible to evaluate and validate the E-CORRIDOR approach, architecture and technology in the context of a security information sharing and analytics services provided to different multimodal transportation enterprises.

The architecture of the ISAC pilot has been designed starting from the requirements (both functional and non-functional) identified taking into account the analytics results and the data collected by the others pilots, Airport-Train (AT) and Car Sharing in Smart Cities (S2C). The architecture contributes to the following E-CORRIDOR objectives (and here reported for the sake of completeness):

- Objective 1: E-CORRIDOR will build a flexible, confidential and privacy-preserving framework for managing data sharing, for several purposes, by different prosumers (i.e., information producer and consumer).
- Objective 2: E-CORRIDOR will define edge-enabled data analytics and prediction services in a collaborative, distributed and confidential way.
- Objective 3: E-CORRIDOR will define a secure and robust platform in holistic manner to keep the communication platform safe from cyber-attacks and ensure service continuity.
- Objective 4: E-CORRIDOR will improve, mature and integrate several existing tools provided by E-CORRIDOR partners and will tailor those to the specific needs of the E-CORRIDOR platform and Pilots.
- Objective 5: the framework and the services developed will be used to deliver a pilot product for Centre of information sharing for multimodal transportation (ISAC).

The ISAC pilot architecture contributes to the objective 1 of E-CORRIDOR framework through the ISAC-BD-01 and ISAC-BD-02. These building blocks are related to the data collection, specifically, the data collected from the public security sources and the data shared by the transportation sector entities. To fulfil this objective the ISAC portal has been designed with the scope of gathering information, adapt the format of the data and finally store them to the ISAC ISI. In addition, the above mentioned architectural block diagrams contribute to achieve the E-CORRIDOR objective 3 thanks to the instantiation of the ISI, DLI through which is guaranteed the security of the data.

The E-CORRIDOR objective 2 and objective 4 are reached with the contribution of the ISAC-BD-03 and ISAC-BD-04. They are architectural blocks related to the ISAC analytics. They provide analytic tools able to aggregate different cyber knowledge to detect, anticipate or mitigate cyber-security threats through information dispatching or security report presentation.

Finally, the objective 5 is reached through the contribution of the entire ISAC architecture which offers components to (i) collect cyber-threat information, (ii) analyze and aggregate collected information to discover new cyber-threat knowledge and (iii) dispatch cyber-threat knowledge to every stakeholder.

Table 3 summarizes the contribution of the ISAC framework (with a focus on its key features) to the E-CORRIDOR objectives.

	Objective 1	Objective 2	Objective 3	Objective 4	Objective 5
ISAC-BD-01	X		X		X
ISAC-BD-02	X		X		X
ISAC-BD-03		X		X	X

ISAC-BD-04		X		X	X

Table 3: Mapping E-CORRIDOR objectives with ISAC BD

8.2. Interconnection with other pilots

The ISAC pilot is an interconnection pilot between the S2C and AT pilot. In fact, as well as collects information from public sources or other ISACs, it exploits information shared by the two pilots mentioned before. Though the collected information increases the cyber-threat knowledge and provides security services to increase security awareness, protect, prevent and mitigate each transportation sector from cyber-attacks.

The S2C pilot shares with the ISAC information about (i) driver and passenger identification and (ii) automotive intrusion detection/prevention results. Such data are analyzed and aggregated by the ISAC analytics to present them structurally through visualization tools that offer a global view of the cyber threat. Such data representation permits the identification of anomalous patterns and risks that can affect a set of vehicles.

The AT pilot shares airport-specific information related to the interconnection network devices present in the airport (e.g., video surveillance camera models, operating systems, software versions). The ISAC pilot can offer security awareness, providing a security report of each airport device through its knowledge in vulnerabilities, exploits, attack patterns, and mitigations.

In addition, the ISAC provides to each pilot the cyber-threat notification service that permits a transportation company to keep up to date on interesting security topics like vulnerabilities in aircraft systems, automotive system incidents, or more specific cyber-attacks.

9. Conclusion and Future Works

In this document, we have described the logical architecture of the ISAC pilot, focusing on the chosen architectural model, explaining the interactions among components, defining the operations specific of this pilot, the data type and the expected analytics. This deliverable shows that all the requirements presented in Deliverable D4.1 [1] are addressed by the presented architecture, which ensures the possibility to collect data, perform analysis, dispatch and visualize the results. The complexity of this scenario is represented by the need to aggregate and analyse different data in order to discover new cyber-threats and provide to the consumer an intuitive and a custom view of the security in its transportation sector. Another challenge is the management of the huge amount of information that the ISAC collects continuously. In the next months the architecture will be implemented and maturated, following the guidelines from WP5 and the analytics results offered by each pilot. This process is expected to be completed at month 26.

A. Appendix

A.1. Definition and Abbreviations

Term	Meaning
AMB	Airport Managing bodies
API	Application Programming Interface
AT	Airport Transportation
CAN	Controller Area Network
CTI	Cyber-Threat Information
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DLI	Data Sharing Agreement (DSA) Lifecycle Infrastructure
DMO	Data Manipulation Object
DSA	Data Sharing Agreement
FMC	Fundamental Modeling Concepts
HTTP	Hypertext Transfer Protocol
NLP	Natural Language Processing
IAI	Information Analytics Infrastructure
ISAC	Information Sharing Analysis Center
ISI	Information Sharing Infrastructure
JSON	JavaScript Object Notation
S2C	Car sharing in Smart Cities
SSL	Secure Sockets Layer
STIX	Structured Threat Information Expression

A.2. Use Cases – Analytics mapping

Table 4 shows the mapping between the ISAC use cases and the IAI E-CORRIDOR analytics.

Analytic Type	**Analytic Name**	**ISAC-UC-01 Public CTI data collection**	**ISAC-UC-02 ISAC-MMT sharing data**	**ISAC-UC-03 Data sharing agreement**	**ISAC-UC-04 Run ISAC-MMT security analysis**	**ISAC-UC-05 Cyber-threat notification**	**ISAC-UC-06 Specific transportation sector data collection**	**ISAC-UC-07 Run local analytic**	**ISAC-UC-08 CTI visualization**
Data analytics for driver and passenger identification	E-CORRIDOR-IAI-SR: Secure Routine–driver identification		X	X			X	X	
	E-CORRIDOR-IAI-SR :Driver DNA		X	X			X	X	
Intrusion detection technologies (IDS)	E-CORRIDOR-IAI-CANIPS: CAN bus IPS – EARNEST		X	X			X	X	
	E-CORRIDOR-IAI-CANIDS: Automotive		X	X			X	X	

	Intrusion Detection								
ISAC analytics	ISAC-IAI-CDL: Cyber data label assignment	X			X	X			
	ISAC-IAI-CDV: Cyber data visualization	X			X	X			X

Table 4: Use cases - Analytics mapping

Bibliography

1. Mari S, Giorgi G. Deliverable D4.1 [Internet]. 2020. Available from: https://e-corridor.eu/wp-content/uploads/2020/12/E-CORRIDOR_D4.1_Final.pdf

2. Costantino G, Matteucci I. CANDY CREAM - Hacking infotainment android systems to command instrument cluster via can data frame. In: Proceedings - 22nd IEEE International Conference on Computational Science and Engineering and 17th IEEE International Conference on Embedded and Ubiquitous Computing, CSE/EUC 2019. 2019.

3. Al-Mhiqani MN, Ahmad R, Yassin W, Hassan A, Abidin ZZ, Ali NS, et al. Cyber-security incidents: A review cases in cyber-physical systems. Int J Adv Comput Sci Appl. 2018;

4. ATEŞ SS, KAFALI H, ÜZÜLMEZ M, LIK H. INVESTIGATING CRITICAL POINTS OF CYBER SECURITY: PREVENTION TERROR ATTACKS IN AIRPORTS. Electron Turkish Stud. 2017;12(32).

5. Mitra S, Ransbotham S. Information disclosure and the diffusion of information security attacks. Inf Syst Res. 2015;

6. Caimi C, Manea M, Ciampoli P, Martinelli F, Mori P, Costantino G, et al. Deliverable 5.1. 2020; Available from: https://e-corridor.eu/wp-content/uploads/2020/12/E-CORRIDOR_D5.1_final.pdf

7. Xu H, Kotov A, Dong M, Carcone AI, Zhu D, Naar-King S. Text classification with topic-based word embedding and Convolutional Neural Networks. In: ACM-BCB 2016 - 7th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics. 2016.

8. Xu J, Xu B, Wang P, Zheng S, Tian G, Zhao J, et al. Self-Taught convolutional neural networks for short text clustering. Neural Networks. 2017;