D5.2 - SPHINX Visualization Dashboards v1

WP5 – Analysis and Decision Making

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for
Health-Care Industry

Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

© SPHINX Consortium, 2020

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Document information

Grant Agreement Number	826183	Acronym	SPHINX	
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry			
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures			
Funding scheme	RIA - Research and Innovation action			
Start Date	1stJanuary 2019	**Duration**	36 months	
Project URL	http://sphinx-project.eu/			
EU Project Officer	Reza RAZAVI (CNECT/H/03)			
Project Coordinator	National Technical University of Athens - NTUA			
Deliverable	D5.2 Visualization Dashboards v1			
Work Package	WP5 – Analysis and Decision Making			
Date of Delivery	**Contractual**	M22	**Actual**	M22
Nature	R - Report	**Dissemination Level**	P – Public	
Lead Beneficiary	SIMAVI			
Responsible Authors	Radu Popescu, Dana Oniga	**Email**	radu.popescu@siveco.ro, dana.oniga@siveco.ro	
		Phone		
Reviewer(s):	George Doukas (NTUA), Yannis Nikoloudakis (HMU)			
Keywords	Interactive Dashboards			

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	10/09/2020	Draft	ToC	Catalin Danila (SIMAVI)
0.20	13/10/2020	Draft	Content	Catalin Danila (SIMAVI)
0.30	14/10/2020	Draft	Internal Review	Yannis Nikoloudakis (HMU); George Doukas (NTUA)
0.40	20/10/2020	Draft	Address Reviewers' Comments	Catalin Danila (SIMAVI);
0.50	21/10/2020	Draft	Address Reviewers' Comments	Radu Popescu (SIMAVI)
0.60	27/10/2020	Pre - Final	Address Reviewers' Comments	Dana Oniga (SIMAVI)
0.70	29/10/2020	Pre - Final	Quality Control	George Doukas (NTUA)
1.00	29/10/2020	Final	Final	Christos Ntanos (NTUA)

Executive Summary

Deliverable D5.2 Visualization Dashboards v1 presents the first results of task T5.2 Advanced Visualization Dashboards implementation, as part of WP5 - Analysis and Decision Making. All activities performed for the design and the development of the first version of the Interactive Dashboard SPHINX component (ID) are documented in the following four chapters, detailing the technical background and other important aspects.

This component is part of the SPHINX architecture, belonging to the block "Decision Support System and Interactive Dashboards", which presents information to the system's users in an intuitive and actionable way, adopting multiple panels displaying high-level status, statistical data, charts and histograms.

This deliverable contributes to the achievement of milestone MS5: First set of SPHINX services & prototype modules completed - First Integrate approach at the end of M20.

Contents

Table of Figures

List of Abbreviations

ABBREVIATION	EXPLANATION
AD	Anomaly Detection
AE	Analytic Engine
BBTR	Blockchain Based Threats Registry
DSS	Decision Support System
DTM	Data Traffic Monitoring
HP	Honeypot
ID	Interactive Dashboards
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
KB	Knowledge Base – Decision Support System
RCRA	Real-time Cyber Risk Assessment
SIEM	Security Information and Event Management
VAaaS	Vulnerability Assessment as a Service
WP	Work Package

1 Introduction

1.1 Purpose & Scope

The purpose of this document is to describe the systematic work performed under the task *T5.2 Advanced Visualization Dashboards (WP5 – Analysis and Decision Making)* between months M10 to M22 of SPHINX project. This deliverable covers the activities of research, design and development performed during the first iteration of development for the SPHINX Interactive Dashboards (ID) Component. The component provides the users with an advanced graphic interface for the SPHINX Toolkit.

1.2 Structure of the deliverable

This deliverable covers four chapters. The first one represents the introduction and the rationale for writing this document and its relations with other WPs & Tasks. Chapter 2 contains a general overview of the subject of Interactive Dashboards. Chapter 3 describes the Interactive Dashboards Component (ID), covering its role in the SPHINX Ecosystem, technical and architectural details, and integrations with other SPHINX components. The last chapter resumes the status of the development direction, including the technologies used for ID.

1.3 Relation to other WPs & Tasks

The development effort described in this report is based on the deliverables created within *WP2 Conceptualisation, Use Cases and System Architecture*, starting with *D2.3 SPHINX Architecture v1, D2.4 Use Cases Definition and Requirements Document v1*, *D2.5 Requirements and Guidelines v1*, and *D2.6 SPHINX Architecture v2*. Design, development and implementation principles were used based on recommendations from *WP6: SPHINX Common Integration Platform & Incremental Strategy*.

The inputs of ID are established in relation with components from *WP3 Cyber Security risk assessment & Beyond – Sphinx Intelligence*, *WP4 SPHINX Toolkits* and *WP5 Analysis and Decision Making*.

The ID component will be integrated, validated and tested in the context of *WP6: SPHINX Common Integration Platform & Incremental Strategy*, during tasks *T6.4 System integration execution that* will address the actual integration of outcomes from WP4 and WP5, and *T6.5 Testing of Integrated SPHINX platform*.

The second iteration of development of the ID component will include feedback received from the integration testing activities and from the end users during the pilots' testing and validation period within *WP7 Technology Validation Pilots and Privacy assessment*. Task *T7.2 System functional testing and validation* is aimed to verify that the deployed SPHINX components to the pilot sites meet the functional, operational and technical requirements as described in other WPs and will gather the evaluation results of the validation pilot release (M25-M27) and the second validation pilot release (M32-M34).

2 General Overview

The SPHINX ID Component represents an important element in SPHINX System. It is the point of access in the SPHINX system. The ID component manages the users and their rights in collaboration with Service Manager component. It centralizes the access to the front-ends of the SPHINX components; it allows the other SPHINX components to present their data in interactive graphs. Additionally, it facilitates the creation of forecasts and answers to business questions about the IT infrastructure.

Importantly, the ID component collects data from ten SPHINX components and provides the users with the ability to interact with the data in a dynamic way, to create their own information processes and have great flexibility regarding the analysis of their security system.

Different types of panels present data in an easy-to-access manner, in graphical, statistical, tabular and temporal formats, offering an intuitive visualisation of relevant cyber security information. This component also manages the SPHINX alerts and notifications that are designed to enable rapid situational awareness and understanding for the users.

3 Overview of Interactive Dashboards

3.1 Scope of Interactive Dashboards

The SPHINX system generates alerts and notifications based on a large amount of data. The Interactive Dashboard Component of SPHINX intends to help users visualize, explore and analyse the data generated by the other SPHINX components, identify trends and better understand the cybersecurity aspects of the network infrastructure.

ID is based primarily on the open-source visualization and analytics software Grafana [1]. The main functionalities of this component are:

- Display interactive graphs and trends of the data from SPHINX components, notifications and alerts;
- Create dashboards that group the graphs in order to present to the user the relevant data
- Manage the contact information of the users responsible for cybersecurity. These users will be alerted in case of cybersecurity incidents;
- Display proposed actions in case they exist to specific alerts.

The ID component is described in the following sections of the document.

3.2 Requirements

The following table describes how the functional and usability requirements, as presented in the deliverable *D2.6 SPHINX Architecture v2,* are answered and solved in the building and development of the ID component.

Requirement ID	Description and Rationale	Functionalities
ID-F-010	The ID component implements intelligent User Interfaces supporting a multi-dimensional approach. It presents data and information in the appropriate formats (e.g., charts, tabular information, colours) and implements adequate push-based notification mechanisms to emphasise urgency or new information requiring action.	The ID uses Grafana as the main tool, which contains intelligent mechanisms for displaying data in different formats and colours (graphs, bar gauges, tables, stats). It contains notifications of several types depending on the user's preference (alerts, notifications, errors, etc.).
ID-F-020	The ID component supports users to easily interact with a large amount of information regarding system data, including personal data, through intuitive and efficient mechanisms.	ID supports many different storage backends (data sources like PostgreSQL, Elasticsearch) for table or time-series data. The data presented in dashboards can be filtered, aggregated, summarized.
ID-F-030	The ID component enables the enrichment (in quantity and quality) of the degrees of freedom for user interaction with the SPHINX Platform and, concurrently, with the real processes in the IT infrastructure.	The ID allows the user to create their dashboards, combining existing graphics with new graphics. The user can also combine multiple graphics from different dashboards in one place. The time frame can be changed from the dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Requirement ID	Description and Rationale	Functionalities
		settings or via graphs. Also, the user can sort tables by columns or by the labels in case of the graphs and view detailed data by hover the graphs. The alert panel allows searching and pagination.
ID-F-040	The ID component provides an advanced analytic data visualisation engine that is capable of visually presenting intuitive data on the IT ecosystem's network and users' behaviour. Descriptive statistics and graphs (pie, bar and scatter plots) allow the IT operator to rapidly acknowledge detected suspicious network and user behaviour and take appropriate mitigation measures.	The ID shows the cybersecurity-related data in several types of panels, such as Pie Charts, Bar Gauges, Scatter Plots, Graphs, Tables, Sankey Diagrams, Stats, Worldmap and custom plugins such as the alert panel that allows staff notification to take the necessary measures in time.
ID-F-050	The ID component includes a list of individuals to be alerted in case of forecasted, suspected or ongoing cyber security incidents. Alerting mechanisms include dashboard displays, emails and text messages to ensure appropriate recipients are informed at all times. The alerts consider rules such as incident classification and severity type.	The ID allows the administrator to add a list of people who can be notified in case of alerts. The alert panel contains important fields such as description, date and time, possible location and severity of alerts. When an alert is detected, it will be displayed in the Dashboard and in the meantime is sent to staff through e-mail.
ID-F-060	The ID component enables the classification of the automated alerts or notifications issued of imminent, ongoing and forecasted cyber threats, incidents and attacks. The classification scheme shall allow the easy identification of vulnerabilities, risks, threats, events, incidents or attacks, as well as of situations worth monitoring or requiring urgent intervention. The ID component allows users to filter the registered alerts by category.	ID will retrieve data from each component regarding alerts or notifications and it will display them based on categories.
ID-F-070	The ID component enables users to establish the parameters of their own dashboard views, based on their role and duties concerning the operation of the IT ecosystem.	ID allows users to add their queries for panels, where they can build their Dashboards, setting different permissions for other users (edit, view).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Requirement ID	Description and Rationale	Functionalities
ID-F-080	The ID component provides customised cyber security report containing: • comprehensive visual analytics (e.g., charts, tabular information, statistics); • statistical information on registered cyber security events and incidents in the IT ecosystem, including successful and unsuccessful hacking attempts and type of attack: spam, email trap, malware, phishing, database injection, anomalous user and network behaviours; • time and duration of successful cyber attacks to the IT ecosystem along with list of the affected assets; identification and location of the organisation affected by the cyber attack.	Regarding the first point of the list, a user can add its own queries to build graphs, tables, pie charts. For the last two points, ID can display statistical information in collaboration with other components. Grafana has the feature of downloading JSON and CSV files from panels or Dashboards.
ID-F-090	The ID component aggregates all the alerts generated by the individual SPHINX tools and depicts them in tabular format as follows: - The first column in the alert table shows an alert number and its generated date, time and location; - the second column shows the classification of each alert (i.e. CRITICAL, ALERT, ERROR, INFORMATIONAL) depending on the associated level of criticality; - the third column identifies the specific SPHINX tool or service that generated the associated alert; - and the fourth column displays the alert status through a dropdown menu with the options Closed, Open, Ignore, Acknowledge and Empty Field (the initial state). As the user selects one option, the table row is immediately updated and registers also the user's name and the date when the action was performed. This information is locked and only the system's administrator may unlock the locked alert status field; The fifth column displays the system's proposed course of action and the risk assessment tools available in the SPHINX system. The user may sort the alert table by date, alert classification, SPHINX tool and alert status. The table supports pagination.	The alert panel plug-in contains every column (plus Details that redirects the user to components to see a more detailed report) specified in the requirement and functionalities (sorting for every column, pagination, number of rows on a page, search tool).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Requirement ID	Description and Rationale	Functionalities
ID-F-100	The ID component presents the spatiotemporal information about each generated alert, such as the date and time and the location (i.e., the location of the targeted hospital).	The alert table will contain timestamp and location, as specified in the precedent functionalities.
ID-F-110	The ID component displays a menu bar that includes at least 3 fields: the first field displays the number of critical alerts; the second field provides an option menu allowing the user to visualise various graphs on alert statistics in a separate webpage and to export the alert table in csv or excel files; the third field refers to the dashboard's settings, which enable the user to easily customise/configure the area below the alerts table. This area may display different graphs associated to the operations of specific SPHINX tools or services. Other fields that the menu bar includes are: a field for selecting the display language, a field for searching and querying features and a button to display the list of individuals to contact in case of a cyber security event or incident.	The ID component supports the creation of new dashboards, based on existing panels or newly created panels, so the user can easily customize/configure the information presented to him, In ID every panel (graphs, tables, bar gauges, etc.) can be exported in a CSV format. The missing functionalities will be implemented as custom plugins.
ID-F-120	The ID component allows users to select a status for each alert (i.e. Closed, Open, Ignore, Acknowledge and Empty Field), depending on the action to be taken for that specific alert.	The alert plug-in offers the user the possibility to select the status of the alerts.
ID-F-130	The ID component displays the suggested/proposed actions to be taken in order to mitigate an incident.	The alert table also displays the proposed actions and details coming from SPHINX components.
ID-F-140	The ID component allows the SPHINX administrator to create users and assign roles (e.g. administrator, operator, and observer) in SPHINX. SPHINX users are able to login, logout, setup profile (e.g., name), email and change the password.	Grafana contains a user management module that allows the creation and deletion of users and also to assign roles to the users. Only the administrator can create and add roles to staff.
ID-F-150	The ID component displays a list of all the SPHINX tools and services, including a short description of the tool or service (with an overlay window). Users may choose an item by clicking on it and be redirected to the selected tool or service, without having to login again.	Through a Single Sign-On mechanism, the user can access every component without providing credentials every time. The user can access those features through the alert panel plug-in or through another custom plug-in that contains the list of components. Details about

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Requirement ID	Description and Rationale	Functionalities
		the component will be displayed in a tooltip when a list element is hovered.
ID-F-160	The ID component allows users to visualise data using various graphs, such as time-series, alert statistics. The used visualisation mechanisms enable users to intuitively and efficiently understand the data.	ID will contain dashboards with data from the SPHINX components (for example, for Network Traffic coming from DTM). It enables the user to visualise graphs, alerts, tables, and other panels that make the analyzing easier.
ID-F-170	The ID component allows users to export the data into different file formats, such as Comma-Separated Values (CSV), JavaScript Object Notation (JSON) and excel files.	The user can export Dashboards in JSON and Panels in CSV.
ID-F-180	The ID component contains a list of dashboard settings which enables users to customise/configure the interface, by having a designated area which users can modify. This area displays different graphs associated to the operations of specific SPHINX tools or services.	ID allows the user to modify, delete, add or combine different panels in new dashboards in order to create a personalized view of the data. The user can query data from every SPHINX component.
ID-F-190	The ID component contains a search bar which enables users to easily search for different elements.	ID will contain a search bar in the custom plug-in menu that enables the users to access any element more easily. The alert table contains a search bar to find an alert faster. Grafana has also a functionality based on title and tags.
ID-U-010	The ID component delivers a set of web-based dashboards to present summaries of the relevant data and information associated to each of the SPHINX cyber security tools and services. The main SPHINX dashboard aggregates the relevant data and information of all SPHINX tools and services.	ID is based on Grafana, a web-based application with advanced support for dashboard creation and data visualisations.
ID-U-020	The ID component provides an overview of the cyber security status of an IT organisation. Users are able to conveniently access this function from a single location (e.g., user workstation), provided it is authorised and complies with the SPHINX specifications.	The ID main dashboard will present a resume of the most important panels with data coming from other Sphinx Tools. A user from IT Staff can access it through HTTP/S.The user will be allowed to access the front-end web applications of the other SPHINX

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

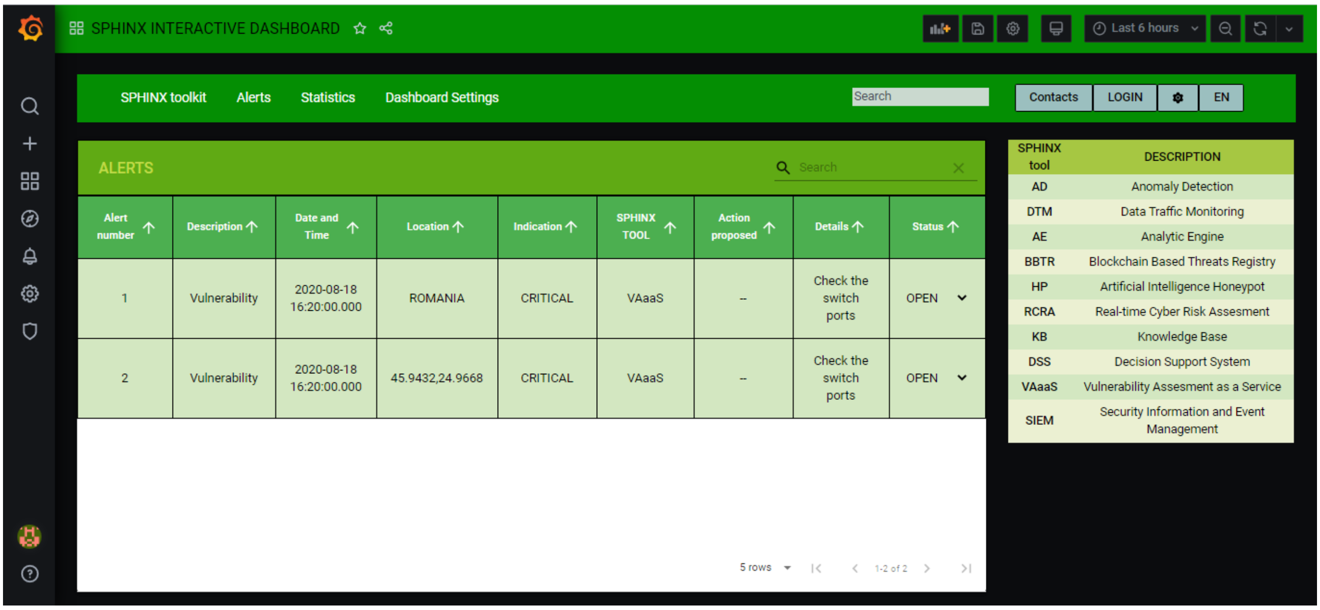
Requirement ID	Description and Rationale	Functionalities
		components using SSO services provided by the Service Manager component, enabling visualization of every component without providing credentials.

3.3 Main Dashboard

The ID component contains a general dashboard that includes the most important information from the SPHINX components, providing a summary of the IT infrastructure data, making it easier for the user to analyze the status of the infrastructure.

It contains three main plugins:

- The first plug-in is a navigation menu that allows the user to display certain charts, depending on user preferences, a search bar for quick access to elements coming from every dashboard, a list of persons from health organizations to be contacted in case of alerts, a functionality for login, settings and language.
- The second plug-in is an alert table, which contains a quick search, column sorting and pagination functionality.
- The last plug-in is a list of SPHINX components where the user can access more details regarding a data coming from a component.



Alert number	Description	Date and Time	Location	Indication	SPHINX TOOL	Action proposed	Details	Status
1	Vulnerability	2020-08-18 16:20:00.000	ROMANIA	CRITICAL	VAaaS	--	Check the switch ports	OPEN
2	Vulnerability	2020-08-18 16:20:00.000	45.9432,24.9668	CRITICAL	VAaaS	--	Check the switch ports	OPEN

SPHINX tool	DESCRIPTION
AD	Anomaly Detection
DTM	Data Traffic Monitoring
AE	Analytic Engine
BBTR	Blockchain Based Threats Registry
HP	Artificial Intelligence Honeypot
RCRA	Real-time Cyber Risk Assesment
KB	Knowledge Base
DSS	Decision Support System
VAaaS	Vulnerability Assesment as a Service
SIEM	Security Information and Event Management

Figure 3.1 SPHINX Main Dashboard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.4 Design Principles

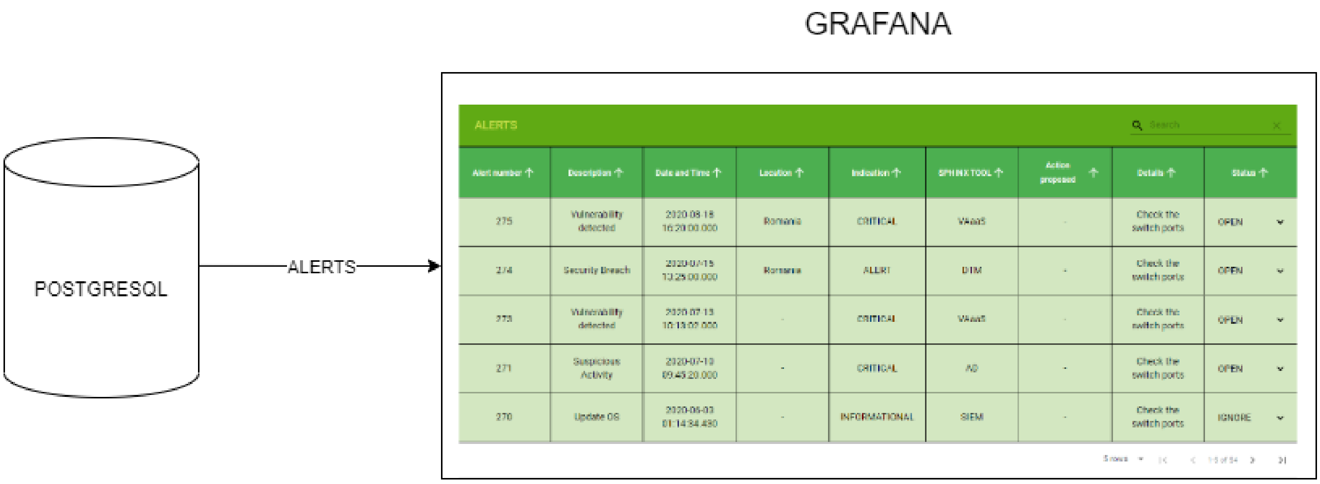
The Interactive Dashboard component presents multiple types of data relevant to IT Infrastructure and User Behaviour in an interactive way, through graphs, alerts, tables, bar gauges and charts, to provide to the user an easier way to analyse data received from its IT infrastructure.

A very important functionality is to alert IT staff through various types of communication channels, chosen by them in case of errors, notifications, critical or minor alerts found by the SPHINX components.

The SPHINX ID is based on Grafana, which is a multi-platform open-source analytics and interactive visualization web application. It provides charts, graphs and alerts when connected to supported data sources. The data sources can be databases (Grafana supports a wide range of time series or relational databases) or web services. As concrete examples of data sources that are used by ID are PostgreSQL and Elasticsearch. Grafana is extensible through a plug-in system. End users can create complex monitoring dashboards using interactive query builders.

For the SPHINX system, a custom plug-in was created to manage the specific requirements for the management of alerts issued from all SPHINX components. The SPHINX components publish their alerts to Kafka and then the alerts are imported in a PostgreSQL database that serves as a data source for the alert management plug-in.

The following images illustrate the ID's alert management using the example of the Data Traffic Monitoring (DTM) component, which generates a large amount of data about network traffic. This data is published to Elasticsearch, which is optimized for the kind of grouping and summarization that is relevant for this component.



ALERTS

Alert number	Description	Date and Time	Location	Indication	SPHINX TOOL	Action proposed	Details	Status
275	Vulnerability detected	2020-08-18 16:20:00.000	Romania	CRITICAL	VAaaS	-	Check the switch ports	OPEN
274	Security Breach	2020-07-15 13:25:00.000	Romania	ALERT	DTM	-	Check the switch ports	OPEN
273	Vulnerability detected	2020-07-13 10:13:02.000	-	CRITICAL	VAaaS	-	Check the switch ports	OPEN
271	Suspicious Activity	2020-07-10 09:45:20.000	-	CRITICAL	AD	-	Check the switch ports	OPEN
270	Update OS	2020-06-03 01:14:34.480	-	INFORMATIONAL	SIEM	-	Check the switch ports	IGNORE

Figure 3.2 SPHINX Alerts Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

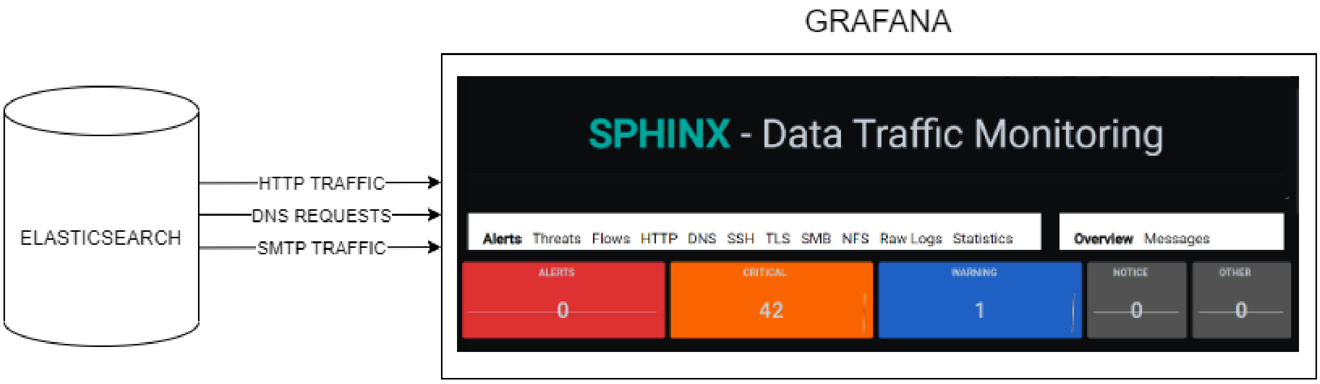


Figure 3.3 SPHINX Dashboard

Figure 3.1 and 3.2 present the alerts plug-in, DTM dashboards (for Network Traffic Analysis) and data sources for data providing, using technologies that make these features possible:

- Grafana;
- Elasticsearch; PostgreSQL.

3.5 Human factor

Interactive Dashboards is mainly about transmitting to the user, in a comprehensible visual manner, information about the security state of the system. ID component, through Grafana, implements state of the art data visualisations techniques that allow the user to see and understand, with minimal effort, the relevant metrics collected about the network infrastructure.

The data visualisations are grouped in dashboards. Grafana provides advanced support for dashboard creation and management. In developing the dashboards, best practices about dashboard development and information architecture documented by the team behind Grafana [2] were taken into considerations.

Such best practices indicate that during the creation of a dashboard the following should be considered:

- a dashboard should answer a question, it should have a goal. The data should be presented from large too small or from general to specific.
- dashboards should reduce cognitive load, not add to it. The dashboards should be easy to interpret. The meaning of the graphs the dashboard contains should be obvious.
- avoid unnecessary dashboard refreshing to reduce the load on the network or backend. If the data changes every hour, the dashboard refresh rate should be set to 1 hour.

Additional best practices, identified by [5], [6] suggest:

- identify the key data and make it stand out. This helps the user identify what's important in an instant and saves the user time
- use information architecture in designing the dashboard. The information in the dashboard should be structured by taking into account how the user's eyes scan the page (studies identified patterns like F-pattern or Z-pattern where the locations where the user's eyes rest take the form of letters F or Z).
- use consistent design language and colour scheme

The dashboard can be classified into three general categories [5], [7]:

- Operational dashboards – these dashboards help the user see what's happening right now

- Analytical dashboards – these dashboards give the user a clear view of performance trends and potential problems
- Strategic dashboards – this type of dashboard lets the user track their main strategic goals via KPIs

SPHINX ID component will incorporate all three types of dashboards.

It will be further configured to add, edit or delete notification channels in order to ensure that the appointed IT contacts shall be notified. The administrator can select channels like Discord, Email, Google Hangouts Chat, Kafka, Microsoft Teams, Prometheus Alertmanager, Slack and many other supported notifiers. The administrator can add or delete permissions to their teams and can define alert rules on graphics with different queries like overcoming packets coming from a port, for example.

3.6 Technical Details

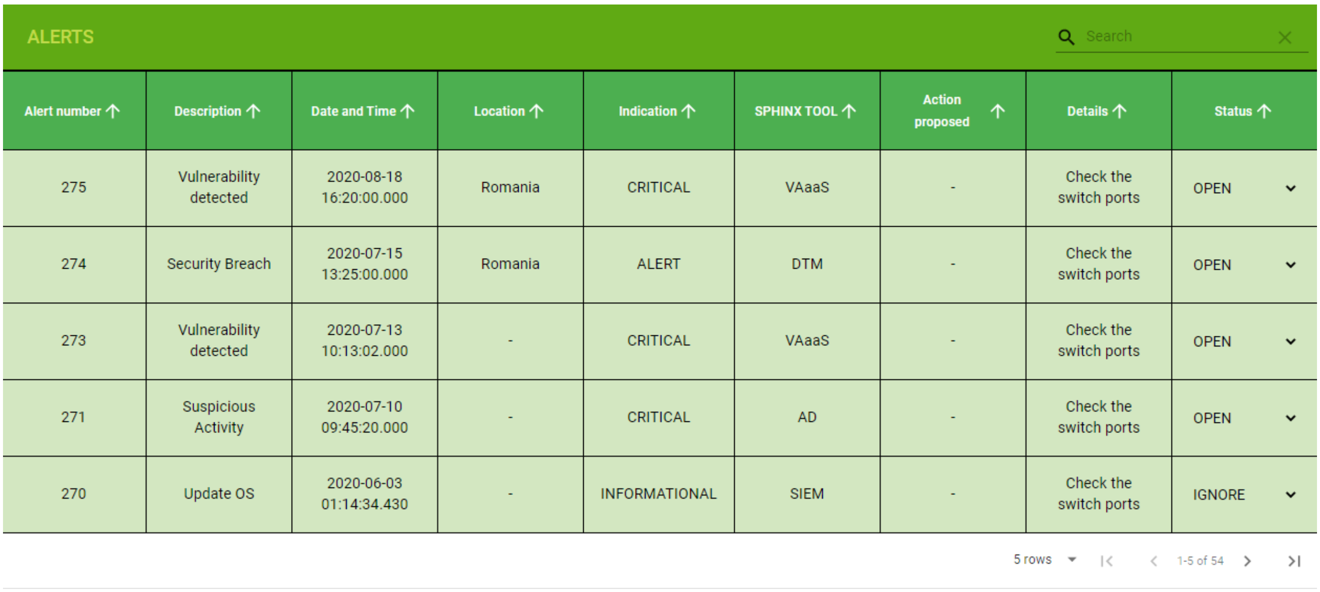
3.6.1 Data sources

Grafana supports natively many different backends for the data. It also has a plug-in based extension mechanism for loading data from a new type of backend.

The Alert Plug-in centralizes the alerts and notifications from all the SPHINX components. This plug-in uses PostgreSQL as a data source. The flow of data from the SPHINX components to PostgreSQL is presented below:

- the components publish their alerts, as JSON messages, to the messaging bus used in SPHINX (Kafka)
- KSQLDB is used to aggregate the alerts from all components in a single stream of messages
- KSQLDB is used to load to PostgreSQL the unified stream of alerts

The panels used in the dashboards of Data Traffic Monitoring component load their data from Elasticsearch, which is optimized for storing time-series data. The DTM data is loaded to Elasticsearch using Logstash, a data processing pipeline with support for a multitude of sources and destinations.



ALERTS

Alert number ↑	Description ↑	Date and Time ↑	Location ↑	Indication ↑	SPHINX TOOL ↑	Action proposed ↑	Details ↑	Status ↑
275	Vulnerability detected	2020-08-18 16:20:00.000	Romania	CRITICAL	VAaaS	-	Check the switch ports	OPEN
274	Security Breach	2020-07-15 13:25:00.000	Romania	ALERT	DTM	-	Check the switch ports	OPEN
273	Vulnerability detected	2020-07-13 10:13:02.000	-	CRITICAL	VAaaS	-	Check the switch ports	OPEN
271	Suspicious Activity	2020-07-10 09:45:20.000	-	CRITICAL	AD	-	Check the switch ports	OPEN
270	Update OS	2020-06-03 01:14:34.430	-	INFORMATIONAL	SIEM	-	Check the switch ports	IGNORE

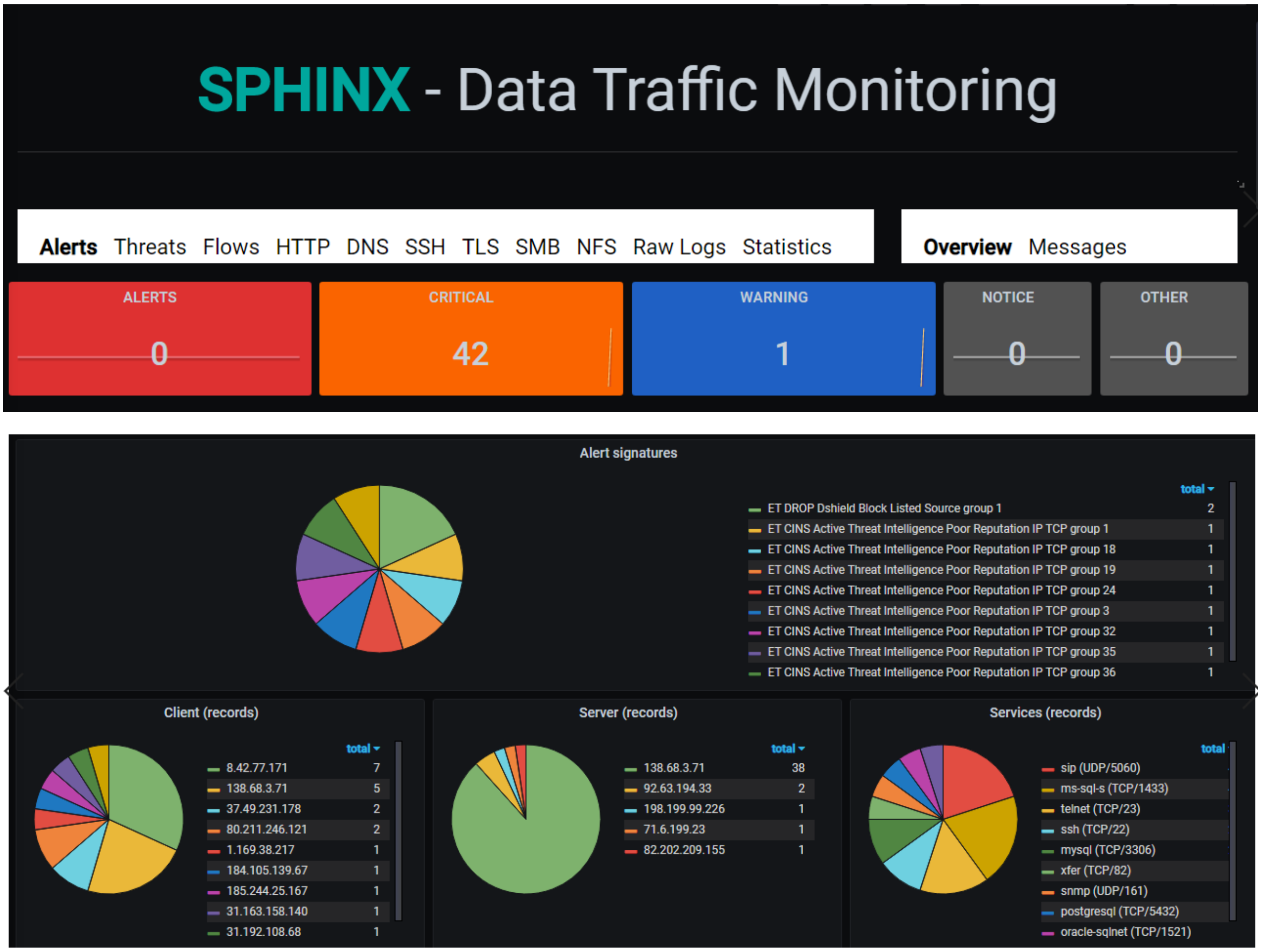
5 rows ▾ |< < 1-5 of 54 > >|

Figure 3.4 SPHINX ID Alert Table

Data coming from DTM is organized in 26 dashboards. The dashboards fall into several broad categories:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- General Dashboard for DTM
- Alerts
    - Overview
    - Messages
- Threats
    - Overview
    - Messages
- Flows
    - Overview
    - Talkers
    - Services
    - Sankey
    - Geo IP
    - Messages
- HTTP
    - Overview
    - Messages
- DNS
    - Overview
    - Messages
- SSH
    - Overview
    - Messages
- TLS
    - Overview
    - Messages
- SMB
    - Overview
    - Messages
- NFS
    - Overview
    - Messages
- Raw Logs
- Statistics



SPHINX - Data Traffic Monitoring

Alerts Threats Flows HTTP DNS SSH TLS SMB NFS Raw Logs Statistics

Overview Messages

ALERTS	CRITICAL	WARNING	NOTICE	OTHER
0	42	1	0	0

Alert signatures

	total
ET DROP Dshield Block Listed Source group 1	2
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 1	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 18	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 19	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 24	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 3	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 32	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 35	1
ET CINS Active Threat Intelligence Poor Reputation IP TCP group 36	1

Client (records)

	total
8.42.77.171	7
138.68.3.71	5
37.49.231.178	2
80.211.246.121	2
1.169.38.217	1
184.105.139.67	1
185.244.25.167	1
31.163.158.140	1
31.192.108.68	1

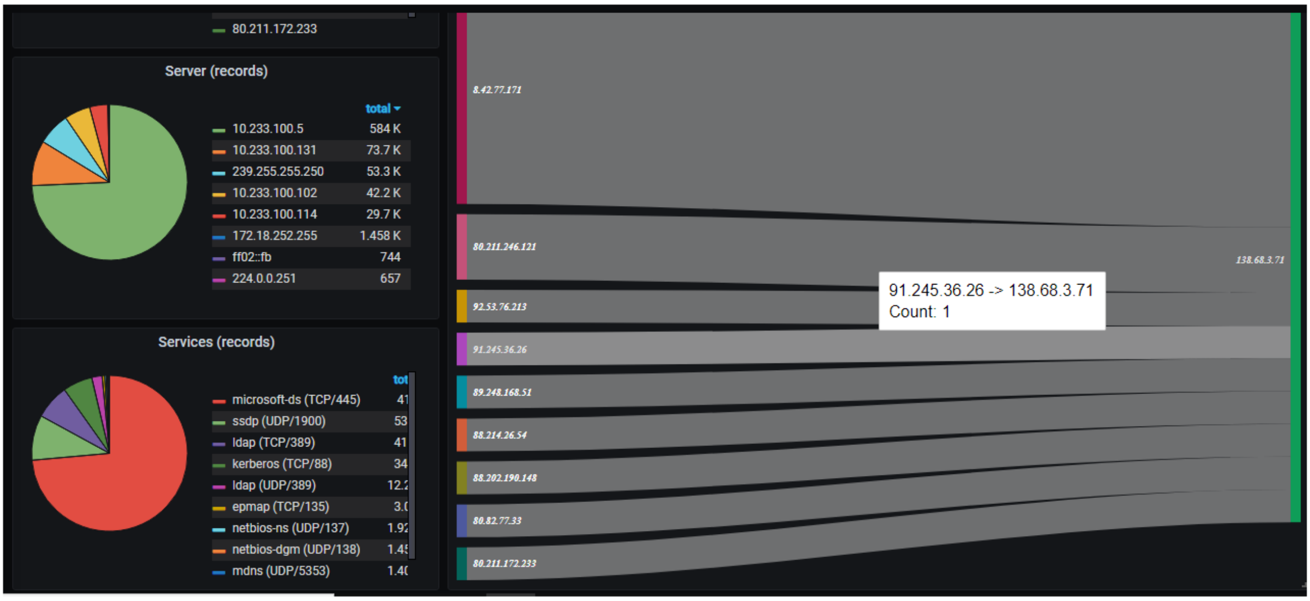
Server (records)

	total
138.68.3.71	38
92.63.194.33	2
198.199.99.226	1
71.6.199.23	1
82.202.209.155	1

Services (records)

	total
sip (UDP/5060)	
ms-sql-s (TCP/1433)	
telnet (TCP/23)	
ssh (TCP/22)	
mysql (TCP/3306)	
xfer (TCP/82)	
snmp (UDP/161)	
postgresql (TCP/5432)	
oracle-sqlnet (TCP/1521)	

Figure 3.5 DTM Alerts Overview Dashboard



— 80.211.172.233

Server (records)

	total ▾
🟩 10.233.100.5	584 K
🟧 10.233.100.131	73.7 K
🟦 239.255.255.250	53.3 K
🟨 10.233.100.102	42.2 K
🟥 10.233.100.114	29.7 K
🟦 172.18.252.255	1.458 K
🟪 ff02::fb	744
🟪 224.0.0.251	657

Services (records)

	tot
🟥 microsoft-ds (TCP/445)	41
🟩 ssdp (UDP/1900)	53
🟪 ldap (TCP/389)	41
🟩 kerberos (TCP/88)	34
🟪 ldap (UDP/389)	12.2
🟨 epmap (TCP/135)	3.0
🟦 netbios-ns (UDP/137)	1.92
🟧 netbios-dgm (UDP/138)	1.45
🟦 mdns (UDP/5353)	1.40

91.245.36.26 -> 138.68.3.71
Count: 1

Figure 3.6 DTM Flows Overview Dashboard

The Flows Dashboards in figure 3.4 illustrates how traffic detected by Data Traffic Monitoring Component can be analysed using a Sankey diagram and the IPs with highest data transfers can be identified.

According to the information presented above, the technical details can be illustrated in two figures, as follows:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- The infrastructure for Alerting purposes:

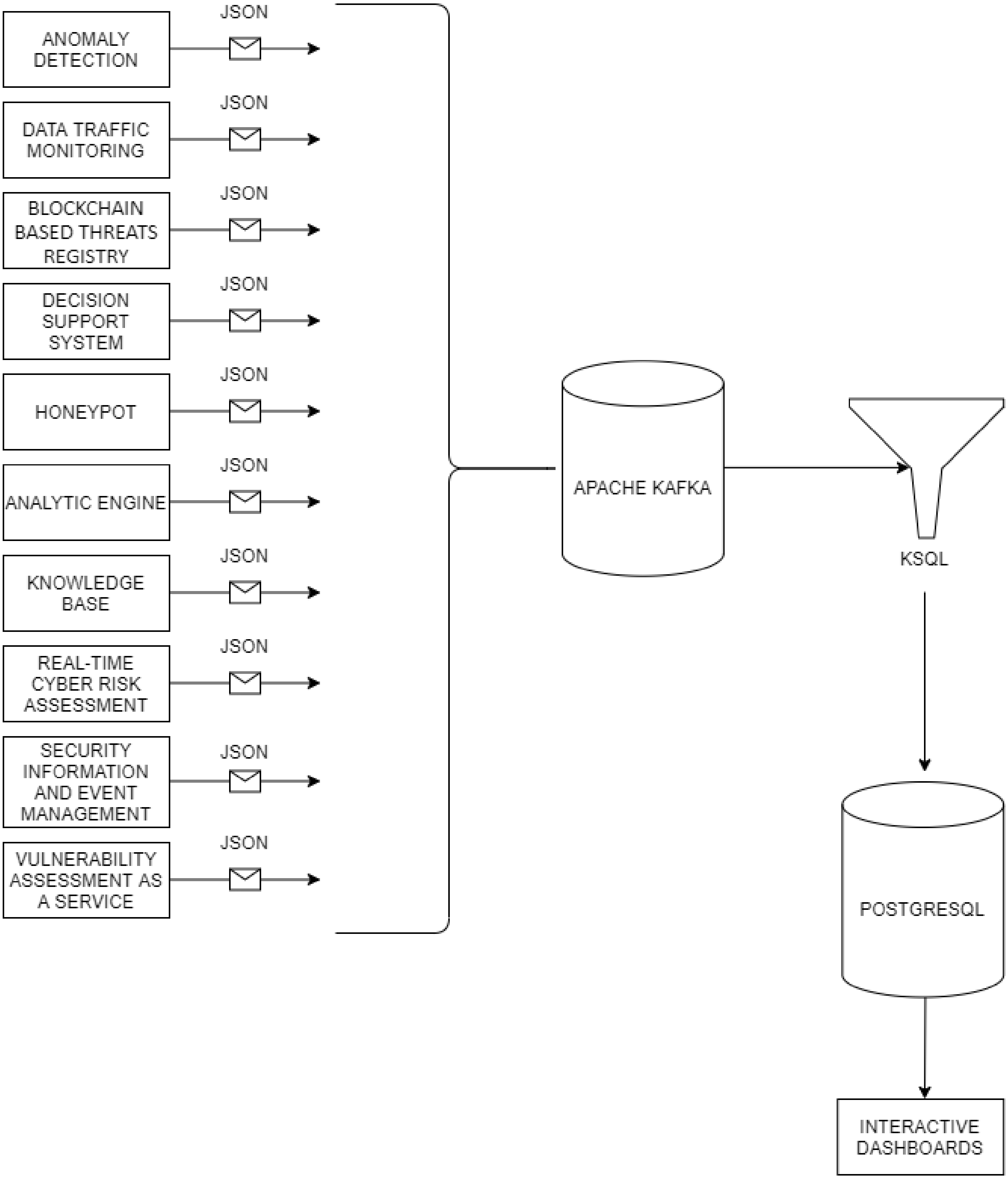


Figure 3.7 SPHINX ID Alerting Technical Details

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Infrastructure for displaying of DTM data in ID:

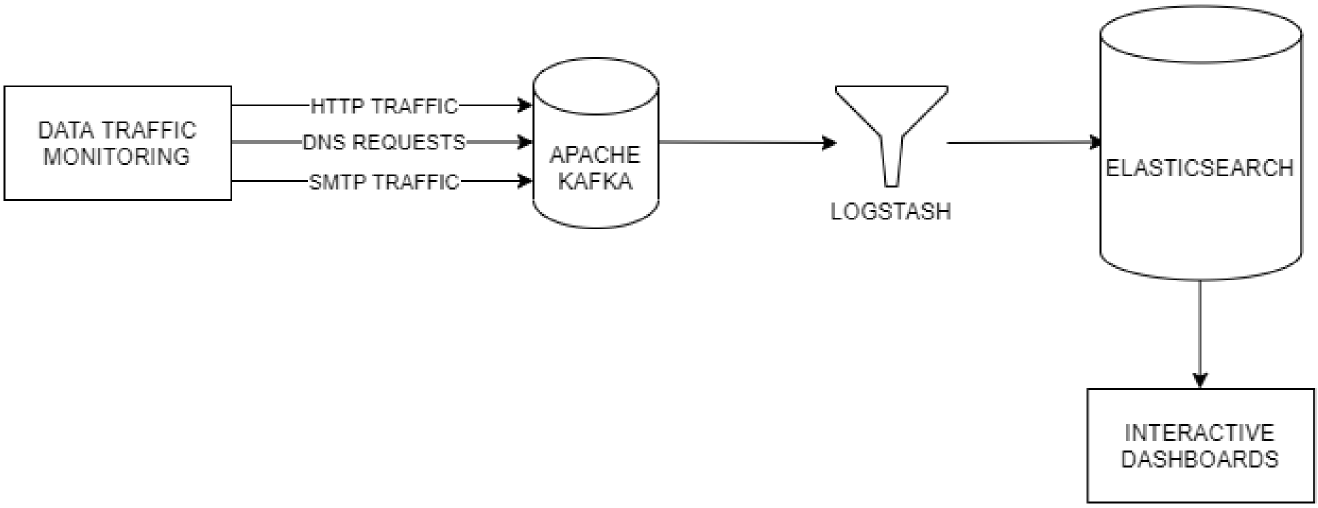


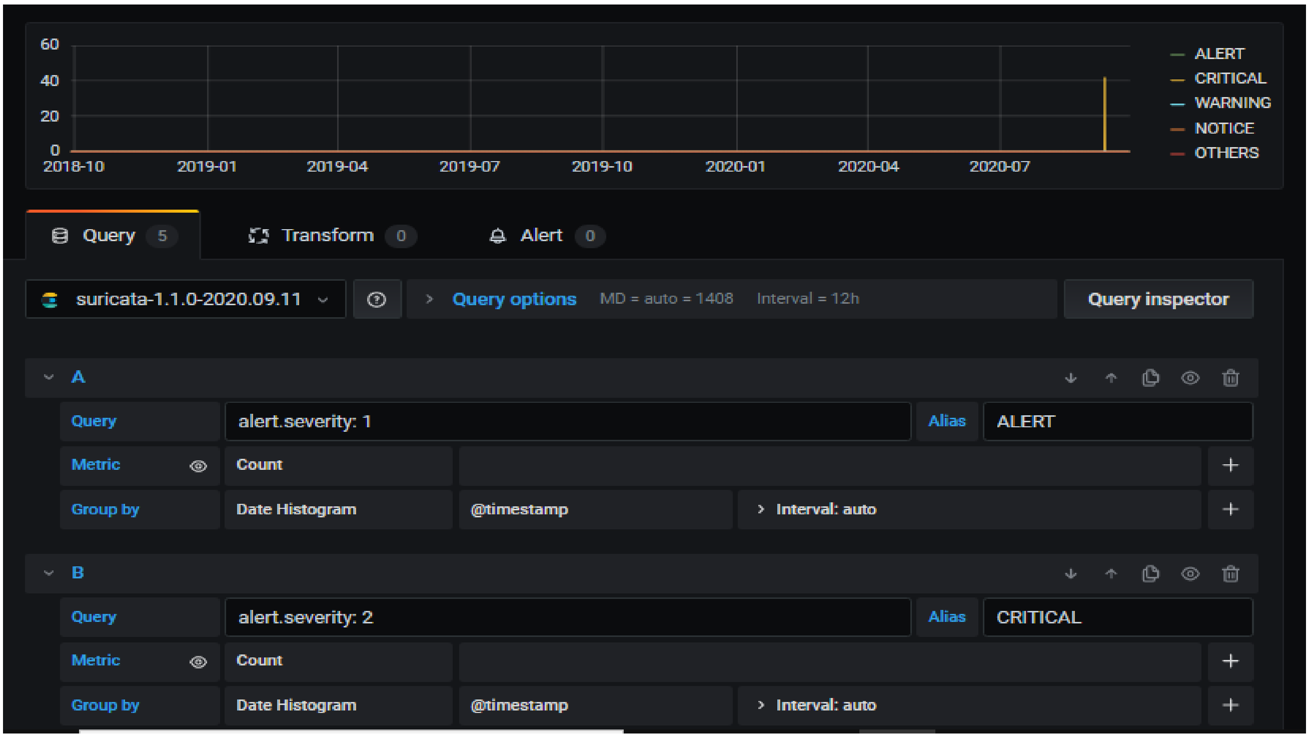
Figure 3.8 SPHINX ID Graphics for DTM Technical Details

3.6.2 Dashboard Customizations

DTM component offers users the possibility to create their customized dashboards depending on their preferences. For example, the web server administrator can create dashboards with only the visualisation related to the web servers. Or, if the user wants to see only graphics on the source IPs, specific graphics can be selected or added to separate dashboards.

Grafana also allows users to mix their panels in different ways:

- mixed, if they want to combine data from different data sources;
- grouping queries from the same Data sources;
- mixed with multiple queries.



suricata-1.1.0-2020.09.11

MD = auto = 1408 Interval = 12h

A

Query: alert.severity: 1 Alias: ALERT
Metric: Count
Group by: Date Histogram @timestamp › Interval: auto

B

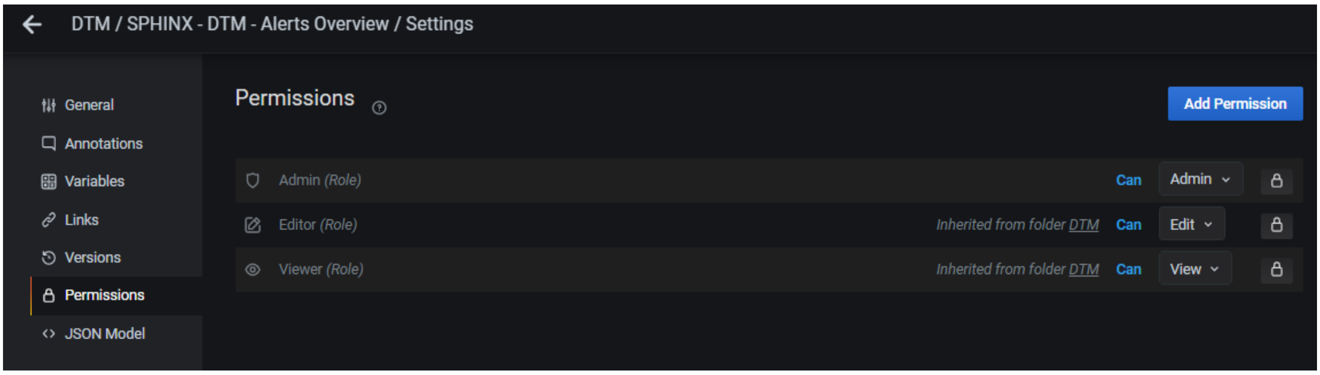
Query: alert.severity: 2 Alias: CRITICAL
Metric: Count
Group by: Date Histogram @timestamp › Interval: auto

Figure 3.9 Multiple Queries from Data source

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.6.3 User Management

Permission management can be determined by the healthcare organisation's IT infrastructure administrator, establishing the roles of others in the team. The following figure depicts the categories of permissions that the administrator can grant.



DTM / SPHINX - DTM - Alerts Overview / Settings

Permissions

Admin (Role) Can Admin

Editor (Role) Inherited from folder DTM Can Edit

Viewer (Role) Inherited from folder DTM Can View

Figure 3.10 User management permissions

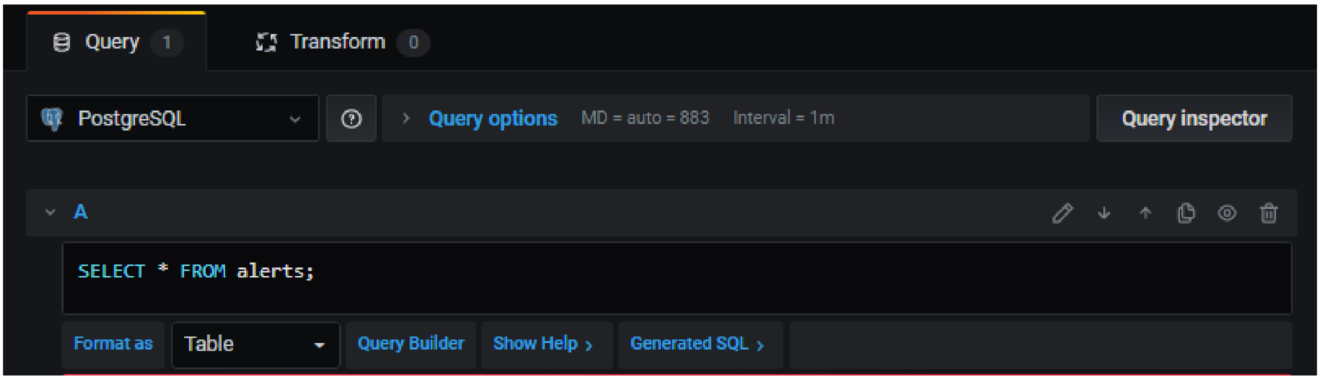
3.6.4 Grafana

Grafana is an open-source visualization and analytics software that allows making queries, visualization, alerts, and explore metrics no matter where they are stored. It provides tools to turn the time-series database (TSDB) data into beautiful graphs and visualizations [1]. The SPHINX ID Component uses this tool to have a more dynamic way of analysing captured web traffic packets.

Grafana allows several functionalities, including composing and choosing relevant graphics from several dashboards, adding, deleting and editing permissions for IT staff and different types of notification channels for alerting.

3.6.5 PostgreSQL

PostgreSQL is a free and open-source relational database management system (RDBMS) emphasizing extensibility and SQL compliance. Grafana integrates different types of data sources, having PSQL included. As mentioned above in the Technical Details, PostgreSQL is used for storing data from the DTM and the Anomaly Detection (AD) components.



PostgreSQL

MD = auto = 883 Interval = 1m

```
SELECT * FROM alerts;
```

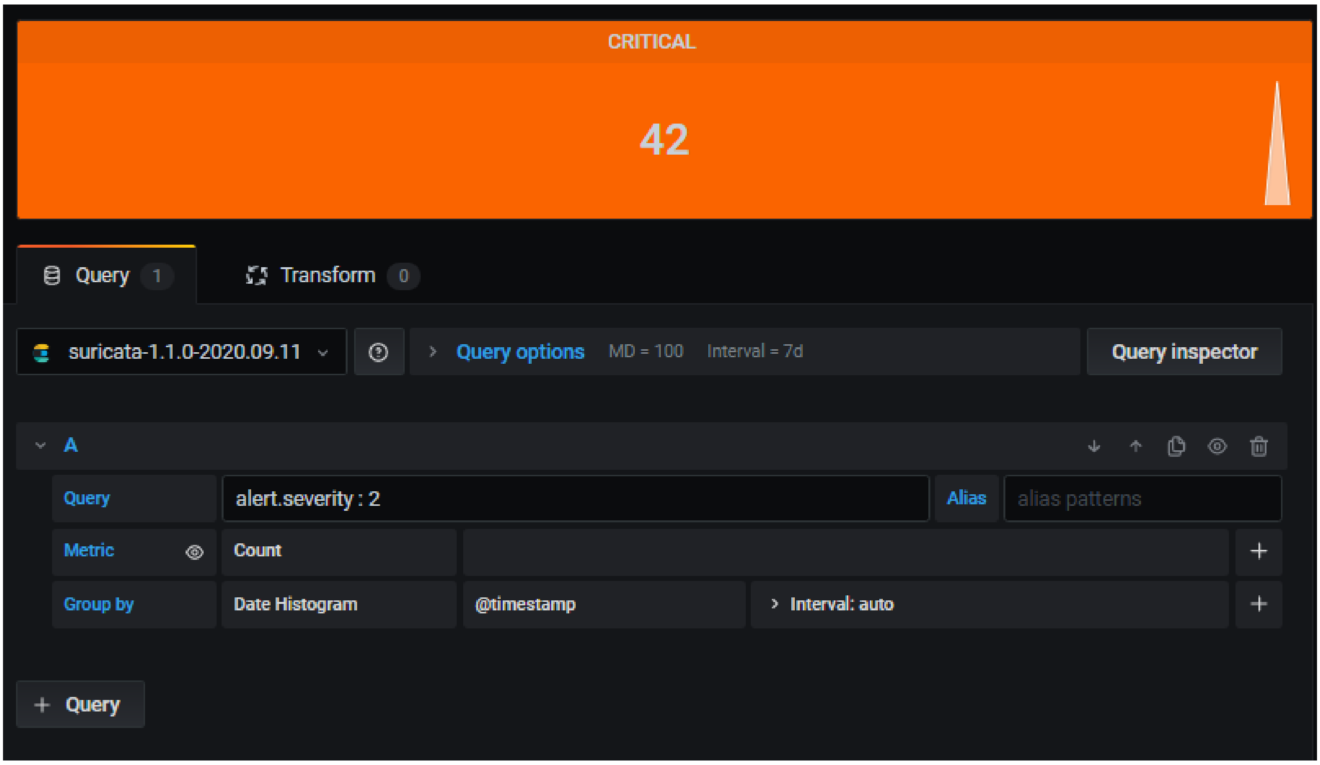
Format as Table

Figure 3.11 Grafana PSQL Query for Alerts

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.6.6 Elasticsearch

Elasticsearch is a search engine which provides a distributed, multitenant-capable full-text search engine with a HTTP web interface and schema-free JSON documents. It is very useful for time-series data.



CRITICAL

42

suricata-1.1.0-2020.09.11

Query options MD = 100 Interval = 7d

A

Query: alert.severity : 2

Alias: alias patterns

Metric: Count

Group by: Date Histogram @timestamp Interval: auto

Figure 3.12 Elasticsearch Query for Critical Alerts DTM

3.6.7 Kafka

Kafka[3] is an open-source tool that handles real-time data feed, fulfilling three key functionalities:

- To publish (write) and subscribe to (read) streams of events
- To store streams of events durably and reliably for as long as you want.
- To process streams of events as they occur or retrospectively. [3]

Kafka It is very helpful for the ID component for it supports the management of the data transmitted in a JSON format from the SPHINX components.

3.6.8 KSQL

KSQL [4] is an event streaming database purpose-built to help create stream processing applications on top of Apache Kafka. Regarding the alert capturing, Grafana plug-in is a very helpful tool for creating a union between all the alerts of the components.

3.6.9 Logstash

Logstash is a free and open server-side data-processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to Elasticsearch, making data available for Grafana.

3.6.10 Single Sign-On

ID, in collaboration with the Service Manager component, will implement the authentication and authorization service, allowing users of the healthcare organisation's IT staff to access all components without the need to re-enter credentials for each one. In this way, the use of the SPHINX system will be more easily accessible.

3.7 Interactive Dashboards in SPHINX

ID component supports the operation of the majority of the other components in the SPHINX ecosystem. The relationships between ID and the other SPHINX components are represented in the following image:

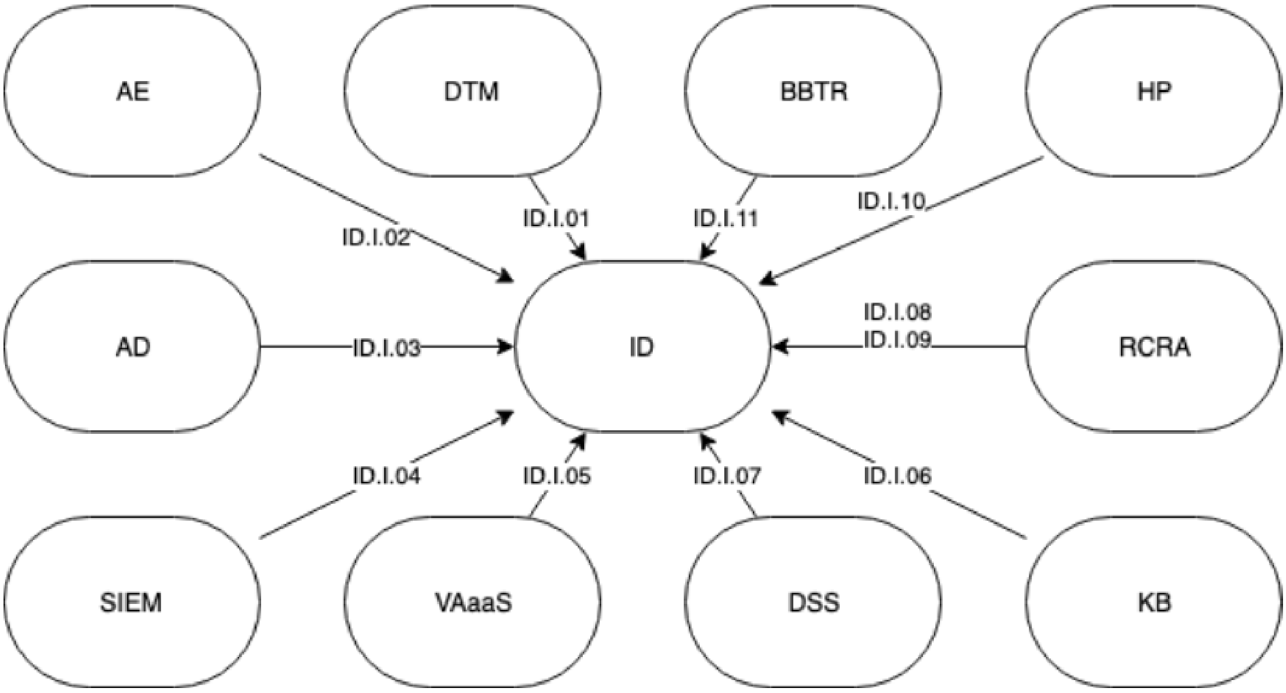


Figure 3.13 SPHINX ID Collaboration Diagram

The ID is related to ten components, each with its own interfaces, having the following rules:

- ID receives traffic data from Data Traffic Monitoring to display a highly user-friendly and interactive way relevant traffic data. The users can visualise and interact with traffic statistics (graphics) and notifications and alerts about suspicious traffic data.

- ID receives cyber threats and attacks data in JSON files from Analytic Engine to display a highly user-friendly and interactive way relevant cyber threats and attacks. The users will see them and act upon statistics (graphics) and notifications and alerts about cyber threats and attacks.

- ID receives detected anomalous system and user behaviour data in JSON files from Anomaly Detection to display in a highly user-friendly and interactive way relevant data on detected anomalies provided by the AD component. The users are able to visualise in order to mitigate any problems based on statistics (graphics) and notifications and alerts about the detected anomalous system and user behaviours.

- ID receives detected security information and events data from Security Information and Event Management to display in a highly user-friendly and interactive way relevant data on security information and events provided by the SIEM component. The users can visualise and act upon statistics (graphics) and notifications and alerts about registered security information and events.

- ID receives vulnerability assessment reports from Vulnerability Assessment as a Service to be displayed in a highly user-friendly and interactive way.
- ID receives overall cybersecurity information from Knowledge Base to display graphics about IT's infrastructure's overall cybersecurity information history, status and forecast provided.
- ID receives suggested decisions and proposed courses of action and their consequences from Decision Support System to display in a highly user-friendly and interactive way the suggested decisions and proposed courses of action and their associated consequences (impact) provided by the Decision Support System component. The users could visualise and act based on the suggested decisions and proposed courses of action (including decisional graphics).
- ID receives a list of cybersecurity risks from Real-time Cyber Risk Assessment to display in a highly user-friendly and interactive way relevant information about the system's security risk level (list of risks, including indices and consequences) provided by the RCRA component.
- ID receives warnings and alert notifications on forecasted from Real-time Cyber Risk Assessment to display in a highly user-friendly and interactive way relevant warnings and alerts on forecasted risks provided by the RCRA component.
- ID receives a list of detected cyber-attacks from Honeypot to display in a highly user-friendly and interactive way detected cyber-attacks provided by the HP component.
- ID receives a list of new cyber threats to display in a highly user-friendly and interactive way new cyber threats provided by the Blockchain Based Threats Registry component.

4 Summary and Conclusions

This deliverable presented the current status of the development of the SPHINX Interactive Dashboard component. ID displays data from other SPHINX components interactively for the user. The selected tools that were used to build this component were described in the chapters 2 and 3.

This deliverable covers the first iteration of development for the ID component. The work on ID will continue during the second and final iteration. Lessons learned during the pilots and integration testing will be included in the development effort for the 2nd iteration.

5 References

[1] Grafana – The Analytics Platform https://grafana.com/grafana/

[2] Grafana – Best practices https://grafana.com/docs/grafana/latest/best-practices/

[3] Kafka – Event Streaming Platform https://kafka.apache.org/intro#intro_platform

[4] KSQL – Event Streaming Database https://ksqldb.io/

[5] Dashboard Design: best practices and examples - https://www.justinmind.com/blog/dashboard-design-best-practices-ux-ui/

[6] F-Shaped Pattern of Reading on the Web: Misunderstood, But Still Relevant (Even on Mobile) - https://www.nngroup.com/articles/f-shaped-pattern-reading-web-content/

[7] What Do We Talk About When We Talk About Dashboards? - https://research.tableau.com/sites/default/files/Dash-boardsConspiracy_final.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.