University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Postgraduate Program of Studies
MSc Digital Systems Security

Master Thesis

Analysis on Security Orchestration Automation and Response (SOAR) platforms for Security Operation Centers

Supervisor Professor: Dr. Christos Xenakis

Name-Surname	E-mail	Student ID.
Dimitrios Lalos	dlalos681@gmail.com	MTE2016

Piraeus
4/8/2022

Περίληψη

Στη σημερινή εποχή, κυβερνήσεις και οργανισμοί στηρίζονται όλο και περισσότερο σε ψηφιακά περιβάλλοντα για την παροχή των υπηρεσιών τους. Ως αποτέλεσμα, εγκληματικές δραστηριότητες , οι οποίες παραδοσιακά στόχευαν σε αυτές τα υπηρεσίες, έχουν εμπλακεί σε έναν κυβερνοπόλεμο μεγάλης κλίμακας. Για την μείωση αυτών των απειλών, ο δημόσιος και ιδιωτικός τομέας, χρησιμοποιούν τα Κέντρα Επιχειρήσεων Ασφαλείας, μέρη όπου οι αναλυτές αποκρίνονται ενεργητικά στις απειλές, παρέχοντας ένα μηχανισμό άμυνας προς τους κακόβουλους δρώντες. Ένα εξειδικευμένο μέτρο που χρησιμοποιείται από τα Κέντρα Επιχειρήσεων είναι η χρήση λογισμικού Ασφάλειας Ενορχήστρωσης Αυτοματοποίησης και Απόκρισης. Αυτό το λογισμικό παρέχει στον αναλυτή ενισχυμένες δυνατότητες αυτοματισμού, ώστε να επιτηρούν τους ψηφιακούς τους πόρους και να αποκρίνονται αποτελεσματικά στις κυβερνοαπειλές. Στόχος της παρούσας εργασίας είναι η ανάλυση και η επίδειξη του λογισμικού, των δυνατοτήτων, καθώς και τι παρέχει στους σύγχρονους αναλυτές.

Λέξεις Κλειδιά: κυβερνοαπειλές, μείωση, λογισμικό, αυτοματισμός, απόκριση, ασφάλεια

Abstract

Nowadays, governments and organizations rely more and more on digital environments in order to provide their services. As a result, criminal activities that traditionally targeted those services have engaged in a large scale cyberwar. In order to mitigate those threats, public and private sectors use Security Operation Centers, places where analysts actively respond to threats, providing a defence mechanism to those malicious actors. An advanced measure used in modern SOCs is Security Orchestration Automation and Response software. This software provides the analysts with enhanced automation capabilities in order to monitor their digital assets and effectively respond to cyber threats. The aim of this master thesis is to analyze and demonstrate this software, its abilities, as well as what its provisions to modern analysts.

Key Words: cyberthreats, mitigation, software, automation, response, security

Table of Figures

Table of Content

Chapter 1: Introduction

The rapid increase in cyber-attacks in recent years has given the right to claim that modern days are defined by a continuous digital warfare. Comprehensive adoption of digital solutions from the governments worldwide have made critical services like healthcare or defence, susceptible to malicious actors that try to disrupt services continuity and even question a state's digital sovereignty. On January 26, 2022, the President of the United States, Joe Biden, issued a memorandum which sought to improve U.S. cybersecurity capabilities. More specifically, all U.S. Government agencies require to move towards zero trust cybersecurity principles.[1] Those principles can be implemented through the S.O.A.R. technology.

S.O.A.R. stands for Security Orchestration Automation and Response. The reason for the necessity of such a software is that it provides the only feasible way for the Security Operations Centers worldwide to handle the large volume of security alerts, as well as integrate all the tools in order to operate effectively.

The aim of this Master Thesis is to examine different S.O.A.R. solutions and present their impact in Security Operations Centers. In the second chapter, a theoretical background will be presented, examining two different approaches that define SOC functionality, the SIEM – centric approach and the insertion of the S.O.A.R. platform. In chapter 3, an overview of the work already conducted upon the S.O.A.R. solution will be presented and analyzed.

In the fourth and fifth chapters the requirements of the thesis will be defined, and a high level and detailed design will be provided in order to set up the context for the examination and demonstration of the presented solutions.

In chapter 6, the solutions will be presented. Every software will be presented in specific categories, such as architecture, data enrichment, correlation and forensic analysis, data visualization and playbooks and automation. Those topics will present the base, for the demonstration part in the next chapters.

[1] Executive Office of the President – Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, available at: https://whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

In chapter 7, an initial analysis of the demonstration scenarios will be presented. The platforms were tested in engaging in potential and realistic threats that can occur in a corporate or organizational environment.

In chapter 8, the demonstration of the use cases will be presented. The results of the use case scenarios will be presented in Conclusions.

Chapter 2: Theoretical Background

Section 1: SIEM – centric approach to SOC engagements

Nowadays, cyberattacks have become a more and more common threat to organizations. From national critical infrastructure to enterprise critical assets, malicious actors try to find and exploit new vulnerabilities, extending the attack surface in order to achieve their goals. To efficiently defend from those threats, enterprises and state actors have heavily relied upon Security Operation Centers.

A Security Operation Center (SOC) provides monitoring, detection and response capabilities to analysts, creating layers of defence that protect all critical assets of an organization. Therefore, a SOC can be defined as a centralized cyber security structure, that can implement a number of defensive security functions, such as monitoring, detection, response, threat analysis, threat management, digital forensics and more. Those functions are performed with the use of software and/or hardware, dedicated to produce logs that describe potential security events or incidents. Those are the data sources and are important for the analysts in order to perform the necessary correlation and respond to potential threats. A software that is used to help the analysts perform their tasks is a Security Information and Event Management platform, or a SIEM.

A SIEM is a platform that communicates with all the data sources in a SOC. It then provides the investigator with a comprehensive User Interface that consists of multiple dashboards containing the information from those data sources. The analyst uses those information to build his or her cases of potential breaches. There are many SIEM solutions available, not only as enterprise editions, but also as community or open source, mitigating the cost for small to medium businesses.

Even though a SIEM made the security analysts work more efficiently, it was not implemented by all SOCs. Some believed that endpoint and network protection could be implemented efficiently without centralized management. The exponential increase in cyberattacks in recent years proved that this solution was ineffective. More and more organizations started to rely on centralized security management, making the SIEM a necessary acquisition of all modern SOCs. This approach made the SIEM a critical component for security operations and security analysts used it extensively to address new threats.

For some years, the SIEM – centric approach has been effective and is still being utilized by many security organizations. However, due to the volatility of cyber

operations and the evolution of cyberattacks, the implementation of this approach started becoming problematic.

Section 2: The need of automation - definition of SOAR

In recent years, security analysts and investigators find it more and more difficult to effectively engage with the new emerging threats. The use of a SIEM in modern SOCs, even though it is considered a reliable mitigation measure, has become problematic. The difficulty in integrating new monitoring solutions to existing SIEM technologies in order to become effective is one of the reasons behind the issue. The other important reason is the large volume of alerts created per day in the Security Operation Center. According to a survey published in 2020, security alerts have increased at least substantially (twice as many alerts) at 70% in the last five years. This has contributed to significant increase of the fatigue levels of security teams, deeming them in many cases ineffective to deal with the increased number of threats. It is also important to mention that almost 88% of the analysts have reported that they face challenges with their SIEM solutions. The most important issue reported was again the high number of alerts. Here it must be clarified that a security alert in a Security Operations Center does not always involve a critical issue. In many situations it involves a false positive alert, that must be identified and ignored by the analysts. But an analyst must have the required experience and competence in order to perform effective identification of such false positives, something that becomes even more difficult with the existing volume of alerts.

A solution that has been proposed and utilized on many occasions is that of automation. By utilizing automation in security investigations and proposing mitigation measures based on the automation of the procedures can drastically reduce response time from the analysts, making them more effective. The name of the software that has been introduced for this purpose is S.O.A.R. (Security Orchestration Automation and Response).

A S.O.A.R. can be defined as a collection of software solutions and tools that provide the capability to security organizations to streamline security operations in

three key areas of a SOC. More specifically, threat and vulnerability management, incident response and security operations automation.[2]

Providing a more thorough explanation, Security Orchestration is the solution to the problem of integration of new security tools and disparate security systems. It is considered as the connected layer that streamlines security processes and powers security automation. Security Automation is the automated handling of different tasks related to security operations. Automation involves not only defence oriented tasks, like vulnerability scanning and log – searching but also tasks related to prevention, as it will be analyzed in the following chapters. Finally, Security Response is the ability provided by the software, for the analyst to choose among a set of potential automated responses, in order to effectively counter an existing threat.

The use of a S.O.A.R software provides the analysts the opportunity to focus on responding to real threats for the organization and not get distracted by repetitive tasks that can now by integrated and automated.

[2] "What is a SOAR?", by Rapid7, available at: https://www.rapid7.com/solutions/security-orchestration-and-automation

Chapter 3: Related Work

The term security orchestration was firstly introduced by Gartner in 2017 in order to describe the functions performed by the newly developed software to engage incident response, security automation, case management and also other integrations. More specifically, Gartner defined S.O.A.R. as technologies that enable organizations to collect data from various sources, where incident analysis and triage can be performed in order to leverage a combination of human – machine power in order to help define, prioritize and drive standardized incident response activities.[3]

The next one who mentioned the evolution and maturing of S.O.A.R. platforms was Jon Oltsik, mentioning the rapid adoption of S.O.A.R. solutions of many security vendors over the past few years. [4] It is also important to mention his reference regarding S.O.A.R. as an analyst – centric security operations technology.[5] His analysis provided the new context regarding security operations, a context that remains even today. He described how the security operations moved from a SIEM – centric and in general, a more software – centric approach, to an analyst – centric one. Even though many have argued that S.O.A.R. technologies will lead to the automation of the tier I tasks in a SOC, leading to eventually less analysts being employed, Oltsik argues that S.O.A.R. technologies will empower and evolve level 1 analysts, offering new weapons to counter evolving threats. Some of those weapons involve noise cancelling assistance providing a scaling solution and acting as a proxy for the analyst, integrated data that can be viewed by only one console, canned models and routines with highly customizable templates and also continuous learning and sharing being able over time to recognize patterns of an attack and suggest tasks and processes that were most effective in the past. As a result, a S.O.A.R. platform can become more accessible and friendly to inexperienced analysts and can help evolve experienced analysts' capabilities.

---

[3] "Security Orchestration, Automation and Response (SOAR)", Gartner, 2017, available at: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

[4] Jon Oltsik, "The evolution of security operations, automation and orchestration, CSO, 2018, available at: https://www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html

[5] Jon Oltsik, "The rise of analyst-centric security operations technologies", CSO, 2018, available at: https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html

Chapter 4: Definition of Requirements

In this master thesis an analysis of different S.O.A.R. solutions will be presented. The aim of the analysis is to present the plethora of features of a Security Orchestration Automation and Response software that give modern analysts and investigators more tools to counter existing and emerging threats in cyberspace. The solutions that will be analyzed will contain software that has a community edition, freely available to users. The software will operate in virtualize environments. The categories that will be presented are architecture, data enrichment, correlation and forensic analysis, data visualization and playbooks and automation.

After the analysis and presentation of the platforms, a demonstration of each solution will be conducted. The aim of the demonstration is to present how those solutions respond to realistic everyday threats. Every platform will be used in different attack simulation scenarios. Those scenarios are needed in order to present a realistic view of SOAR software in modern operations. The results form the presentation and demonstration will be presented in Conclusions.

Chapter 5: High Level and Detailed Design

For each of the three solutions presented, different design patterns were followed. The biggest challenge in the implementation is the scalability problem, as the solutions were presented in a virtual environment, as it was described in the requirements.

For the Cortex XSOAR, the solution, along with its different components was implemented in a hybrid environment, containing containerized applications and a virtual machine. In order to implement the solution, firstly a VM was used with an Ubuntu Linux Distribution. Above the virtualized Linux kernel, the Docker-host application was installed. Containerized environment is not a resource – exhaustive solution and many containers can be implemented in isolation in the same Docker-host. Each Docker container used the resources provided to the host (the resources provided to the Linux VM).

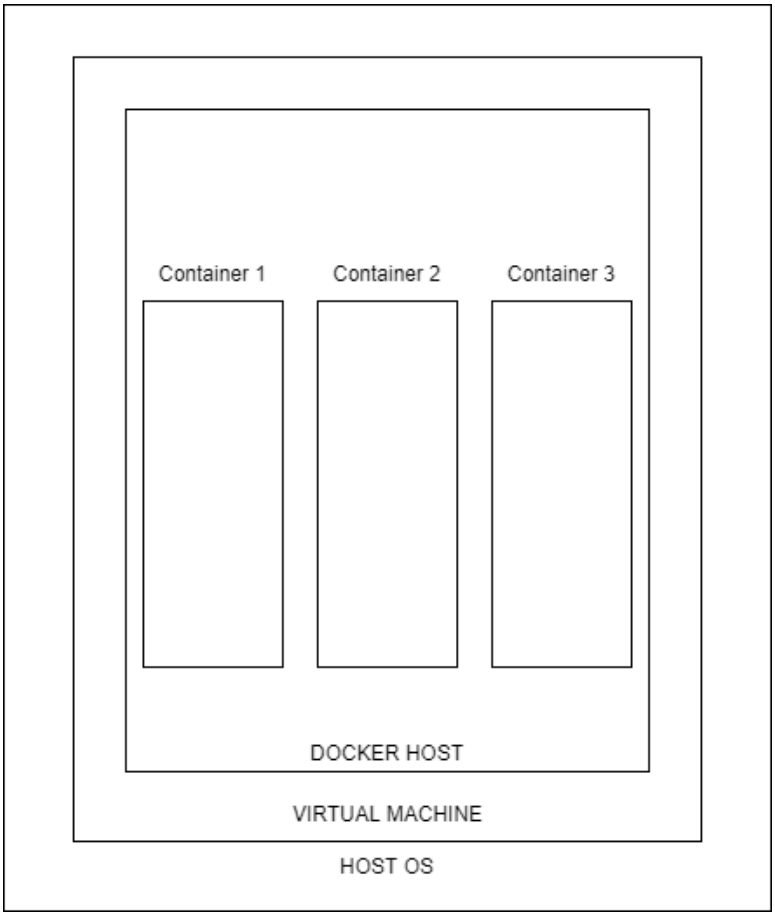


Figure 1: Virtualization Architecture

Every container operated in isolation and was connected with the other containers via a bridged network that is implemented by default in the Docker-host.

Splunk SOAR was utilized solely by virtualization software. A virtual machine was created (using Virtual Box) and the S.O.A.R. platform was installed on this virtual machine.

For the implementation of Siemplify SOAR a third approach was used. The software was utilized in a cloud environment, as its new editions are integrated with Google Cloud. The implementation of the S.O.A.R. software in different environments provided useful insight about the efficiency of each implementation and how to best address the big problem of scalability.

Chapter 6: Development

Section 1: Palo Alto XSOAR

Architecture

The first SOC scenario was created with the implementation of Cortex XSOAR, a solution provided by Palo Alto. XSOAR is available as a community edition with a limitation in available automations that can be implemented per day. However, it is considered efficient for testing and evaluation purposes. XSOAR stands for Extended Security Orchestration Automation and Response. It provides the functionality of a S.O.A.R. platform integrated with threat intel management. This involves parsing, management and act on threat intelligence, a comprehensive threat feed aggregation and also intelligence sharing and response.

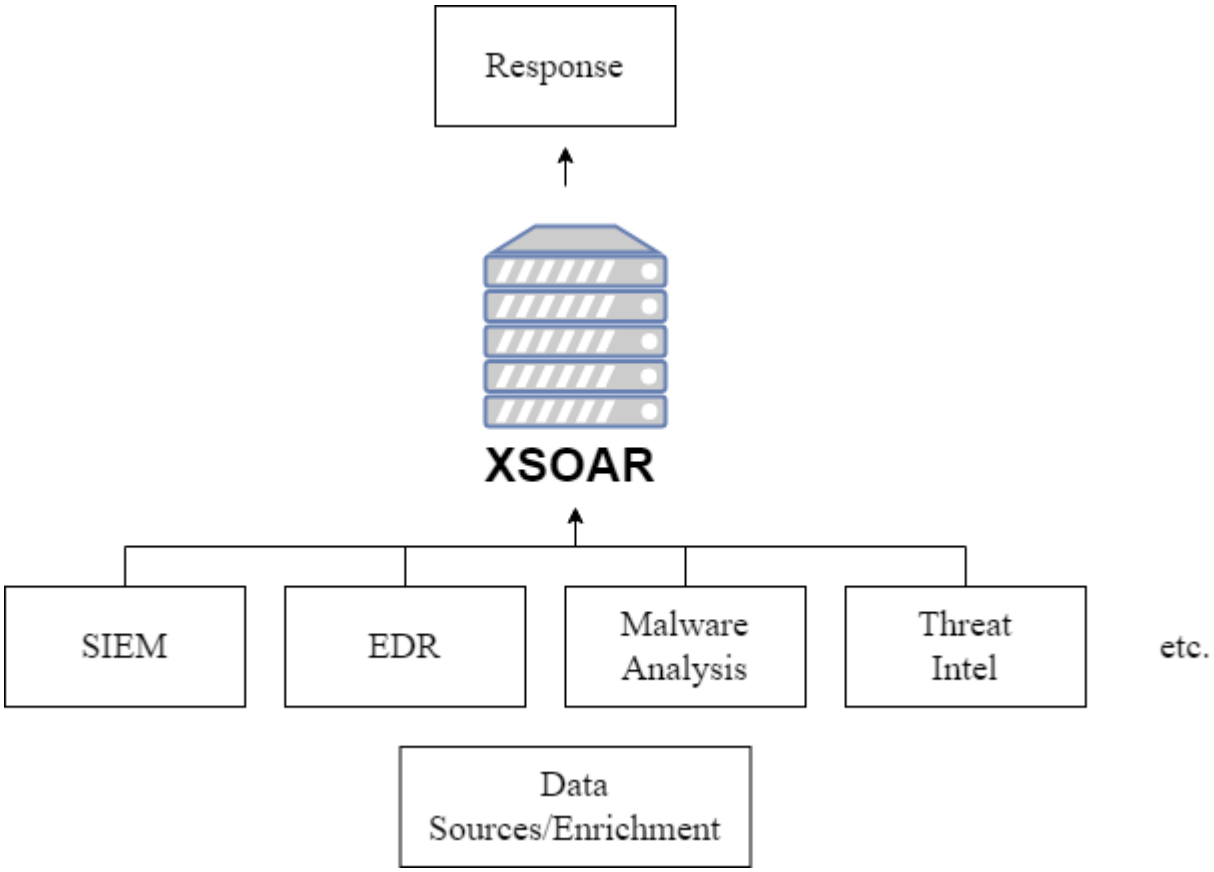


Figure 2: XSOAR Architecture

For the scenario, an analytics engine, Elasticsearch, was also implemented. By leveraging its indexing capabilities, the XSOAR can perform more efficient threat hunting. Elasticsearch was utilized above a Beat agent, which was used as a source of alerts, providing data enrichment. The analyst is able to visualize those alerts in XSOAR's war room , something that will be further analyzed in a later chapter. Even

though, Kibana can also be implemented as an extra visualization solution, in the scenario the visualization was provided merely from XSOAR platform.

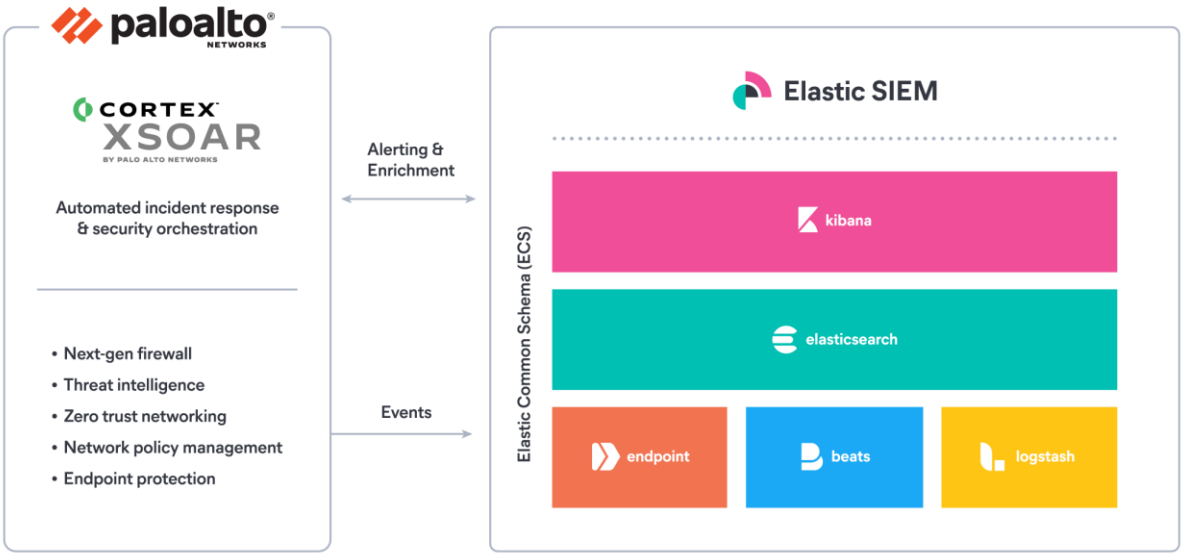


Figure 3: Elasticsearch integration with Cortex XSOAR[6]

Apart from Elasticsearch, Cortex XSOAR has been enriched with other data sources that provide threat intelligence, becoming extremely important for investigations and collection of evidence. Along with Elasticsearch, the following data enrichments have been implemented.

- Malware Bazaar
- Mitre Att&ack
- OpenPhish
- urlscan.io
- VirusTotal
- who.is
- GreyNoise
- IPinfo v2
- Filebeat with Snort IDS were also connected to Elasticsearch.

[6] *Elasticsearch integration with Cortex XSOAR,* available at: https://www.elastic.co/partners/palo-alto-networks/

Malware Bazaar

It is a project provided by abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.[7] It provides an extended database with new malware samples that is constantly being updated.

Mitre Att&ack

It is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.[8]

OpenPhish

A freely available project, containing Phishing Intelligence in the form of a continuously updated database. In addition, the database contains metadata that can be used for detecting and analyzing cyber incidents, searching for patterns and trends, or act as a training or validation dataset for AI applications.[9]

urlscan.io

As its name suggests, it is a free service to scan and analyze websites. When a URL is submitted to urlscan.io, an automated process will browse to the URL like a regular user and record the activity that this page navigation creates.[10]

VirusTotal

It is a well-known tool, with a community edition, that searches IPs, URLs or files, for malicious content. In order to perform its analysis, it uses a wide list of antivirus software with comprehensive details upon its results. [11]

who.is

It is a similar tool to VirusTotal, that conducts analysis to given IPs, domain names or websites.[12]

GreyNoise

A tool that collects, analyzes and labels data on IPs that scan and attack the entire internet, saturating security tools with noise. It helps analysts waste less time on

[7] More information available at: https://bazaar.abuse.ch/
[8] More information available at: https://attack.mitre.org/
[9] More information available at: https://openphish.com/phishing_database.html
[10] More information available at: https://urlscan.io/about/
[11] More information available at: https://www.virustotal.com/gui/home/upload
[12] More information available at: https://who.is/

irrelevant or harmless activity, and spend more time focused on targeted and emerging threats.[13]

IPinfo v2

A tool used to provide data about IP addresses, like geolocation data, VPN detection, hosted domains API, mobile carrier device, etc.

Snort IDS

It is considered a comprehensive Network Intrusion Detection System and it can also be used as an Intrusion Prevention System (IPS). It has extensive monitoring capabilities over the target network. [14]

[13] More information available at: https://www.greynoise.io/
[14] More Information available at: https://snort.org/

Data Enrichment

The procedure of alerting takes place in XSOAR through the creation of instances. An instance is an instantiation of an enrichment data source. Through instances, XSOAR receives the input for further analysis. In the scenario to be examined, four containers were created in Docker environment , in order to implement the different technologies used to support XSOAR. From all the data sources, Elasticsearch was the one that was implemented separately , as well as an Ubuntu container that will host the Snort IDS. All the other data sources were available through the web, so their instances needed to be created only in the XSOAR environment. The instructions for the implementation of the following architecture can be found in elasticsearch official documentation.[15]

```
root@soar:/home/user/Desktop# docker ps
CONTAINER ID   IMAGE                                                  COMMAND
           NAMES
a11151c89b0a   docker.elastic.co/elasticsearch/elasticsearch:7.17.0   "/bin/tini -- /usr/l…"
>9300/tcp   elasticsearch
4ac36a2abf33   demisto/python3:3.9.7.24076                            "python /tmp/pyrunne…"
           demistoserver_pyexec-9328d2e5-d4c5-4320-818a-9c8d200384a6-demistopython33.9.7.24076
f19114bc5b92   demisto/python:2.7.18.24398                            "python /tmp/pyrunne…"
           demistoserver_pyexec-35a51b80-8da3-4465-8294-6ed323ef1ed5-demistopython2.7.18.24398
fa1845214dec   ubuntu                                                 "bash"
           zealous_kapitsa
root@soar:/home/user/Desktop#
```

Figure 4: Container creation

As it is depicted, the containers hosting XSOAR and the two containers for supporting the platform were created. Afterwards the network configuration must be checked in order to adjust the IP addresses needed for the configuration of Filebeat and Elasticsearch server. The following was implemented by an inspection of the network created in Docker environment, the bridge network. Using the command:

- docker inspect bridge,

the addresses of all the containers are retrieved.

[15] The edition of the elasticsearch software, as well as instructions are available at: https://www.elastic.co/guide/en/elasticsearch/reference/7.17/docker.html

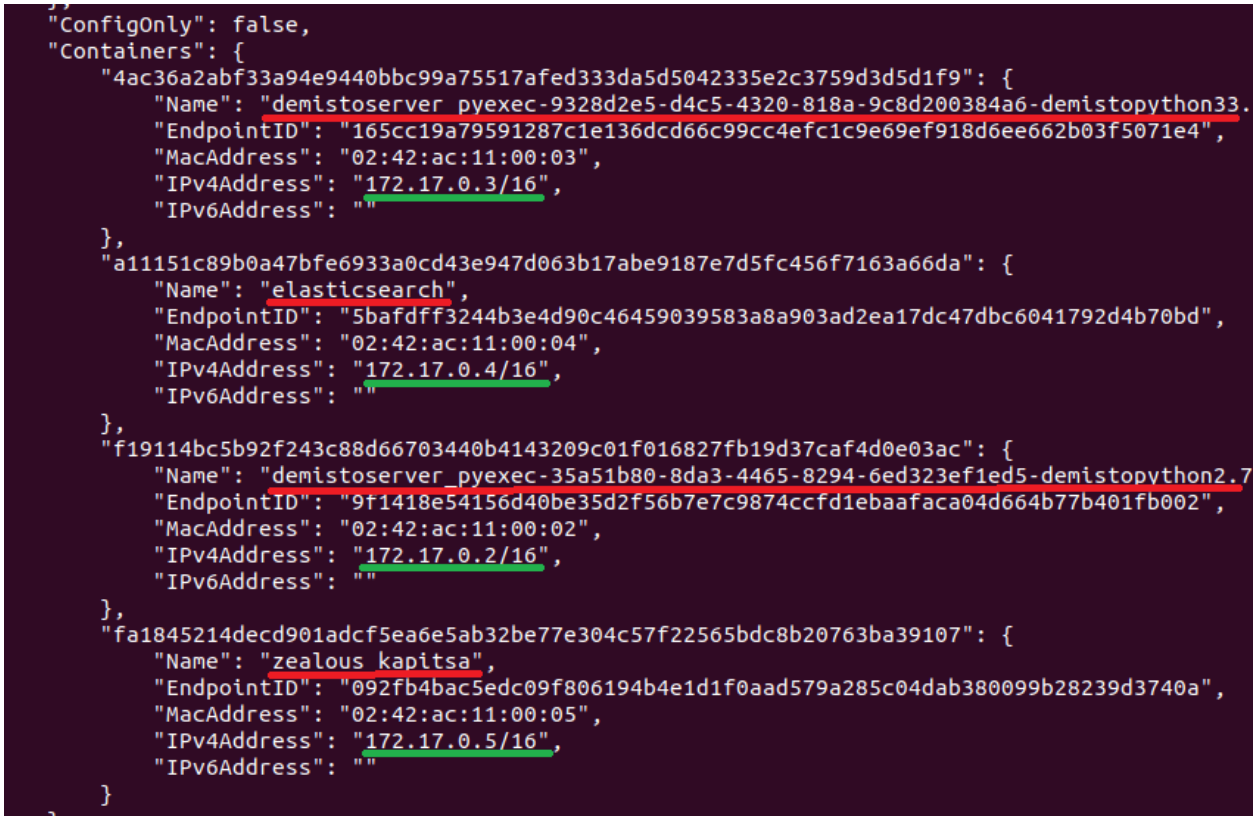
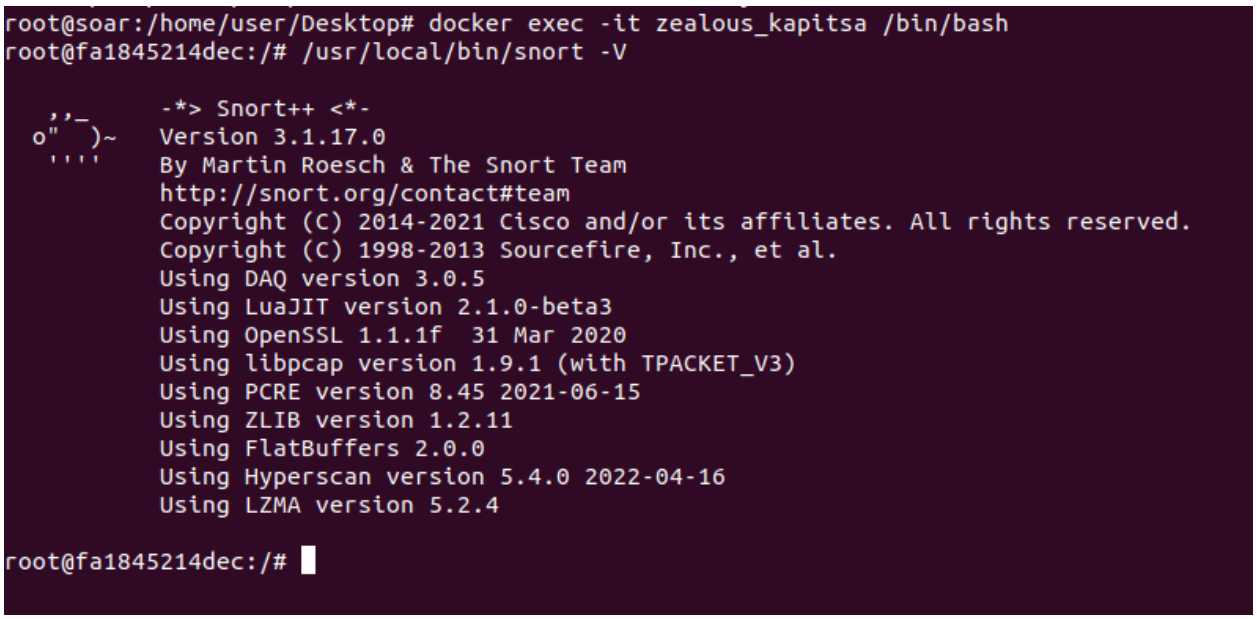


Figure 5: Network Inspection

In addition, in the Ubuntu container Filebeat and Snort IDS were installed.[16] As shown, the Snort version 3.1.17.0 was utilized.



[16] Filebeat installation, available at: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-installation-configuration.html and Snort installation, available at: https://snort.org/

Figure 6: Docker execution

In order for the Elasticsearch indexing to be activated, an Elasticsearch instance must be created in Cortex XSOAR. This can be achieved in the Integrations section of the platform. XSOAR supports a wide variety of ready to use integrations, as well as the capability for the user to create his or her own integrations.

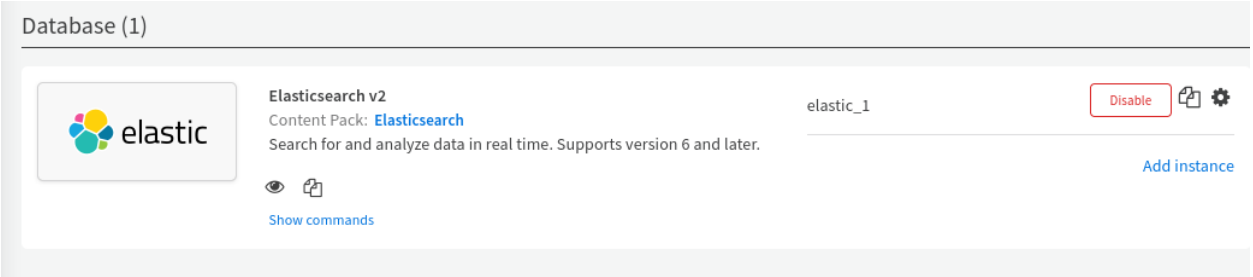


Figure 7: elastic instance created in XSOAR

With the same way, the other integrations were also achieved. In order to integrate a web based service, an API was retrieved and inserted to XSOAR to activate the integration. As an example, the VirusTotal integration, will be demonstrated.

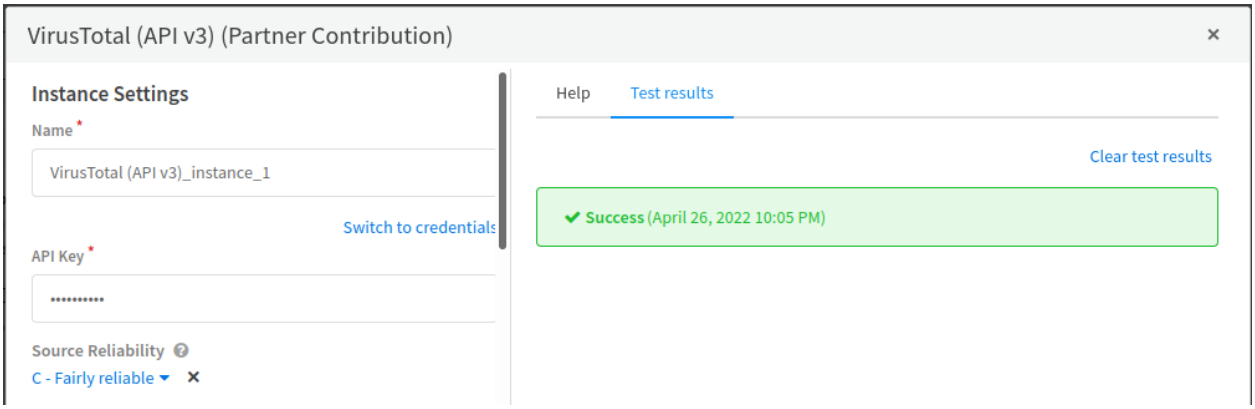


Figure 8: VirusTotal instance created in XSOAR

In instance settings, a Name for the integration is decided and then, the API key, provided by the vendor was inserted. After that, the user can test if the integration was successfully established between XSOAR and VirusTotal. With the same way, instances for all XSOAR integrations were created.

Correlation and Forensic Analysis

Through its integrations, XSOAR can be efficiently used to provide forensic analysis and threat hunting. Its integrations can be used unseparated, in an environment called War Room. In a War Room, cases can be assigned to analysts, and investigations can take place, in order to conduct further analysis to security incidents. A brief example will be presented, for a clearer picture in the above mentioned information.

Firstly, the analyst can use IPinfo v2, to extract information about a given IP address (for demonstration purposes, the address examined was not a malicious one. In the evaluation chapter, the platform reaction to realistic use cases will be examined).

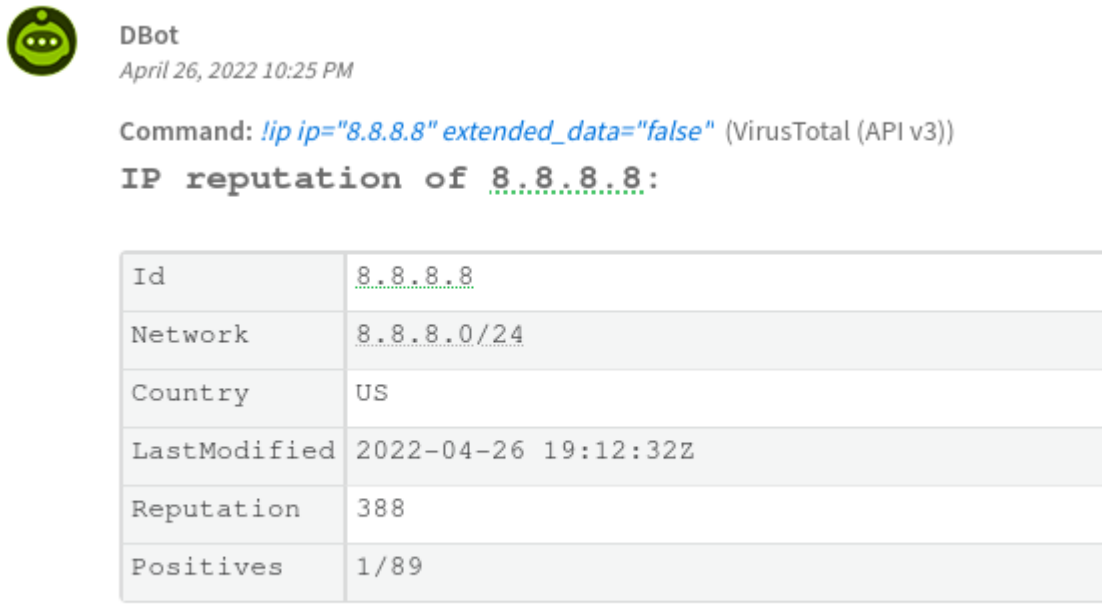


Figure 9: Start of an investigation on a given IP

As it is depicted, the initial command triggers the VirusTotal instance, providing some initial information. After the command (all the instances provide a set of commands that can be used in War Room during investigations), the first information about the IP is retrieved. As shown below, IPinfo provides Geo location information.

Command: *!ip ip="8.8.8.8"* (ipinfo_v2)

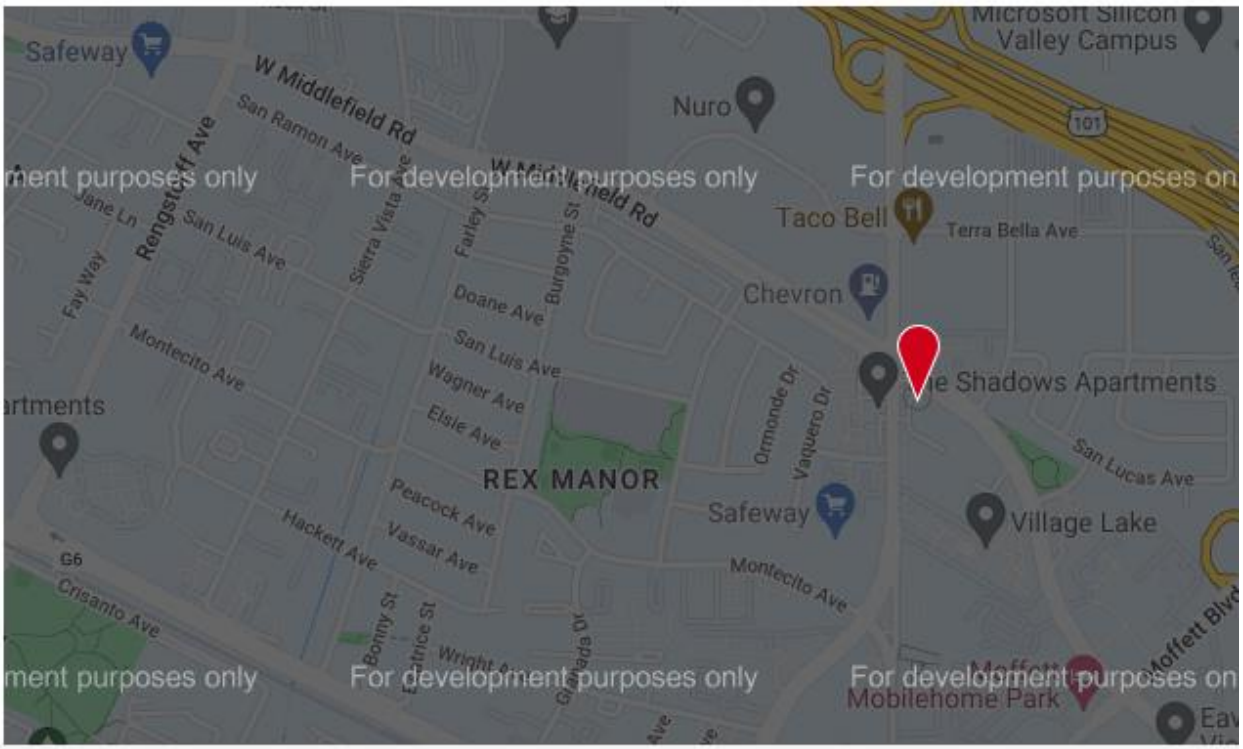


Figure 10: Geo-Location information on the Google Maps

anycast	true
city	Mountain View
country	US
hostname	dns.google
ip	8.8.8.8
lat	37.4056
lng	-122.0775
loc	37.4056,-122.0775
org	AS15169 Google LLC
postal	94043
readme	https://ipinfo.io/missingauth
region	California
timezone	America/Los_Angeles

Figure 11: Geo-Location information in text format

In the next phase, the GreyNoise instance automatically provides additional information about the target, with also indicators that can show if the target is suspicious or malicious.

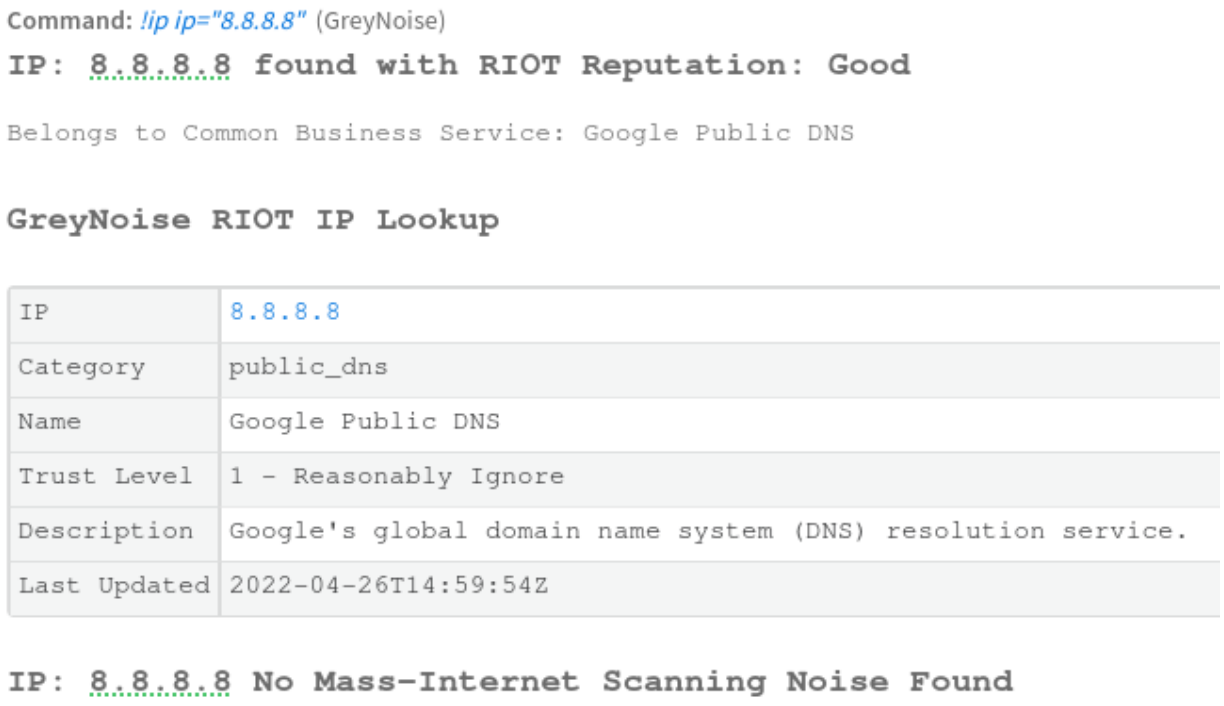


Figure 12: Reputation information about the target IP

The information provided by the platform, supports the investigation, giving the analyst extra insight and helping him reach a fact-based decision. XSOAR enhances the user's options by providing input from different data sources in one integrated environment.

Data Visualization

Dashboards are one of the most important aspects of a S.O.A.R. engine. It is crucial that an analyst receives coherent and comprehensive information about the current state of operations, as well as on demand intelligence about an ongoing security incident. Traditional SOCs used to have dashboards scattered in many monitors, making an analyst's job burdensome and demanding. A S.O.A.R. platform succeeds by integrating different sources of data, to provide a holistic view, in only one monitor, that is able to consist of all the dashboards needed by the investigator.

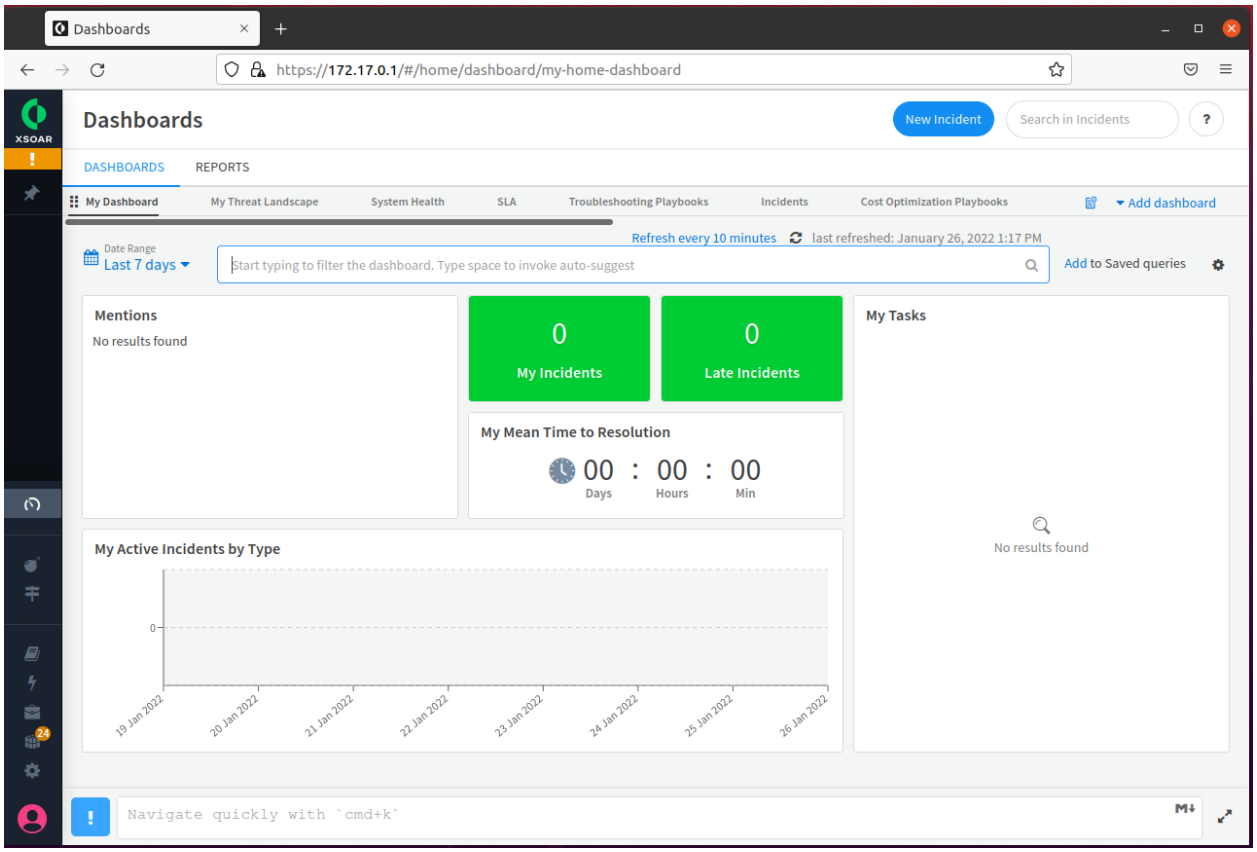


Figure 13: XSOAR Dashboards

In Cortex XSOAR, by installation, the following dashboard tabs are provided:

- Incidents, such as, their severity type, their assigned handler, active or unactive ones etc.
- System Health, which is an overview of the available resources in use (CPU, Disk Space, RAM) with colored indicators
- SLA, information about the requested Service Level Agreement (the level of detail presented in logs, according to the selected option).

There are also other tabs available (Threat Landscape, Troubleshooting Playbooks, Threat Intel Feeds, etc.) , according to the integrations that are enabled by the analyst.

An analyst can change the appearance of a dashboard, by choosing his or her color of choice for the categorization of security events (malicious, suspicious, benign, unknown) and also create a new dashboard with the information needed for a specific investigation. Another useful option is the ability for the analyst to share his or her dashboards with other peers that were also assigned in an investigation. [17]

[17] Dashboard overview, Cortex XSOAR administrator's Guide, available at: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-2/cortex-xsoar admin/dashboards/dashboard-overview

Playbooks and Automation

As it has been already stated, the S.O.A.R. platform relies on responding to security incidents through automation. Automation is utilized with playbooks, flowcharts that describe the actions that will be taken, in case of an incident.

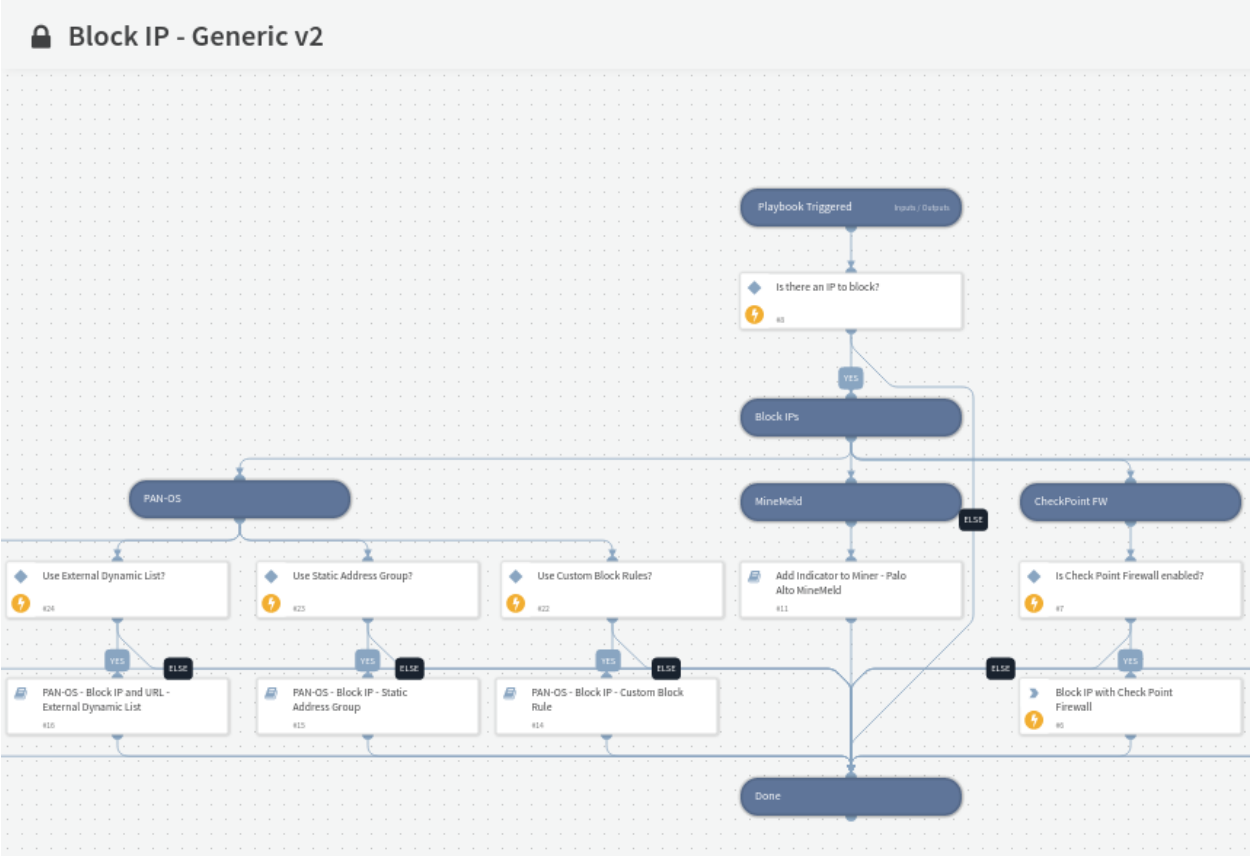


Figure 14: Utilization of a playbook

In the image above, a series of actions is presented, in case of traffic from a suspicious IP. The data enrichment that has already occurred, increases the credibility of the actions taken automatically by the platform. The person that authorizes the execution of a playbook is the security analyst who handles the security incident. Playbook executions are suggestions made by the XSOAR, upon intelligence gathered from different data sources. The correlation of data results in suggested actions.

A further look into the creation and implementation of a playbook, reveals that playbooks are created using scripts, like python scripts. The analyst can insert a new playbook and a new integration by writing directly in python. That way, XSOAR capabilities can be further extended as there is no limit to the number of integrations and automations that can be implemented.

Section 2: Splunk SOAR

Architecture

Splunk SOAR (formerly known as Phantom), has a unique architecture, relied in other Splunk security solutions, but also allowing interoperability with custom security tools, creating a system in which data is presented to the analyst real time, providing him extensive capabilities, in order to resolve potential issues and threats.

The uniqueness of Splunk SOAR architecture derives from the way the data are formatted and structured in order to create cases for the investigator involving potential incidents. The fundamental structure is the same as in other solutions. SOAR receives data from data enrichment sources and then, using automated playbooks, provides a solution to the analyst, reducing the complexity of operations.

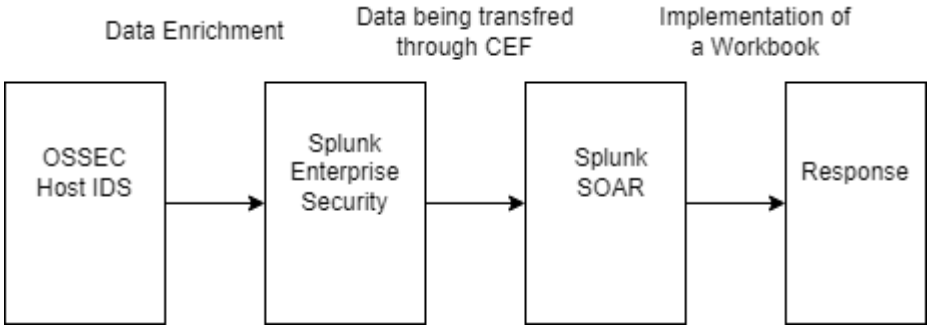


Figure 15: Splunk SOAR Architecture

Data enrichment sources are provided through solutions such as Intrusion Detection Systems , Firewalls, or SIEMs. In the use case examined, the data were created in a Host IDS, then parsed to a SIEM and finally were presented in the SOAR platform. In order to parse the data from the IDS, a format called Common Event Format (CEF) was utilized. This way the data were transferred in a structure to the SOAR. The CEF is a log management standard, improving the interoperability between different security solutions. In order to connect SOAR with the SIEM solution, integrations were created, called apps. Apps provide a connector to the SOAR, acting basically as in all the other similar solutions (integrations in XSOAR and also apps, in Shuffle). The events created in Splunk SOAR are defined as containers. A container can be a comprehensive case, assigned to an analyst. It is structured as a JSON, providing an overview of the information an analyst needs to proceed his or her investigation. It has different labels, that categorize it and consists of different artifacts. An artifact is also a JSON file

providing evidence, an investigator needs, to proceed to specific actions on a case. Potential actions an analyst can implement involve the execution of automations, called playbooks. A case may take data from different containers. Playbooks involved in the resolution of a case are described as a Workbook, which is a broader algorithm of steps the analyst has to execute, in order for the case to be closed.

In the following use case, a Splunk SOAR was implemented, using different data sources to provide the necessary enrichment. As a direct data source, the OSSEC Host Intrusion Detection System (HIDS) was configured along with a Splunk Enterprise Security solution. These solutions represent the assets of the Splunk SOAR. The data were then transferred to the platform in order to create containers and build a test case. Splunk SOAR has also some built-in functionality, involving apps with web APIs, like PhishTank, that can be utilized by default for investigations.

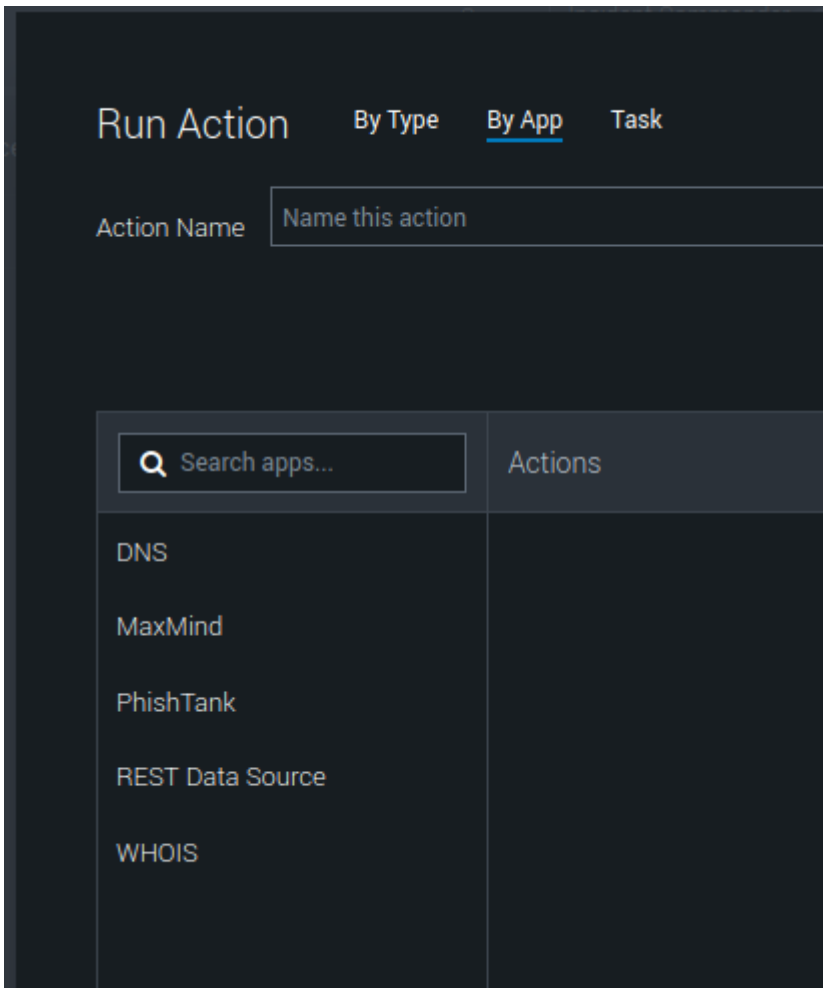


Figure 16: Built-in investigation apps in Splunk SOAR

Data Enrichment

Splunk SOAR data enrichment was utilized by the use of apps. An app is an integration that allows SOAR to use the data from direct sources. In the examined case, an OSSEC Host IDS was configured to transfer the data to a Splunk Enterprise Security solution, or Splunk SIEM. The data were then parsed to SOAR in the Common Event Format (CEF), through its created app.

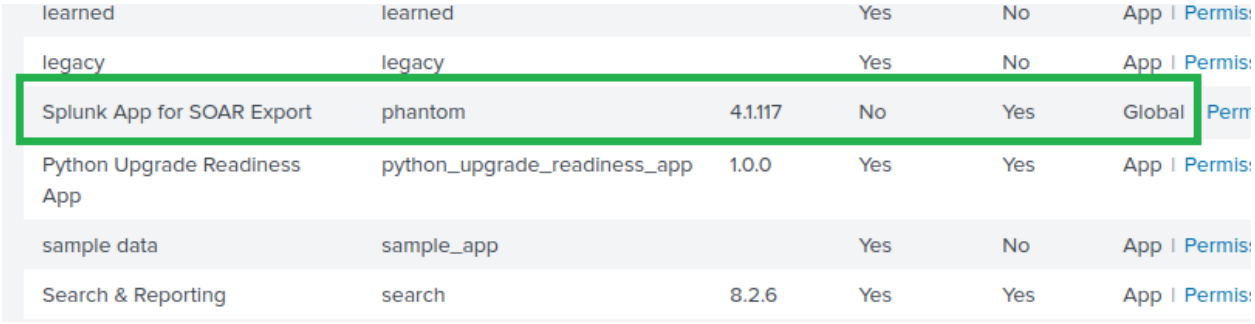


Figure 17: Data enrichment in Splunk SOAR. Part I

Splunk provides a ready to use app that is used for SIEM – SOAR integration . In order for the app to be implemented, SIEM recognized the SOAR platform as a virtual server to establish network connection.

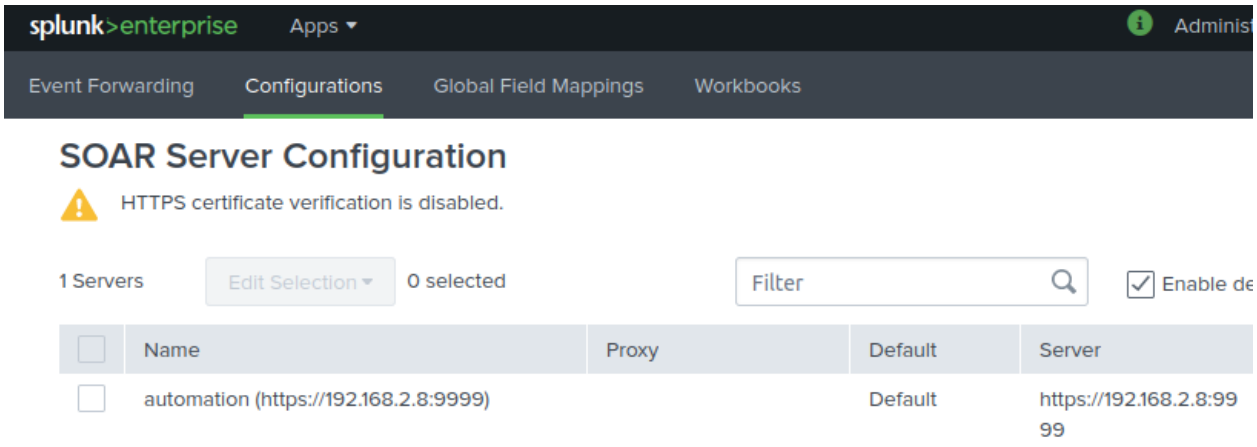


Figure 18: Data enrichment in Splunk SOAR. Part II

After the configuration succeeded, the data were visible in the SOAR platform. SOAR uses extensive dashboards to visualize the data and present the analyst with a comprehensive solution for his or her investigations.

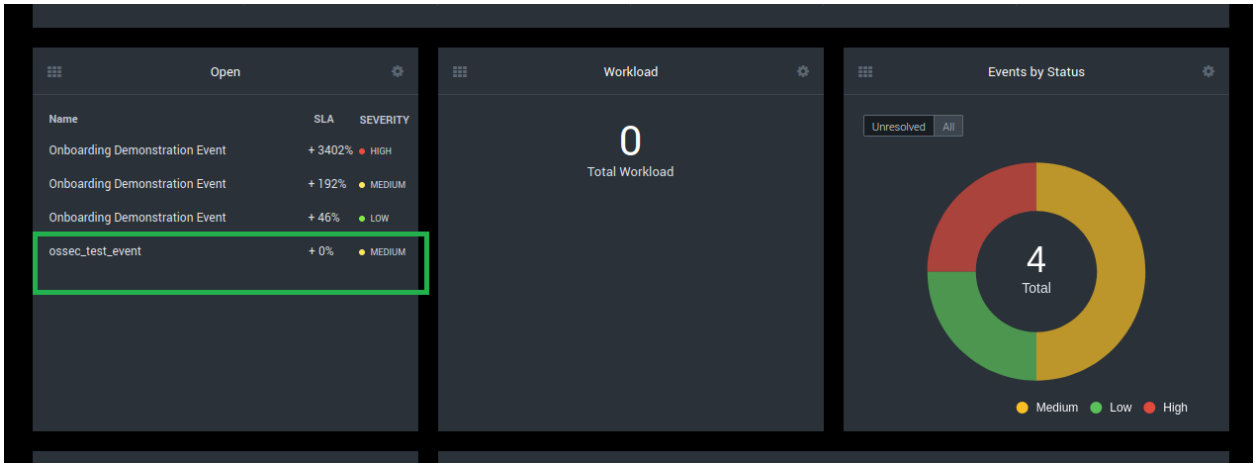


Figure 19: Data enrichment in Splunk SOAR. Part III

It is also important to mention the interoperability between the different solutions that successfully make security events available to Splunk SOAR for further investigation. From the SIEM solution the parameters can be set by the analyst, in order for the event to be instantly categorized by SOAR.

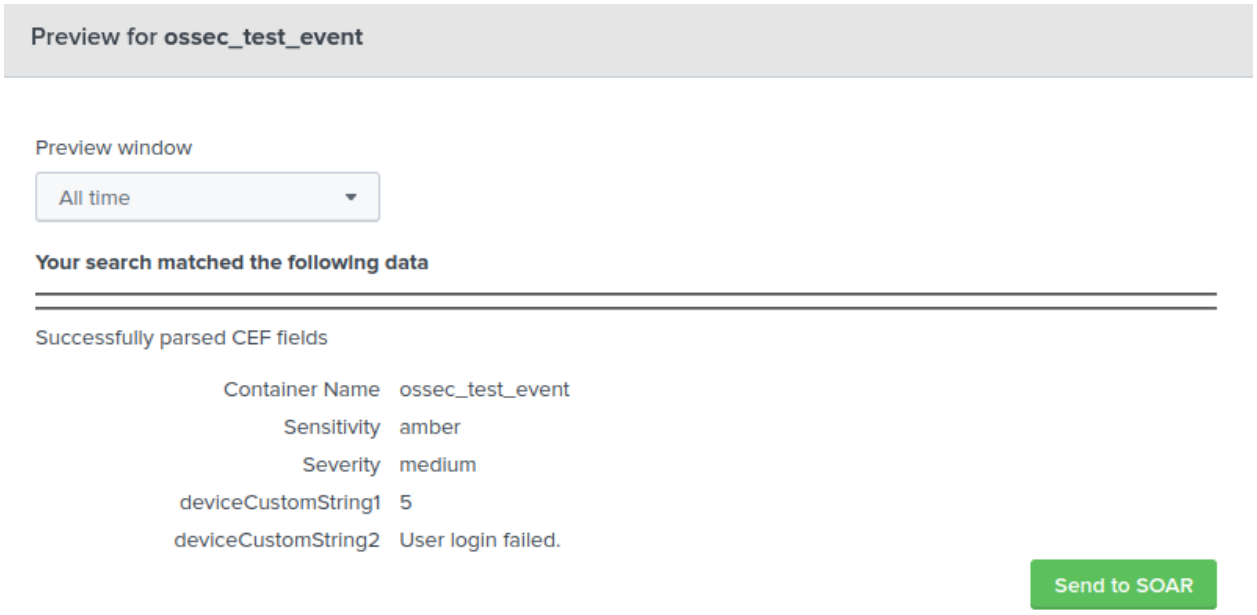


Figure 20: Preview of an event creation

Parameters like the sensitivity of the event, its severity and further description can be inserted to SOAR by the analyst, providing extra functionality in the SOAR platform.

Correlation and Forensic Analysis

As previously mentioned, Splunk SOAR provides a comprehensive investigation section and also tools in order for the analyst to implement effective response. Firstly, the administrator is able to assign the different security events to the analysts of his or her team.

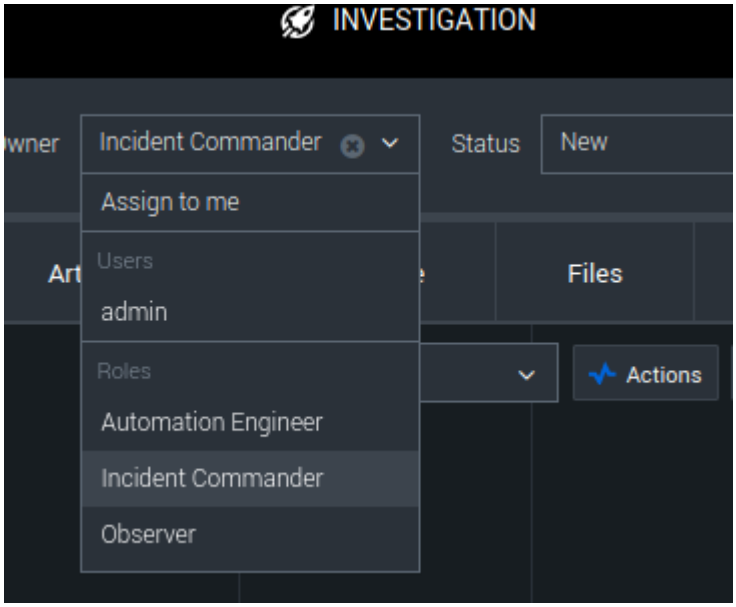


Figure 21: Investigation analysis

After event assignment, the analyst has access to a timeline that provides some initial information about the event. There is also the Artifact section, where the analyst derives more information about the events that built his case. The events are presented in CEF format from data sources, so the analyst is able to better correlate the data and conclude about the required form of action.

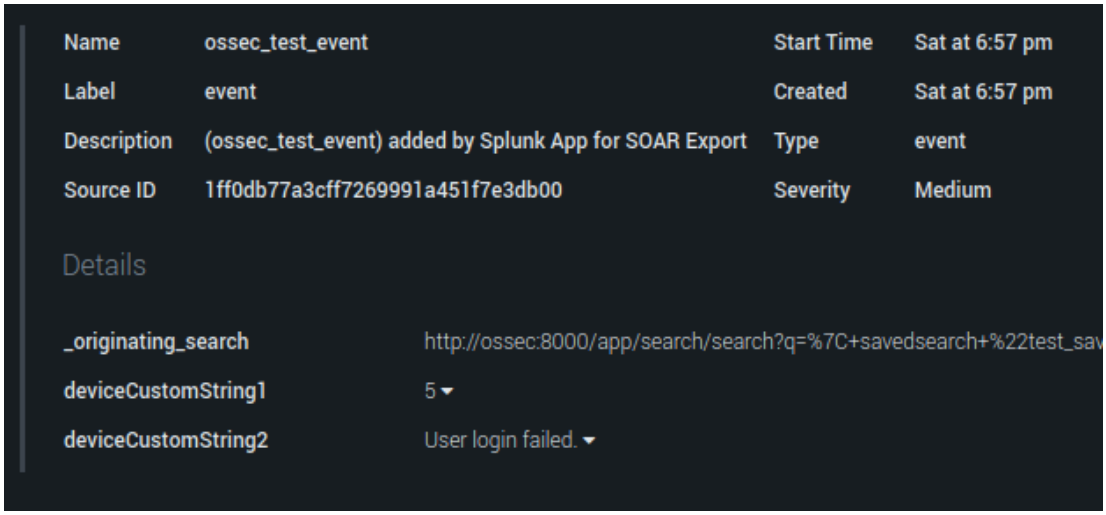


Figure 22: Event Information in CEF format

After examining the artifacts of a container, the analyst can proceed to the evidence section, where she or he can further correlate data from different sources, to strengthen the assigned case. Finally, after closing the case, a report can be produced, summarizing the key findings and also the action taken.[18]

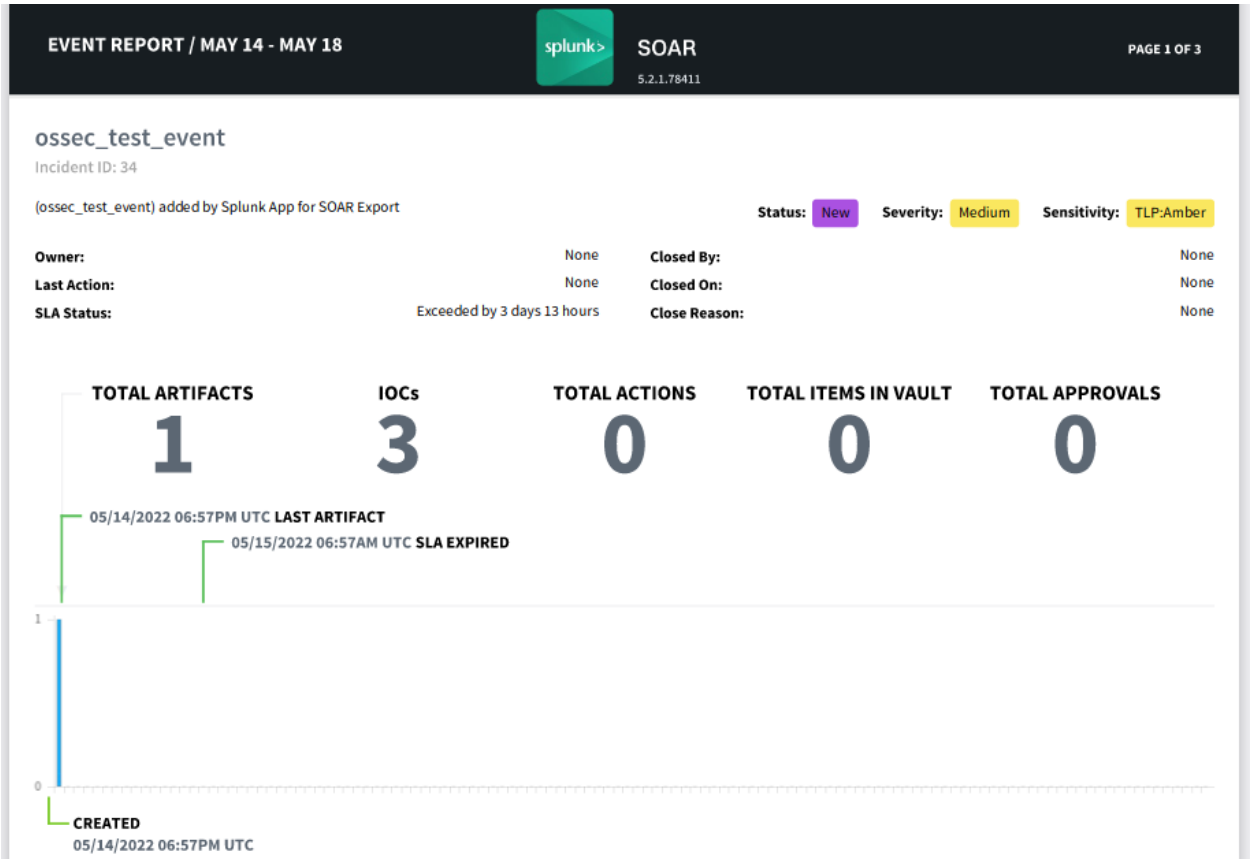


Figure 23: Investigation Report

[18] Splunk SOAR Reporting, available at: https://docs.splunk.com/Documentation/SOAR/current/User/Reporting

Data Visualization

One of the features that makes Splunk SOAR a comprehensive security automation solution are its extensive dashboards. By them, the user can engage a potential threat without having to use all the different data sources that are divided in many monitors and screens, reducing the complexity of operations. Dashboards may contain multiple information, varying from an events label, its severity or status. They may also contain data about the frequency of security event occurrence.

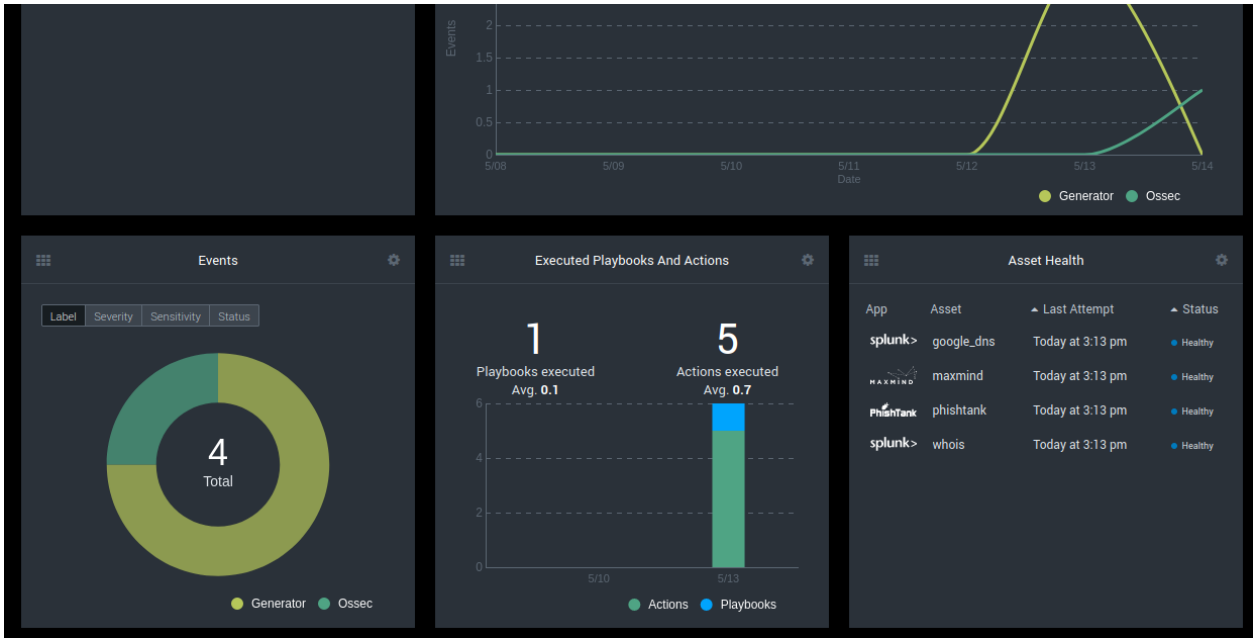


Figure 24: Dashboards

Another interesting and important factor is the health of all the apps deployed in the SOAR platform. This way the SOAR engineer can be notified whether an app has lost connectivity in the flow of information.

As mentioned before, the analyst can use the information provided to successfully resolve a case. He or she can have an overview of the playbooks and actions that have been implemented in order to build evidence and also generate a detailed report.

Playbooks and Automation

As mentioned in previous chapter, Splunk SOAR utilizes automation through playbooks and workbooks. Basically, a workbook provides a broad and more general idea of the response actions to a potential threat. It consists of two or more playbooks that execute all the automation tasks required. In the example bellow, a simple playbook implementation will be examined and analyzed in order to further explore the capabilities of Splunk automation.

As in Cortex XSOAR, Splunk according to its edition, possesses one or more ready to use playbooks. These playbooks can be used in various modes, according to the configuration of the SOAR engineer. In the created use case, the following configurations were implemented:

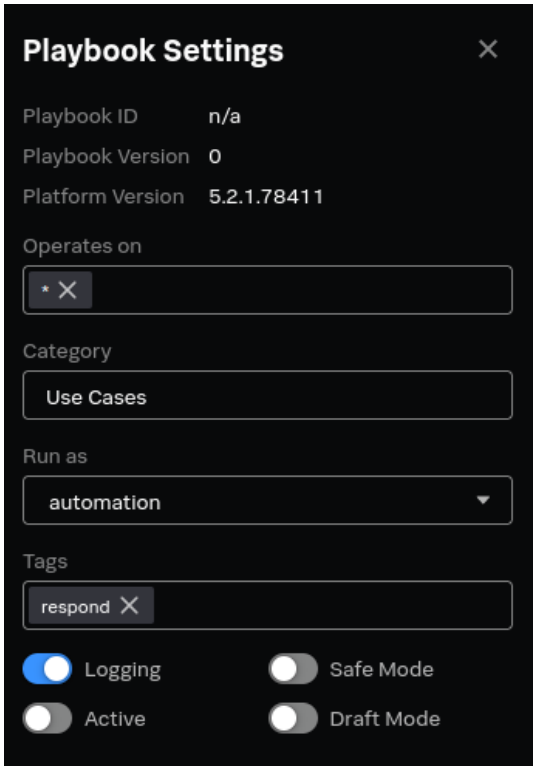


Figure 25: Playbook Settings

The engineer can define how broadly the playbook can operate (the * options declares that it will operate in all events) and also a category for the playbook (in this case the category used was Use Cases). The modes available, are the option to use the playbook in a Safe Mode, to test it in Draft Mode or to enable Logging capabilities for debugging purposes. Finally, an engineer can set a playbook as active in order to be executed automatically when a new event is alerted to the platform.

After the initial configuration, the playbook editor is ready to be enhanced by new actions.

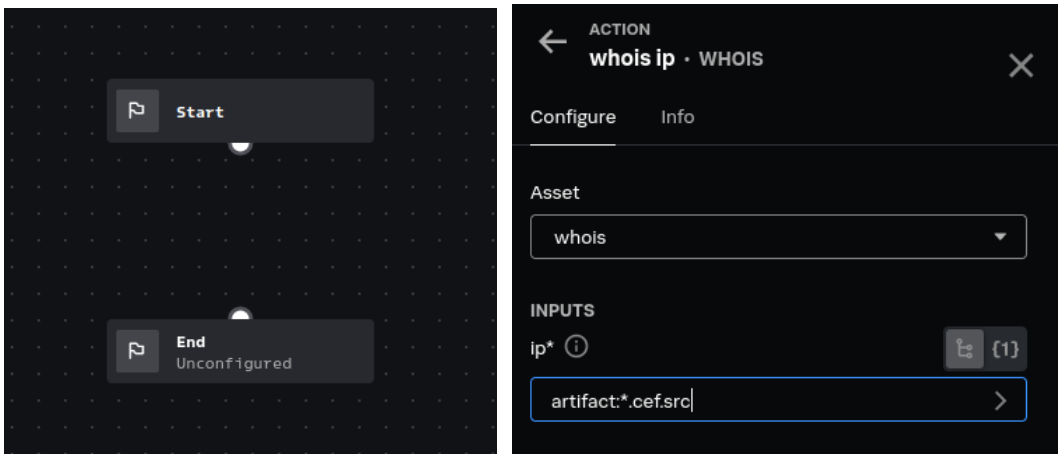


Figure 26: Playbook Editor and Action Configuration

For the examined use case, the WhoIs app was added to the execution workflow and was parameterized in order to search the received source IP of a security event.

As it can be observed, the implemented action receives its argument from the properties of the event artifact, as it was sent to the platform in a CEF. This format dictates that every artifact or container is presented in a JSON format with a specific structure. That structure makes it feasible for the platform to pass the requested values to the app. After its configuration, the app is added as a new action in the playbook, providing extra functionality. The final form of the playbook created is the following:

Figure 27:Final Playbook Design

This test playbook can then become active, in order to be implemented in every new event that arrives to Splunk SOAR from a data enrichment source. All the activities utilized are documented in the Recent Activity template providing the analysts with a history of their course of actions during the response to a security event or incident.

Section 3: Siemplify SOAR

Architecture

Siemplify SOAR is considered one of the most robust and comprehensive SOAR solutions available. As mentioned before, in its newest editions it uses a cloud approach, simplifying the installation procedure for the user in order to let him or her focus on the analyst point of view.

Siemplify follows generally a similar pattern, like other solutions. It uses data sources that provide the necessary enrichment. Then it ingests these data in its platform and stores them in a data base using indexing. Finally, it uses the data in order to conduct investigations and provide response to potential threats. Bellow, a representation of the first phase of the data ingestion is provided.[19]

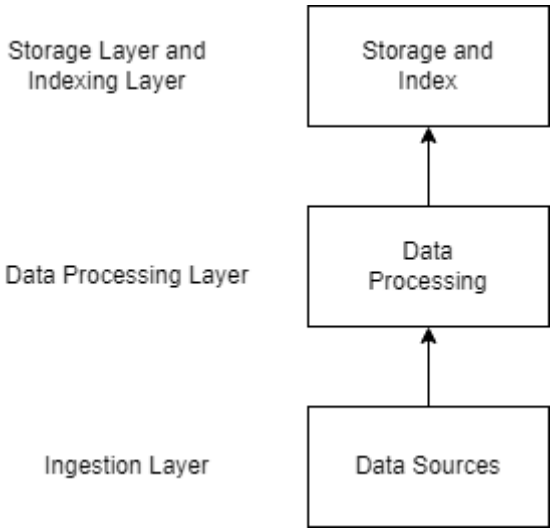


Figure 28: Siemplify Architecture Part 1

As observed, in the first layer the ingestion of the data into the platform is performed. In order for the platform to ingest third party data, it uses packages called integrations. Those packages contain the connectors, a part of code written in Python, responsible for the connection of the data source. This procedure is concluded in the second layer, where the parsing and enrichment of data takes place. Then the data is being stored in databases in the storage layer. There is also an indexing layer for the indexing of the data.

After the storage and indexing layers, the data is ready to be used in investigations, analyzed by the users and provide insight that will lead to incident response.

[19] Siemplify Architecture Overview, available at: https://documents.siemplify.co/en/articles/71-architecture-overview

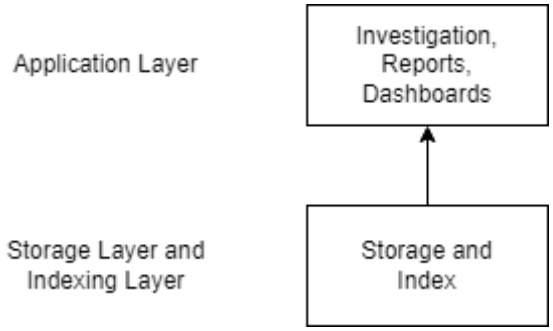


Figure 29: Siemplify Architecture Part 1I

Response is provided by actions used in automated playbooks. An action is part of an integration. It executes an API call to an external product or service. An example can be the triggering of VirusTotal API when analyzing a potentially dangerous hash or IP.

The playbooks are workflows of actions or blocks, that follow after a trigger is activated. The blocks play the part of a sub-playbook that contains input and output parameters.

For the examination and evaluation of Siemplify SOAR, integrations were used that provide public APIs for testing purposes.

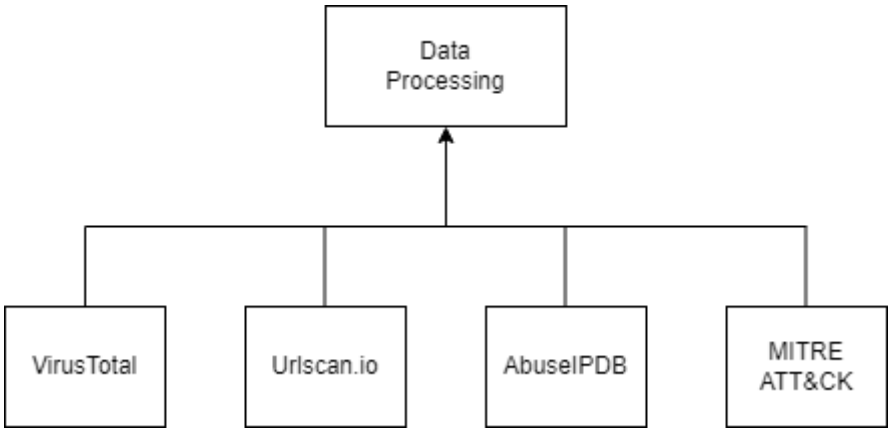
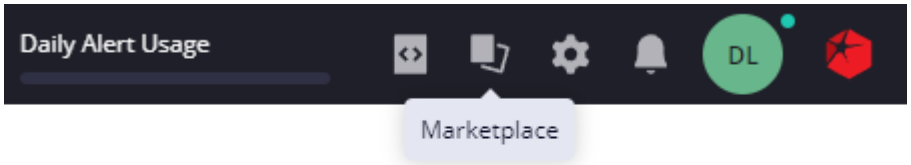


Figure 30: Siemplify Data Sources

In order to achieve data enrichment, the APIs from VirusTotal, Urlscan.io, AbuseIPDB and MITRE ATT&CK were utilized. They will then be used to create playbooks for use cases.

Data Enrichment

As it was previously mentioned, public APIs from web applications were used to provide the necessary enrichment to the platform. Those apps were integrated into Siemplify SOAR from ready-to-use integrations provided in the marketplace of the platform, easily available to the analyst.



After accessing the Marketplace, the engineer choses from a wide list the integrations he or she wishes to use. Then he or she downloads the integration through the UI environment. In order for the integration to become functional, it needs to be configured.

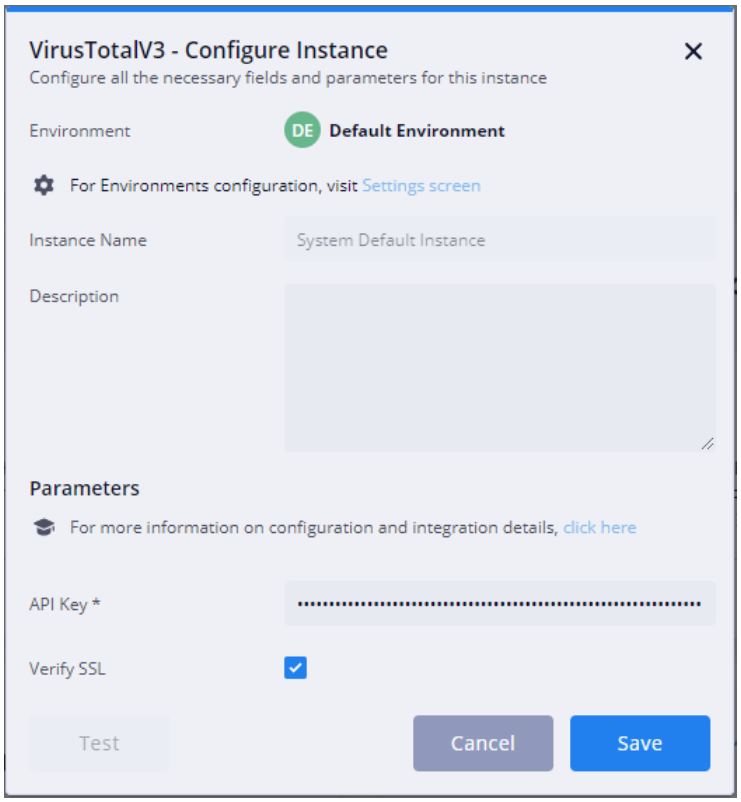


Figure 31: VirusTotal integration configuration

To configure VirusTotal, the user has to insert the API key, provided by creating an account to the application. Then, the user must test the integration, to enable its features to the platform.

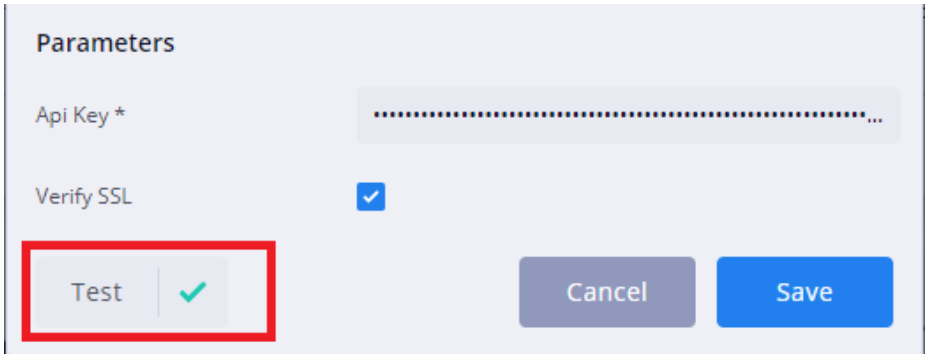


Figure 32: VirusTotal integration testing

After the successful testing, the integration can be used in the SOAR environment. Similarly, the instances of Urlscan.io and AbuseIPDB were enabled. The MITRE ATT&CK application is provided as an integrated part of Siemplify SOAR by default.

Correlation and Digital Forensics

Data correlation is a fundamental feature of every SOAR platform. Siemplify SOAR utilizes data correlation through its integrations presented to the analyst in comprehensive dashboards. Data can be correlated and clustered in order to serve various purposes. Siemplify supports the creation of different environments and the use of different instances of data sources for each environment. For example, an environment can be a Business Unit of an Enterprise (Berlin Business Unit, Athens Business Unit etc.) Each environment can use its own integrations, or the engineer may choose to apply all the integrations of the platform to all the different environments. To create an environment, the engineer has to define its unique network characteristics, as well as domains and sub-domains.

Alerts derived from one or more environments can be clustered together developing cases. A case is a container that stores all important investigation information that will be later examined by the analyst. For the creation of a case, a maximum number of alerts is defined (e.g., 20 alerts associated with the specific case). If this number is exceeded, the platform falls back to an overflow case, that has an extended capacity for alerts. For the example that is going to be demonstrated, a case was created from alerts derived from invalid web certificates.

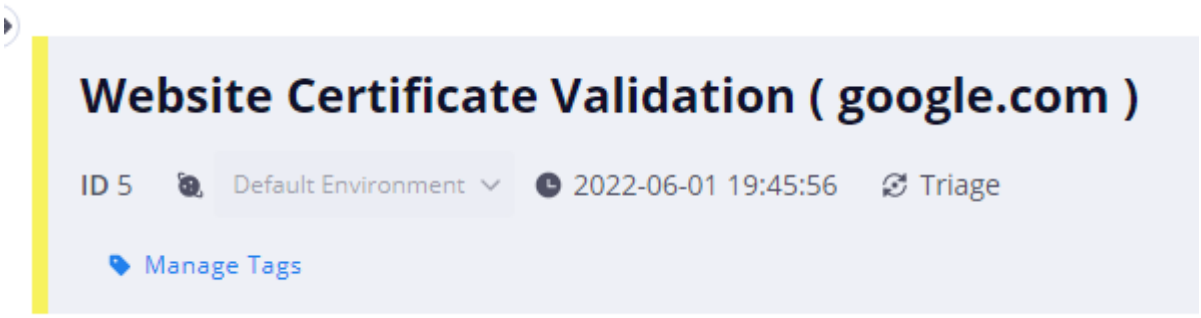


Figure 33: Case creation

For testing purposes, the site that was examined was google.com, that possesses a valid certificate.

After entering the target website, data sources that are already integrated to the platform and were mentioned previously, can be activated as a block and as part of the workflow of a playbook.

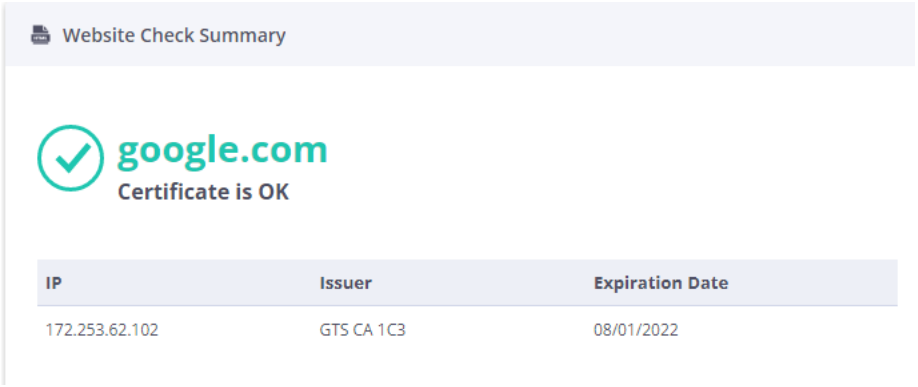


Figure 34: Case testing

As observed, the website has provided a valid certificate. At the analyst dashboard, more information can be presented from different data sources, further building the case.

Figure 35: Integrated Information Part 1

Except the certificate details, the analyst can further investigate the target website, by viewing a screenshot taken automatically of the site environment.

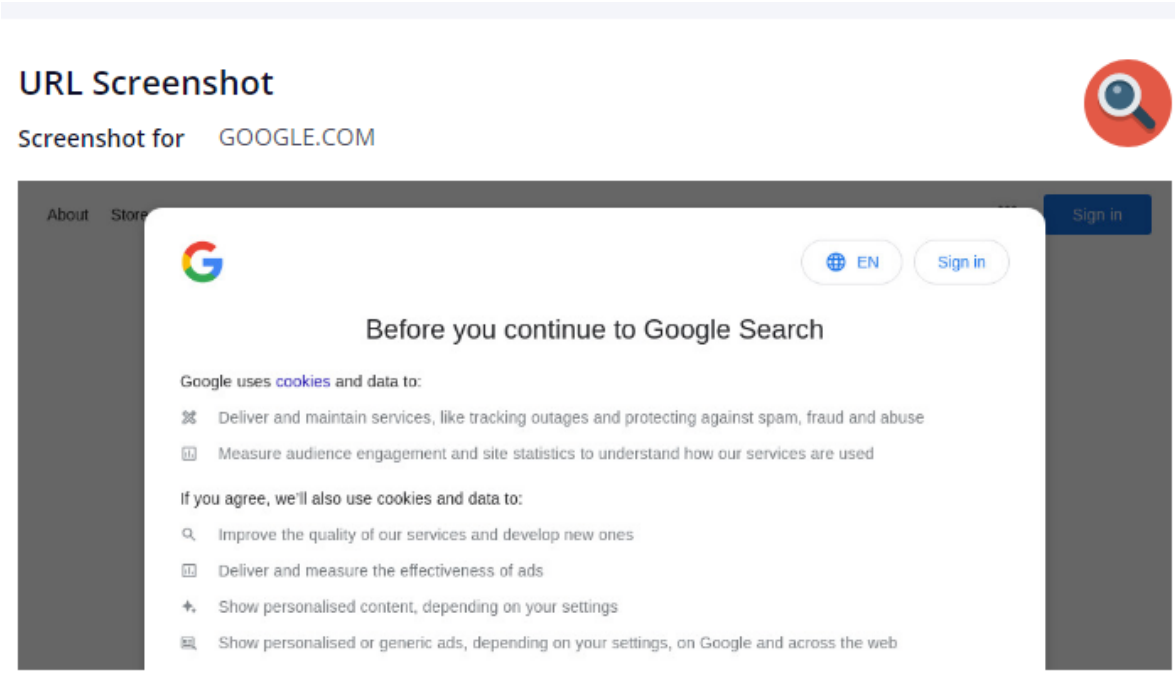


Figure 36: Integrated Information Part 2

After the analyst has received all the necessary information of the data sources available, he can decide the response strategy. This strategy is utilized by the implementation of an automated playbook, that uses a flowchart with all the information presented, in order to provide a suggested solution.

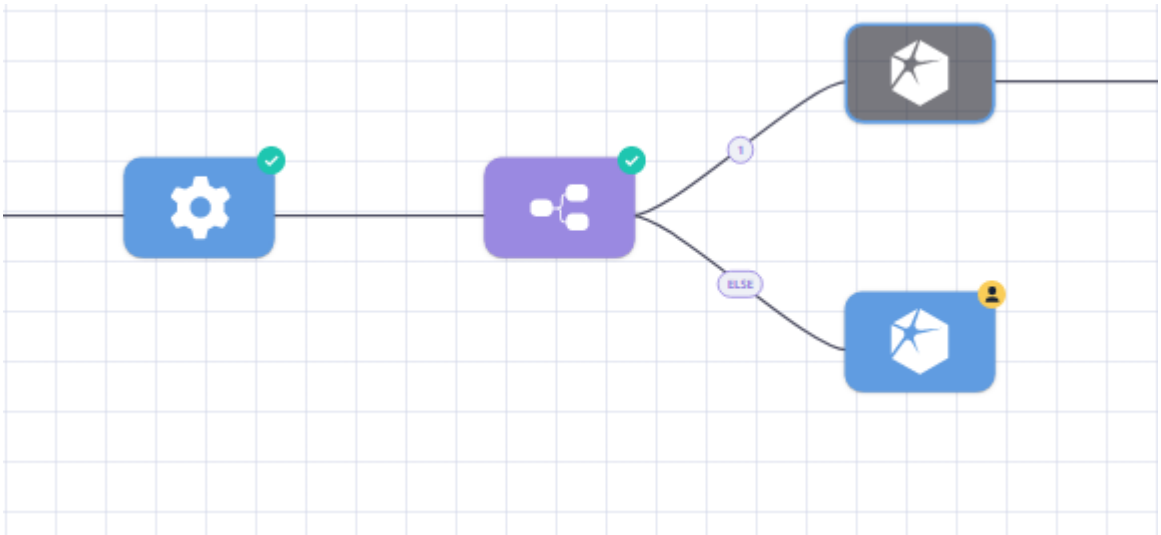


Figure 37: Playbook utilization

The investigator can choose to manually respond to the recommended action, or even allow the response to be implemented automatically. The manual response gives the analyst access to all the information needed to perform threat hunting activities ,as well as the capability to escalate the threat and start a remediation flow.

Data Visualization

Siemplify has developed a comprehensive and user friendly environment that enables analysts to fully utilize its capabilities. Every analyst has a Homepage section, where he or she encounters potentially unresolved cases that were assigned to them, as well as pending actions that require manual confirmation to proceed.

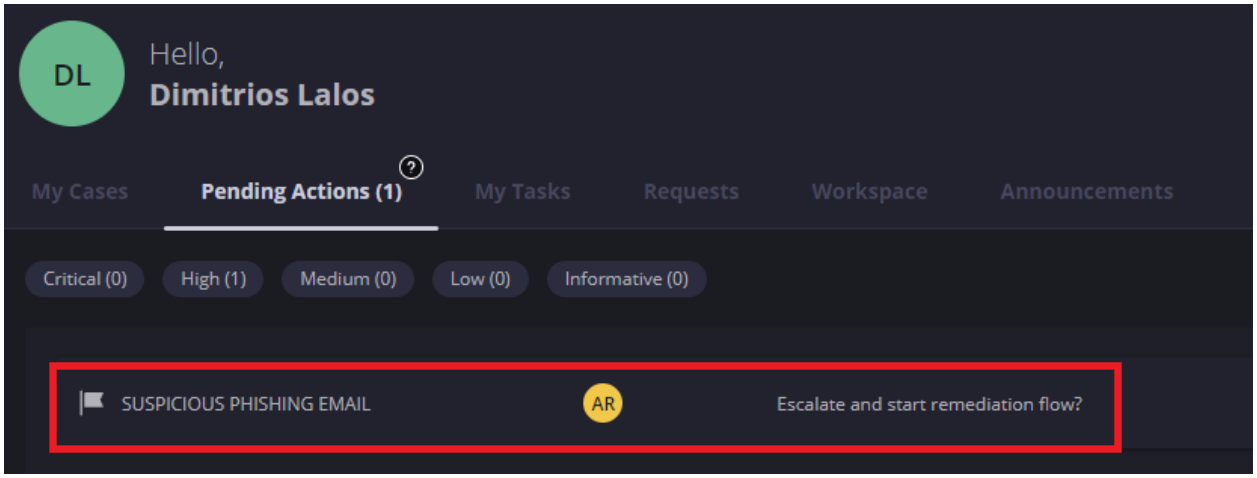


Figure 38: Dashboards - Homepage

Except the Pending Actions page, Homepage provides analysts with view, over their tasks or announcements and a Workspace, where the analyst can gather the evidence collected from various cases.

In Dashboards, the analyst has a high level overview of the number of cases that have been created, potential return of investment and other relevant information. A plethora of changes and customizations can be performed to apply to every user individually. The analyst can choose to see metrics from a specific environment (Business Unit) or a general view from all the environments. Dashboards can be exported or used in reports. An analyst can create high quality reports, using the Analytics tool Tableau, which is provided as an integrated part of the platform. He can also set a time scheduler, in order to email requested reports to stakeholders.

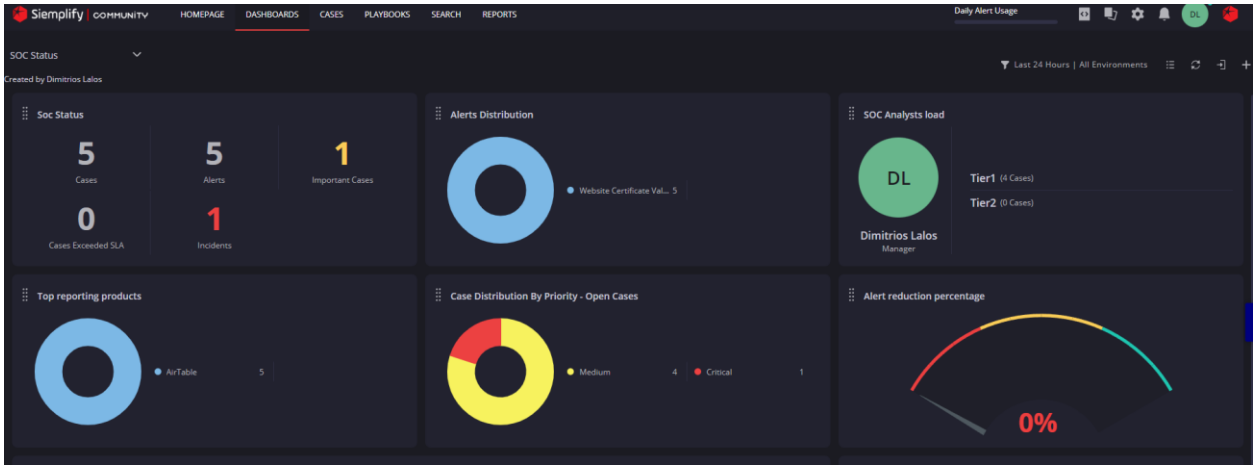


Figure 39: Dashboards – Widgets

An investigator can create his or her own widgets and add them to the Dashboards, making the page fully customizable.

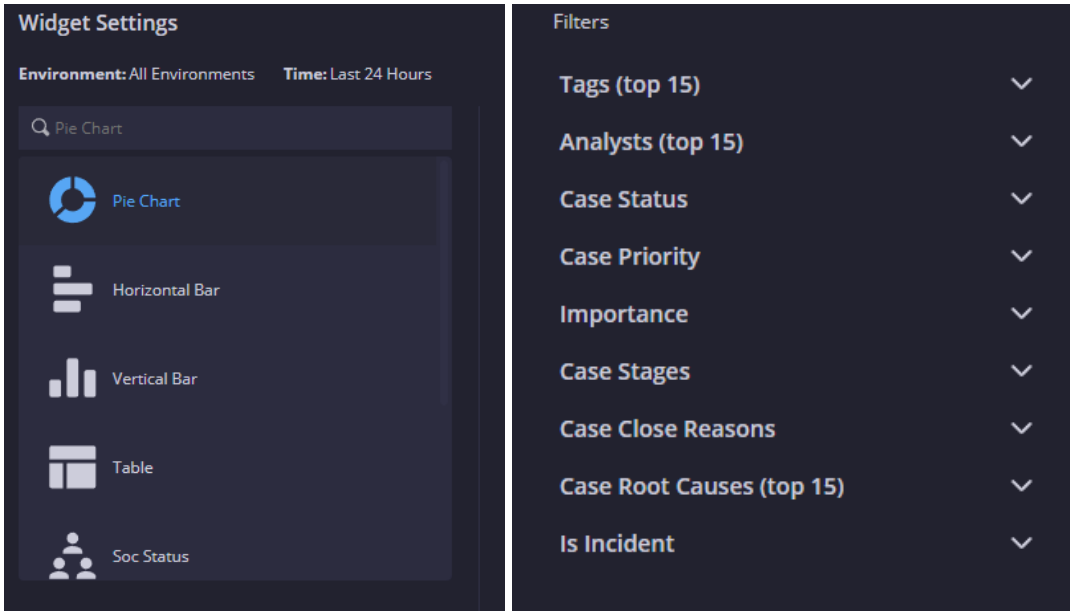


Figure 40: Dashboards – Widgets

In Widget Settings, the type of the data representation can be selected, as well as other important information that help customize the dashboard to the user's needs. At a higher level, the analyst can choose which type of widget will be implemented in a dashboard, as well as customizations about the widget position, size, etc.. This can be achieved through the Views, from the Settings section.

After the Dashboards section, analyst can visualize information on every case assigned. This can be achieved from the Cases section. There visualizations help the investigator build his or her cases and lead them to efficient response. One of the visualizations available is the Attack Visualization.

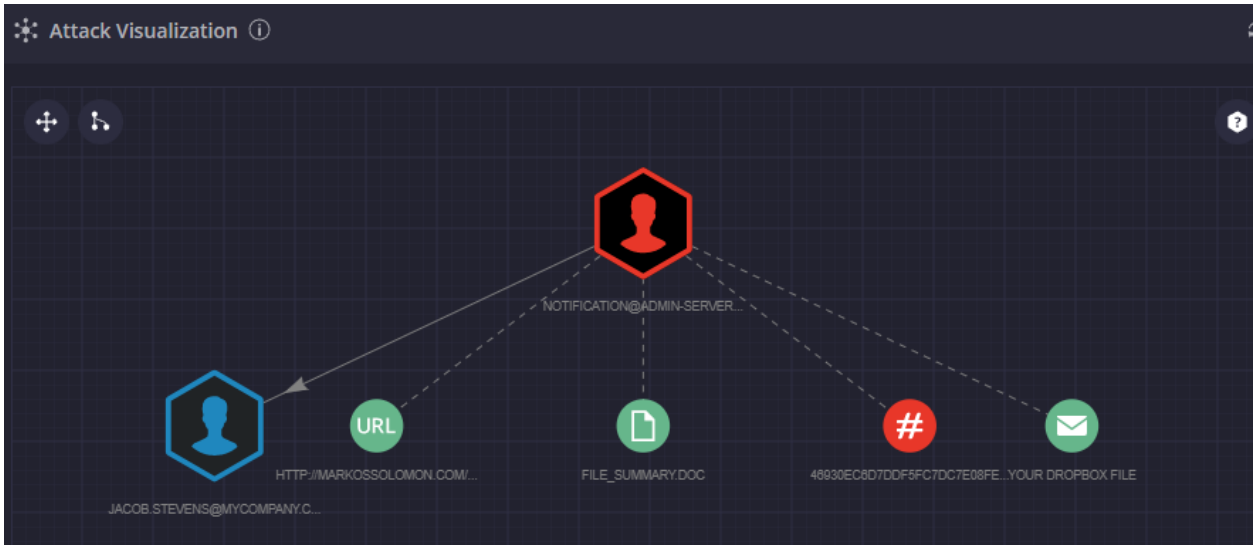


Figure 41: Cases – Attack Visualization

There, the user can investigate on the organizational assets that might have been infected from a potential breach and correlate these information. Information can also be visualized about the attacked employee, Indicators of Compromise, information from Mitre Att&ck, or screenshots from the attack.

The analyst can also receive visualized data concerning intel on potential ongoing threat campaigns that use the same TTPs to conduct their malicious activities.

Playbooks and Automation

As mentioned before, playbooks play an essential role, not only to respond to existing threats, but also to build a case from an attack, using the algorithmic steps implemented in a playbook. The playbook is composed from blocks. Those are considered to be sub-playbooks and can be used in one or more places inside a playbook. The blocks define specific Actions. Actions are essentially python code that targets a specific API endpoint exposed by a 3rd party product and usually accomplishes a single task. They are part of an Integration of that product to the platform. The blocks are created via drag-and-drop of an Action into a playbook.

Playbooks are essentially workflows or flowcharts, that lead to specific actions, from the automated analysis of the data provided. Usually, a playbook has one or more decision blocks. There the analyst, chooses the response action according to the analysis.

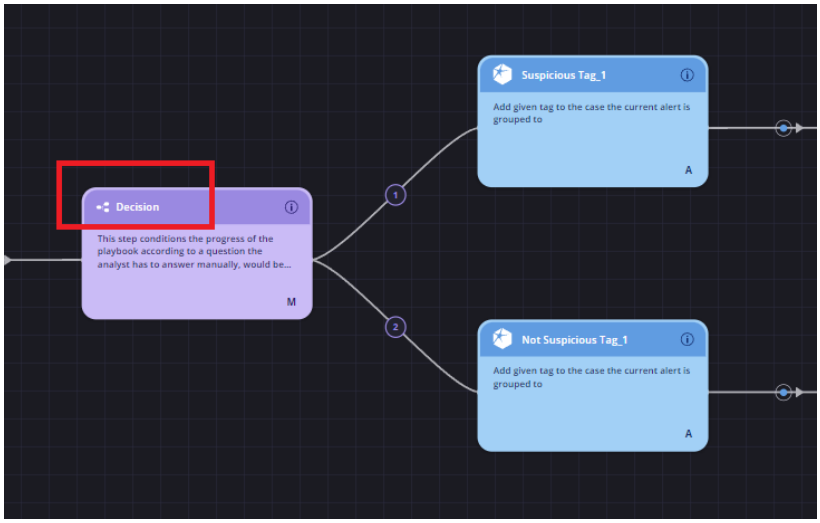


Figure 42: Playbooks – Decision Block

A playbook is initiated by a trigger block. Triggers are enabled usually when a statement becomes true.

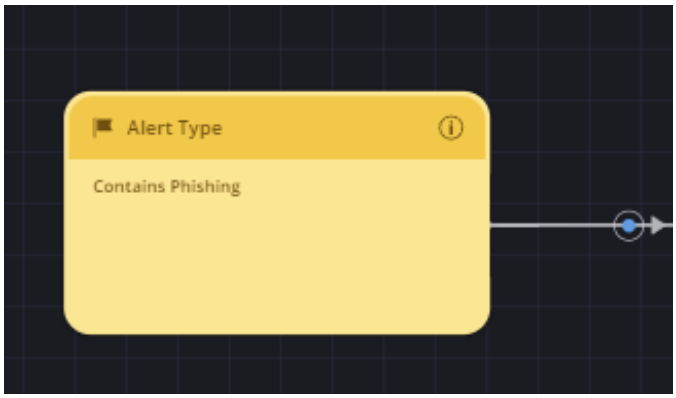


Figure 43: Playbooks – Trigger Block

In the example use case, a trigger block contains a statement that checks the incoming alerts and if an alert contains the word phishing, the playbook is triggered. Usually after the trigger block, a playbook contains enrichment blocks, actions that provide additional information to the analyst.

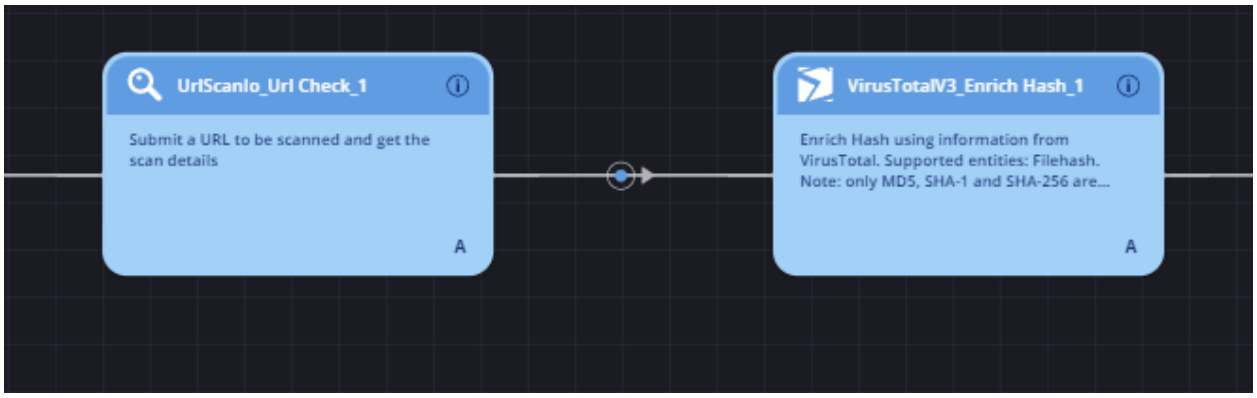


Figure 44: Playbooks – Enrichment Blocks

In our example, two instances were created from two apps that were integrated with the platform, Urlscan.io and VirusTotal.

The examination of the enriched data and the decision taken by the analyst, might change the status of a potential threat (severity level), or initiate a response action, in order for the threat to be contained.

The analyst has the option to test new playbooks in the platform inside a simulator. This provides test alerts and test cases, from which the user can test the functionality of his automation. When the playbook passes the simulator phase, it is then placed in production environment.

Chapter 7: Use Case Analysis

In order to demonstrate the feature and capabilities of the SOAR platforms, use cases will be created and analyzed. Each platform will be used in attack simulations, and each platforms features will be utilized. For the Cortex XSOAR, developed by Palo Alto, a scenario will be implemented, where an analyst uses the software to create a custom incident type, used for an investigation and also utilize an automated response action.

For the Slunk SOAR, the use case involved threat hunting from a potentially malicious IP address. The analyst was given the suspicious IP, and had to engage in analysis and investigation, using the tools provided by the platform in order to decide if the given address was malicious.

For the Siemplify SOAR, a use case was used to simulate an attack in corporate environment. A phishing attack was examined that happened to an employee of the organization and the analyst had to triage the threat and decide whether or not to escalate the incident to a higher level analyst.

Chapter 8: Demonstration

Cortex XSOAR

For demonstration purposes, an XSOAR integration for creating alerts was used. The integration had the role of the attacker, that created the alerts. The alerts were retrieved by the platform and presented to the analyst, who then started the triage. After the categorization of the alerts, the response actions were enabled through a playbook containing the required automations.

To begin with, the analyst created a new incident type, for the categorization of the alerts. Though there are out of the box incident types, XSOAR provides the opportunity to customize the field to the needs of the SOC. After creating the new incident type (XSOAR DEMO – URL Alerts), the incident type was populated with three alerts, created by the alert simulation instance. In order for the alerts to be categorized to the new incident type, classification and mapping processes must occur. Classification provides information about the characteristics of an incident (for example a suspicious URL which is blocked or allowed). Mapping provides all the necessary fields needed to be obtained from the events, in order for the analyst to have a more comprehensive view of his or her case.

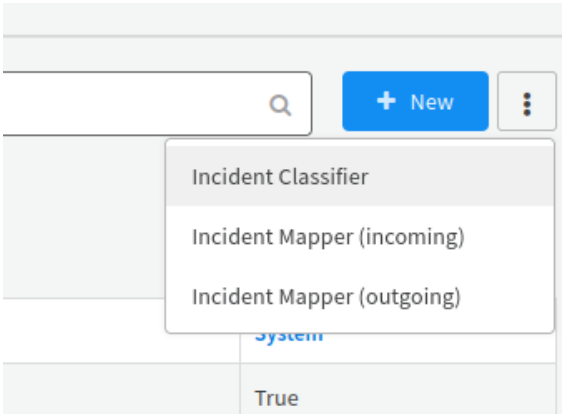


Figure 45: Creation of an incident Classifier

The analyst then creates the classifier in the Classification editor, provided by the platform. The analyst pulls the data (security events) from the instance of the integration mentioned above, or he or she can insert the data in json format. This is usefull for the investigation of a security event, created by third party software, not yet integrated with the platform.

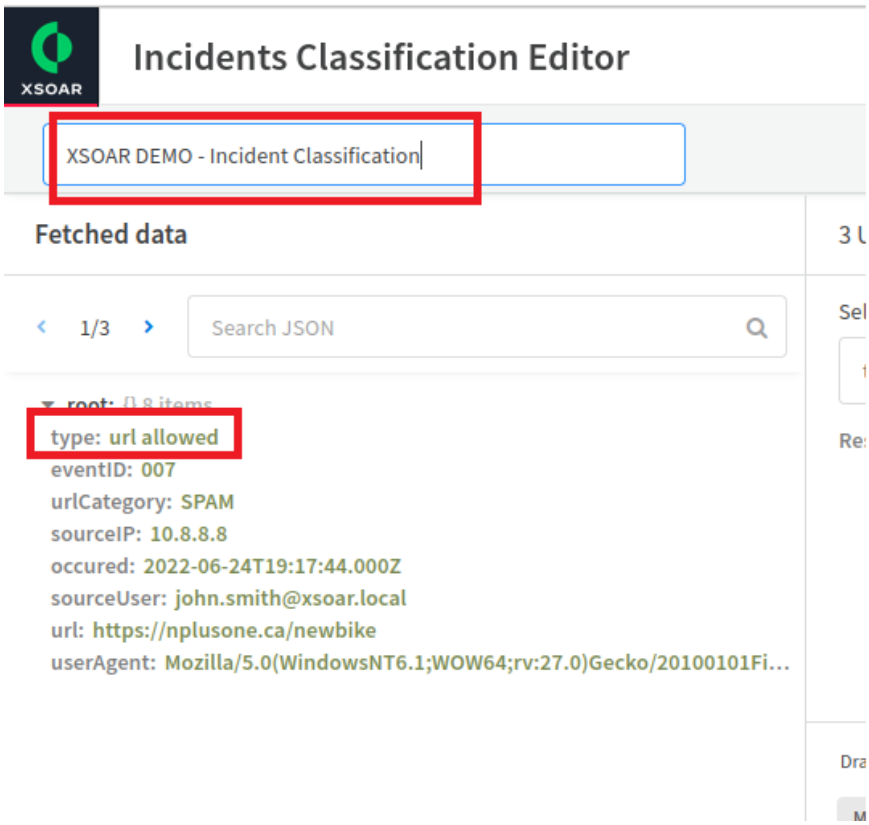


Figure 46: Incidents Classification Editor

In the Classification editor, the analyst assigns the name of the classifier and uses the type filed of the events to create tags for his custom incident type.

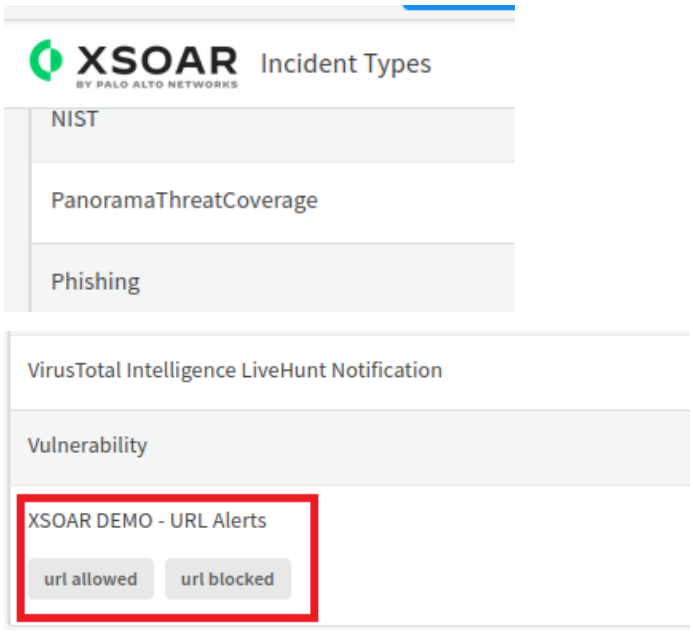


Figure 47: Assigning the tags to the custom incident type

After the classification, the analyst proceeds to incident mapping. With mapping, the analyst is able to use the fields important to his or her investigation. Even though XSOAR comes with a wide variety of incident type fields, again customization is

available, in order for the user to create his own fields. After the creation of the fields they are mapped to those of the security event provided.

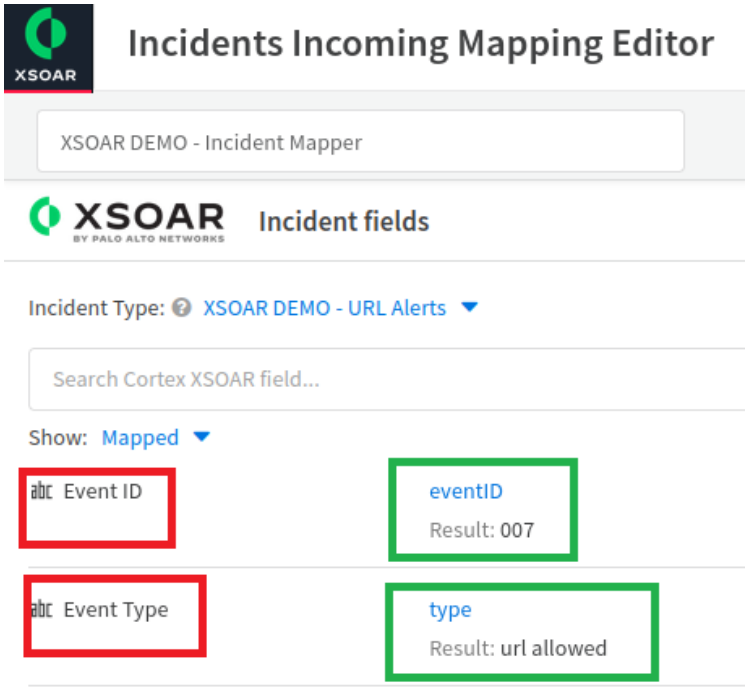


Figure 48: Incident Mapping

The fields mapped in green show also the information that will be derived from the event, after the mapping. The event is presented with all its fields in JSON format.

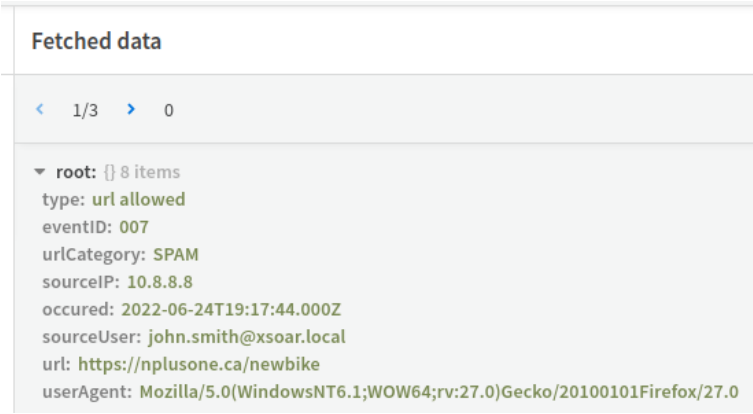


Figure 49: Security Event Format

After utilizing incident classification and mapping, the analyst uses the created classifier and mapper to generate alerts of the customized incident type. For this demonstration, three customized alerts were created and inserted into the platform for investigation.

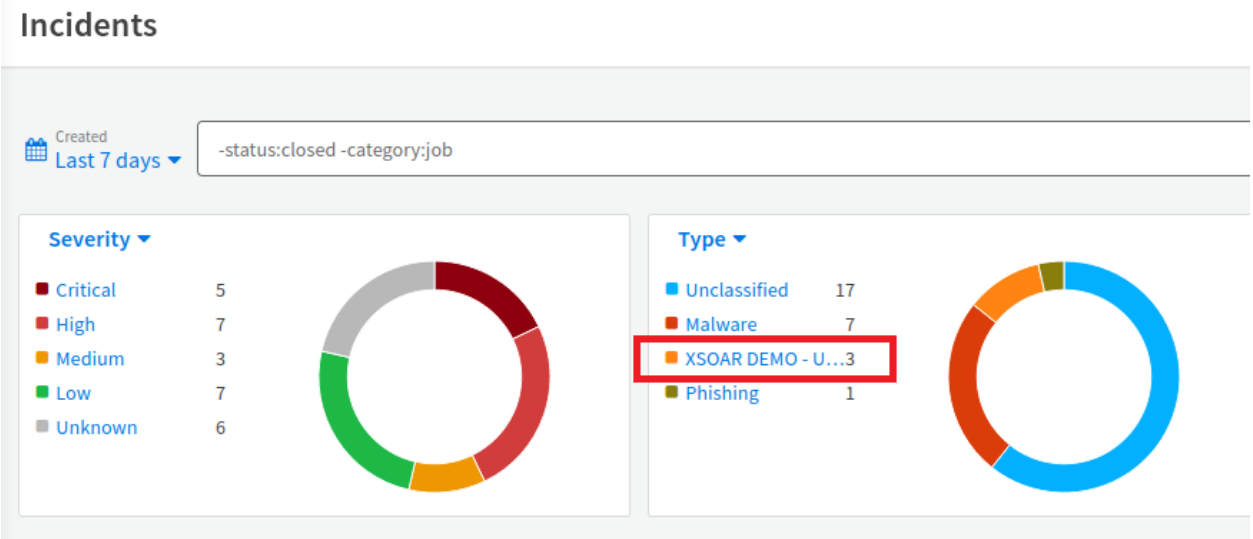


Figure 50: Alert Categorization

Customized incident types are useful when an analyst investigates an exploitation of a potential zero-day vulnerability and wishes to mark specific characteristics of security events.

After creating an incident type, the analyst needs to proceed to response and remediation of the incident. For that purpose a playbook was triggered out of the box, in order to counter the potential threat. The analyst enables the playbook in the Work Plan section of the platform.

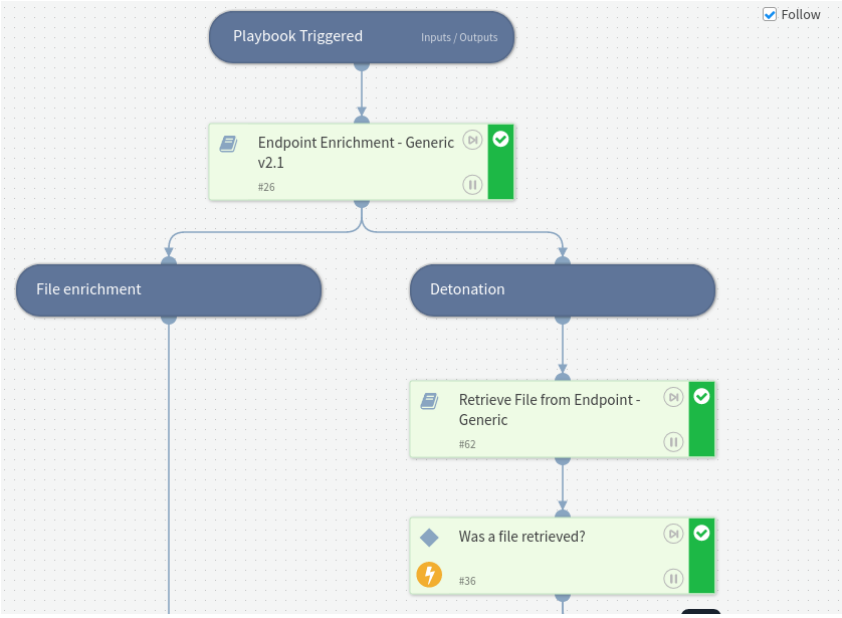


Figure 51: Playbook Triggering

After triggering the playbook, the automation receives the enrichment data in order to proceed with the investigation. The playbooks in Cortex XSOAR are devided in

tasks. Some tasks, like the retrieval of data are performed automatically, whereas other need the user's confirmation to proceed.

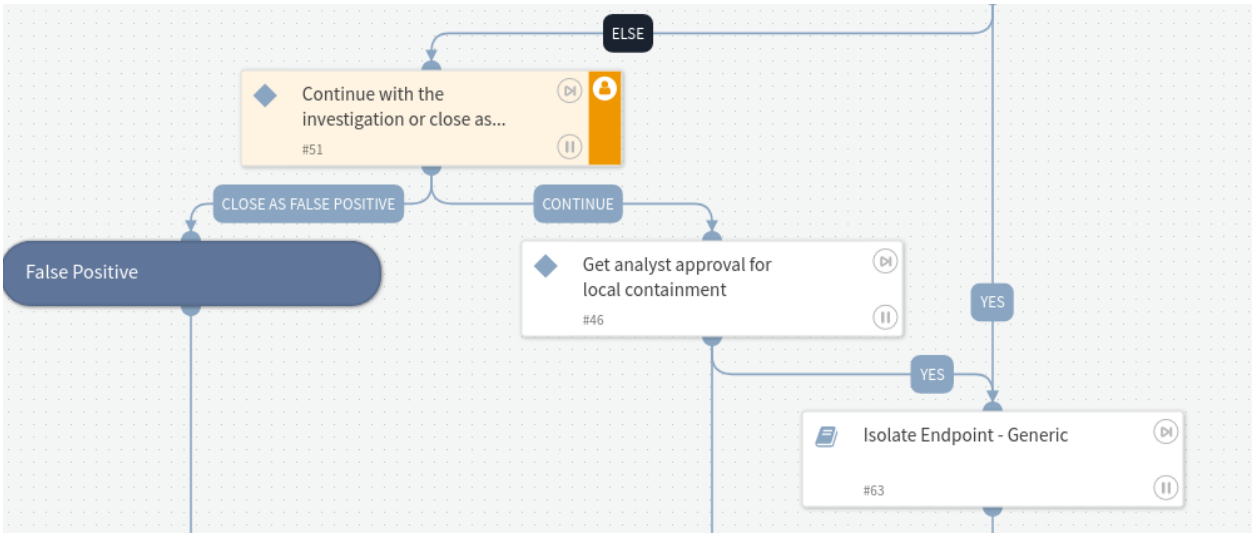


Figure 52: Execution after user's confirmation

As it can be observed, the task requires the analyst to continue the investigation, or close the incident as a false positive. After conducting a first triage, the analyst choses to proceed with the containment of the incident.

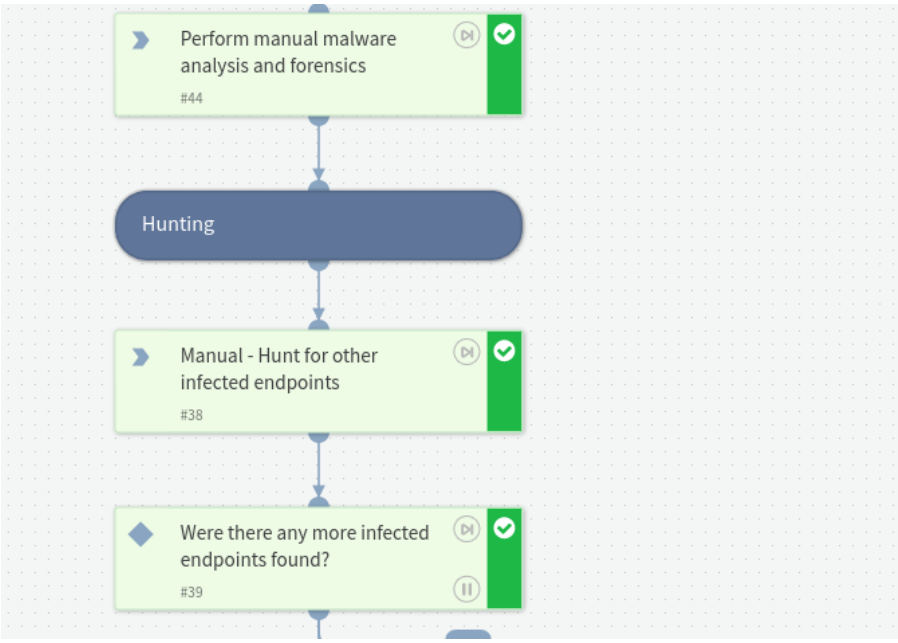


Figure 53: Manual tasks execution

After choosing to contain the incident, the playbook provides a list of tasks that the analst must perform manually to contain the malware detected. After containment, the analyst can perform threat hunting in order to discover other infected endpoints.

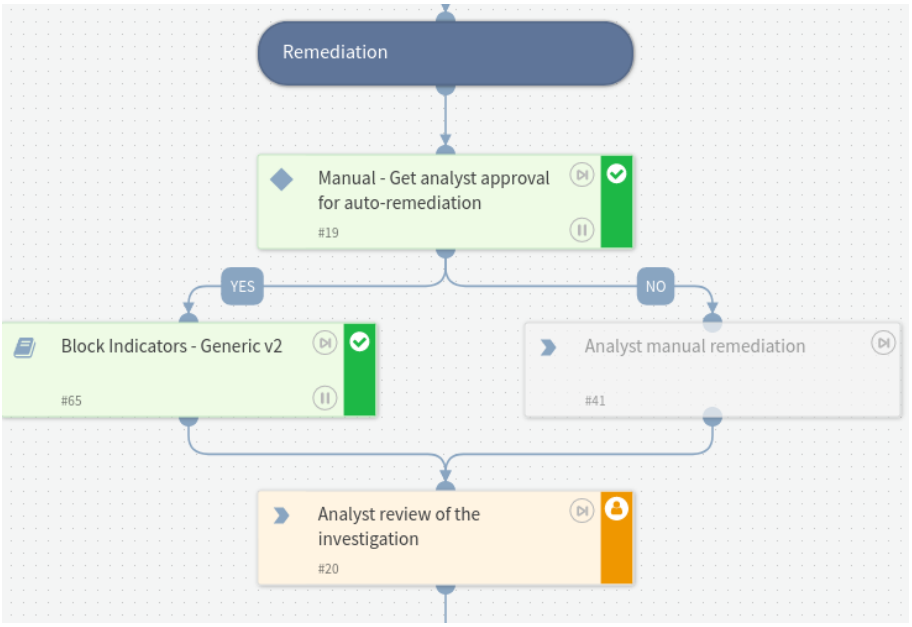


Figure 54: Remediation

After containment, the analyst can proceed to remediation. The platform provides auto-remediation capabilities through the execution of the playbook. After the implementation of rremediation measures, the analyst can review the investigation, creating a detailed report, and close the case.

Splunk SOAR

In the Splunk Use Case, the analyst was given a potentially malicious IP address to conduct threat hunting. The address was provided as a simulated security event of medium severity. The Splunk SOAR provides the analyst with out of the box apps, already installed and configured in the platform.

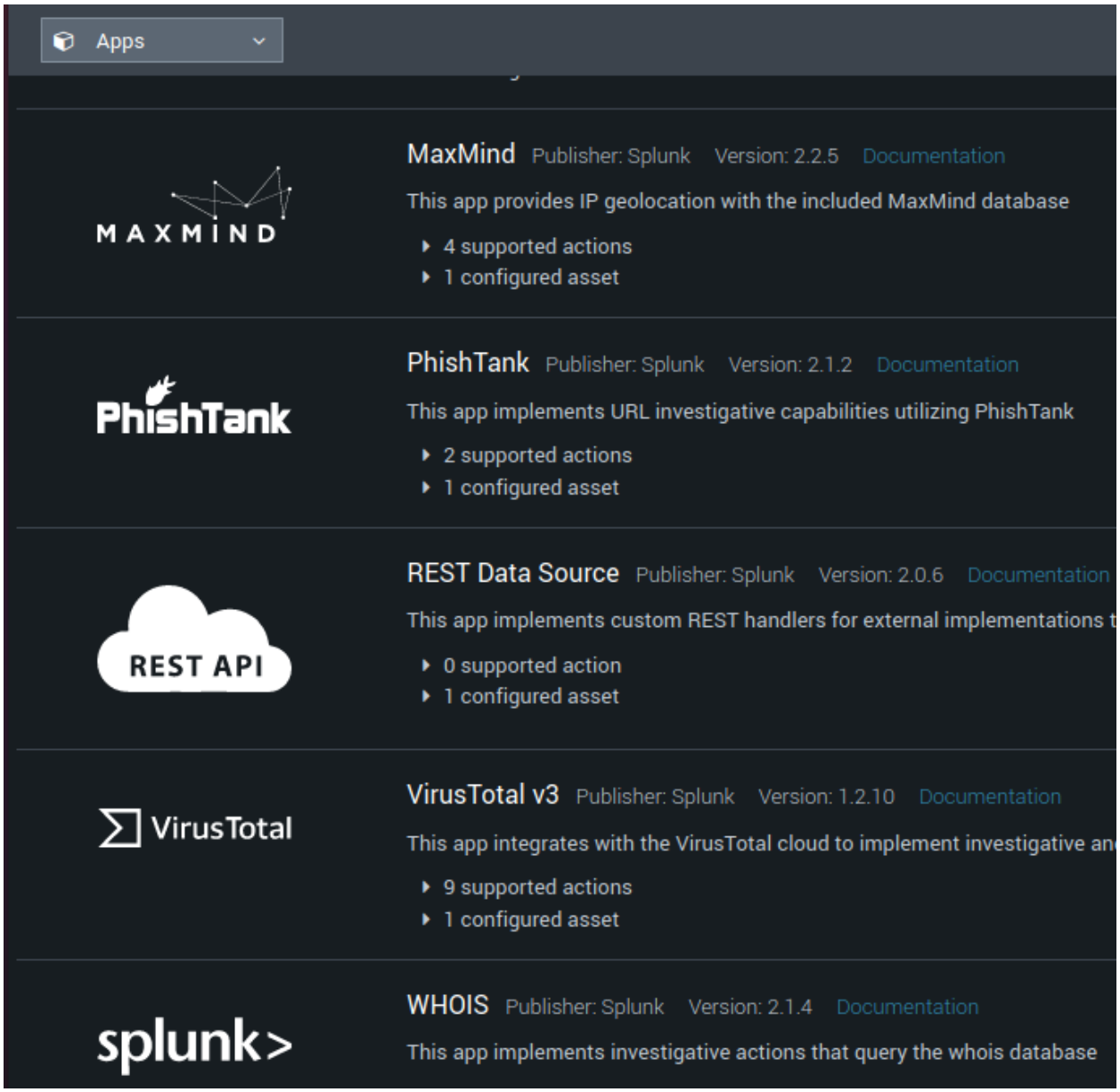


Figure 55: Splunk SOAR Apps

Maxmind, PhishTank, REST Data Source and WHOIS were already installed and configured in Splunk SOAR. Nevertheless, a VirusTotal App was also installed and configured, in order to help the analyst analyze the suspicious IP further.

The security event, appears on the “Events” template, indicating its severity and the need for further investigation.

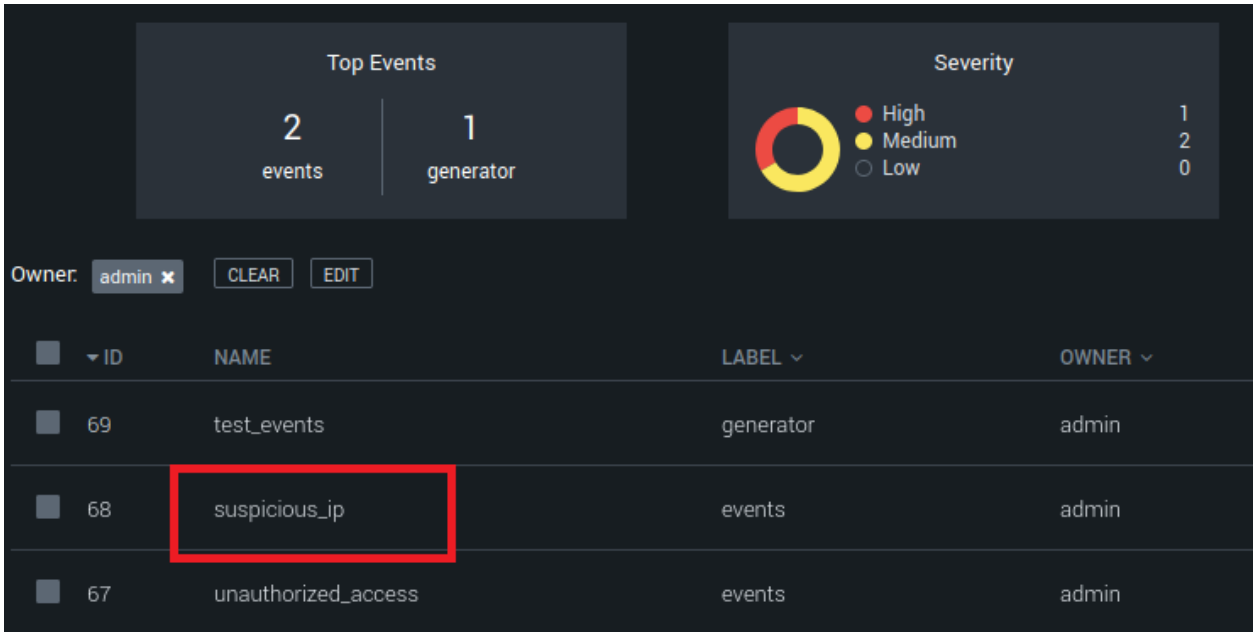


Figure 56: Splunk SOAR Alerts

It is important to remember to Event ID (in our case is 68). This will further assist in testing the implemented solution.

After recognizing the potential incident, the analyst will use a playbook, an automation, that will perform a number of actions on the suspicious IP. The IP has the format of an artifact and is a part of the container that creates the case for the analyst.

For the scenario, a playbook was created from the beginning. The playbook contained instances from the MaxMind, the WHOIS and the VirusTotal apps.

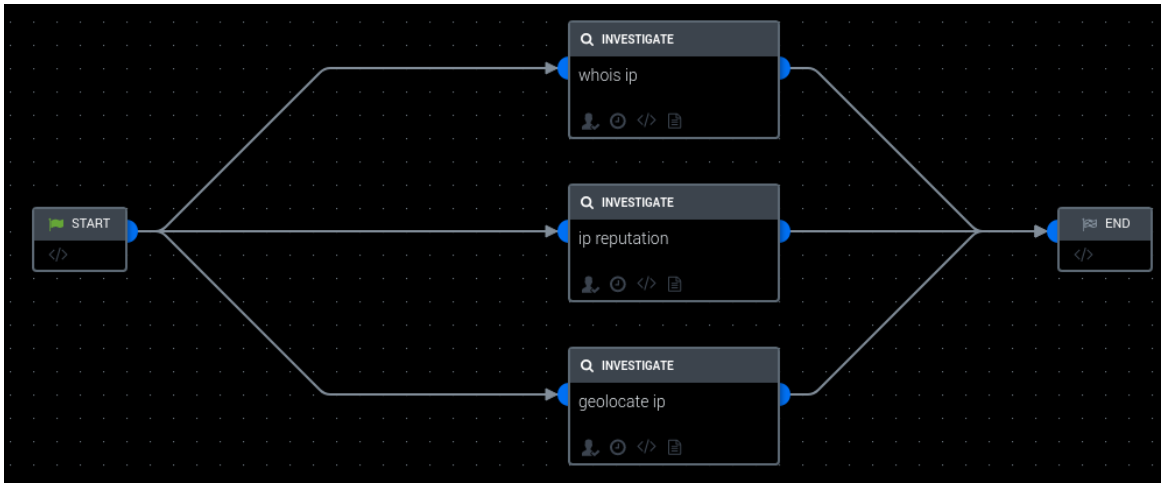


Figure 57: Splunk SOAR Playbook

The apps can provide information like geolocation and ip reputation, assisting the analyst to decide whether the IP is malicious or not. To configure the instances inside the playbook, a parameter is used in CEF (Common Event Format) that is acceptable

by the platform. An example is provided below for the WHOIS app. As it can be observed, the ip used for analysis, is the source (src) ip, in CEF. An instance of the app that is utilized an a case is called Action.

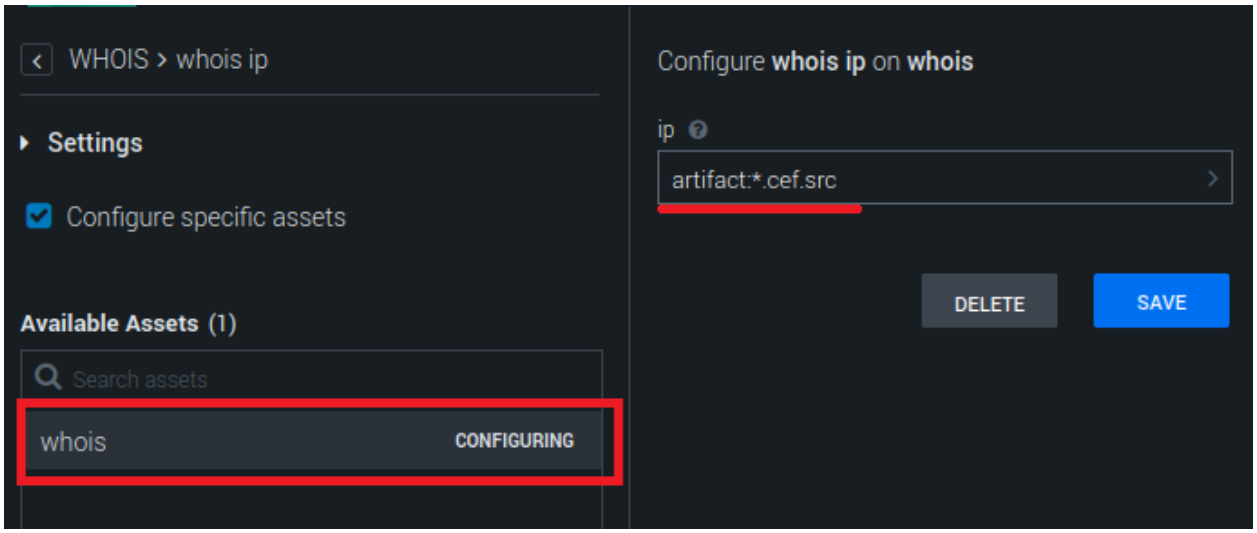


Figure 58: Splunk SOAR Action Configuration

After finalizing the playbook, the analyst is able to use it against the security event. For testing purposes, the Splunk SOAR provides a Debugger terminal that shows all the processes triggered to utilize the playbook.

```
Playbook 'DEMO Playbook' (playbook id: 211) executed (playbook run id: 107) on events 'suspicious_ip'(container id: 68).
   Playbook execution status is 'success'
        Total actions executed: 3
        Action 'whois_ip_2'(whois ip)
           Status: success
                App 'WHOIS' executed the action on asset 'whois'
                   Status: success
                   Parameter: {"ip":"182.113.221.215"}
        Action 'ip_reputation_3'(ip reputation)
           Status: success
                App 'VirusTotal v3' executed the action on asset 'virustotal'
                   Status: success
                   Parameter: {"ip":"182.113.221.215"}
        Action 'geolocate_ip_2'(geolocate ip)
           Status: success
                App 'MaxMind' executed the action on asset 'maxmind'
                   Status: success
                   Parameter: {"ip":"182.113.221.215"}
```

Figure 59: Splunk SOAR Playbook Utilization

As it can be observed, after the implementation of the playbook, the suspcious IP has passed as a parameter in all playbook Actions. These actions provide the analyst with the required information in order to examine the case.

```
'status":"success","message":"Harmless: 81, Malicious: 2, Suspicious: 0, Undetected: 11"}]
```

Figure 60: VirusTotal Information

From Virus Total, information was provided according to the requested ip reputation. Two of the AntiVirus software used by Virus Total, have deemed the ip address as malicious, when the majority considers it as harmless.

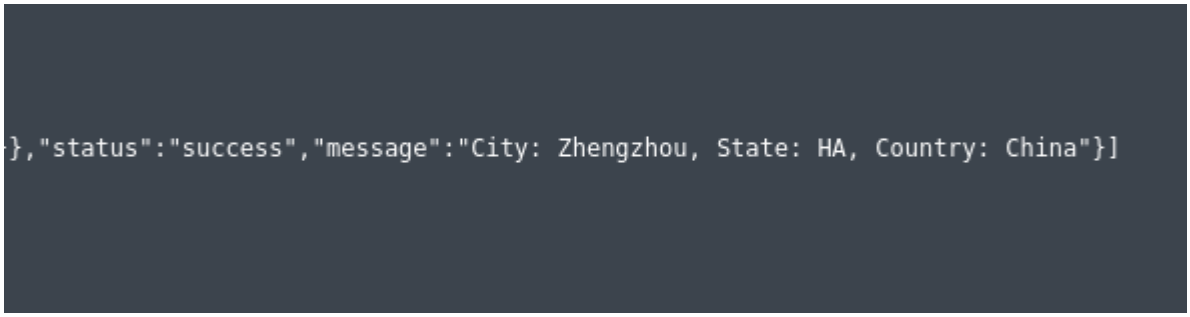


Figure 61: MaxMind Information

From MaxMind, geolocation information about the ip address is provided. By acquiring a Google Maps API, the investigator can also have enhanced visualization through Google Maps.

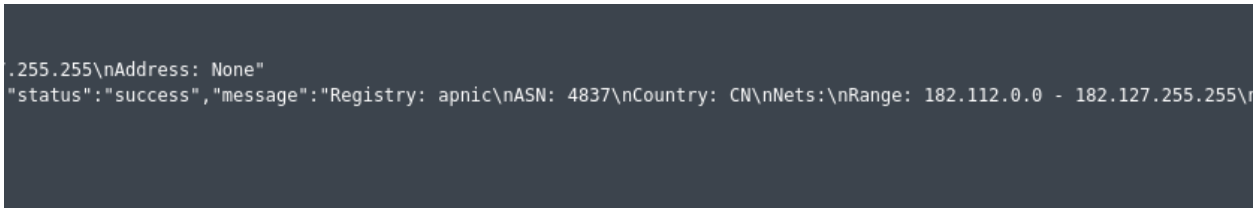


Figure 62: MaxMind Information

Finally, WHOIS provide some additional information about the country of origin and also the network.

The investigator has also access to a Timeline, provided by Splunk, to help build his or her case and future course of action.

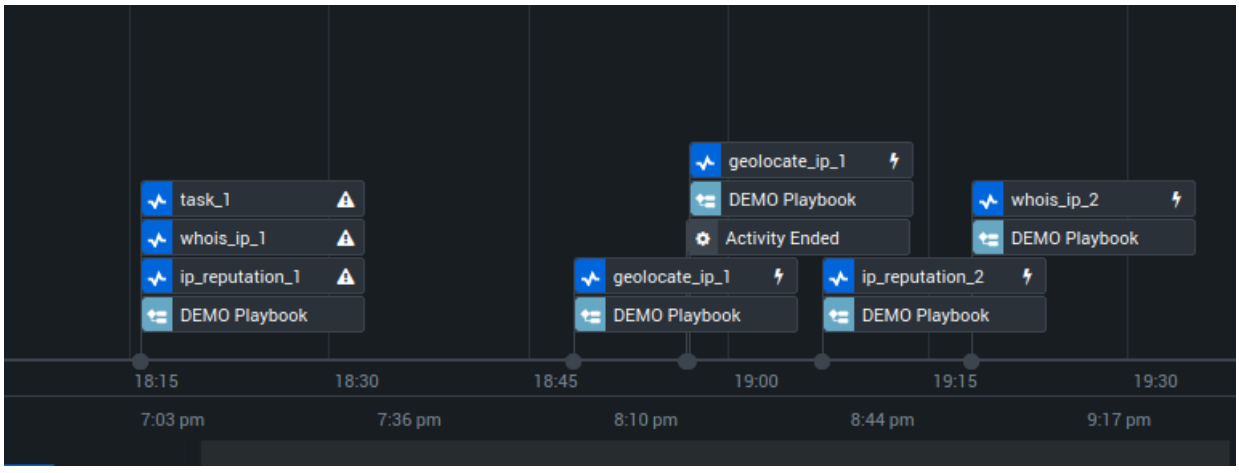


Figure 63: Splunk SOAR Timeline

Using the information provided by the apps in the playbook the analyst can decide whether to close the event as a false positive, investigate further by using a second playbook, or escalate the incident to a higher level analyst.

Siemplify SOAR

For the next scenario, the analyst was engaged in a phishing attack that happened to an employee. The analyst used the Siemplify SOAR to conduct analysis of the attack and the attacker was simulated by one of the platform's out of the box Use Cases. Fistly, all the necessary integrations were installed, in order for the use case to initiate.

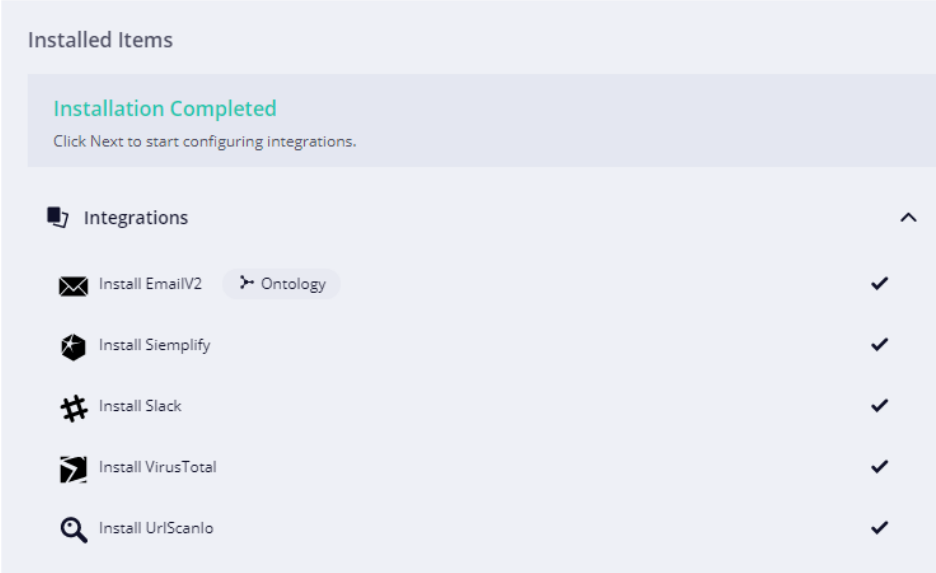


Figure 64: Use Case Dependencies

After the installation, the incident was created in the analyst's initial template, signalling further action.

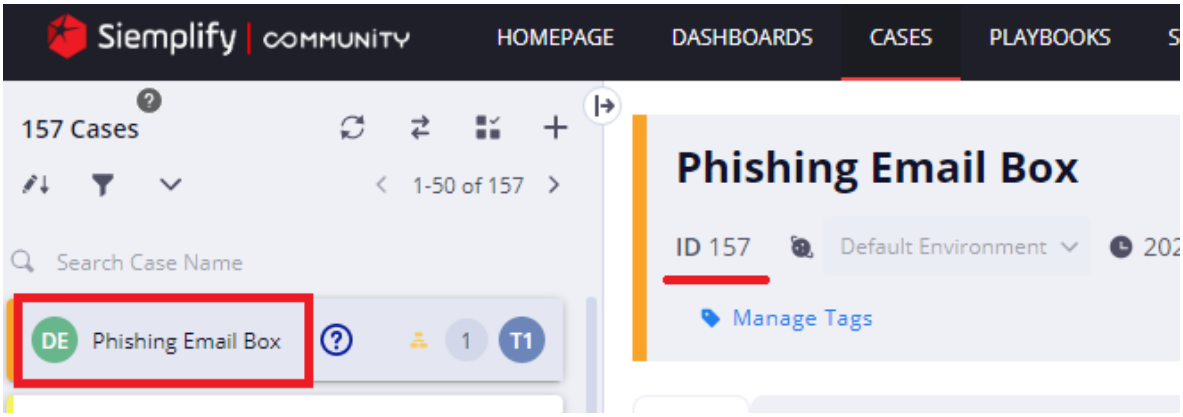


Figure 65: Investigation Initiation

After the initiation phase, the analyst has to conduct an investigation, in order to trigger a response and remediation action. Firstly, the Alerts Highlights provide an initial overview of the incident.

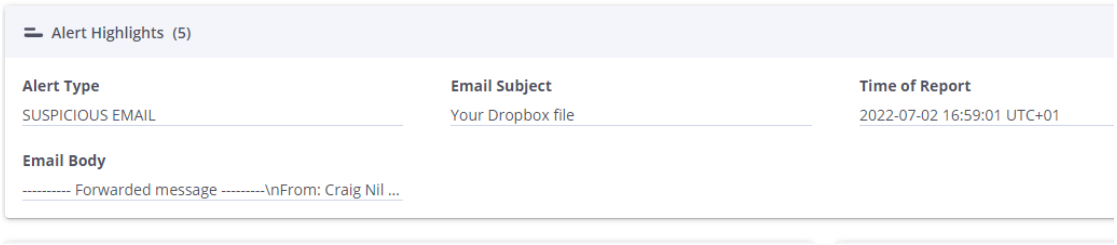


Figure 66: Incident Overview

The analyst retrieves the medium through which the attack was launched (via email) and the phishing attempt involved a Dropbox file. The analyst can also see an overview of the syspicious email, in order to build his or her case.

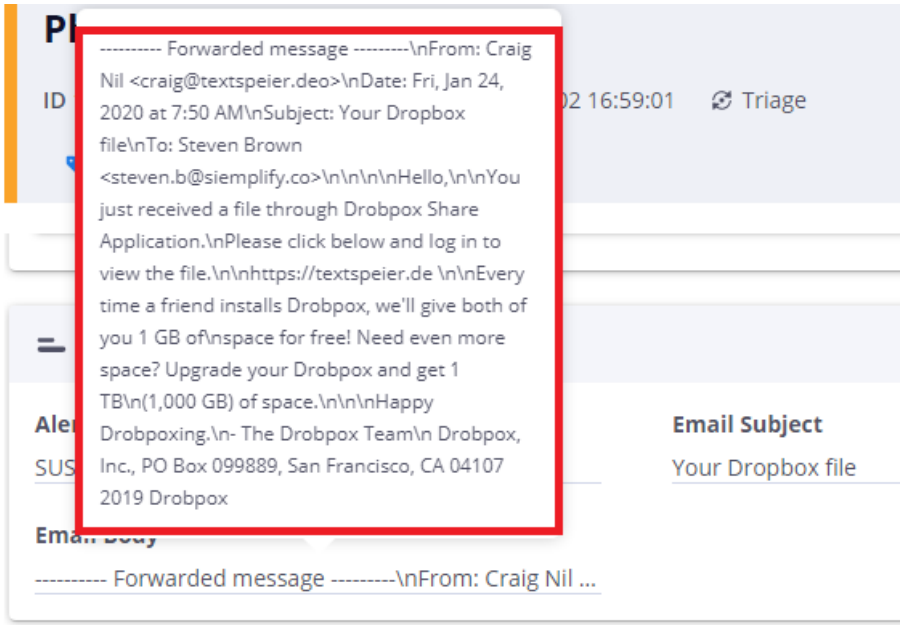


Figure 67: Suspicious Email Overview

After viewing information about the email, the platform provides the analyst a comprehensive view of the attack environment. This can be presented by a visualization, connecting the victim, the potential attacker and all the infected assets of the organization. The investigator also receives information about the victim of the attack, in order to contain a potential breach to the organization internal network.

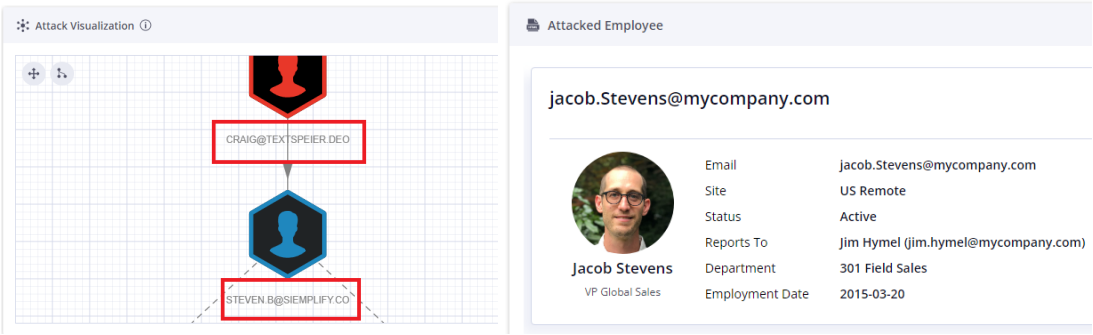


Figure 68: Attack Visualization and Victim Information

Another piece of information that can help the analyst build her or his case is a screenshot from the victim's endpoint, depicting the phishing attempt.

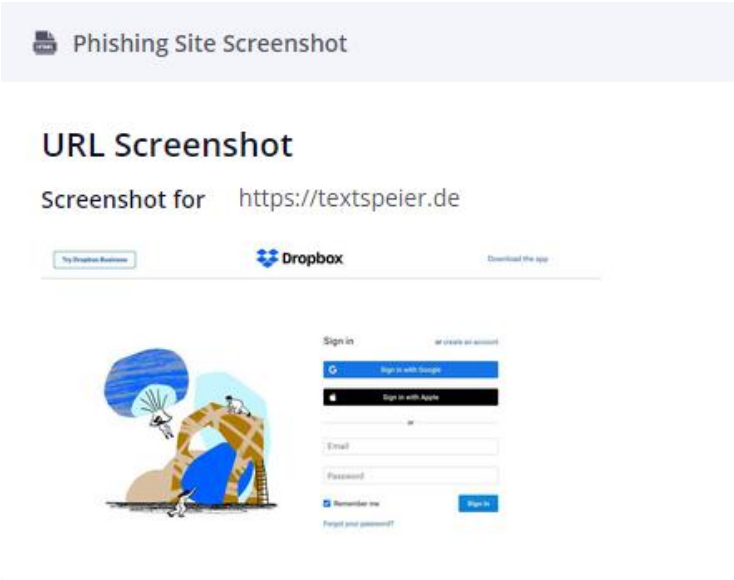


Figure 69: Attack Visualization and Victim Information

As it can be easily observed, the screenshot depicts an exact replica of a Dropbox folder. The analyst has now all the necessary information to initiate response actions. The response is implemented by the utilization of a playbook, containing a set of automated actions. Those actions are represented as nodes of the playbook (in case of XSOAR, they are called tasks), leading to either remediation actions by the platform, or escalation to a higher level of investigation by higher tier analysts.

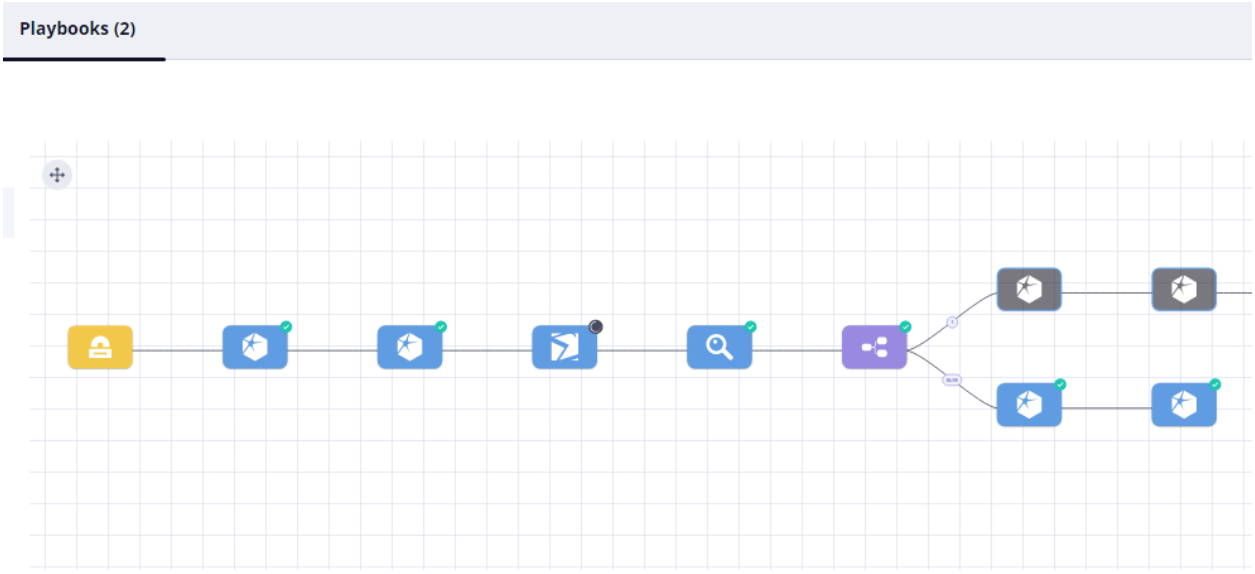


Figure 70: Playbook Overview

The above figure depicts an overview of the used playbook. Each action is connected, leading to a condition. If the condition is *true*, remediation actions are taken against the malicious email. In the opposite case, the risk resulting from the potential attack is marked as low and the case is closed.

Every node, represented an action. In our example, the first action after triggering the playbook was to search for similar past cases, in order to retrieve a potential pattern.

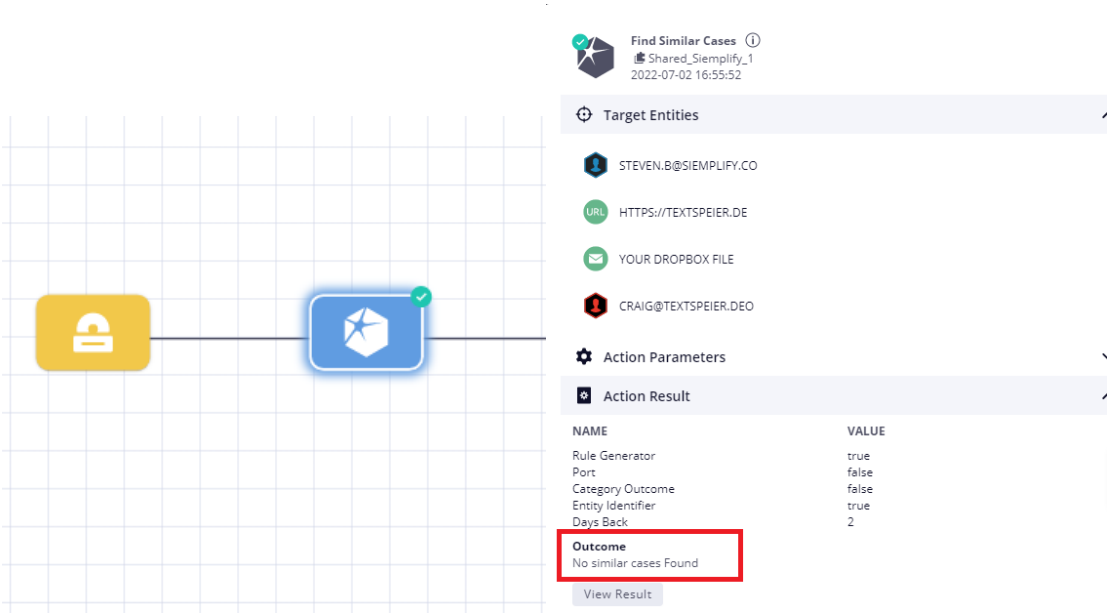


Figure 71: Playbook Actions

In the examined scenario no previous similar cases were found. The flow of actions and questions asked during the implementation, is also depicted below.

Figure 72: Playbook Execution

Each step marked in green represents a successful execution of the requested action. In our case, due to the fact that the data used were simulated, the URL was not malicious and for that reason the platform deems the threat as a low priority, not malicious event.

Conclusions

The analysis and examination of three S.O.A.R. platforms have provided knowledge about their role in a Security Operation Center, their strengths and weaknesses. In terms of their functionality, they are clearly not a standalone solution and act complementary to other security software already deployed in production environments. From the analysis it became clear that the platform was not developed to function as an isolated solution. Its architecture comprises of multiple layers, fairly distinguishable, with features in every layer that can be used by the analysts or investigators in order to mitigate and counter existing or potential threats.

In terms of the data sources provided, the software uses integrations that act as connectors to third party software. This provides support to the analyst, who had to develop and execute multiple repetitive tasks, in order to integrate different third party software to traditional Security Operation Centers. Those connectors are in most cases highly customizable and the analyst with just a few lines of code, or in some cases no code at all, can incorporate sources from threat intelligence, network monitoring, event management, endpoint protection and other solutions.

Although integrating third party software is of significant importance, it could not produce its full potential without extensive correlation capacity. Again, all the platforms provide comprehensive data correlation abilities, giving the analyst the means to engage with investigations, build solid cases and conduct, if needed, threat hunting in order to actively defend against emerging threats.

Another component of the software, that provides support to the users, is that of data visualization. An important problem for modern Security Operations Centers is that different third party software usually demands different monitors, in order to conduct analysis on its data. With S.O.A.R. and its orchestration abilities the analyst has all integrated third party data in one, highly customizable, monitor. With that extra functionality he or she can be engaged in different cases and conduct analysis without unnecessary disturbance.

Last but not least, is the component of automation. This supports the analysts by reducing drastically response times, allowing them to be engaged with and produce more quality results on their analysis and investigations. Automation ability is utilized by the implementation of playbooks or workflows which contain all the steps and the

actions deployed to counter and respond to a security threat. They are designed as flow-charts, and they support the analysts with automated solutions.

All these components were presented and demonstrated in the deployed platforms. Cortex XSOAR from Palo Alto, Siemplify SOAR and Splunk SOAR were deployed in an experimental environment, in different deployment models. The platforms followed similar design patterns, proving that S.O.A.R. is not developed to act as a sole security solution, but as a platform that extends existing capabilities of a modern SOC.

The concept of multiple integrations made the platforms compatible with a plethora of third party software, something that analysts find challenging and time consuming through the repetition of the actions needed. Their work can also be supported by the platforms high level of customization, in order to adapt to every SOC needs.

Threat hunting and data correlation was also provided through a War Room (XSOAR) where the analysts were able to collaborate in real time, or through transferable dashboards and collaboration channels (Splunk SOAR and Siemplify SOAR). All the findings can be presented in highly customizable dashboards, that can help with the decision making process about cases and incidents. After presenting the data, all platforms had report generating abilities, that also help develop a comprehensive view about the impact of potential incidents to the organization.

Also, the platforms' ability to execute simple or complex response playbooks, automating tasks or actions, further established the importance of S.O.A.R. platforms in modern and future Security Operation Centers.

Finally, from the presentation and demonstration, another useful conclusion can be elicited. The low level (Tier I) security analyst was not absent from decision making and response processes in any of the demonstrated scenarios. To the contrary, the level 1 analyst's role was updated to effective and efficient decision making duties, instead of conducting repetitive tasks. This proves that even though SOAR contains extensive automation capabilities, it does not undertake the role of the low level analyst. The software works again complementary to his or her role, providing a set of valuable tools in order to counter emerging threats.

References

Articles

1. Executive Office of the President – Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, available at: https://whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

2. “What is a SOAR?”, by Rapid7, available at: https://www.rapid7.com/solutions/security-orchestration-and-automation

3. “What is SOAR? Definition and Benefits”, by Fireeye, available at: https://www.fireeye.com/products/helix/what-is-soar.html

4. Sharon Shea, SOAR (Security Orchestration, Automation and Response), TechTarget, available at: https://www.techtarget.com/searchsecurity/definition/SOAR

5. “What is SOAR?”, Palo Alto Networks, available at: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

6. Ellyn Kirtley, What is SOAR vs SIEM: Security Solutions Explained, SwimLane, 2022, available at: https://swimlane.com/blog/siem-soar

7. “SOAR Security - What is Security Orchestration, Automation, and Response?”, CheckPoint, available at: https://www.checkpoint.com/cyber-hub/threat-prevention/soar-security-what-is-security-orchestration-automation-and-response/

8. Ali Qamar, “Use a SOAR Security Strategy to Make Your Online Presence More Private”, TechGenix, 2022, available at: https://techgenix.com/soar-security/

9. “Incident Response Automation and Security Orchestration with SOAR”, Exabeam, available at: https://www.exabeam.com/siem-guide/incident-response-and-automation/

10. Rony Sklar, “What is the difference between SIEM and SOAR platforms?”, available at: https://www.peerspot.com/questions/what-is-the-difference-between-siem-and-soar-platforms

11. “Security Orchestration Automation and Response”, Crowdstrike, available at: https://www.crowdstrike.com/cybersecurity-101/security-orchestration-automation-and-response-soar/

12. Jason Miller, “What is SOAR and why do I need it?”, Bitlyft, available at: https://www.bitlyft.com/resources/what-is-soar-how-can-it-improve-detection-and-remediation

13. “What is Security Orchestration, Automation, and Response (SOAR)?”, Cyware, available at: https://cyware.com/educational-guides/security-orchestration-automation-and-response
14. “Why Gartner’s SOAR Model is the Future of IT Security”, Technologent, available at: https://blog.technologent.com/gartner-soar-model-future-it-security
15. Sunil Bakshi , “Improving Efficiency of Security Incident Response Using SOAR”, ISACA, 2019, available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-3/improving-efficiency-of-security-incident-response-using-soar
16. Vladimir Unterfingher, “Security Orchestration Automation and Response (SOAR) Basics: Definition, Components, and Best Practices”, Heimdal Security, available at: https://heimdalsecurity.com/blog/security-orchestration-automation-and-response/
17. Katie Bykowski, “What is SOAR?”, Security Boulevard, 2022, available at: https://securityboulevard.com/2022/02/what-is-soar/
18. “Security Orchestration, Automation and Response (SOAR)”, Gartner, 2017, available at: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
19. Jon Oltsik, “The evolution of security operations, automation and orchestration, CSO, 2018, available at: https://www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html
20. Jon Oltsik, “The rise of analyst-centric security operations technologies”, CSO, 2018, available at: https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html

Documentation

1. “Elasticsearch integration with Cortex XSOAR” Documentation, available at: https://www.elastic.co/partners/palo-alto-networks/
2. Filebeat Documentation, available at: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-installation-configuration.html
3. Snort Documentation, available at: https://snort.org/
4. GreyNoise Documentation, available at: https://www.greynoise.io/
5. Malware Bazaar Documentation, available at: https://bazaar.abuse.ch/
6. Mitre Att&ck Documentation, available at: https://attack.mitre.org/
7. OpenPhish Documentation and Database, available at: https://openphish.com/phishing_database.html
8. Urlscan.io Documentation, available at: https://urlscan.io/about/
9. VirusTotal Documentation, available at: https://www.virustotal.com/gui/home/upload
10. WhoIs Documentation, available at: https://who.is/
11. Cortex XSOAR administrator’s Guide, available at: https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-2/cortex-xsoar admin/dashboards/dashboard-overview
12. Splunk SOAR Documentation, available at: https://docs.splunk.com/Documentation/Phantom/4.10.7/User/Intro
13. Siemplify Documentation, available at: https://documents.siemplify.co/en