SaaS Investigation Tool

Mihai APOSTOL, Bogdan PALINIUC
National Institute for Research and Development in Informatics - ICI Bucharest
mihai.apostol@ici.ro, bogdan.paliniuc@ici.ro

Abstract: Managing security events in a SoC like environment is not an easy task and it can constitute a great challenge, especially for SaaS where the number of security events are overwhelming. Cyber security issues, alerts, events, all need to be investigated and recorded by the SoC analysts and take the appropriate actions. This can be achieved by using a dedicated software application that can manage cybersecurity investigations within multiple computer networks. In this article, it will be described such a software application that can help and drastically increase the SoC analyst's efficiency and the number of security investigations that he can manage. Also, we will focus on how the security event/ alert should be investigated using this proposed software.
Keywords: SoC, SaaS, cyber security investigations, security event, investigation tool.

WHAT IS A SOC?

A SoC (Security Operation Center) is a department directly responsible for the security of an organization regarding network, servers, databases, websites, applications and any other information technology assets. Running 24/7, a SOC is a centralized location where its team is responsible for threat intelligence, vulnerability identification, breach detection, incidence response, identity protection, data protection and access management. In other words, a Security Operation Center is a team of experts who proactively monitor the ability of an organisation to operate securely (Vielberth et al., 2020).

The SoC team is composed of cybersecurity analysts and security engineers, monitoring all the activity on the organization's servers, in databases, networks, but also monitor applications, endpoint devices and websites to identify potential threats to the organization's cybersecurity and counter them as quickly as possible. Also, the SoC team not only identifies security threats, but analyzes them, investigates their source, reports discovered vulnerabilities, and plans to prevent further threats.

Although the number of members in an SoC team varies depending on the size of the organization and the scope of its work, most teams have roughly the same roles and responsibilities. A SoC has a specific role within an organization that uses people, processes and technology to continuously monitor and improve the organization's security posture by preventing, detecting, analyzing and responding to cyber security incidents.

Prevention and detection: from a cybersecurity perspective, prevention will always be more effective and more important. Instead of responding to different threats as they arise, a SoC team monitors the network around the clock, and is able to detect malicious activity

https://doi.org/10.54851/v4i2y202203

and prevent it before it causes damage. When a suspicious event is spotted, it gathers as much information as possible for further investigation.

Investigation: During this stage, the SoC team reviews suspicious activity to determine the nature of a threat and the extent to which it has affected the organization's infrastructure. It looks at the organization's network and operations from a cyber attacker's point of view, looking for key indicators and areas of exposure before they are exploited. The analyst identifies and triages different types of security incidents, seeking to understand how cyber-attacks unfold and how to respond effectively. The SoC Analysts uses information they have about the organization's network and the latest threat research, as well as cyber attacker techniques and trends to effectively triage existing and future security incidents.

Answer: After the investigation stage, the team develops a quick response to fix the problem. As soon as an incident is detected and confirmed, they take action by isolating the affected points, shutting down malicious processes or preventing these processes from running, deleting compromised files or other necessary actions.

Following a security incident, the SOC team works to restore systems and recover lost or compromised data. This may include wiping and rebooting devices, reconfiguring systems or restoring backups. If this step is successful, the network will be returned to its pre-incident state.

WHAT IS A SOC ANALYST?

SoC analysts are among the first ones in an organization to respond to cyber-attacks. They provide intelligence on cyber threats and make improvements to the organizations cyber systems to protect it from attack. To begin with, they analyse security incident reports, then conduct vulnerability assessments and report the findings.

Among the responsibilities of a SoC Analyst we can list (Cichonski et al., 2012):

- Monitoring access security and reporting likely cyber-attacks.
- Performing risk analysis and cybersecurity operations to find existing vulnerabilities that may impact the company.
- Finding security breaches and their root causes.
- Creating reports based on which experts will make changes in the organization's security policies according to its needs.
- Propose strategies to streamline the organization's security.
- Regularly updating the company's cyber security systems to eliminate any risk of cyber-attack.
- Conducting security audits.

SoC analysts have access to a suite of products that can provide insight into the security environment of an organisation. They are trained and certified on the security tools they use and are able to use them effectively.

Security tools include firewalls, intrusion detection and prevention technologies, threat and vulnerability management tools, data loss prevention tools, filtering technologies, traffic inspection solutions, reporting technologies and data analytics platforms. SoC can also access enterprise forensic tools that support incident response investigations.

Using these security monitoring tools, SoC analysts investigate suspicious activity within systems and networks. They can't completely prevent threats from occurring, but they can prevent them from spreading. If a network system is compromised, SoC analysts identify infected equipment and prevent it from spreading to the rest of the network. Analysts can use controls on switches, routers and virtual local area networks (VLANs) to stop the threat from spreading.

SoC analysts would correlate alerts to ensure they represent relevant security incidents. Part of an analyst's role is to contextualize events to understand their impact on the entire cyber system and coordinate real-time response activities with key personnel.

In the event of a security breach, SoC analysts are responsible for proactively notifying those responsible of serious security incidents and mitigating risks before security incidents affect the organization's key infrastructure, and if such an event has occurred, analysts are responsible for ensuring redundancy.

WHAT IS A SAAS?

A SaaS (SoC-as-a-Service) is very similar to a SoC department but it handles more than one company infrastructure. It can handle tens or even hundreds of different networks and companies at a time.

Usually, a SoC department cost and maintenance are very expensive even for a company with a small network and a few employees. As we mentioned before, a SoC department runs 24/7, this means at least 6 SoC analysts, Intrusion detection systems (IDS)/ Intrusion prevention system (IPS) servers, workstations and more. Having these in our view, the cost is already very high for a small to medium business. This is where a SaaS comes in: it's usually based on a monthly or yearly subscription that has a significantly lower cost than a SoC (Vidu, 2020).

By implementing a SoC-as-a-Service solution, an organisation transfers responsibility for cyber security to a team of security specialists. These types of services offer a number of benefits:

Better staffing: Lack of cybersecurity skills means that many organizations struggle to attract and retain qualified cybersecurity staff. A SoC vendor can provide staff to fill this gap.

Access to specialized security expertise: Organizations regularly need access to security experts, such as malware analysts or security architects. These skills are scarce and hard to retain within an organisation. An SoC-as-a-Service provider can provide its customers with access to qualified cybersecurity specialists when needed.

Lower overall costs: Implementing, maintaining and operating a SoC can be quite costly, but by using a SaaS solution, organizations can share the cost of equipment, licenses and salaries.

Up-to-date security: Keeping the tools and applications needed for a SoC up to date is complicated when budgets are tight and the number of vulnerabilities and frequency of cyber-attacks is constantly increasing. A SaaS service provider has the ability to keep the toolset up to date and will provide its customers with state-of-the-art capabilities.

RELATED WORK

Information in how a SoC team manages their investigations are not usually available due to security reasons. Standalone investigation software programs were not found, buy they may be available as proprietary or non-commercial software programs.

Some adopted solutions are cloud based offering an MS-office like environment which is not suitable because it doesn't have features like autocomplete, complex search or other advanced ones beside the ability to have multiple analysts working on the same file but it is known that working with folders, files, documents and spreadsheet tables is not a good idea, especially when you have redundant data constantly coming from sensors.

There are a few IDS (Intrusion detection system) software applications that have a module which allows investigations but with limited control and documentation. Darktrace IDS has an investigation report module (Darktrace Whitepaper, 2020) that allows workstation investigation but not alert investigation. It is based on artificial intelligence and rules for gathering information about the workstation activity. Unfortunately, it takes time for the AI to be trained until the rate of false alerts are low. The module offers information about the device requests, DNS queries, endpoints and some recommendations. Interaction is limited to incident discussion and pinning/unpinning the incident to a dashboard.

PROPOSED SOFTWARE

The Investigation software is a standalone application and not an IDS module because it is needed for multiple clients with different networks and rules. However, it can be integrated as a module in a centralized control interface where all alerts from all networks are displayed in real-time.

Managing investigation can easily be overwhelming for a SaaS, as it can have dozens of clients and networks under the analysts' eyes. Hence, the number of alerts is very high, most of them being only "noise" and false positives

rather than real threats. The proposed software is meant for managing these investigations and the security events. The investigation file, which is a pdf generated document that contains all the information about the specific security event can be sent to the client for informing him of the event and request further action in order to minimize noise events, prevent or mitigate the security event. Also, the file can be sent to the experts responsible for implementing the IDS security rules.

The application can automate some tasks for the analyst: If an alert is documented once, it does not require to be documented again and it will be autocompleted, thus saving a lot of time. It is available for IPs and ports as they give a lot of information about the applications that triggered the specific alert. This information can always be updated by any SoC analyst with their new findings.

Any investigation file will show all related information about the alert, devices, IPs, ports and apps present in any current or previous investigations and also detected in other networks.

The need for this type of application is obvious, as it helps the SoC team to easily manage and investigate any raised alert and be able to communicate with each other regarding their investigation findings. Having so many networks on supervision gets overwhelming.

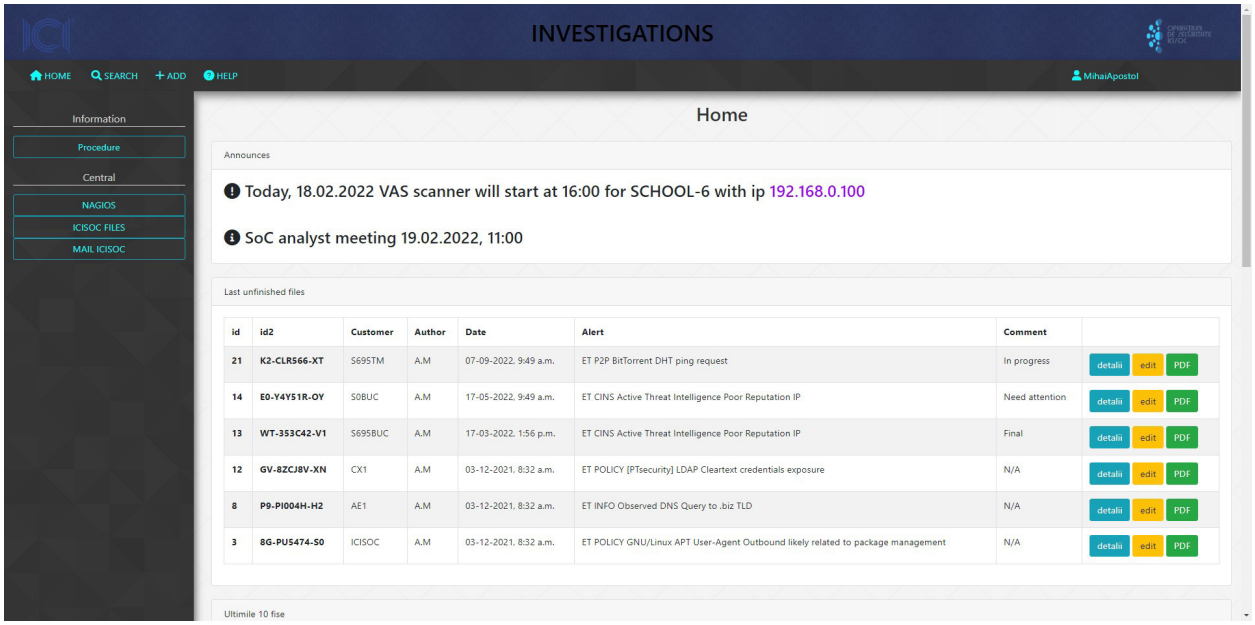


Fig. 1: *Investigation tool homepage*

TECHNOLOGY USED

The development of the web application is based on the Python programming language Django web framework and xhtml2pdf which helps in rendering PDF files using HTML document templates. Also, some front-end features are brought by JavaScript libraries like Bootstrap, TinyMCE, DataTables, Select2 and Datepicker. MariaDB is the relational database used for this application.

It can be deployed using any HTTP/HTTP2 webserver that supports the Django framework like Nginx, Apache or Daphne under Ubuntu 18 LTS and above.

DEVELOPMENT

This application uses the Django default auth/user model. It was not necessary to create a new user model or extend the default one as the default features are enough for the application's purpose: The user can login/logout, request a password change that sends a reset link by email and a profile page. Having permission settings, a user can only be created by an administrator. Users cannot be removed from the database, instead, they can be flagged as inactive by an administrator.

Figure 2 illustrates the database models. The mandatory table that need to be completed in order to open an investigation file is the alert table. Host device table refers to the client device as it can be the source IP or the destination IP of the connection; The same applies for foreign device.

The Page Content table is meant for the home page announcements where the admins can post any type of information (for example, the admin can inform other users to increase their awareness for a certain alert or they can help with a certain investigation) and the procedure page in which the admins can establish investigation procedure and actions. This table mirrors the concept of intranet news.

The software is meant for SaaS but it can easily be modified and used for a SoC by altering the database model clients and all other models that has the clients table as a foreign key.

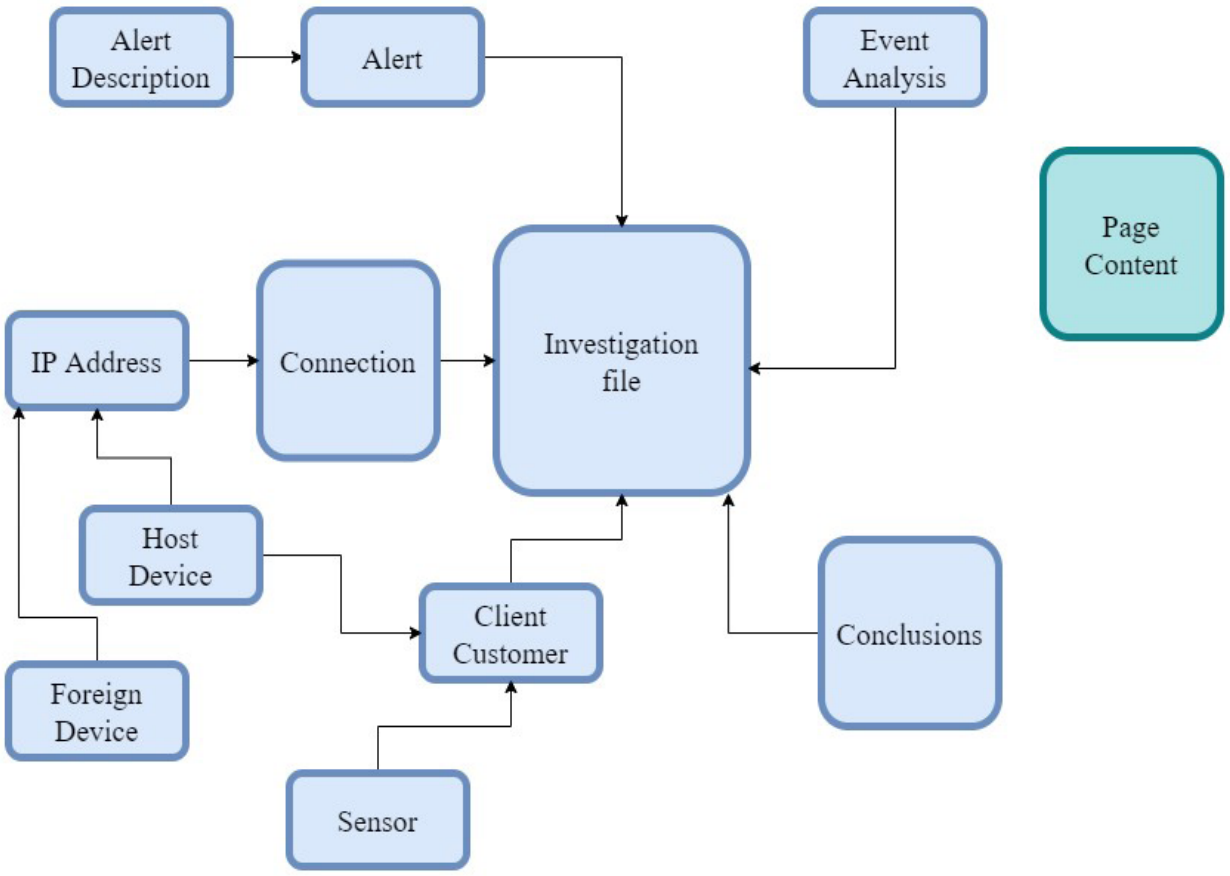


Fig. 2: *Investigation app database model*

MAIN FEATURES

Many important features have been implemented that allow easy investigation over dozens of networks. Automatization is one of the most important ones, as it aims to drastically decrease investigation time by implementing a way to obtain certain information from current or previous investigations and allowing CSV files for automatic handling and insertion of data. Versioning, report management, CSV and PDF file generation are mandatory features facilitating communication with the team, management and clients.

Nothing can be achieved without teamwork. All SoC members can contribute to any investigation process at the same time.

WYSIWYG (what you see is what you get) editors are present to ensure a better structured investigation files and a better reading visibility.

The admin panel allows insertions of news or important tasks for the team as well as basic administration.

Any new investigation file will show related information about the behavior, alert, malicious IPs and apps from the alert and source/destination IPs which are related to previous investigations and also to investigations for other networks. This ensures a lower false positive rate. All IPlike data are differentiated so no confusion can exist between legitimate devices (normal workstation, vulnerability scanner etc.) or malicious foreign ones.

Many other features are present but they are not essential/vital such as access level, advanced search, sensor management and others.

INVESTIGATION FILE

The proposed application is capable of rendering investigation files as PDF files having 5 main sections reflecting the database model in Figure 2:

I. General information: This section offers information about the file itself: The file ID, which is a random generated string of length 12 (10 random and 2 static characters) using capital letters and numbers. It contains the customer Alias (name initials), the creation date of the file and the analyst's initials.

II. Alert: This section is dedicated to the alert documentation. It shows the name of the alert as it appears in the IDS software, alert type, severity and the date of detection or date range in case of multiple same alerts.

III. Connections: In this section, two tables are rendered: The connection table shows all detected connection with source IP, source port, destination IP and destination port. The IPs can be registered with extra information (or added later on) so that it shows the country flag right next to the specific IP. Also, the IP color can be green for knows network IPs, red for foreign malicious IPs, purple for vulnerabilities scanner and black for unknown/undocumented/first seen IPs. The second generated table is a table for used ports. This table is meant for an easy identification of used applications that triggers the alert as it shows the port number, service, a small description and known identified applications that uses the specific port.

IV. Event analysis: This is the most important section in the whole file, it documents the findings of the SoC analyst rendering pictures, text, links and tables. It contains particular information about the alert, device information, malware analysis and other important information with which conclusions and recommendations can be drawn.

V. Conclusions: This is the most important section for the customer as it informs if the event is a positive or a negative one. It also contains tips and recommendations for resolving and mitigating the event or in case of a "noise" event, it only contains a confirmation.

A short example is presented in Figure 3 and 4: A low severity alert regarding torrent activity was investigated. The same alert was investigated in the past for a different customer so the alert description was automatically appended. Also, port 6881 was previously documented so its description and information were automatically inserted. The event analysis section mentions that there is no danger regarding this alert and the destination IPs are not flagged as

malicious. In conclusion, the SoC team needs to know if the customer's security policies allow BitTorrent usage in order to suppress the alert and as a recommendation, the customer needs to scan the specific workstation if the download was not made by a legitimate user.

Investigation File

GENERAL INFORMATION

ID: K2-CLR566-XT **Customer:** S695TM **Date:** 07-09-2022 **Author:** A.M

ALERT

ALERT: ET P2P BitTorrent DHT ping request

ALERT TYPE: Potential Corporate Privacy Violation

SEVERITY: Low **DATE RANGE:** 24-08-2022 -

This alert is triggered when BitTorrent client is detected on the network.

BitTorrent is a communication protocol for peer-to-peer file sharing (P2P), which enables users to distribute data and electronic files over the Internet in a decentralized manner, thus, users exchange files directly with other users.

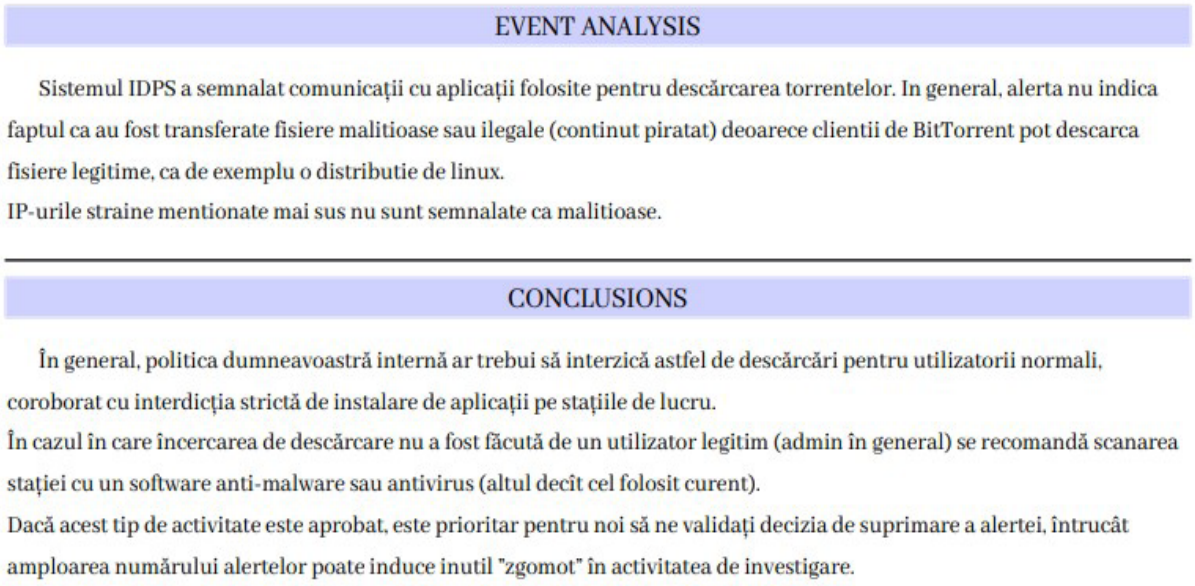
DHT means distributed hash table and is used by BitTorrent clients to find peers via the BitTorrent protocol

CONNECTIONS

source ip	port	destination ip	port
192.168.255.129	6881	94.59.158.61	50177
192.168.255.172	8621	92.4.221.163	8621

Port	service	description	applications
6881	applications	ABC (Another Bittorrent Client), BitTorrent P2P traffic, Azureus P2P traffic (ports 6881-6889)	Bittorrent Client, Age of Conan, World of Tanks, World of Warcraft (WoW) Downloader
50177	N/A	Xsan. Xsan Filesystem Access (Apple storage area network - SAN) Dynamic and/or Private Ports	N/A
8621	irdmi	Intel Remote Desktop Management Interface	EMC NetWorker, Sun Solcitice Backup, iTunes Radio streams

Fig. 3: *Final investigation pdf file part 1*



EVENT ANALYSIS

Sistemul IDPS a semnalat comunicații cu aplicații folosite pentru descărcarea torrentelor. In general, alerta nu indica faptul ca au fost transferate fisiere malitioase sau ilegale (continut piratat) deoarece clientii de BitTorrent pot descarca fisiere legitime, ca de exemplu o distributie de linux.

IP-urile straine mentionate mai sus nu sunt semnalate ca malitioase.

CONCLUSIONS

În general, politica dumneavoastră internă ar trebui să interzică astfel de descărcări pentru utilizatorii normali, coroborat cu interdicția strictă de instalare de aplicații pe stațiile de lucru.

În cazul în care încercarea de descărcare nu a fost făcută de un utilizator legitim (admin în general) se recomandă scanarea stației cu un software anti-malware sau antivirus (altul decît cel folosit curent).

Dacă acest tip de activitate este aprobat, este prioritar pentru noi să ne validați decizia de suprimare a alertei, întrucât amploarea numărului alertelor poate induce inutil "zgomot" în activitatea de investigare.

Fig. 4: *Final investigation pdf file part 2*

INVESTIGATION PROCESS USING THE PROPOSED SOFTWARE

The registration process is implemented as a wizard, including five steps which the SoC analysts must execute in order to complete the investigation file according to SoC procedures.

When the IDS software detects a security issue, it raises an alert that the SoC team can view. The first step taken is to document the alert in the general way – What is the meaning of the alert? What process, event or software is known to trigger that specific alert? After the alert registration, an investigation file can be opened using the newly registered alert.

The next step is to register all the connections that triggered the alert. A connection is represented by a source IP, source port, destination IP and destination port.

This can be done in two ways: if there are a few connections, it can be added manually or if there is a high number of connections, the analyst can prepare a CSV document containing all the connections and upload it in order to register them in bulk. After this, the analyst can document the ports by registering the default service and common applications known for using the ports.

The third step is the most important one: The analyst must document the alert in a particular way, describing what happened, which IPs are responsible for the security event, what is the involved vulnerability and many more information that depends on the alert type. This section can contain screenshots from the IDS software (for example, showing body requests and responses, payloads etc.), from SoC software such as a network protocol analyzer and from external sources such as databases of reported malicious IP addresses.

In the fourth step, conclusions, improvements and recommendations are given regarding the above findings in order to reduce event noise, prevent or mitigate the security issue. After this, the investigation file can be flagged as “completed”.

The final step is to complete the investigation file. This is done by a SoC analyst that has the admin or superuser privileges. This step prevents any incorrect investigations being sent to the client or to the experts responsible for making changes to the security policies and rules.

SOFTWARE IMPROVEMENTS

As with any other software products, new features to implement can always be identified, or the existing ones can be improved, such as geolocation API integration for an easier and shorter investigation time, device identification via MAC address not only by IP can be useful for dynamical networks and many other features.

Other improvements may include the creation of a portal for customers to view their investigation files without sending them via email can eliminate the need to manual send investigation files or, automatically sending a notification email to the customer containing the investigation file.

CONCLUSIONS

It's immediately clear that it is mandatory a software such as this investigation platform to be present in any SOC and SaaS department as it greatly facilitates event investigations, allowing easy management of multiple networks on different sites. In case of a high severity security event, multiple analysts can focus on that single event, improving communication between analysts and having real-time investigation data availability. Also, this software increases the quality of SoC / SaaS offered services, in terms of event reporting. Keeping the client up-to-date with the latest findings will increase the customer's trust.

Investigation modules present on IDS software cannot correlate data with other current or previous incidents and further manual investigations would be needed in these cases, for example, an analyst should know if a certain malicious IP had previously been connected to the network. It is even more difficult in a SaaS environment because investigations become redundant to a certain degree.

Automation plays an important role in cyber security and investigations, saving time and money by eliminating redundant work and implicitly increasing the SoC analyst's cyber security knowledge.

ACKNOWLEDGMENT

The paper has been partly supported by the national PN 19 37 01 02 „Cyber Range for Industrial Control Systems – ROCYRAN", developed in the National Institute for Research and Development in Informatics – ICI Bucharest.

REFERENCE LIST

Cichonski, P., Tom Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Revision 2). Retrieved from Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce website https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

DarkTrace Whitepaper. (2020). D*arktrace Cyber AI Analyst: Augmenting Your Security Team with AI-Driven Investigations.* Retrieved from https://newtech.mt/wp-content/uploads/2020/09/Darktrace-Cyber-AI-Analyst-Augmenting-Your-Security-Team-with-AI-driven-Investigations-1.pdf

Vidu, F. (2020). SOC-as-a-Service. *Romanian Cyber Security Journal*, *2*(1), 69-76.

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access, 8*, 227756-227779. DOI: 10.1109/ACCESS.2020.3045514