Jun Shen

Security Operations Center (SOC) Development for Metropolia Cybersecurity Courses

Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Programme in Information Technology

Bachelor's Thesis

27 May 2025

Abstract

Author:	Jun Shen
Title:	Security Operations Center (SOC) Development for Metropolia Cybersecurity Courses
Number of Pages:	35 pages
Date:	27 May 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	Smart IoT Systems
Supervisors:	Marko Uusitalo, Senior Lecturer

The cybersecurity courses at Metropolia University of Applied Sciences require a Security Operations Center. The objective of the final year project was to build a Security Operations Center for the cybersecurity courses for educational purposes. The Security Operations Center performs the role of monitoring, filtering and analyzing the network traffic for protecting network security. The requirement for the Security Operations Center for the cybersecurity courses was that it is operated in a virtual environment. The virtual environment is based on Proxmox.

The chosen solution for the Security Operation Center utilizes Security Onion, which is a platform that integrates the functions of network defending and monitoring tools.

The process of building the Security Operations Center involved the installation and configuration of Security Onion. Security Onion was installed in a virtual machine on Proxmox. Security Onion was configured with the login account, the IP address and the gateway for Security Onion with an accessible range of hosts and other related information. After the configuration, the operators have been able to access the Security Onion platform by the configured IP address on the local. After building the Security Operations Center, Security Onion has been able to capture data from other local hosts. The Security Onion platform displays data for the operators to investigate the network traffic.

In conclusion, the Security Operations Center for the cybersecurity courses at Metropolia UAS was built after the installation and configuration of Security Onion. The Security Operations Center performs essential functions. However, the configuration of Security Onion needs to be fine-tuned to effectively display alerts.

Keywords: Security Operations Center, Security Onion

Contents

List of Abbreviations

DDoS: Distributed Denial of Service. DDoS is the distributed Denial of Service, which conducts Denial of Service attacks from different sources.

DoS: Denial of Service. DoS is the network attack reduction network speed.

FTP: File Transfer Protocol. FTP is the protocol utilized to transform files through the network.

HIPS: Host-based Intrusion Prevention System. HIPS is a tool utilized to protect the network of the host.

IDS: Intrusion Detection System. IDS is also a tool utilized to protect networks.

IP: Internet protocol. Internet protocol is responsible for addressing and routing data.

IPS: Intrusion Prevention System. IPS is a tool utilized to protect networks.

NGFW: Next Generation Firewall. Next Generation Firewall is the firewall with more functions.

OSI: Open System Interconnection. OSI is a model utilized to describe the network.

SIEM: Security Information Event Management. SIEM is the monitoring tool utilized to monitor network traffic.

SOAR: Security orchestration, automation and response: SOAR is the monitoring tool that can respond to network flow according to predetermined rules.

SOC: Security Operation Center. Security Operation Center is the integrated unit responsible for network security for the organization.

URL: Uniform Resource Locator. Uniform Resource Locator is the address utilized to access websites.

1 Introduction

The Internet has been developing rapidly recently. Companies and other organisations are increasingly relying on the network. Therefore, the importance of cybersecurity is gradually increasing.

The thesis introduces the importance of cybersecurity for business. The categories of attacks and the categories of network security tools are introduced to increase understanding of network security.

Security Operations Centers (SOCs) play an important role in network security. Therefore, the thesis describes what a SOC is and what different categories a SOC can be divided into.

The final objective of the thesis is to present a simple SOC built for cybersecurity courses at Metropolia University of Applied Sciences. The SOC was built to function as a model for educational purposes. The selected SOC solution is a Security Onion solution, which is described in Chapter 6.

2 Importance of Network Security in Business

The network is merged into daily life. Whether enterprises conduct business through the internet or companies manage traditional business, a network is required during the operations. The potential dangers in networking to the business are introduced.

2.1 Networking in Web-based Business

The network performs an essential role for web-based business. For example, e-commerce companies operate business-based on websites. The websites operate based on Internet networking protocols.

The customers engage in shopping by communicating with the e-commerce companies' servers through a series of networking protocols. The customers generally access the shopping website by utilizing the domain name. The domain name is resolved into an Internet Protocol (IP) address, which identifies the communication target. The operations by customers are transmitted to the IP address as data packets. The e-commerce company's server with the IP address receives data packets and performs corresponding reactions. [1.]

Trading between customers and the e-commerce companies is highly dependent on the networking. The attacks on the network can cause significant losses to the company.

Networking also takes part in the internal communication of the web-based companies. The company utilizes networks to promote team collaboration, enhancing real-time information access. [2.]

Confidential business information such as the amount of goods in inventory and supplier information are likely to be stored within internal accessible servers. The internal accessibility of confidential business information ensures efficiency for the company. However, accessibility through networks also means information is at danger.

2.2 Networking in Traditional Business

In the meantime, a network also performs an important role in traditional business. For example, a physical clothing shop in a shopping center conducts business offline. Normally the cash registers and POS terminals need real time access to networks. In addition, there are advertising displays that need network connectivity.

Similarly to the web-based companies, the traditional companies also require devices to store confidential business information. According to the type of

stored information and scale of the company, the trouble caused by data breaching can range in scale.

3 Common Types of Attacks and Malware

There are different types of threat actors, who are intending to conduct cybercrimes. A portion of them is conducting crimes for self-validation whereas another portion is conducting crimes for financial purposes. Aside from the purpose, the threat actors cause problems for companies. [3.]

The network of the company is operated by different types of network protocols. Companies with large scale network infrastructures have a large number of devices in the network. Therefore, the networks of companies are likely to have a certain number of vulnerabilities. The vulnerabilities are the weaknesses that can be exploited by the threat actors.

There is a way to classify the attacks from threat actors. The attacks are categorized as

- Reconnaissance Attacks
- Access Attacks
- Denial of Service (DoS) Attacks.

[4.]

3.1 Reconnaissance Attacks

The reconnaissance attack is the first type of attack to conduct. The reconnaissance attack performs the role of gathering information from the target network. The information gathered is the assistance for the threat actors to conduct further attacks. [5.]

The reconnaissance attack is conducted by different approaches. The public websites, such as Google search and the official website from the target

company, are utilized as the initial step to gather information. The “ping” and port scan are utilized to determine available IP, ports and services from the target network. Vulnerability scanners and exploitation tools are utilized to investigate further information. [5.]

3.2 Access Attacks

The purpose of access attacks is to obtain accessibility to the confidential data from the target company. During access attacks, the vulnerabilities of authentication services, web services and File Transfer Protocol (FTP) are utilized. [6.]

There are several approaches to achieve the purpose of the threat actors. Two of the approaches are described in the following.

3.2.1 Password Attacks

A password attack is a common approach utilized by the threat actors to obtain a password. The attack is performed using password cracking tools. [6.]

3.2.2 Spoofing Attacks

The threat actors can disguise their own device as an authorized device. The approach is considered as spoofing. The disguise can be Mac spoofing, IP address spoofing and other related matters. [6.]

3.3 DoS Attacks

A DoS attack is the type of attack that interrupts or reduces the speed of network transmission. DoS attacks are conducted by sending significant quantity of data or sending the maliciously formatted packets to the network. [7.]

3.3.1 Buffer Overflow Attack

The buffer overflow attack can be utilized in a DoS attack and can also be utilized on access attacks. The threat actor enters the inputs that are unexpected. For example, if the threat actor enters a number that is larger than the expected range of the application on the server, the application cannot handle the input and stores the number in a buffer. [8.]

The threat actor repeats the process and causes a significant quantity of numbers being stored in the buffer. The stored numbers may cost or overwrite memory in the buffer and eventually cause harm to the system. [8.]

The buffer overflow is a common vulnerability that is exploited by the threat actors.

3.3.2 DDoS Attacks

A Distributed Denial of Service (DDoS) attack is similar to a DoS attack. During the DDoS attack, the threat actors conduct DoS attacks towards the same target from a significant number of sources. The DDoS attack is conducted on a wider scale and may cause more serious harm to the target compared to the DoS. [7.]

DDoS attacks require zombies, which are the infected hosts prepared to be the source of the DDoS attacks. The threat actors can prepare the zombies with different approaches. The threat actors may purchase zombies from underground economy. Mirai is one of the malware that is utilized to convert devices into zombies. [7.]

3.4 Malware

Malware is malicious software that is utilized to describe a program or code which can cause harm to systems. Malware often attempts to damage, disable

or invade network devices. The objectives of utilizing malware can be financial, political or demonstrate their competences. [9.]

There are different types of malware. Four types of malware are introduced in the section.

3.4.1 Viruses

The virus is the type of malware that has the ability to duplicate itself within the device. The virus is embedded within the executable file. The execution of viruses is controllable by the threat actor. The threat actor can design the virus to be activated at certain times. The virus searches for other executable files and may intend to infect all uninfected files when it is activated. [10.]

The virus usually requires human assistance to spread. For example, email is a common approach to spread viruses. The USB, CD and other physical devices are also media to spread viruses. [10.]

The purpose of the virus varies. The virus may be executed to display an unsettling image. The virus may be utilized to result in damage to data by the threat actor. [10.]

3.4.2 Trojan Horses

Trojan horse is software with hidden malicious code. A Trojan horse pretends to be innocuous. The Trojan is usually attached to digital games and executed when it is installed on the target device. [11.]

The Trojan horse can perform different roles in cybercrimes. The Trojan horse can result in damage immediately after being installed. The Trojan horse can create a back door and provide accessibility for the threat actors. Periodically, stealing data and transmitting data to the threat actors can also be the role of

the Trojan horse. The difficulty of detecting the Trojan horse is also an issue. [11.]

3.4.3 Worm

A worm is a type of malware that is similar to the virus. The worm has the ability to duplicate itself. However, the worm can conduct duplication by exploiting the vulnerabilities of networks without human assistance. Therefore, the execution of the worm only requires initial participation of threat actors. The worm has the ability to spread itself through the network. [12.]

The duplication of the worm is conducted by attacking the system by exploiting its vulnerabilities. The worm duplicates itself to the attacked system after being exploited successfully. The duplication of the worm between systems can result in reducing the network speed. The worm can also provide a back door for the threat actors to conduct DoS attacks. [12.]

3.4.4 Ransomware

Ransomware is the type of malware utilized to demand a ransom. Typically, a threat actor utilizes ransomware to encrypt the data and systems of the victims. Then, the threat actor demands the ransom to be exchanged for encryption key. [13.]

The cybercrime is conducted by embedding the ransomware malware within email or malicious advertising [13].

4 Defending Tools and Monitoring Tools

There are different types of potential network attacks from the threat actors. The attacks can result in unpredictable loss within the organisation. Therefore, the tools for protecting the network have a significant role. The tools are also utilized in building the SOC.

4.1 Defending Tools

Constantly, there are potential attacks towards the network. Therefore, defending is significant to be maintained consistently. Defending tools can deny most network attacks.

Various defending tools are presented in subsequent sections.

4.1.1 Firewall

A firewall is utilized to monitor, filter and take control of network traffic. The firewall operates based on predetermined rules that are designed by the security team. According to the requirements, the firewall can filter traffic by source and destination IP address, ports of transport and protocol types. [14.]

The firewall protects the network from unauthorized access. Different types of attacks, such as viruses, phishing emails, and DoS attacks, are also the threats that are blocked by the firewall. [14.]

4.1.2 Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are tools that can be utilized to detect network traffic. An IPS protects and denies traffic whereas an IDS warns about potential threat traffic. The IPS is more scalable. The IPS and the IDS are deployed as sensors and detect the network traffic through signatures. The signatures are rules utilized for detection. The detection target includes network attacks and security breaches. The IPS and the IDS also perform the function of information gathering. For example, the IPS detects the traffic and drops the malicious traffic. The information collected in the process is sent to the network security management console as logs. [15.]

The IDS and the IPS have their own advantages and disadvantages. The IDS has the advantage that it does not result in impact on the network. However, the

IDS cannot stop the packet that is detected potentially to be harmful. The IDS is relatively more vulnerable to be deceived by threat actors. [16.]

The IPS can stop the packet according to the detection. The IPS can utilize stream normalization techniques. However, the IPS may result in latency to the network, and false positives can prevent legitimate traffic. [16.]

The selection between the IPS and the IDS depends on the deployer. The combination of IPS and IDS can be utilized as a defending solution.

A host-based IPS (HIPS) is an IPS utilized to protect a crucial computer with significant information. The HIPS can provide the function of private information protection, prevent harmful applications and detect potential threats. [17.]

4.1.3 Next Generation Firewall (NGFW)

A Next Generation Firewall (NGFW) is an advanced device that integrates functions of several security devices. The NGFW is a combination of a firewall, an IPS and a monitoring tool. The NGFW has more advanced functionality, and it can limit traffic based on an actual recognized application, not just IP address and port. [18.]

4.2 Monitoring Tools

Most of the time, the defending tools can protect the network from threat actors. However, unidentified attacks of the defending system may enter the network. Oriented attacks that are designed to exploit the vulnerabilities of the network of the organisation are also difficult to be detected and defended. Therefore, the monitoring tools are important in the situation.

The monitoring tools are utilized to monitor the network traffic. The monitoring tools, for example, perform the functions of gathering information from sources in the network, analyzing and filtering the information and so forth.

Various monitoring tools are presented in subsequent sections.

4.2.1 Network Protocol Analyzers

Network protocol analyzers are a category of programs that are utilized to capture network traffic. The network protocol analyzers provide the visualized user interface for the analysts to investigate the network traffic. The network protocol analyzers can capture traffic in data packets format. Therefore, the analysts can utilize the network protocol analyzers to analyze the real-time traffic in packets during the network attacks. [19.]

The network protocol analyzers provide data that can be analysed and recorded. Therefore, network protocol analyzers are also valuable tools for network development and education after the network attacks. [19.]

There are several options for network protocol analyzers, such as Tcpdump Wireshark. Wireshark is a popular network protocol analyzers tool that is utilized in different platforms. The available platforms include Windows, Linux and Mac OS. Wireshark can perform the function of capturing frames and save the frames to PCAP files. Wireshark can also be utilized to analyse PCAP files, including PCAP files captured by Wireshark and other software. [19.]

4.2.2 NetFlow

NetFlow is a type of Cisco IOS technology that also supports non-Cisco platforms. The information about packets that flow through Cisco routers and multilayer switches is gathered by NetFlow. NetFlow is utilized to monitor network security and analyze the traffic flow. [20.]

The information gathered by NetFlow does not include the content of the flow. NetFlow captures the IP addresses of source and destination devices, the length of the communication period and the quantity of transferred data. [20.]

4.2.3 Security Information Event Management (SIEM)

Security Information Event Management (SIEM) is the technology utilized to gather logs from network devices within the network, manage the logs and analyze the security events. SIEM software is utilized in enterprise organizations. [21.]

The logs that are transformed to SIEM have different categories of sources. The defending tools such as firewalls and IPSs are the source of logs. The SIEM software also includes physical devices, such as routers, switches, hosts and servers as source of logs. [21.]

The SIEM software manages logs from the entire organization and provides the support to detect potential security threats. The SIEM software also provides alerts for detected potential security threats. The alerts provide detailed information about the source, such as usernames of the users and MAC addresses of the devices. [21.]

There are different choices of SIEM software, such as Splunk Enterprise Security and ELK.

4.2.4 Security Orchestration, Automation and Response (SOAR)

The Security Orchestration, Automation and Response (SOAR) performs a similar role as the SIEM software. SOAR and SIEM both perform the roles of gathering information, managing information and analyzing alerts. SOAR can respond automatically based on the rules predetermined by the security team. [21.]

The predetermined playbooks for the SOAR software create rules according to various categories of threats. Therefore, SOAR can perform functions when facing threats. The automation of SOAR provides analysts spare time to handle more urgent threats. [21.]

5 Modern SOC

An SOC is a centralized facility. A team of cybersecurity experts at an organization conduct monitoring, detection, analyzing and responding to security incidents within the SOC. Reducing the influences of the cyberattacks, ensuring the safety of the information assets of organization, and protecting the sensitive data are the primary objective of the SOC. The SOC operates continuously throughout the year, ensuring availability 24 hours a day, 7 days a week, 365 days a year. [22.]

The building of the SOC requires various types of resources. The elements and the categories of the SOC for the organizations in reality are presented in the next section.

5.1 Elements of SOC

The SOC has three major elements. The elements are listed below:

- people
- processes
- technologies.

[23.]

The three elements perform significant roles for functional SOCs.

5.1.1 People

An SOC for a large organisation is required to manage a significant amount of information. It is essential to separate the tasks by categories. There are three types of tier roles for analysts:

- tier 1 alert analyst
- tier 2 incident responder
- tier 3 threat hunter

- the SOC manager.

[24.]

The alert analysts perform the roles of monitoring and verifying the alerts. The verified alert can result in a report that is sent towards the tire 2 analysts. The incident responders are analysts responsible for investigating the received alerts and advise on actions to be taken. The threat hunters are professionals that have expert-level skill in network security. The threat hunters have abilities to investigate the malware and determine the solutions to repair their impact. The threat hunters also participate in deploying threat detection and detection potential threats. The SOC managers are responsible for managing the SOC and performing the roles of contacting the organizations. [24.]

5.1.2 Processes

In the operating of the SOC, the process begins with the security alerts from the SIEM software. The analyst researches the alerts to determine the authenticity of the alerts. The alerts determined to be threat are forwarded to the investigator. [25.]

The incidents that the investigators cannot solve are forwarded to the tier 2 incident responders. The incident responders are responsible for investigating the incidents. While the incident responders are not able to manage the incident, the incident is forwarded to the tier 3 threat hunters. The threat hunters have professional expertise in investigating the incident. [25.]

5.1.3 Technologies

SOC utilizes various categories of security tools to protect the network. The defending tools, such as the IPS and firewalls, are utilized for defending and providing logs.

The monitoring tools, such as the SIEM, are utilized to gather logs and provide visibility into network traffic for analysts.

5.2 Categories of SOCs

There are various categories of SOCs that organizations can consider as options. The categories include the following:

- SOC-as-a-Service
- multifunction SOC
- co-managed SOC
- dedicated SOC
- command SOC.

[26.]

The categories of SOCs have different advantages and disadvantages. The organization requires to research the categories before making a decision based on their own situation.

5.2.1 SOC-as-a-Service

SOC-as-a-Service is a category of SOCs that the SOC-as-a-Service vendor offers as a SOC service to the organisation [26].

The SOC-as-a-Service has the advantage of being cost-effective in that the organisation is not required to prepare resources for the SOC. The disadvantage of the SOC-as-a-Service is that the reliability and quality of the service cannot be ensured. [26.]

5.2.2 Multifunction SOC

Multifunction SOC is the category of SOC that, the network operations and the security operations are placed together [26].

The resources and infrastructure can be shared by the operations for the network and security. An effective method of resource utilization is taking advantage of the multifunction SOC category. However, the distribution of the resource between the network operation and the security operation can result in conflict. [26.]

5.2.3 Co-managed SOC

Co-managed SOC is a category of SOCs that combines external services and internal SOC operations [26].

A co-managed SOC has the advantage that the organisation is able to determine the components to be arranged by external services. The organisation is able to maintain the essential components of the SOC internally. Furthermore, the partially external services reduce the expenses of the organisation. [26.]

The disadvantage is that the co-managed SOC is commonly handled by managed security service providers. The unconsidered selection of cooperators may result in risks. [26.]

5.2.4 Dedicated SOC

Dedicated SOC is a category of SOCs that is operated completely by the organization [26].

The advantage of dedicated SOCs is that an entire SOC, such as people and infrastructure, is considered and managed by the organization. The operation status and managed data logs during the operation of the SOC are visible for the organisation. The SOC can also be designed according to the network of the organisation. [26.]

The disadvantage of a dedicated SOC is enormous expenses. Trained professionals, infrastructure and managing can result in constantly large expenses. [26.]

5.2.5 Command SOC

Command SOC is a category of SOCs that is distributed in different territories [26].

The resource required is very big, and the command SOC is extremely difficult to deploy. The command SOC is a SOC that is available for a very limited number of organizations. [26.]

6 Comparing SOC Solutions

The SOC solution is the structure of building a SOC. There are various categories of SOC solutions.

The goal of the present study was to build a SOC for the security courses at Metropolia University of Applied Sciences. Open-source SOC solutions were considered as optimized options.

Four open-source SOC solutions are presented below:

- Wazuh
- TheHive
- Elasticsearch
- Security Onion.

[27.]

6.1 Wazuh

The Wazuh platform integrates the functions of XDR and SIEM. Wazuh performs log analysis, network monitoring, file security monitoring and configuration assessment. [28.]

The agents that are utilized to support Wazuh are lightweight. The agents can be deployed on various categories of network devices in the organisation. Distributed deployment provides overall visibility of the network infrastructure. [27.]

6.2 TheHive

TheHive is an effective tool that can provide support for SOC. TheHive also performs roles in Computer Emergency Response Teams, Computer Security Incident Response Teams and other security professions that participate in network security incident handling. [29.]

TheHive can collaborate with various security solutions, and it can perform the role of communicating between security tools. TheHive promotes the communication within the SOC teams and improves the efficiency while facing security incidents. [27.]

6.3 Elasticsearch

Elasticsearch is a detection and analytics engine. Elasticsearch is a part of Elastic Stack. Beats is utilized to transform data, and Logstash is utilized to forward data. Kibana provides visualization for the Elastic Stack. The combination of the different parts of Elastic Stack supports the functions required for SOC. [30.]

Elasticsearch provides the function of real-time data analyses. The distributed feature allows Elasticsearch to handle a significant quantity of datasets. The

large-scale community also provides a significant number of additional resources that can be utilized. [31.]

6.4 Security Onion

Security Onion is a SOC solution that integrates defensive tools such as intrusion prevention systems (IPSs) and monitoring tools such as network detection and log management. Security Onion integrates various security tools, such as Zeek, Suricata and Elastic Stack, that are introduced in section 6.3. The combination of the advantages of the various utilized tools provides functionality to Security Onion. [32.]

6.5 Selection of SOC Solution

The SOC built for the security courses at Metropolia UAS is for educational purposes. A valuable feature is that it works in a straightforward way. Security Onion is software that is straightforward in terms of installation and configuration operations. The thoughtfully constructed visualization also results in an uncomplicated platform.

The selection of Security Onion was also determined by the functionality of Security Onion. The combination of the diverse defending and monitoring functions resulted in the platform built by Security Onion to be the most suitable model for education.

7 Implementation of Building SOC

The three elements of SOC are people, processes and technologies. The SOC built for the cybersecurity courses is suitable for education. Therefore, the people element of the SOC was not included in the recent building structure. The technologies and processes are presented below.

7.1 Technologies

The determined solution for building the SOC is Security Onion. It is straightforward to initiate the operation of the SOC using Security Onion. And the SOC had to be built in the laboratory of the university of applied sciences. In general, the laboratory is running within a virtual environment. Therefore, building the SOC can be divided into three phases, which are listed below.

- Creating virtual machine in the virtual environment for Security Onion.
- Installing and configuring Security Onion.
- Determining the status of Security Onion after configuration.

7.1.1 Creating Virtual Machine

The laboratory is operating on the virtualization platform. The virtual environment platform utilized is Proxmox.

Proxmox is a virtual environment platform with open-source server management. The Linux containers, storage, networking and the hypervisor are integrated on Proxmox. Proxmox provides a user interface for managing virtual machines and disaster recovery tools. [33.]

The ISO file of Security Onion was downloaded on the local host to initiate the creation process. Proxmox enables uploading the files into its storage from the local host. Therefore, the uploading function was utilized to upload the ISO file of Security Onion.

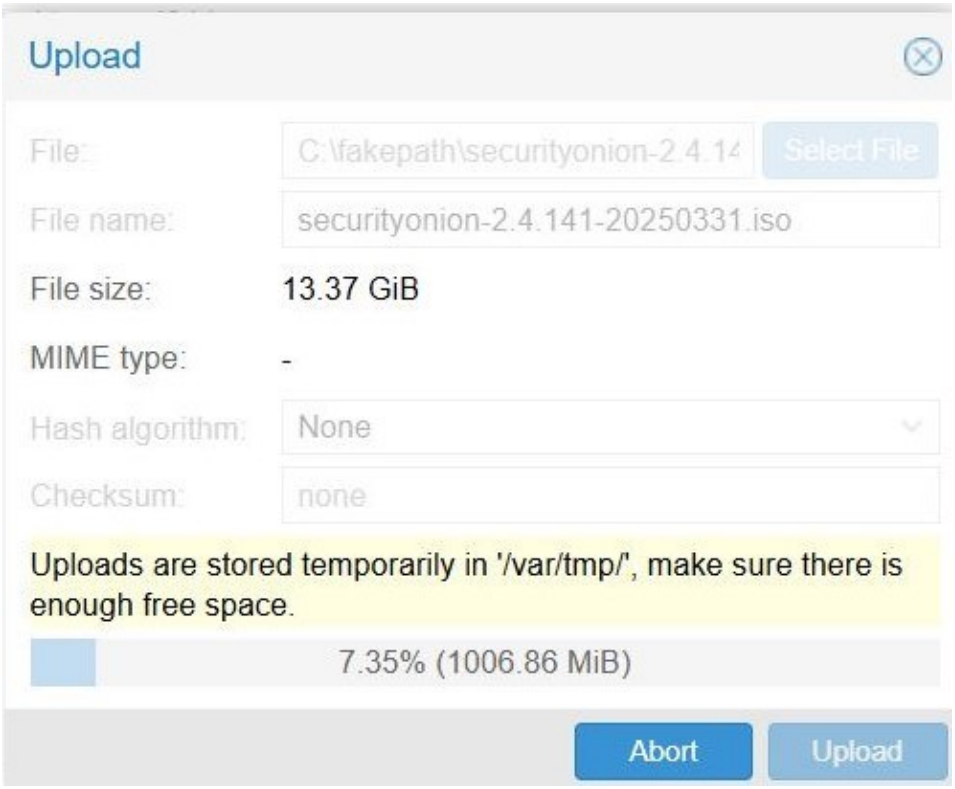

Figure 1. The ISO file uploaded to Proxmox storage.

As presented in Figure 1, the ISO file of Security Onion was being uploaded to storage ‘/var/tmp/’ in Proxmox. The uploaded ISO file was utilized to create the virtual machine for Security Onion.

After the ISO file was uploaded, the virtual machine for operating Security Onion was in the process of being created.

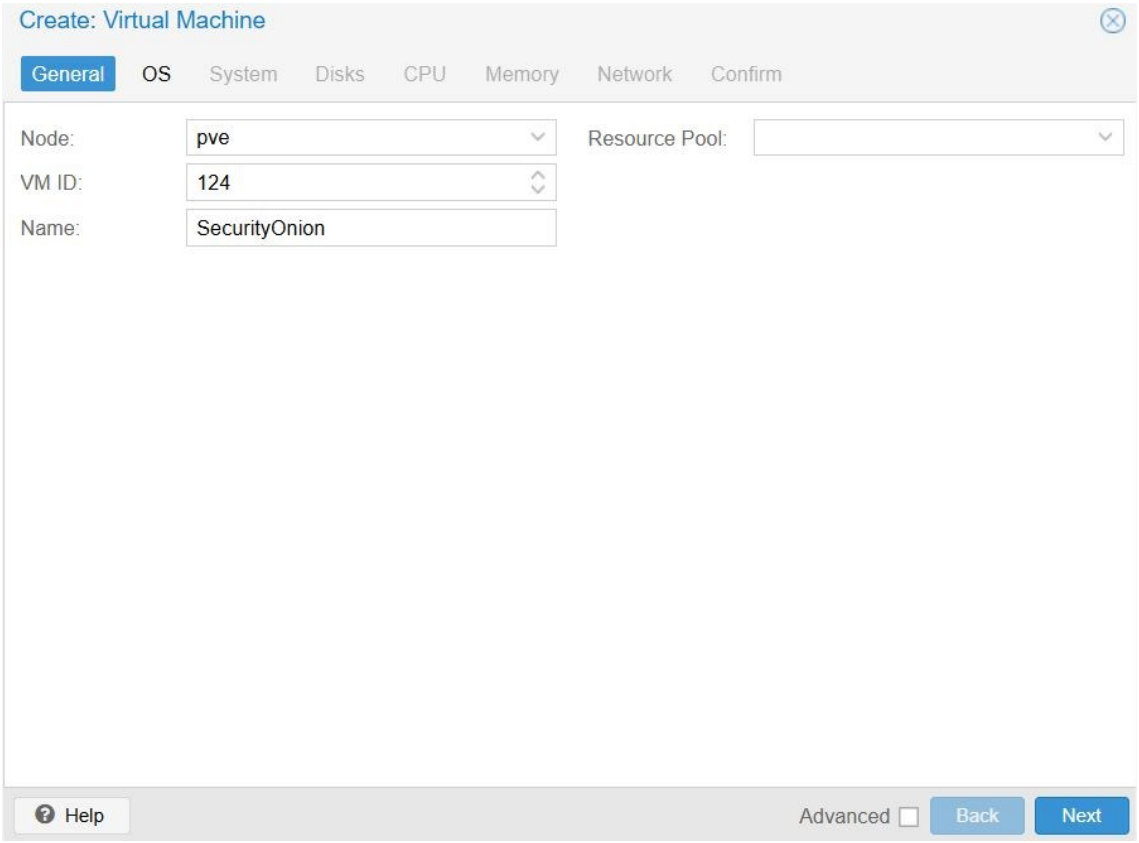

Figure 2. The page for creating the virtual machine.

As presented in Figure 2, the virtual machine was created with an assigned ID on the determined node. The ID is unique for virtual machines that determine the identity of the machine. The assigned ID for the virtual machine of Security Onion was 124.

Figure 2 presents the first page of configuring the virtual machine. The OS, Systems, Disks, CPU, Memory and Network were configured afterwards for the virtual machine.

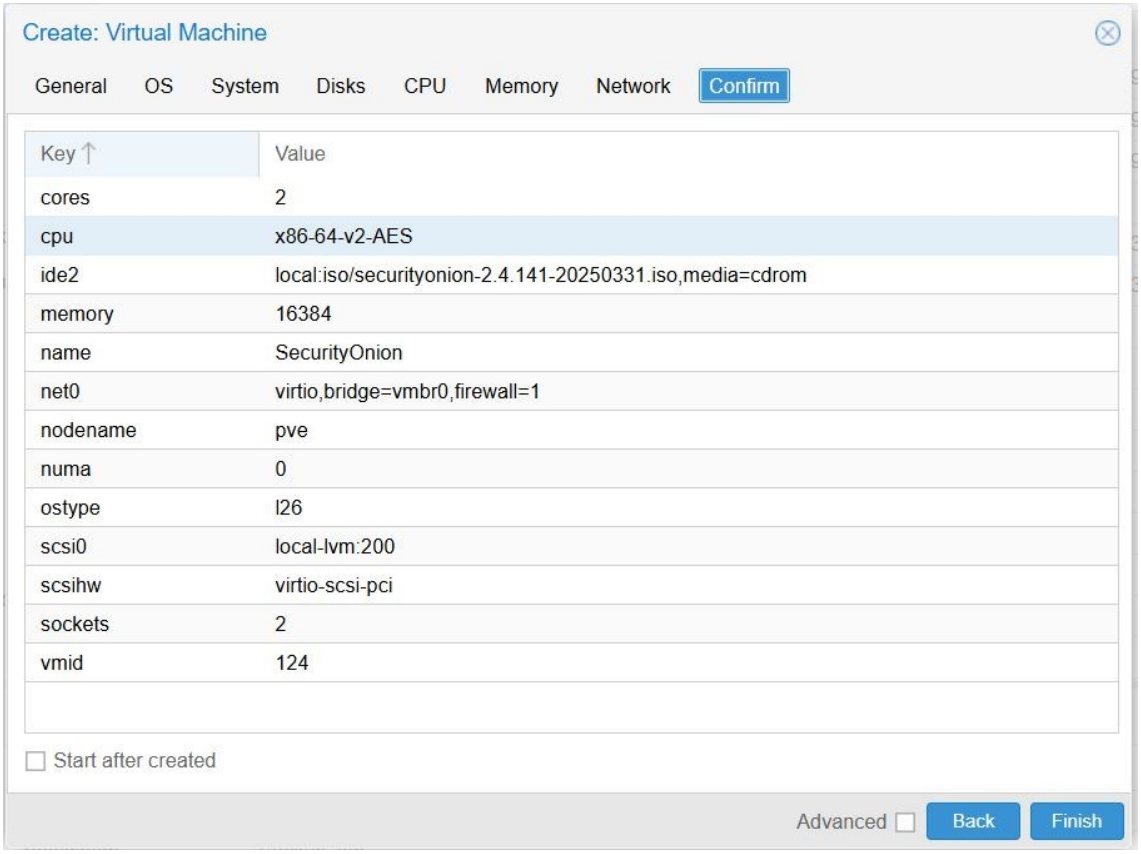

Figure 3. Confirmation page for creating the virtual machine.

Figure 3 presents the confirmation page for creating the virtual machine of Security Onion. The information about the virtual machine settings was displayed on the page. The number of cores and memory were following the instructions provided by Security Onion.

After the configuration, the virtual machine with the ISO file of Security Onion was created.

According to the instructions about Security Onion configuration, the virtual machine requires two network interfaces for configuring and monitoring. The virtual machine that was created has one network interface. Therefore, another interface should be added to the virtual machine.

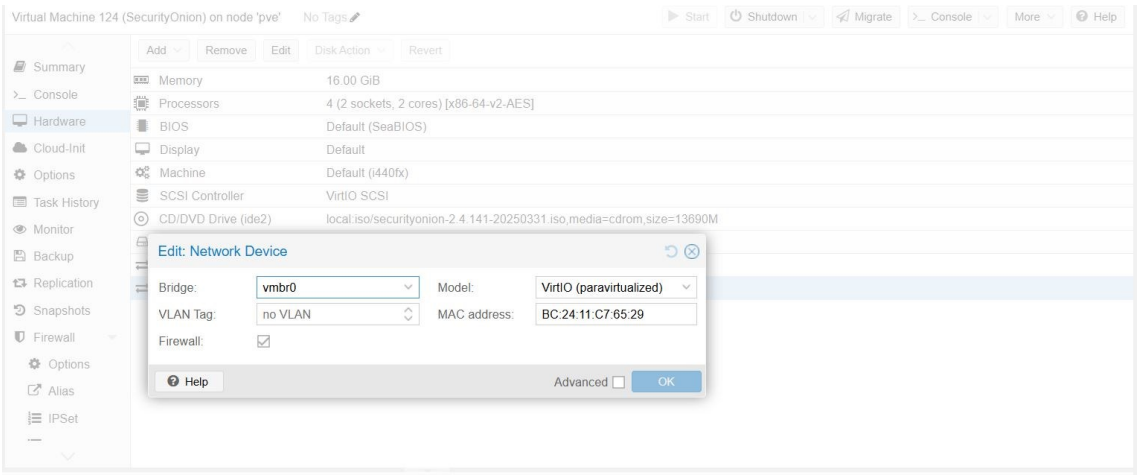

Figure 4. Page adding network interface.

The page presented in Figure 4 is the page for adding the network interface. The chosen bridge was “vmbr0”, which is a Linux bridge.

After the second network interface was added, the virtual machine for Security Onion was created. The following phase was to install and configure Security Onion.

7.1.2 Installing and Configuring Security Onion

The installation and configuration were operated on the virtual machine. Therefore, the virtual machine was initiated first.

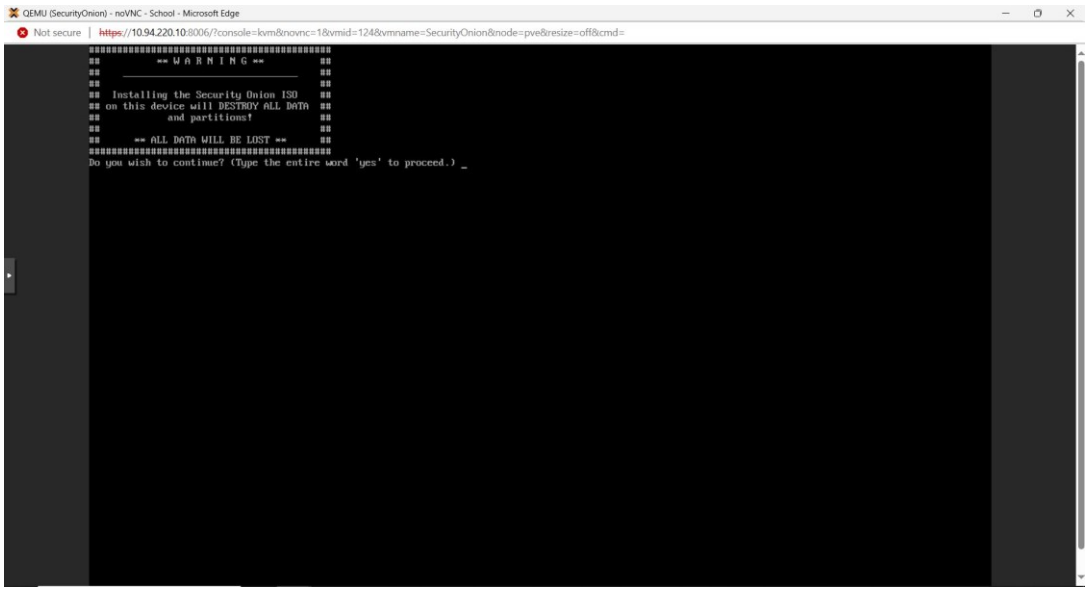

Figure 5. Initial page of virtual machine.

After the virtual machine was initiated, Security Onion was prepared for installation automatically. After entering “yes”, the installation began.

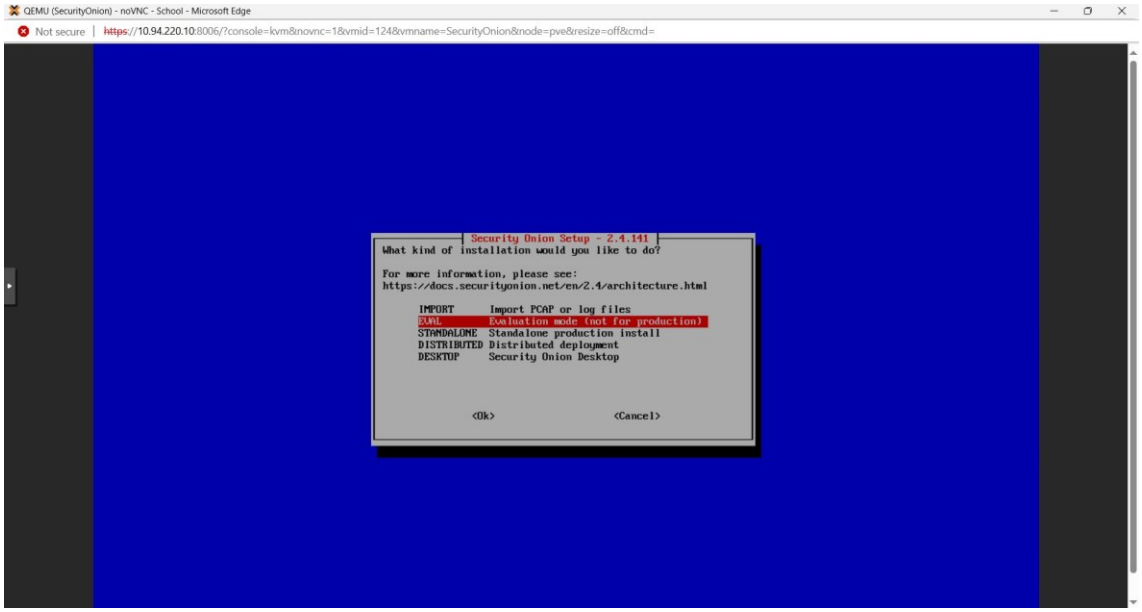

Figure 6. Page request for the version of the installation from the operator.

After the first installation, Security Onion requested for configuration from the operator. Figure 8 presents one of the configuration pages, which shows the system request for the version of Security Onion to be installed.

There are some common options to be chosen for the version of Security Onion. EVAL represents evaluation. This option is the version for classroom and limited scale laboratory usage. [34.]

The standalone version only requires one device, which makes it similar to the evaluation version. The standalone version is utilized in production usage. [34.]

The distributed version deploys the distributed environment. Multiple nodes are required for the distributed environment. [34.]

The standalone version was chosen as the version for the SOC. The standalone version can be utilized for production, which made the standalone version a suitable model for education. Meanwhile, the distributed version requires more resources than the other versions.

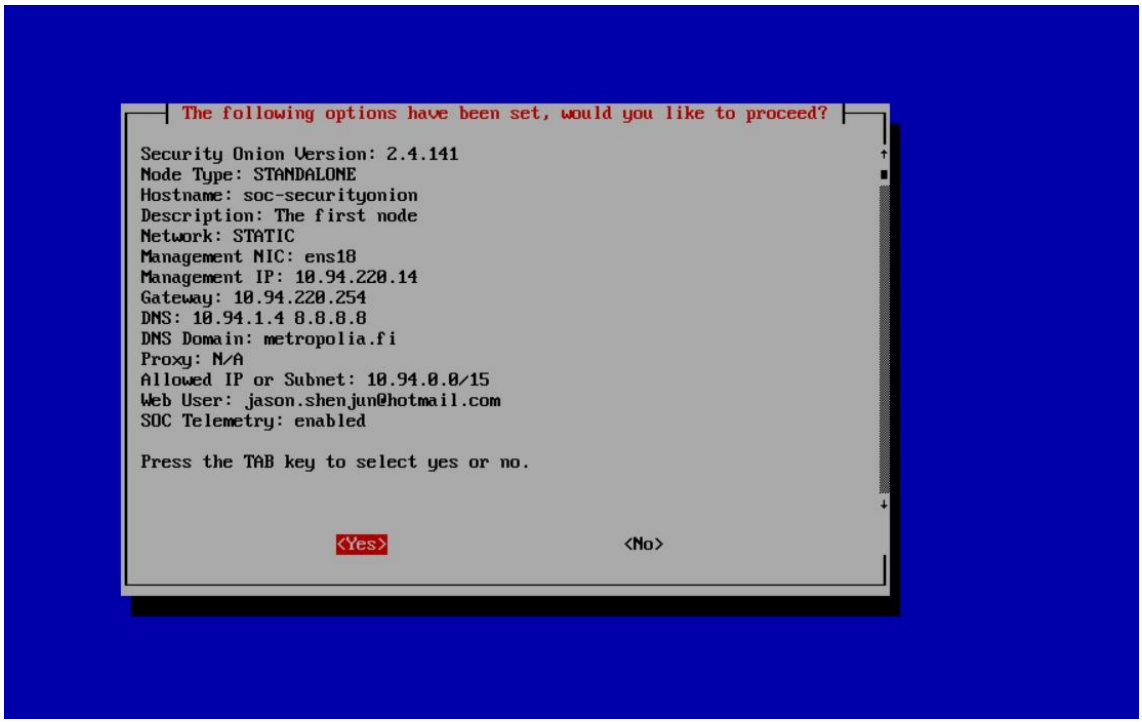

Figure 7. Confirmation page of the configuration.

After the configuration, the system presented the entire configuration for confirmation from the operator, as presented in Figure 7. The second

installation began after completing the configuration. Then, the installation and configuration were completed.

7.1.3 Determining Status of the Security Onion

The login page appeared after the installation and configuration were entirely completed. The preconfigured username and password were utilized to log in to Security Onion. The code seen in Listing 1 was utilized to determine the status of the Security Onion operation after login:

```
Sudo so-status
```

Listing 1. Code determining the Security Onion status.

The operation of Security Onion required preparation time. The operation took around 15 minutes after the virtual machine restarted.

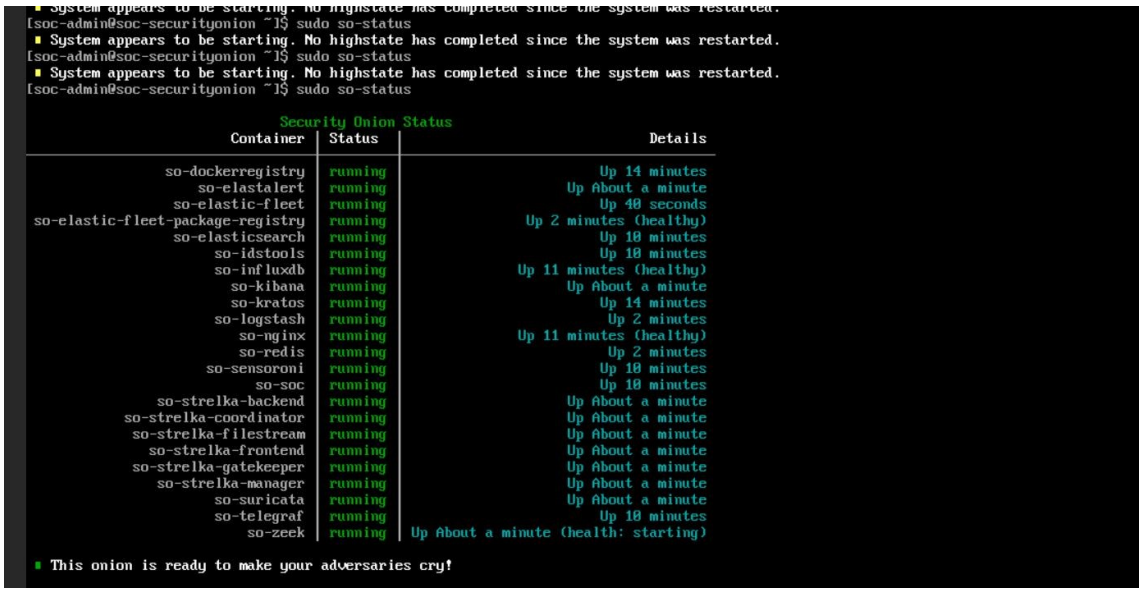

Figure 8. The status indicating that Security Onion is operating.

Figure 8 presents the running containers of Security Onion, which indicates the status of Security Onion, showing that it is operating.

After Security Onion was determined to be operating, the IP address of the management interface could be utilized to access the interface of Security Onion. The IP address was configured during the Security Onion configuration.

The username and password are required to log in to enter the interface. The username was configured as the mail address during the configuration.

Figure 9. Security Onion interface.

Figure 9 presents the interface of Security Onion after login. The dashboard interface that is displayed in Figure 9 shows the overview of data in Security Onion.

Security Onion can gather and manage logs from other security tools. Therefore, firewalls and other devices need to be configured to send log information to Security Onion.

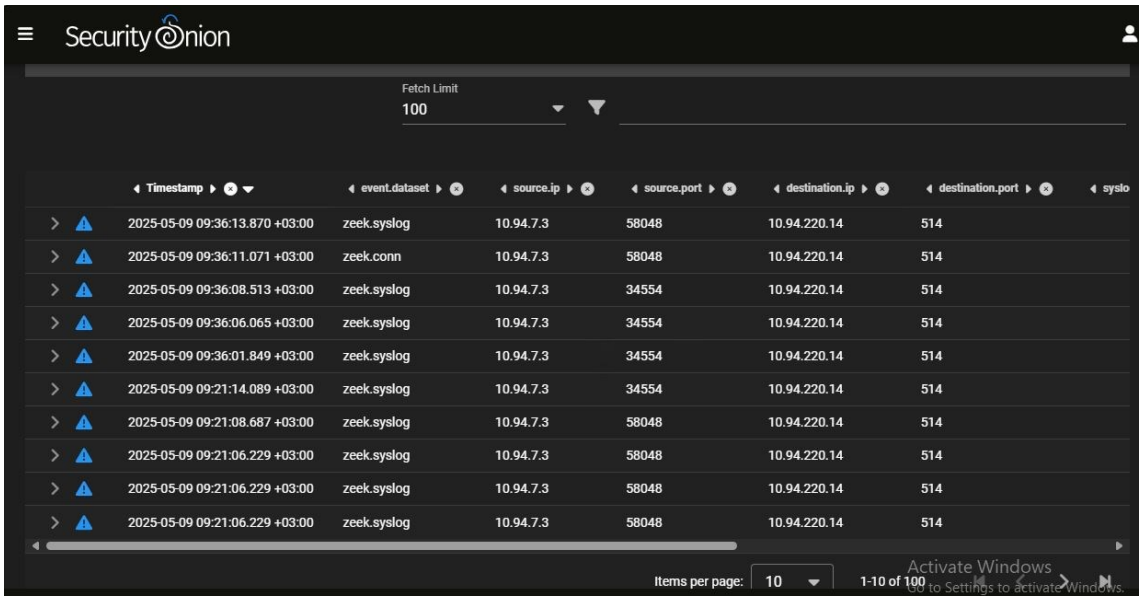

Figure 10. Data captured by Security Onion.

Figure 10 presents the data captured by Security Onion. The data is displayed in the dashboard. There are source IP addresses and ports to determine the initiator. There are also destination IP addresses and ports to determine the target. The time stamp and event type also support investigating.

7.2 Processes in Security Onion

As introduced in section 5.1.2, the process begins with the security alerts from the SIEM software. Therefore, the process of operating Security Onion begins with an investigation of alert pages.

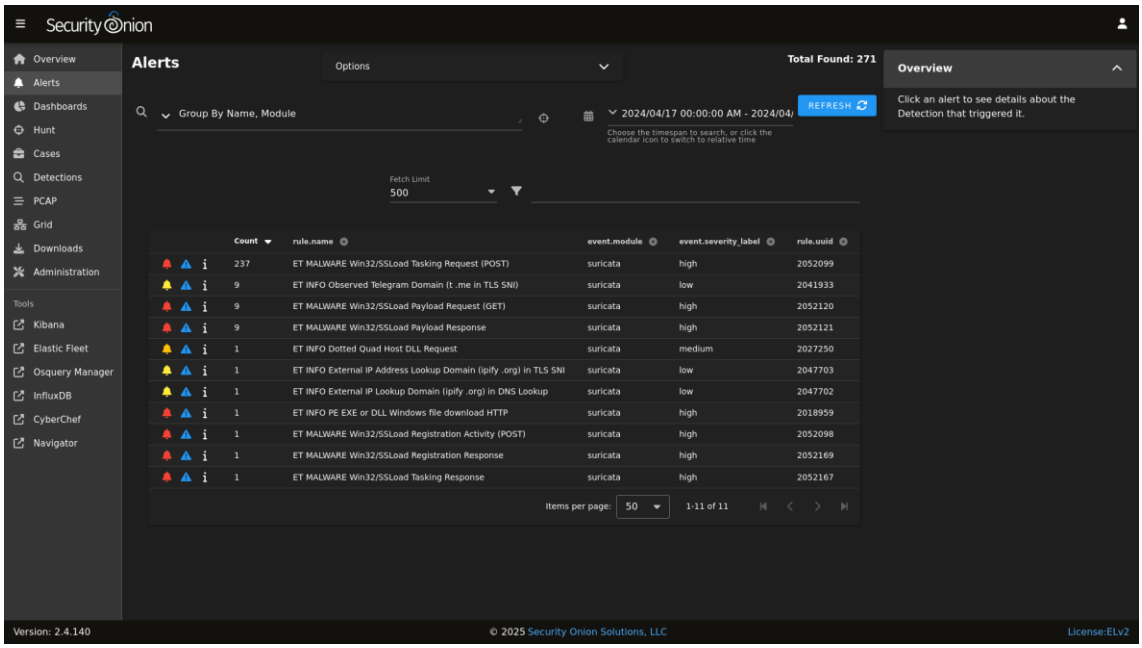

Figure 11. Alert page from Security Onion documentation website [35].

Figure 11 presents the alerts page from the Security Onion documentation website. Security Onion generates and displays information in the alerts page, when it detects threat. The analysts can monitor and analyse the information of potential threats on this page. The analysts can select the alert to investigate.

The people element is removed from the recent SOC. Therefore, the analyst is not required to forward the alerts in the process.

The integrated tools are the advantage of Security Onion. Kibana is one of the tools. The Kibana interface can be entered from Security Onion. Kibana is part of the Elastic Stack that was introduced in section 6.3.

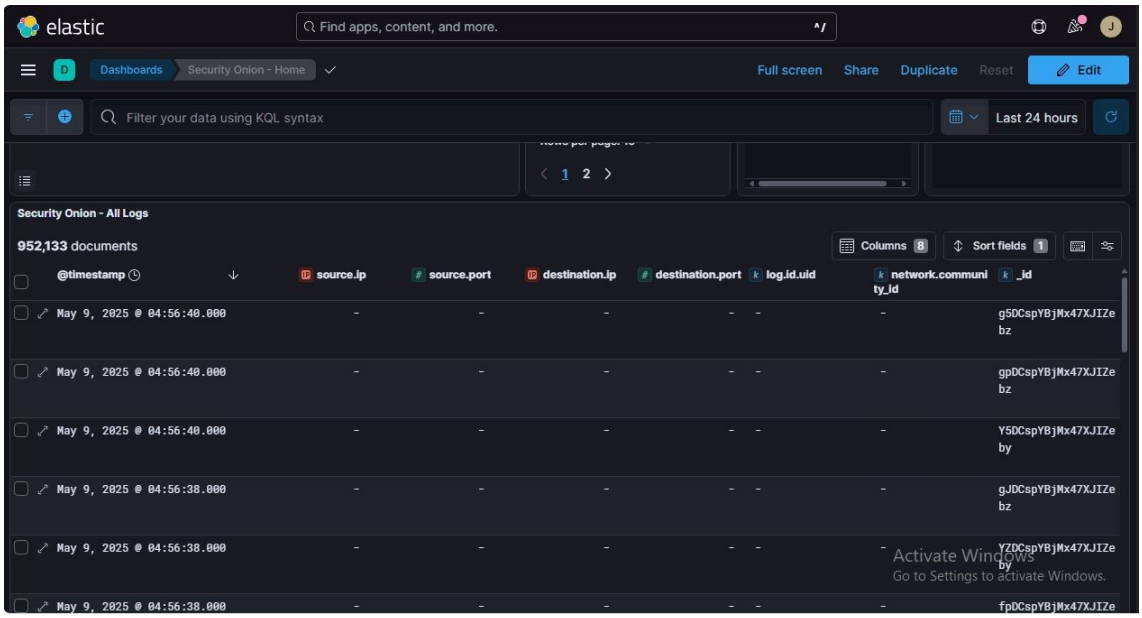

Figure 12. Logs section from the Kibana interface.

Figure 12 presents the logs section on the Kibana interface. Kibana serves as an alternative interface for Security Onion. Kibana provides visualized data to be analyzed for the analysts.

8 Conclusion

The study discusses network attacks and network security protecting. The Security Operations Center (SOC) is discussed in terms of elements, categories and options.

The goal of the study was to build an SOC for the cybersecurity courses at Metropolia University of Applied Sciences. Security Onion was selected as the SOC solution. Security Onion was installed and configured in the Proxmox virtual environment. The status of Security Onion is operational in the virtual machine.

The generated interface of Security Onion is accessible from endpoints in the laboratory at Metropolia UAS. Security Onion is also able to detect traffic flow

from a network. However, the configuration of Security Onion still needs to be fine-tuned to effectively display alerts.

References

1 IONOS editorial team. 2019. How to access websites. https://www.ionos.com/digitalguide/websites/web-development/how-are-websites-accessed/

2 GeoSn0w. 2025. The Role of Networking Technologies in Modern Business Operations. https://idevicecentral.com/guides/the-role-of-networking-technologies-in-modern-business-operations/. Accessed 6 May 2025.

3 Cisco. (n.d.). CyberOps Associate: Module 1, Section 2.1. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=17f3229b-7b08-5959-ac10-1b220017cad6. Accessed 21 May 2025.

4 Cisco. (n.d.). CyberOps Associate: Module 14, Section 2.1. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=784bf3eb-66e2-51a8-9151-4c503858715c. Accessed 21 May 2025.

5 Cisco. (n.d.). CyberOps Associate: Module 14, Section 2.2. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=581f6749-7caf-5c1b-a131-5d5d28dae5cf. Accessed 6 May 2025.

6 Cisco. (n.d.). CyberOps Associate: Module 14, Section 2.4. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=854a7dd7-ebe7-5b47-ac36-4bf4c29c55e9. Accessed 6 May 2025.

7 Cisco. (n.d.). CyberOps Associate: Module 14, Section 3.2. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=6a497d0d-39e9-52cd-b3d5-800abbc9d405. Accessed 6 May 2025.

8 Cisco. (n.d.). CyberOps Associate: Module 14, Section 3.5. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=858a5149-6d23-5b0e-bee9-2e0c0f62d44f. Accessed 6 May 2025.

9 Malwarebytes. (n.d.). What is malware?. https://www.malwarebytes.com/malware. Accessed 6 May 2025.

10 Cisco. (n.d.). CyberOps Associate: Module 14, Section 1.2. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=7189c694-c3ca-5b01-8ef0-1dbd9ea9d312. Accessed 6 May 2025.

11 Cisco. (n.d.). CyberOps Associate: Module 14, Section 1.3. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=18755675-5cbb-563d-97f8-69bad3f5f94f. Accessed 6 May 2025.

12 Cisco. (n.d.). CyberOps Associate: Module 14, Section 1.5. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=3ab0a719-a500-56f6-8f02-5e0f8b821668. Accessed 6 May 2025.

13 Matthew Kosinski. (n.d.). What is ransomware?. https://www.ibm.com/think/topics/ransomware. Accessed 7 May 2025.

14 Fortinet, Inc. (n.d.). What Is A Firewall?. https://www.fortinet.com/resources/cyberglossary/firewall. Accessed 7 May 2025.

15 Cisco. (n.d.). CyberOps Associate: Module 12, Section 2.5. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=72babf25-3093-5765-a238-73d14c9e33a3. Accessed 7 May 2025.

16 Cisco. (n.d.). CyberOps Associate: Module 12, Section 2.6. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=0d30b5dd-2ec0-54cf-872b-14cda4b27000. Accessed 7 May 2025.

17 Antonia Din. 2022. Taking Host Intrusion Prevention System (HIPS) Apart. https://heimdalsecurity.com/blog/taking-host-intrusion-prevention-system-hips-apart/#:~:text=An%20abbreviation%20for%20Host-based%20Intrusion%20Prevention%20System%2C%20HIPS,information%20against%20intrusions%2C%20infections%2C%20and%20other%20Internet%20malware. Accessed 7 May 2025.

18 Cisco. (n.d.). CyberOps Associate: Module 25, Section 3.7. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=3146e102-0c14-59ea-969e-fae4252579fe. Accessed 8 May 2025.

19 Cisco. (n.d.). CyberOps Associate: Module 15, Section 2.2. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=0191a5f7-045d-5b08-8cd6-6405ba93815a. Accessed 8 May 2025.

20 Cisco. (n.d.). CyberOps Associate: Module 15, Section 2.3. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=2107f8d3-c3f6-5329-8449-7ef1b9be38b9. Accessed 8 May 2025.

21 Cisco. (n.d.). CyberOps Associate: Module 15, Section 2.4. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-

c063cb6121ee&tab=curriculum&view=f8964cac-7aba-53b7-aeb5-7ba3adb4faee. Accessed 8 May 2025.

22 SentinelOne. 2025. What is SOC (Security Operations Center)?. https://www.sentinelone.com/cybersecurity-101/services/what-is-security-operations-center-soc/. Accessed 9 May 2025.

23 Cisco. (n.d.). CyberOps Associate: Module 2, Section 1.1. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=e84fe985-b9d5-50c8-844b-2fd64eeeca86. Accessed 21 May 2025.

24 Cisco. (n.d.). CyberOps Associate: Module 2, Section 1.2. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=5d5f6669-5e8b-5d21-8af2-3b2a9ada7023. Accessed 9 May 2025.

25 Cisco. (n.d.). CyberOps Associate: Module 2, Section 1.3. https://www.netacad.com/launch?id=6033098f-f735-405c-9997-c063cb6121ee&tab=curriculum&view=6f7e2ad9-3863-5201-b32c-f84a2df0113f. Accessed 9 May 2025.

26 Ron Samson. (n.d.). Five Security Operations Center Models Compared: Find The Right SOC Model. https://www.clearnetwork.com/types-of-security-operations-centers-soc/. Accessed 9 May 2025.

27 sennovate. (n.d.). Top 5 Open Source Solutions for Building a Security Operations Center in 2024. https://sennovate.com/top-5-open-source-solutions-for-building-a-security-operations-center-in-2024/. Accessed 10 May 2025.

28 Wazuh. (n.d.). Getting started with Wazuh. https://documentation.wazuh.com/current/getting-started/components/index.html. Accessed 10 May 2025.

29 StrangeBee. (n.d.). TheHive Documentation. https://docs.strangebee.com/thehive/overview/. Accessed 10 May 2025.

30 geeksforgeeks. 2024. What is Elastic Search and Why is It Used. https://www.geeksforgeeks.org/what-is-elastic-search-and-why-is-it-used/. Accessed 10 May 2025.

31 geeksforgeeks. 2024. What is Elastic Search and Why is It Used. https://www.geeksforgeeks.org/advantages-and-disadvantages-of-elasticsearch/. Accessed 10 May 2025.

32 Security Onion Solutions, LLC. (n.d.). Security Onion 2. https://securityonionsolutions.com/software. Accessed 10 May 2025.

33 Proxmox Server Solutions GmbH. (n.d.). Proxmox Virtual Environment. https://www.proxmox.com/en/products/proxmox-virtual-environment/overview. Accessed 10 May 2025.

34 SecurityOnion. (n.d.). Configuration. https://docs.securityonion.net/en/2.4/configuration.html. Accessed 12 May 2025.

35 SecurityOnion. (n.d.). Security Onion Console (SOC). https://docs.securityonion.net/en/2.4/alerts.html. Accessed 12 May 2025.