# Decision Support System for Situational Awareness of Cybersecurity Operations Centre

---

**Author:**

Mashael Zaid Alshaikhi

**Supervisor:**

Neetesh Saxena

**Moderator:**

Michael Daley

A dissertation submitted in partial fulfillment of
the requirements for the degree of:

**Master of Cybersecurity**

November 5, 2021

School of Computer Science and Informatics

**Cardiff University**

# TABLE OF CONTANTS

# Abstract

The increasing number of cybersecurity threats and incidents, with the dependence on cyberspace to conduct most of the operations contributed to the need of efficient Cybersecurity Operation Centres (SOCs) to secure the operations of critical infrastructures. However, most of SOCs are facing challenges hindering the cybersecurity operators from achieving cyber situational awareness (CSA) and making an appropriate decision. Therefore, recommending a Decision Support System (DSS) for CSA of SOCs was necessary to speed up decision-making processes in the first place, enhance cyber resilience, reduce threats and vulnerabilities, share information and forecast the extent to which an organisation may suffer a cybersecurity incident in the near future. In addition, we proposed a OOPDA model that supports the concept of achieving CSA must be a continuous (loop) process as well as CSA and decision-making are not separate processes but are strictly connected. To further strengthen the proposed model, various components and tools that would help achieve and maintain CSA have been provided, defined, and classified based on the proposed model (OOPDA).

# List of Figures

# List of Tables

# List of Abbreviations and Acronyms

| | |
|---|---|
| SOCs | Cybersecurity Operation Centres |
| NCSC | National Cyber Security Centres |
| SA | Situational Awareness |
| CSA | Cyber Situational Awareness |
| DSS | Decision Support System |
| CIs | Critical Infrastructures |
| URL | Uniform Resource Locator |
| NCA | National Cybersecurity Authority |
| CND | Computer Network Defence |
| IDS | Intrusion Detection Systems |
| IPS | Intrusion Prevention Systems |
| SIEM | Security Information and Event Management |
| GRC | Governance Risk Compliance |
| UEBA | User and Entity Behaviour Analytics |
| TIP | Threat Intelligence Platforms |
| EDR | Endpoint Detection and Remediation |
| OODA | Observe, Orient, Decide, Act model |
| ECSA | Effective Cyber Situational Awareness model |
| CSAM | Cyber Situational Awareness Model |
| VA | Visual Analytics |
| CRT | Cyber Red Teaming |
| CVE | Common Vulnerabilities and Exposures |
| DSR | Design Science Research |
| GUI | Graphical User Interfaces |
| CSS | Cascading Style Sheets |
| HTML | Hyper Text Markup Language |
| APT | Advanced Persistent Threat |

# Chapter 1: Introduction

## 1.1 Research Motivation

The growing use of cyberspace has reached a point where a wide range of social, political, informational, economic, and military activities are dependent on it (Stone 2015). As a result, computer networks and systems have increased in complexity and sophistication (Husák et al. 2020). Consequently, the need to secure the critical infrastructures through establishing Cybersecurity Operation Centres (SOCs) is becoming paramount. There are conditions that contribute to the success of such centres; there should be a continuous perception of the cyber environment, an understanding of the current security situation, and the ability to project how the situation will evolve, which is referred to as a cyber situational awareness (CSA) (Raulerson 2013; Jirsík 2018). Many studies in the cyber domain confirm the significant role of CSA in cyber security, as it allows cybersecurity operators to deal with the complexity of today's networks and threat landscapes (Franke and Brynielsson 2014). In other words, by building and maintaining CSA, an operator will be able to make an informed decision regarding a security situation.

Further, there has been a fast growth of cyber security threats and incidents in recent years, which the recent reports of SOCs have confirmed, and each year new records have been reached. According to Factoring Chain International (2020) the annual review of the National Cyber Security Centre (NCSC), in the United Kingdom, there was a 10% rise in the number of cyber incidents and a 33% increase in the number of victims compared to 2019. Consequently, they have received around 23.2 million reports of hacking victims and 672,810 reports related to phishing URLs. Due to the increasing rate of cyber threats and incidents with the networks and systems' complexity, recommending a Decision Support System (DSS) for cyber situational awareness of cybersecurity operation centres is necessary to speed up decision-making processes in the first place, enhance cyber resilience, reduce vulnerabilities, manage risks, share information and forecast the extent to which an organisation may suffer a cybersecurity incident in the near future.

## 1.2 Research Statement

Cybersecurity operation centres are considered a new phenomenon around the world (Maathuis et al. 2021). In the United Kingdom, the first NCSC was established in 2016 (Factoring Chain International 2020). While in Saudi Arabia, the concept of these centres was introduced in 2017 (National Cybersecurity Authority 2021). According to Agyepong et al. (2020), Alharbi (2020), and Husák et al. (2020), most of SOCs are facing some challenges that hinder the cybersecurity operators from achieving CSA and making an appropriate decision, e.g., the variety of toolsets, data challenges, and limited budget. The variety in toolsets poses unprecedented challenges for cybersecurity operators to be effective. To clarify, cybersecurity operators will need a variety of information from different data sources to make an informed decision. Therefore, they will have to use monitoring tools, data analysis tools for comprehended data, and then visualisation tools for presenting the results. Thus, the operators have to switch between a number of tools and different analysis workflows to retrieve the needed information, which creates a highly manual-intensive process that hampers cyber operations and CSA. Regardless that every tool has specific properties, functions, and performance to consider. In terms of the data, the volume captured and produced by the used toolsets provides an operator with a massive amount of data, usually in a raw form, which provides little understanding to an operator and negatively affects the resulting decisions. Therefore, there is a need for an integrated tool to improve the decisions by providing CSA on a unified platform and addressing the SOC operations challenges. Based on that, this research will study these questions:

- What are the challenges that hinder the cybersecurity operators from achieving cyber situational awareness and taking appropriate decisions?
- How can cyber situational awareness be improved for cybersecurity operation centres, and which is the suitable cyber situational awareness model to follow?
- What are the requirements to establish a decision support system for the cyber situational awareness of cybersecurity operation centres?

## 1.3 Research Aim and Objectives

The main aim of this research is to recommend a decision support system to provide cybersecurity operators in operation centres the ability to make decisions through achieving cyber situational awareness. The overall objectives of this research are:

- Improve Cyber Situational Awareness for the decision making process
- Identify the general requirements to establish a DSS for CSA of SOCs.
- Recommend a decision support system for CSA of SOCs.

## 1.4 Dissertation Organization

This dissertation's structure is organised as follows:

**Chapter 2 Background and Literature Review**: this chapter will explain the background of the most related information of the research pillars, which are the decision support system, the cybersecurity operations centres, and situational awareness. In addition, the literature reviews that have been conducted, it is explained in this chapter.

**Chapter 3 Methodology**: This chapter is concerned with explaining the methodologies that have been selected, which are Design Science Research methodology.

**Chapter 4 The System Requirements and Design**: in this chapter the basic requirements for establishing DSS for CSA of SOCs are outlined. Further, the recommended system is explained.

**Chapter 5 Results and Evaluation**: this chapter presents the research results after studying and analysing the related work and SA models to improve SOCs CSA as well as decision-making processes. In addition, the recommended system was evaluated based on scenarios of common attack patterns that SOCs teams face frequently.

**Chapter 6 Conclusion and Future Work**: it summarizes the research results and highlights the future work.

# Chapter 2: Background and Literature Review

## 2.1 Overview

To facilitate understanding the following chapters, this chapter will concern to explain the general concepts and backgrounds of the research pillars, the decision support concept and system, the cybersecurity operations centres and its operations, and situational awareness. In addition, the literature reviews will be presented with three parts.

## 2.2 Concept of Decision-Making

Generally, a decision is a choice. Either a choice about a course of action, a strategy for action, or a choice leading to a particular required objective (Druzdzel and Flynn 2011). Therefore, the concept of decision-making can be defined as a cognitive and non-random process leading to selecting specific courses of action among multiple strategies (ibid). Based on Nadu (2016) , there are five main elements of a decision situation: know the goals, define the relevant alternatives, prioritise the alternatives, observe the decision environment, and the decision-maker's knowledge. A decision-maker should first have goals that must be achieved in a situation, then determine the relevant alternatives and if they can be implemented to achieve goals or solve an existing problem. They must be aware of the internal and external factors of the environment that could influence their decisions. The self-awareness of their capability to make a decision is also critical.

The value of decision-making and the type of decisions vary in an organisation. For example, in a SOC, there are functional levels (Zimmerman 2014). At the first level, the analysts can make various short-term decisions in terms of monitoring, control of operations, and deciding which tasks to solve. At the second level, the experts have distinct roles, such as investigating deeply and making more complex decisions. While at the top level, the managers will be focused on managerial decisions, such as corporate performance, macro-allocations of resources, and long-term decisions. However, at all functional levels, the employees of an organisation make decisions, regardless of their values and types.

## 2.3 Types of Decision-Making

The types of decisions are categorised based on general factors, decisions could be highly structured or completely unstructured, single-stage or multiple-stage, or with or without risk and uncertainty of the outcome (Alexander 2002; Druzdzel and Flynn 2011).

- **Structured decisions:** Decisions made with certainty when well-known procedures are applied readily to all of the stages of decision-making, resulting in standard solutions for repetitive problems. They are distinguished by clear or specific decision criteria and a limited number of alternatives so that their consequences can be known without any complexity.
- **Semi-structured decisions:** Decisions made with a case of risk, which can result in several outcomes. The decision-makers, in this case, should know the risk probability of events occurring, such as taking into consideration the probabilities connected with any uncontrolled input.
- **Unstructured decisions:** Decisions made with a case of uncertainty, in which none of the decision-making stages is structured. They are characterised by a lack of definite decision criteria, difficulty in identifying a precise set of alternatives, and a high level of uncertainty regarding the consequences.

## 2.4 Decision Support System (DSS)

The decision-making process is critical for managing any organisation and should not be based on presumption, intuition or personal judgments. It should rely on automation, scientific, and statistical studies (Khodashahri and Sarabi 2013). Therefore, having a system to support the decision-making process is considered critical. A DSS could be defined as a computerised system that gathers and analyses data and synthesises it to produce comprehensive information that can be used to support the decision-making process(Andersson 2010; Druzdzel and Flynn 2011). Such systems are currently used in different applications, such as medical diagnoses, catastrophe avoidance, agriculture, sustainable development, sales projections, inventory organisation, and cybersecurity. DSSs assist these fields in making more informed decisions, timely problem-solving, and improved efficiency in dealing with issues or operations, planning, and management (Garc 2021). In general, DSSs have a common architecture that basically consists of three components: a knowledge base, user interfaces, and models to infer the decisions. Decision models could be based on algorithms, such as classification trees, neural networks, or fuzzy logic (ibid).

The main objective for DSSs that are being built today is to assist decision-makers through the presentation of information in an easy-to-understand way, generate many types of reports based on user specifications, and visualise information graphically (Galipalli and Madyala 2012). In other words, a DSS can be a counsellor beside a decision-maker. Due to this, DSSs could also be expressed as flexible and interactive computer systems (Khodashahri and Sarabi 2013). Therefore, the existence of these systems in any environment will undoubtedly help to improve and optimise the quality of decisions through creating better realisation since they bring together data and knowledge from different areas and sources to provide users with information beyond the usual reports and summaries.

## 2.5 Decision Support System Characteristics

Although it is difficult to define standard DSS characteristics, the key aspects that distinguish DSS from other systems can be stated as follows, based on Andersson (2010), Druzdzel and Flynn (2011), Galipalli and Madyala (2012):

- Assists the decision-maker in decision-making process.
- Improves the effectiveness of decision-making process.
- Supports the decision-maker at various levels.
- Addresses semi/un-structured decision-making types.
- Creates general-purpose models or a simulation of capabilities.
- Provides a rapid response mechanism to a decision-maker request for information.
- Should be able to provide the required information regarding any decision environment.
- Should be flexible to accommodate a variety of management styles.

- Should be user-friendly and have graphical interfaces.
- Has the ability to access a variety of data sources and formats.
- Has the ability to integrate with other systems or applications.

## 2.6 Cybersecurity Operation Centre (SOC)

### 2.6.1 SOC Definition

For the most accurate definition of a Cybersecurity Operation Centre (SOC), it is defined by what it does. According to Zimmerman (2014), a SOC essentially employs people, processes, and technology to improve an organisation's security on an ongoing basis. It is a team of cybersecurity analysts and experts assembled to monitor, analyse, detect, respond to, report on, and prevent cybersecurity incidents using a combination of technology solutions and a strong set of processes. They monitor and analyse activities on networks, servers, endpoints, databases, applications, websites, and systems around the clock to detect any suspicious activity that may indicate a security incident. Since the timely detection and response of a security incident is critical for the effectiveness of a SOC team, the organisation that employs a SOC team must defend against intrusions and incidents regardless of source, time of day, or attack type (ibid). Further, SOC teams have a responsibility to ensure that security incidents are properly investigated and reported to the national SOC as well.

### 2.6.2 SOC Mission

A SOC is commonly supervised by a SOC manager and contains analysts and experts in specific fields, such as penetration testers, incident response, or threat hunters, for example. The centre might be internal or external to the organisation they serve. As a result, they can range from small (five-person) to large (national) operation centres (Zimmerman 2014). However, the mission statement typically includes the following elements:

1. Preventing cybersecurity incidents through:
   a. analysing threats constantly
   b. scanning for vulnerabilities
   c. deploying the countermeasure

d. updating the security policy continually

2. Real-time monitoring and detecting against any intrusions.
3. Responding to confirmed incidents.
4. Providing cyber situational awareness.
5. Reporting cybersecurity status, incidents, and trends to organisations.
6. Engineering and operating Computer Network Defence (CND) technologies, such as IDS and data collection/analysis systems (ibid).

## 2.6.3 SOC Tools & Technologies

The success or failure of a mission will depend on the ability of a SOC team to understand the indicators at the right time by using a number of tools and technologies. A normal SOC should include firewalls, intrusion prevention/detection systems (IPS/IDS), breach detection solutions, vulnerability assessment solutions, and security information and event management (SIEM) systems. In terms of advanced SOCs (national), it could also have Governance Risk Compliance (GRC) software, user and entity behaviour analytics (UEBA), application and database scanners, threat intelligence platforms (TIP) ,and endpoint detection and remediation (EDR) (Zimmerman 2014).

### 2.6.3.1 Firewalls

A firewall is considered in network security as the first line of defence. It monitors the network traffic and determines whether certain traffic should be allowed or blocked depending on a set of security rules, also called barriers. These security barriers are established between the trusted secure internal networks and any untrusted outside networks, such as the internet. These barriers could be set up in two locations, either on dedicated devices on the network or the user devices, also called endpoints. A firewall can be hardware, software or both (CISCO 2021).

### 2.6.3.2 Intrusion prevention/detection systems (IPS/IDS)

Intrusion detection is the process of monitoring and analysing events in a system or network for signals of potential incidents, such as security policy violations or threats. An intrusion detection system (IDS) is a piece of software that automates the detection of intrusions. An intrusion prevention system (IPS) is software that combines the capabilities of an intrusion detection system (IDS) with extra features to help prevent events (Arshad et al. 2020).

#### 2.6.3.3 Security information and event management (SIEM) system

SIEMs support many organisations by providing next-generation detection, analytics, and response (Solarwinds 2021). It is essentially a combination of Security Information Management (SIM) and Security Event Management (SEM) systems:

- **Security Information Management (SIM)** systems collect, normalise, and analyse log data from various sources across the network as firewalls to offer a real-time view of events and activity. In some cases, a SIM can automate responses to potential events.
- **Security Event Management (SEM)** systems review specific types of events for real-time threat analysis, visualisation, and incident response. It can also incorporate threat intelligence tools that use up-to-date databases of known attackers to identify suspicious activities like suspect authentications or logins.

The combination of SIM and SEM results in a SIEM designed to simplify and automate important processes. Thus, SIEM monitors and aggregates security log data from a variety of sources to offer an overview of potential network risks that would be practically difficult to identify with standalone, simple technologies or human efforts. However, SIEM will not eliminate the necessity for other security technologies. In fact, it gathers information from these tools to enable the user to analyse and correlate data to improve the situational awareness of what is happening across a system or network (ibid).

### 2.6.4 SOC Operations Flow

In terms of the operational flow inside a SOC, there are mainly two tiers (Zimmerman 2014). **Tier 1** refers to a set of analysts devoted to real-time alert triage, which deals with phone calls and a variety of routine tasks. At this level, the analyst determines if an alert could be suspicious and decides whether a case will be created and escalated to tier 2. The case is then defined according to various categories of potential risk, such as type of incident, targeted asset or information, or impacted mission. As a rule, this level allows a period of between one and fifteen minutes to examine each event of interest to avoid getting behind on the real-time events that come across their consoles. If an event takes longer than fifteen minutes to evaluate, it should be escalated to tier 2 for in-depth analysis. **Tier 2** is where experts accept cases from tier 1 and perform in-depth analysis to determine what happened and what next action needs to be taken. This decision could take weeks because they may need to investigate all the necessary data to determine the event's extent and severity. As tier 2 is not responsible for real-time monitoring and is staffed with more experienced analysts, they are able to take the time to fully analyse each activity set, gather additional information and coordinate with constituents. Generally, the responsibility of tier 2 is to determine whether a potential incident occurred or not.

### 2.6.5 SOC Capabilities

As discussed by Zimmerman (2014) , SOCs have become responsible for providing certain capabilities to satisfy an organisation's network monitoring and defence needs. **Table 1** illustrates a comprehensive list of common capabilities that a SOC may provide, with understanding that it is difficult to cover all of them. One of the main capabilities is continually feeding cyber intelligence into SOC monitoring tools, as it is a key to keeping up with the emerging threats. As a SOC is in a constant race to maintain security with the changing environment and threat landscape, the cyber intelligence includes news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts that help the SOC keep up with evolving cyber threats. This cyber intelligence information must be timely, relevant, accurate, specific, and actionable regarding an incident, vulnerability, or threat.

Truly successful SOCs utilise security automation to become effective and efficient. By combining highly skilled security analysts with security automation, organisations may increase their analytical power to enhance security measures and better defend against data breaches and cyber-attacks.

**Table 1: SOC Capabilities**

| SOC Capabilities | Examples |
|---|---|
| **Real-Time Analysis** | Call Centre, Real-Time Monitoring and Triage |
| **Intelligence and Trending** | Cyber Intelligence Collection and Analysis, Cyber Intelligence Distribution, Cyber Intelligence Creation, Cyber Intelligence Fusion, Trending, Threat Assessment |
| **Incident Analysis and Response** | Incident Analysis, Tradecraft Analysis, Incident Response Coordination, Countermeasure Implementation, On-site Incident Response, Remote Incident Response |
| **Artefact Analysis** | Forensic Artefact Handling, Malware and Implant Analysis, Forensic Artefact Analysis |
| **SOC Tool Life-Cycle Support** | Border Protection Device O&M, SOC Infrastructure O&M, Sensor Tuning and Maintenance, Custom Signature Creation, Tool, Engineering and Deployment, Tool Research and Development |
| **Audit and Insider Threat** | Audit Data Collection and Distribution, Audit Content Creation and Management, Insider Threat Case Support, Insider Threat Case Investigation |
| **Scanning and Assessment** | Network Mapping, Vulnerability Scanning, Vulnerability Assessment, Penetration Testing |
| **Outreach** | Product Assessment, Security Consulting, Training and Awareness Building, Situational Awareness, Redistribution of TTPs, Media Relations |

## 2.7 Situational Awareness

The most commonly accepted definition of Situational Awareness (SA) in a generic context can be used as a basis for many areas, such as power grids and medicine, is given by Endsley (1988). This definition describes situational awareness as:

> *“The perception of the elements in the environment within a volume of time and* space, the comprehension of their meaning and the projection of their status in the *near future”.*

The words “perception,” “comprehension” and “projection” indicate a progressive increase in the awareness levels from the basic perception of important data to interpretation and the combination of data into knowledge to predict future events and their implications. Situational awareness can be seen from several perspectives; from a technical viewpoint, SA comes down to collecting, processing, and fusing data. On the other hand, the cognitive side of SA concerns the human capacity to understand the technical implications and draw conclusions in order to come up with informed decisions (Gutzwiller 2019).

## 2.8 Literature Review

Three areas were focused on to reach our goals in this research. First, the SOC environment and particularly the challenges that hinder analysts from making an informed decision. Second, exploring how to improve the CSA of SOC, through studying and analysing the prominent research on CSA. Third, focusing on understanding and analysing the related proposed systems.

### 2.8.1 SOCs Challenges

Based on a systematic literature review conducted on papers published between 2008 and 2018 on SOCs, there are twelve challenges the SOC analysts faced, confirming the need for further research to address these challenges (Agyepong et al. 2020). The challenges are shown in **Table 2**, with some of the solutions suggested in the same paper. Whereas in papers by Chamiekara et al. (2018) and Husák et al. (2020), the focus was more on identifying and discussing the contemporary challenges of CSA. In general, they correspond with the previous research. However, they mentioned some new aspects of challenges, such as the volume and variety in toolsets and how they may be considered unprecedented challenges for the cyber operators to be most effective. The volume and variety in toolsets are also confirmed as challenges by a survey in 2017 of 412 IT and security professionals by the Enterprise Strategy Group. The findings were that 40% of respondents use between 10 and 25 security tools, and 30% use between 26 to 50 cybersecurity tools (Analytics 2017). Also, another study conducted in 2017 of financial services organisations by Ovum, a market research firm, found that a majority of respondents 73% are running more than 25 cybersecurity tools, and 9% mentioned that they are running more than 100 security tools (Bricata 2017).

Furthermore, according to Chamiekara et al. (2018) and Alharbi (2020), an insufficient budget is one of the more significant challenges that SOCs currently face. Although there are some automated SOC tools, they proved that they are too costly for some medium-sized organisations and many small-scale companies to utilise. Therefore, in this research, we are interested in addressing some of the SOC challenges described in **Table 2** alongside some suggested solutions from the previous papers that could be adopted for the recommended system.

**Table 2: The Challenges and Solutions**

| Challenges | Suggested Solutions | Interested to address |
|---|---|---|
| **The volume of alerts that are presented to the analysts** | • Limiting alerts to important assets/devices.<br>• Filtering out unnecessary alerts (noise). | ✓ |
| **The number of false alerts (positive/negatives)** | • For reducing false positive alerts, tune policies and machine learning, and businesses can also put in more effort into addressing misconfiguration issues to reduce the burden on analysts.<br>• For reducing false negative alerts, analysts have to rely on other signs on the network, such as using behavioural analytical techniques to identify malicious activity. | ✗ |
| **Incident management complexity** | • Escalation options for experts (tier 2) internal or external of the organisation, to ensure that the impact of any attack is minimised or removed. | ✓ |
| **Sophisticated attacks** | • Analysts have been recommended to depend on their experience to thwart attacks. | ✗ |
| **Lack of skills and experience** | • Periodic training and encouraging the experts to write comments regarding their activities. | ✗ |
| **Inadequate communication between teams** | • Add Chat as a feature.<br>• Enable analysts to add some comments or clarifications when they decide on certain actions. | ✓ |

| | | |
|---|---|---|
| **Tacit knowledge** | • Including playbooks or run books, as well as well-documented processes, that less experienced personnel can refer to when making decisions in SOCs. | × |
| **Manual and repetitive processes** | • Provide a workflow automation for the repetitive security alerts.<br>• Provide ready-made templates for drafting important reports on the system. | ✓ |
| **Workloads and analysts' burnout** | • These challenges are considered an active area of research for finding solutions. | × |
| **The lack of adequate metrics and measures for assessing the efforts of analysts** | • Present the time to detect an incident.<br>• Calculate the average time taken to respond to an incident.<br>• Determine the number of alerts analysed at the end of a shift.<br>• Present the number of tickets closed per day. | ✓ |
| **The volume and variety in toolsets and insufficient budget.** | • New integrated cybersecurity tools and should be open source.<br>• The existing tools should readily share all the data they collect or generate with other cybersecurity tools. | ✓ |

### 2.8.2 Cyber Situational Awareness (CSA)

CSA is considered as a subset of general SA concerning the cyber domain. Therefore, it could extend Endsley's generic definition of SA and define it as:

> *"*The perception of the elements in the **[cyber]** environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near *future"*(Jirsík 2018).

As stated in several sources regarding the cybersecurity domain, improving CSA in an environment will positively affect the decision-making regarding its cybersecurity (Barford et al. 2010; Jirsík 2018). In order to enhance the cybersecurity operations, a SOC will aim to raise the level of CSA, in turn raising the level of decision-making. Several prominent CSA studies and models have been studied, explained, and analysed for this research. The selected SA models will be explained in the following paragraphs, and brief explanations will be found in **Table 3,** while the analysis results are detailed in Chapter 5. The first selected model is Endsley SA which demonstrates how SA provides a primary basis for decision-making in dynamic systems. It consists of three levels: perception, comprehension, projection. It illustrates the applications of SA (decision, performance of action, feedback) and the variables that can influence the development and maintenance, such as environmental and individual factors. However, Artman (2000)  model cannot guarantee success in the cyber domain. The second model is the OODA Loop (Observe, Orient, Decide, Act). It is considered a general model for supporting decision-making processes (Boyd 1996). In spite of that, Klein et al. (2011) describe an approach to fit a cyber defence system into the OODA loop. They mentioned that the "observe" phase could be satisfied by using sensors, such as host monitoring software, IDSs, antivirus scanners, and firewall logging to collect data. Whereas in the "orient" phase, the information from the sensors is classified and associated with data and policies already known in the system to form a better picture of the environment. In the "decide" phase, the system will provide actions that could be appropriate for resolving a problem or optimising the cyber security, taking into account that the final decision should be made by the user. While the "act" phase simply involves fulfilling the newly decided change. Further, there is significant research behind the ARMOUR Project of Defence Research & Development Canada, which was interested in automating Computer Network Defence (CND) capabilities based on the OODA model (Sawilla and Wiemer 2011). For example, the paper by Nakhla et al. (2017) describes the cyber defence integration framework, situational awareness, and automated mission-oriented decision support according to the OODA model. The other model that has been studied built an automated discovery tool for CSA, as proposed by Okolica et al. (2009). This model describes three functions (sense, evaluate and assess) compatible with the Endsly levels (perception, comprehension and projection), as they argue that any SA system must perform these three functions. While the fourth model is the Effective Cyber Situational Awareness model (ECSA) that focuses on a particular type of SA. Specifically, the SA within a computer network through applying network monitoring, thus providing better insight about the network status than regular SA. The next model, presented by Pahi et al. (2017), enhances the protection of CIs at the national level. It can manage cyber security incidents through multilevel monitoring and information-sharing, leading to early detection of sophisticated attacks against national CIs. It is specific and limited to national cybersecurity, whereas this research is aimed to enhance the CSA of limited-scale SOC organisations. The final model, MITRE (Zimmerman 2014), provided one of the significant studies in terms of improving SOC. They also described the practice of gaining CSA related to SOC, and divided CSA into three components: information, analytics, and visualisation. Information such as sensor data, cyber intel, events, vulnerabilities, and threats should be interpreted, processed, and depicted in visual form. They also divided CSA into three related, deeply coupled, and equally important areas: network, mission, and threat.

**Table 3: CSA Models**

| Abbrv. | Model | Focus | The Model Levels Description |
|---|---|---|---|
| **SAM** | Situation Awareness Model (1995) | Cognitive decision-making | 1. **Perception** of the elements in the environment<br>2. **Comprehension** of the current situation<br>3. **Projection** of future status |
| **OODA** | OODA Loop (1976) | Cognitive decision-making | 1. **Observe** involves the perception of some features of the environment.<br>2. **Orient** refers to orienting within a specific environment.<br>3. **Decide** involves deciding what are the next steps.<br>4. **Act** involves implementing what has been decided. |
| **CSAM** | Cyber Situational Awareness Model (2009) | Business continuity planning and CSA | 1. **Sense** - The function includes data gathering through sensors.<br>2. **Evaluate** - The system complies this information into a concept which matches to already existing threat concepts.<br>3. **Assess** - The system predicts possible future activities and attacks. |
| **ECSA** | Effective Cyber Situational Awareness (2014) | Computer networks | 1. **Network Awareness** – the enumeration of assets and of defence capabilities.<br>2. **Threat /Attack Awareness** – the current situation picture of possible attacks and vectors against the network.<br>3. **Operational/Mission Awareness –** the SA of the operation e.g., how decreased or degraded network operations will affect the mission of the network. |
| **NCSA** | Cyber Situational Awareness Model for National Cyber Security Centres (2017) | Information sharing and multilevel monitoring of cyber attacks | Sharing information goes through these levels:<br>**1. Organisations**<br>**2. National Cyber Security Centre**<br>3. **Decision-Makers** |
| **MIRTE-CSA** | MIRTE-Cyber Situational Awareness (2014) | Organisation network, mission, and threats | **1. Information –** Sensor data, contextual data, cyber intel, news events, vendor product vulnerabilities, threats, and tasking<br>**2. Analytics –** Interpreting and processing this information<br>**3. Visualisation –** Depicting SA information in visual form |

After exploring some of the SA models, the following paragraphs will summarise some of the significant research in the CSA field.

Barford et al. (2010) published important paper that summarised some CSA viewpoints of the renowned researchers and highlighted seven aspects of the required awareness for cyberspace. The seven factors to be aware of are: the current situation, the attack impact, the attacker behaviour, how situations evolve, why/how the current situation is caused, the quality of the collected information and potential future situations. Another paper (Gamification 2015) proposed a general architecture for CSA systems, emphasising the need for more research in CSA systems to improve cybersecurity and outlined some of the basic requirements of such systems. Their proposed architecture includes a multi-sensor fusion process, information exchange with trusted partner organisations, enabling operators to modify and add information, and visualisation. They argued that these points are required for achieving proper SA of cybersecurity infrastructure. Tianfield (2017) and Hellesen (2019) have similar opinions about the CSA architecture, stating that it should include data collection, pre-processing and normalisation, internal storage, correlation, visualisation and external sharing. They also confirm a lack of an integrated SA framework for cyber infrastructures, and more research should be done on what else the architecture should include. In addition, Moye et al. (2015) considered a consolidated security information repository and the visualisation of all data stored in the repository with dynamic risk assessment and management as the general requirements to establish a Cyber Defence Situation Awareness System (CDSAS) for MN CD2 Nations and NATO.

It is noted that most of the related research discusses what could be the optimal way to achieve awareness of the cyber domain in terms of definitions and concepts. There are surprisingly few taxonomies or overviews of the required components, particularly from a technical or applied perspective (Husák et al. 2020a). In other words, the fundamental building block of any situational awareness tool (data) is an area that needs more research before it can be addressed. The following paragraphs will present some of the research that partly contributed to defining the data required to achieve cyber awareness in order to integrate the information and reach a complete picture of this research. Evesti et al. (2017) suggest various components and tools used to achieve and maintain CSA by providing a CSA taxonomy consisting of data gathering (operational and strategic), analysis, and visualisation. However, this taxonomy does not conform to the general models and definitions of SA and CSA. It is missing the categorisation of projection level and the related tools and approaches. To overcome the limitations of the Evesti et al. taxonomy, Husák et al. (2020) outlined an updated taxonomy of CSA, which adapted the taxonomy to reflect the three-level model of SA by Endsley. In this paper, Dressler et al. (2014)

discussed six operational data classes necessary to develop a holistic operational picture for establishing SA in cyberspace. The six classes of operational data are: the threat environment, anomalous activity, vulnerabilities, key cyber terrain, operational readiness, and a grip of ongoing operations. They also argue that when a system effectively uses these key data components, it will provide the decision-maker with accurate information and an understanding of the operational cyber environment. Also, the authors confirm the relevance of SA in cyber defence and the benefit of visualisation and sharing information with the operators. In addition, Komárková et al. (2018) present CRUSOE, an extensible, layered data model for attaining and keeping information on cyber situational awareness, through keeping track of missions, systems, networks, hosts, threats, detection and response capabilities, and access control in the network of an organisation.

### 2.8.3 The Related Systems

Although there is an increase in attention for suggesting solutions to provide valuable information and support the CSA, most works were focused on network and visualisation. As noted, visualisation is tightly connected with CSA and plays an important role in situation comprehension. Thus, the use of visual analytic environments for enhancing security is considered one of the commonly proposed solutions. For that, Angelini and Santucci (2015) proposed a Visual Analytics (VA) system based on a geographical view for network monitoring to help security operators understand the impact of security incidents on the mission in real-time. The proposed system has two layers, one for representing the compromised network nodes by highlighting them in red, allowing the monitors to identify them quickly, and the second layer for merging compromised nodes with their impact on the organisation. Although their approach is useful for detecting actually compromised nodes, it does not provide additional information such as the reasons behind it, such as vulnerabilities, or the impact of the mitigation action when conducted. Also, from the network level, Matta and Husak (2021) presented a dashboard for network security management that allows the user to get context to a particular host in the network by presenting its dependencies, fingerprints, and vulnerabilities in a hierarchy tree view. The prominent method of visualising and analysing network security posture is the

CyGraph system introduced by Noel et al. (2016). CyGraph can be used to build a predictive model of possible attack paths, identify critical vulnerabilities, correlate network events to known vulnerability paths, and know the dependencies among mission requirements and the critical network assets. It also offers a variety of analytic and visual capabilities such as dynamics, layering, grouping, filtering, and hierarchical graphs. Nevertheless, several studies have confirmed that the complex tool is too complicated to be used effectively, as it needs an effort to recognise valuable information in such graphs, and it requires a high number of inputs that may not always be provided in practice (Komárková et al. 2018; Matta and Husak 2021). In the same domain of visualising the network attacks paths but with some differences, Yuen et al. (2015) designed an Automated Cyber Red Teaming (ACRT) prototype based on the cyber red team context to improve the network situation analysis capabilities through displaying network attack paths at different levels. The system uses automated planning and knowledge representation techniques to enhance the CSA of human decision-makers. Although they contribute to automating the CRT activities, they admit that the proposed system is in its infancy. Among the attempts to provide an insight into the network, Brosset et al. (2017) made a device for visualising abnormal network events (alerts) in a user-friendly way, using colours, sound and information scrolling. This device can be directly connected to the network monitored in order to aggregate information received from IDS. However, it is still under development and needs some control components such as an administration web page.

As the main contribution of this research is to propose a solution that serves the SOC environment, providing a technical solution regarding the collaboration among SOC teams is required for increasing overall CSA and informed decisions. As each team member works at different levels or has their personal expertise, knowledge and experience that allows them to generate their own awareness for the cyber situation, consequently sharing this awareness with other team members is the key to generating a comprehensive understanding of the overall situation for the purpose of team decision-making. Considering that collaboration is important among a cyber team, Huang et al. (2016) suggest a fuzzy set-based method that allows cyber analysts to quantify their preference and reach consensus decisions on the cyber-attack types that are most acceptable by the entire team. Their suggestion is limited only to determining the attack type, taking a vote on several possibilities and then accepting the highest as a result. Further, the proposed Expert System is a decision support system also based on a fuzzy model for providing SA in national SOCs (Graf et al. 2016). It brings information automatically aggregated from security information systems and expert knowledge to support cyber analysts in the decision-making process of raising alerts. Skopik et al. (2015) introduced a novel model and a system architecture based on incident clustering to secure participating organisations by establishing a (national) situational awareness. Furthermore, Imanimehr et al. (2020) suggested the conceptual architecture of an Information Sharing and Alerting System (ISAS) for addressing the lack of information sharing by collecting cyber information from different CIs and sharing them. Their proposal contributes to enhancing national SA, but they emphasise the importance of sharing information and view it as an obligation rather than a requirement to encounter cyber threats and protect CIs. Oltramari et al. (2013) represent the general requirements for building a cognitive system for decision support with the capability of simulating defensive and offensive cyber-operations by focusing on cognitive and ontological factors and assessing human performance in a simulated environment. The main objective of their approach is to use it in scalable synthetic environments for training human decision-makers, which is close to being a game theory. In addition, the general requirements that were written are useful just for building a simulated system. Furthermore, Roldan-Molina et al. (2017) proposed a decision support system for estimating the cyber risk probability and threat analysis through the semantic level with ontology-based knowledge representation and inference supported by widely adopted standards such as CVE. However, it only accepts one data source (Nexpose) as input and does not support advanced graphical interfaces.

**Table 4** will be summary all the pervious explained system by outlining their limitations, what are the security area that they supported, and if they proposed their systems for a specific target.

## Table 4: The Related Systems

| The related Systems | The target | The supported area | Limitations |
|---|---|---|---|
| **The Visual Analytics (VA) system (geographical view)** | **General** | **VA+ Network security** | ✖ It only aimed to highlight the compromised nodes in the network in red for quick detection process, without additional information. |
| **The dashboard for network security management** | **Cybersecurity teams and SOCs** | **Network security management** | ✖ The visualisation is only for one node of the network.<br>✖ It is semi-automatic, there are some data inputs that should be filled in manually. |
| **CyGraph** | **General** | **Visual Analytics** | ✖ It is a complex tool and too complicated to be used effectively. |
| **The Automated Cyber Red Teaming (ACRT) System** | **Cyber Red Team** | **Network security (attacks paths)** | ✖ Under development, it has not been implemented or tested. |
| **The device that visualises the abnormal network events (alerts)** | **General** | **Network security (alerts)** | ✖ Under development, it has not been implemented or tested. |
| **CSA-support system that based on fuzzy sets of team opinions.** | **General** | **Information Sharing** | ✖ It only aimed to determine the attack type based on collecting the analysts' opinions.<br>✖ Missing the visualisation component. |
| **The expert system that is based on a fuzzy model** | **National SOCs** | **Decision about alert raising** | ✖ The system output is only a numerical value (0 or 1) that presents whether an alarm should be activated or not, without any details.<br>✖ It does not generate a report of the status or suggest remediation actions.<br>✖ Missing the visualisation of the collected information. |
| **The system that based on incident clustering** | **National SOCs** | **Analysis of the incident reports** | ✖ It is specific for establishing a (national) SA. |
| **Information Sharing and Alert System (ISAS)** | **National SOCs** | **Information Sharing** | ✖ It is specific for establishing a (national) SA. |
| **The cognitive system for decision support** | **General** | **Cognitive SA+ simulating cyber operations** | ✖ It is specific for simulating defensive and offensive cyber-operations. |
| **The decision support system (C3-SEC)** | **Information and communications technological infrastructure.** | **Cybersecurity Risk Management** | ✖ It depends on one data source: (Nexpose) vulnerability scanner. |

## 2.9 Summary

In summary, after understanding the research background and reviewing the literatures, some gaps have been noted, and they need to be addressed to improve CSA of SOCs. Firstly, there are number of challenges facing the analysts regarding CSA, they are determined with some solutions that might be taken into account when designing the system. Secondly, to enhance CSA and the decision making process, they must be integrated into a single model. Thirdly, there is a need for identify the data sources that help for achieving CSA. Fourthly, most of the existing proposed systems have limitations. Furthermore, the literature review helped identify the basic requirements for the system and its design.

# Chapter 3: Methodology

## 3.1 Overview Methodology

The underlying methodology for this study is Design Science Research (DSR), a special type of design research that has its roots in engineering, computer science and management, and information systems (Hevner et al. 2004). Design Science is utilised for research projects that aim to enhance human knowledge and organisations' potential by designing and developing artefacts. Artefacts could be ideas, methods, constructs, designed objects, instantiations, models, recommendations, software applications, or new theories (Johannesson and Perjons 2012). All these artefacts have the goal in common of supporting people when they face problems in some practice. An important outcome of this type of research is the effect of the artefact on the environment. Also, DSR aims to generate knowledge about the desired goals and requirements of the artefacts and how to design the artefacts to achieve them (ibid). Thus, conducting DSR is the way to promote this research. In the following sections, the research approach is illustrated in detail with a description of the methods for data collection.

## 3.2 Research approach

This research followed five activities defined by Johannesson and Perjons (2012): explicate problem, outline artefact and define requirements, design and develop artefact, demonstrate artefact, and evaluate artefact. In this case, the focus is on defining requirements and designing a DSS for SOC as a research artefact. The following sub-sections will describe the activities in detail:

### 3.2.1 Explicate the problem

The goal of this exercise is to clarify the practical problem behind the DS process and ask why it is important to address or even investigate its underlying causes. The problem, as defined by Johannesson and Perjons (2012), is an undesirable state of affairs or a gap between the desired state and the current state. In this research, the goal of this activity was to clarify the problems experienced by the cybersecurity operator who has a responsibility to make decisions and why it is important to be solved? Or in other words, what are the underlying causes that hinder the cybersecurity operator from achieving CSA and making an appropriate decision? To answer, there was a focus on gaining knowledge about the environment (SOC), exploring how to improve their CSA, and analysing the existing related works.

### 3.2.2 Outline the artefact and define the requirements

Here, the goal is to outline a solution that can address the explicated problem in the form of a system and defined requirements. The question that this activity addressed was; how a system could be addressed the explicated problem and which requirements on this system are important for the cybersecurity operator? For answering this question, the gained knowledge from the first activity has been used for determining the requirements that should be included in the system to address the problem.

### 3.2.3 Design and develop the artefact

At this point, the goal is to design a system fulfilling the defined requirements in the previous activity. This activity can also be described as designing a system addressing the explicated problem and fulfilling the defined requirements. The result will primarily be illustrations with descriptive knowledge about the design decisions taken and their rationale. Generally, there are two sub-activities in this activity; generate a design or search and select from a number of suitable solutions until obtaining the optimal solution. Thus, the second process is selected for this research, as it can be viewed as a systematic exploration of the solution. In fact, designing and developing a system combines reusing and adapting components from existing solutions and combining them in an acceptable way. Therefore, related solutions have been analysed through studying previous work, both in research literature and systems used in the environment. Regardless of the resources used in creating a design, it is valuable to document the design rationale. A design rationale should contain the reasons and justifications behind design decisions, alternative decisions considered and the arguments leading to the decisions. In fact, a design rationale can be one of the most valuable outputs of a design experiment since it documents the reasoning behind design decisions.

### 3.2.4 Demonstrate the artefact

The goal of this fourth activity within the method is to demonstrate the system use, thereby proving its importance and relevance. In other words, how will the recommended system be used to address the explicated problem? The answer to this question will consist of an account describing how the artefact works in some scenarios. A demonstration shows that the artefact can solve aspects of the problem in illustrative scenarios and help communicate the idea behind the artefact to an audience vividly and convincingly. The selected scenarios could be fictitious, well-documented cases from literature, real-life cases, or a combination of these. Cases from real life typically provide better external validity, but fictitious cases can sometimes be preferable as they can be designed to demonstrate the viability of the artefact under similar conditions.

### 3.2.5 Evaluate the artefact

The goal here is to determine how well the system is able to solve the explicated problem and to what extent it fulfils the requirements. There are two evaluation strategies: ex-ante evaluation, where the artefact is evaluated without being used, or ex-post evaluation, which requires the artefact to be employed in the environment. In our case, the choice was an ex-ante evaluation. The evaluation will be based on reasoning arguments and arguing that the recommended system fulfils the defined requirements and can solve the explicated problem. This form of evaluation is also called informed argument, a common type of claim that the artefact fulfils a requirement because it has a certain design (Hevner et al. 2004).

# Chapter 4: Design and Implementation

## 4.1 Overview

This chapter was divided into two sections: first the basic requirements for establishing DSS for CSA of SOCs are outlined based on the gained knowledge of the literature reviews, second the recommended system (DSS-CSA) is explained according to the proposed model (OOPDA) Observe, Orient, Predict, Decide and Act.

## 4.2 The Basic Requirements to Establish a DSS-CSA of SOC

There is a set of requirements that are provided as a basic information for establishing a Decision Support System for Cyber Situational Awareness of Cybersecurity Operation Centres. The requirements are not exhaustive but they will address some of the essential areas and functionalities. Basically, when a DSS-CSA will be established, it should be based on the following requirements:

- **The system should utilise multiple data sources,** such as antivirus software, firewalls, IDS/IPS, vulnerability scanners, asset information, cyber threat intelligence and SIEM.
- **The received data should be cleaned and normalized,** as each data source will provide data with different structure and format. The data normalization process could be done based on standardized formats, specific time/size, organizational policies, or other metrics. In order to prepare the data to be readable, comprehensible, or prepare it for the correlation or sharing with external organizations (Jirsík 2018; Hellesen 2019).
- **The system should have a data repository** where all the received data collected from many data sources is located. The main goals of having a repository is to consolidate data from various sources, and to enable more normalization and correlation for conducting cyber operations (Moye et al. 2015; Jirsík 2018; Hellesen 2019).

- **The stored data in the repository should be visualised** in an effective way that optimises the SOC security operator's CSA. Many methods could be used, such as colours, charts, tables, geographical views, node-link graphs, generic to detailed views, timelines highlighting temporal patterns and relationships, treemaps, or hierarchical visualisation techniques. In addition, zooming in/out and filtering features are considered visualisation techniques.
- **A course of action should be provided** to support the decision-making processes.
- **Sharing cyber information** with trusted partner organisations and the NSOC is the exchange of knowledge about threats, incidents, vulnerabilities, mitigation actions, and leading practices. Such sharing is important to improve CSA and the decision-making process of the SOC security operators.
- **The system should provide a future situation assessment** by identifying the critical assets that are used to support key mission objectives (asset criticality assessment), identifying the risks to such assets based on known vulnerabilities (vulnerability assessment), filtering and correlating the security events that need operator attention, assessing threats to mission objectives based on known threats such as asset failure (threat assessment), assessing the known impacts of an incident (impact assessment), and assessing the overall risk to mission objectives based on the potential for an incident to occur and the risk of further impact due to ongoing incidents (risk assessment) (Moye et al. 2015).

## 4.3 The Recommended System (DSS-CSA)

The recommended system (DSS-CSA) is designed based on the identified requirements and integrated some valuable features of the existing tools to improve the cybersecurity operations. It illustrates the important of utilising multiple data sources, having a data repository to correlate and normalize data, having a high-level overview as a security dashboard, presenting the endpoints with all the related information from alerts, vulnerabilities, and security recommendations. In addition, it presents some response actions that could help to handle the threats and incidents, and supports the idea of sharing information and reporting to NCSC.

The DSS-CSA is designed according to the CSA model; Observe, Orient, Predict, Decide and Act (OOPDA) (see chapter.5). **Figure 1** presents the system data flow based on the five phases (OOPDA). In the **Observe** phase**,** all the required data should be collected and stored in a database through the use of data source connectors. The system's data (entities and relations) is structured according to the CRUSOE data model, as it provides the required data in terms of cyber defence and can be used as a basic database. Depending on that, the stored data could include asset information, network topology, vulnerabilities, security events/alerts, access control information, firewall policies, incidents information, and response actions. The data sources used to gather such data could be IDSs, firewalls, vulnerability scanners, management systems (SIEM), or antivirus software. The database contributes by consolidating, correlating, and fusing data. Therefore, it is treated as a higher sensitivity component regarding data security (confidentiality, integrity, and availability). In the **Orient** phase, the stored data should first be analysed to deduce the exact threat level, type of attack and associated risks. After that, the stored data with the analysis results should be displayed visually, tailored to the operator's needs in order to enable data comprehension and decision-making. In the recommended system, some visual components are considered during the design, such as colour coding, charts, tables, symbols, generic to detailed views, attack graphs, mission dependency views as a treemap, filtering and a dashboard. While in the **Predict** phase, there should be a predictive situation assessment to address the future incidents by the discovered threats and vulnerabilities. In the **Decide** phase**,** there are two methods for making decisions, the recommended remediation that is generated from the used tools (automated CoAs) or a new response action that the operator may take. For example, suppose a recommended remediation was (install a software patch) to fix a critical vulnerability in host A. In that case, the operator can open a ticket and wait or decide to isolate the vulnerable host as a response action. For that, the system must be designed to provide these two concepts of CoAs. In the **Act** phase, the courses of action that are selected in the decide phase are implemented. Then the observe phase processes detect changes and the effects of these actions. Thus, all phases of the OOPDA loop run continuously and concurrently.

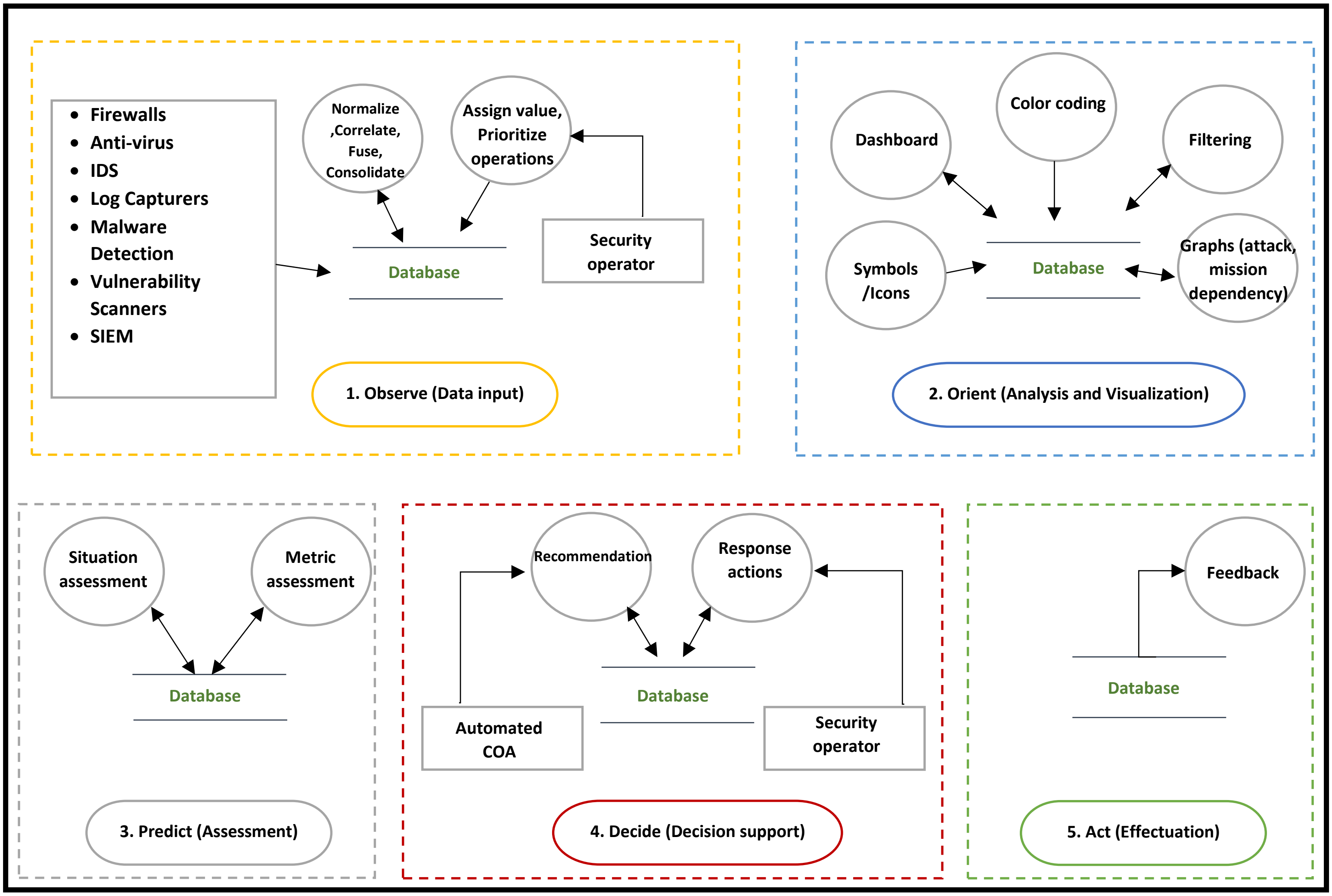


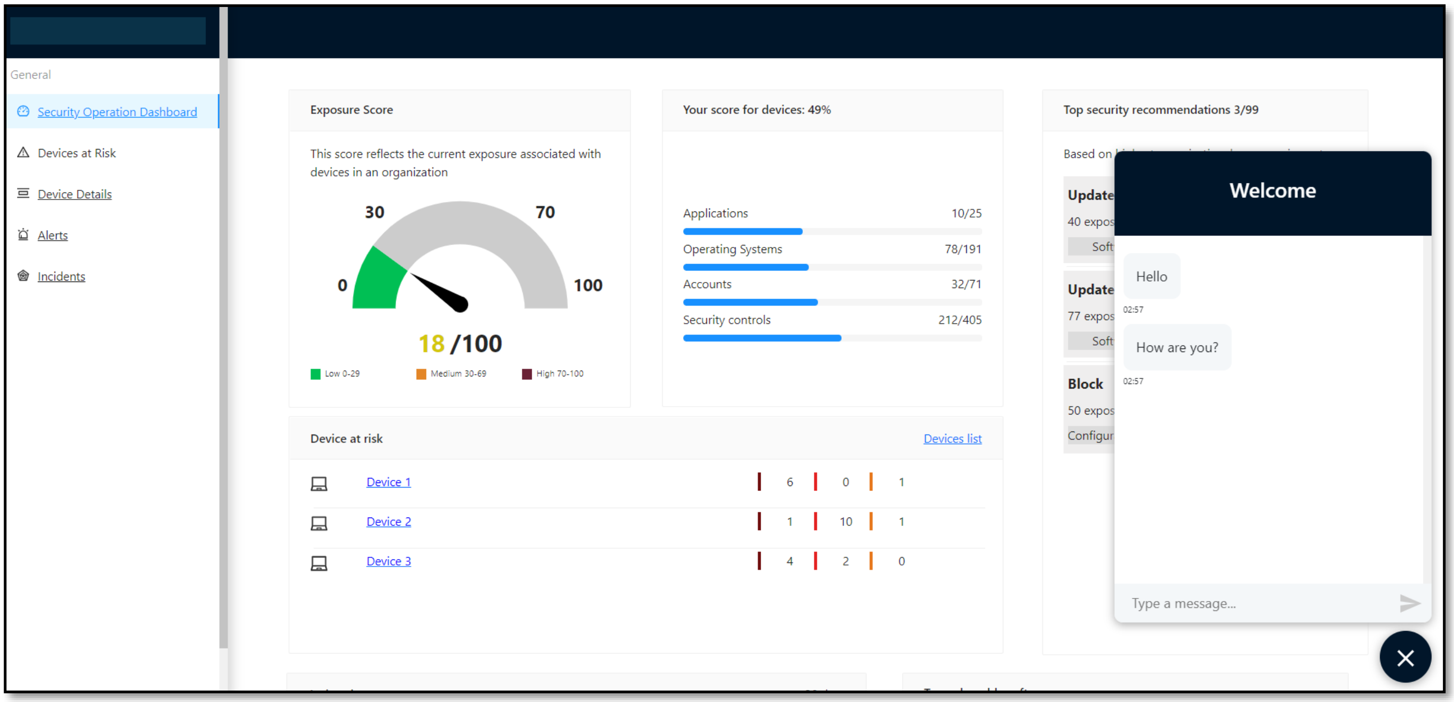
**Figure 1: The DSS-CSA Data Flow**

## 4.4 The System Designing

The Ant Design framework was used for designing the system as a prototype. Ant Design is an open-source code that provides a comprehensive package of design guidelines, resources and development tools for building rich, interactive graphical user interfaces (GUI). It supports many design languages; thus, the system prototype is implemented by using a collection of design languages, such as HTML, CSS, and JavaScript with React UI libraries. Before using the Ant Design framework, it was recommended to correctly install and configure Node.js v8 in the work environment (AntDesign).

## 4.5 The System Components

The system consists of five main interfaces: Security Operation Dashboard, Devises at Risk, Device Details, Alerts, and Incidents, presented in **Figure 2** on the left. Each interface will be explained in detail in the following sections. In addition, for supporting the communication between team chat feature is added, **Figure 2**.



This score reflects the current exposure associated with devices in an organization

| | |
|---|---|
| Applications | 10/25 |
| Operating Systems | 78/191 |
| Accounts | 32/71 |
| Security controls | 212/405 |

| | | | |
|---|---|---|---|
| Device 1 | 6 | 0 | 1 |
| Device 2 | 1 | 10 | 1 |
| Device 3 | 4 | 2 | 0 |

Hello
02:57

How are you?
02:57

**Figure 2: Chat Feature**

### 4.5.1 Security Dashboard

The security dashboard is designed to provide a high-level overview for the SOC security operator. It displays six cards, and each card will be explained in the following paragraphs:

1. **Device Exposure Score Card**

This card aims to quickly display the current state of the organisation's devices that risk exposure to vulnerabilities, such as cyber threats/attacks. **Figure 3**. The exposure score could be visualised by colour coding and classified into levels, such as 0–29 low exposure score (green), 30–69 medium exposure score (yellow), and 70–100 high exposure score (red). The goal is to decrease the exposure score as much as possible to be more secure and be in the green area because a low exposure score means that the organisation devices are less vulnerable to exploitation. For determining the score, there are several factors to take into account based on (Microsoft 2021): a) the number and type of threats and vulnerabilities that discovered in each device, b) the likelihood of being breached, c) the assigned value of each device by the operator, and d) the number of relevant alerts that are raised from the device. Therefore, each device will have a score, and the average score is the exposure score of all the organisation's devices.

### 2. Device Security Score Card

This card views the security posture of the organisation devices by monitoring the operating systems, applications, accounts, and security controls of the organisation, **Figure 3**.

The aim is to increase the score, as a higher score means that the organisation devices are more resilient against cyber threats/attacks. For example, when an operator recognises that they remediated 10 out of 25 of the applications security configuration issues, they would be motivated to complete the list of issues. The data in this card results from using a vulnerability scanner tool with an endpoint configuration management tool that would discover misconfigured assets, map configurations to the detected vulnerabilities and monitor changes to the security control configuration of all assets.

### 3. Top Security Recommendations Card

This displays the most important security recommendations related to the detected threats and vulnerabilities, **Figure 3**. Such recommendations could be collected by also using an endpoint configuration management tool, for example. Each recommendation is connected or mapped to a particular vulnerability, and this vulnerability could be found in a number of devices. Therefore, to improve the SA, this card also displays the total number of vulnerable devices that need this recommendation to be applied to them. In terms of prioritising the security recommendations, the number of vulnerable devices and their criticality is considered as well as the characteristics of the vulnerability and its impact. To take action, the security operator could click on any recommendation to see its details on the security recommendation page.

### 4. Active Alerts Card

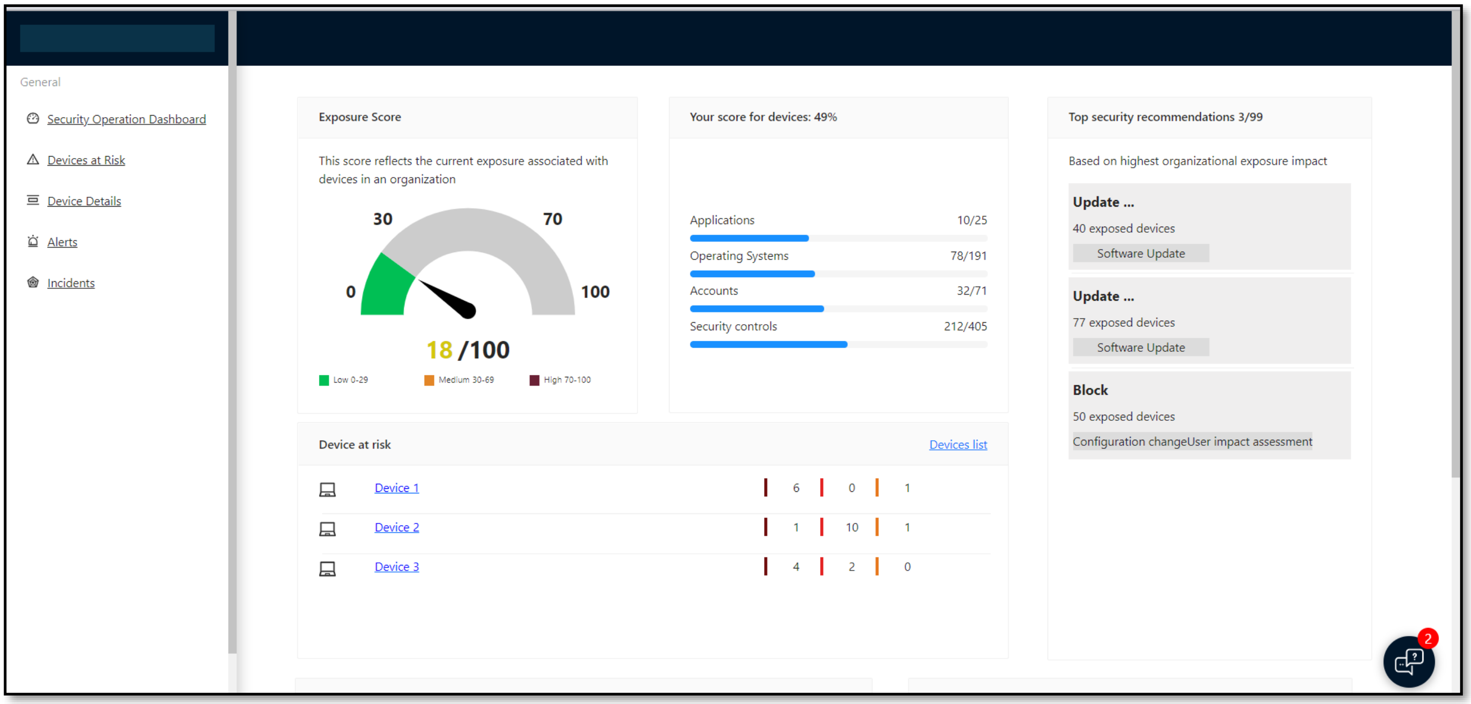
This card views the active alerts with their categorisations (high, medium, low) based on severity levels and visualises them in a coloured ring, **Figure 4**. In addition, it displays the overall number of alerts inside the ring. A list of the most severe alerts is displayed under the ring with a short description of what it is and when it was raised. To investigate an alert, the security operator could click on it to see its detail page.

### 5. Top Devices at Risk Card

This card displays a list of devices that have the highest number of active alerts, **Figure 3**. The alerts for each device are categorised by severity levels and shown next to the device's name. To take further steps regarding these devices, either click the device name to know the device details or click the devices list at the top of the card to go directly to the "Devices at Risk" page that displays a list of all devices in the network with active alerts.

### 6. Top Vulnerable Software Card

This card supports the real-time visibility of the most vulnerable software installed on the devices, displaying the number of threats and vulnerabilities they may have, **Figure 4**.



General

Security Operation Dashboard

Devices at Risk

Device Details

Alerts

Incidents

Exposure Score

This score reflects the current exposure associated with devices in an organization

Your score for devices: 49%

| | |
|---|---|
| Applications | 10/25 |
| Operating Systems | 78/191 |
| Accounts | 32/71 |
| Security controls | 212/405 |

Top security recommendations 3/99

Based on highest organizational exposure impact

**Update ...**
40 exposed devices
Software Update

**Update ...**
77 exposed devices
Software Update

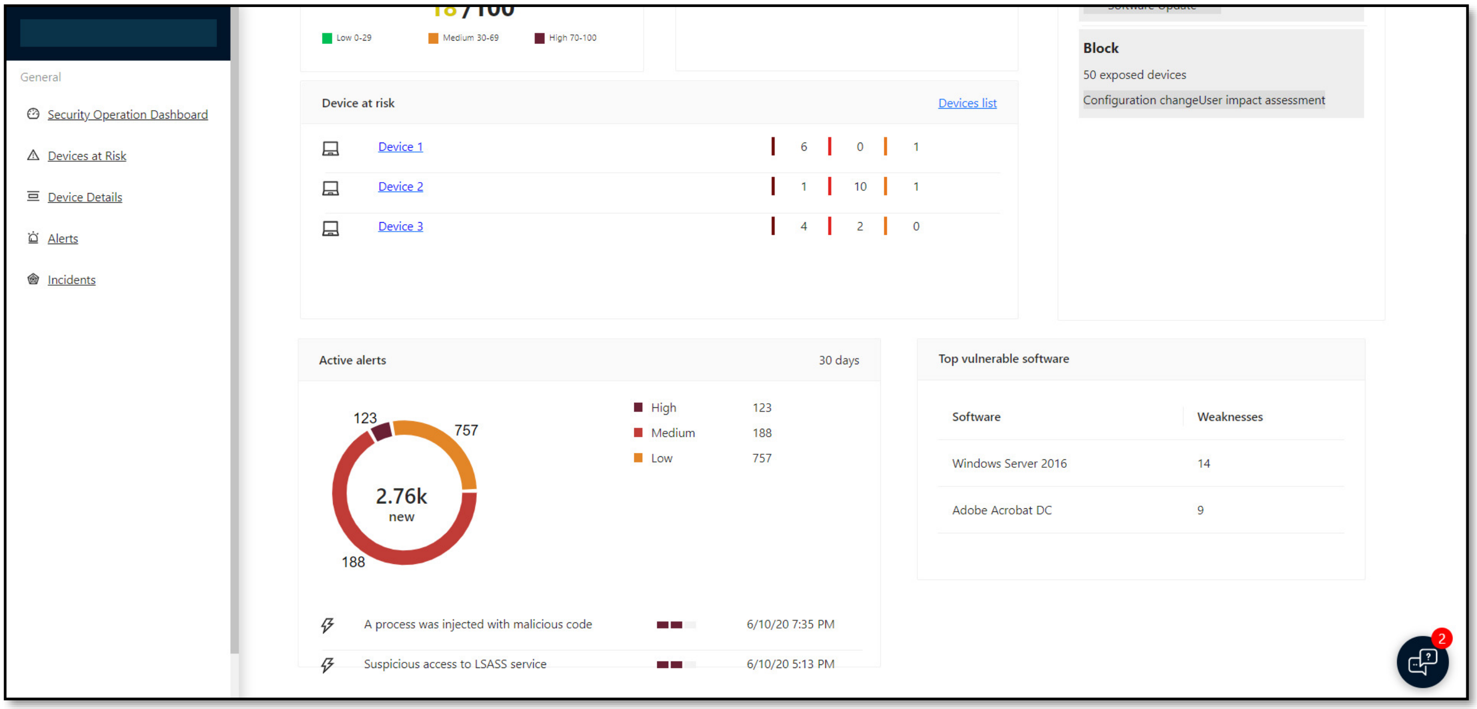
**Block**
50 exposed devices
Configuration changeUser impact assessment

Device at risk

Devices list

| | | | |
|---|---|---|---|
| Device 1 | 6 | 0 | 1 |
| Device 2 | 1 | 10 | 1 |
| Device 3 | 4 | 2 | 0 |

**Figure 3: The Security Dashboard (1)**



General

Security Operation Dashboard

Devices at Risk

Device Details

Alerts

Incidents

Software Update

**Block**
50 exposed devices
Configuration changeUser impact assessment

Device at risk

Devices list

| | | | |
|---|---|---|---|
| Device 1 | 6 | 0 | 1 |
| Device 2 | 1 | 10 | 1 |
| Device 3 | 4 | 2 | 0 |

Active alerts 30 days

| | |
|---|---|
| 🟥 High | 123 |
| 🟥 Medium | 188 |
| 🟧 Low | 757 |

| | |
|---|---|
| A process was injected with malicious code | 6/10/20 7:35 PM |
| Suspicious access to LSASS service | 6/10/20 5:13 PM |

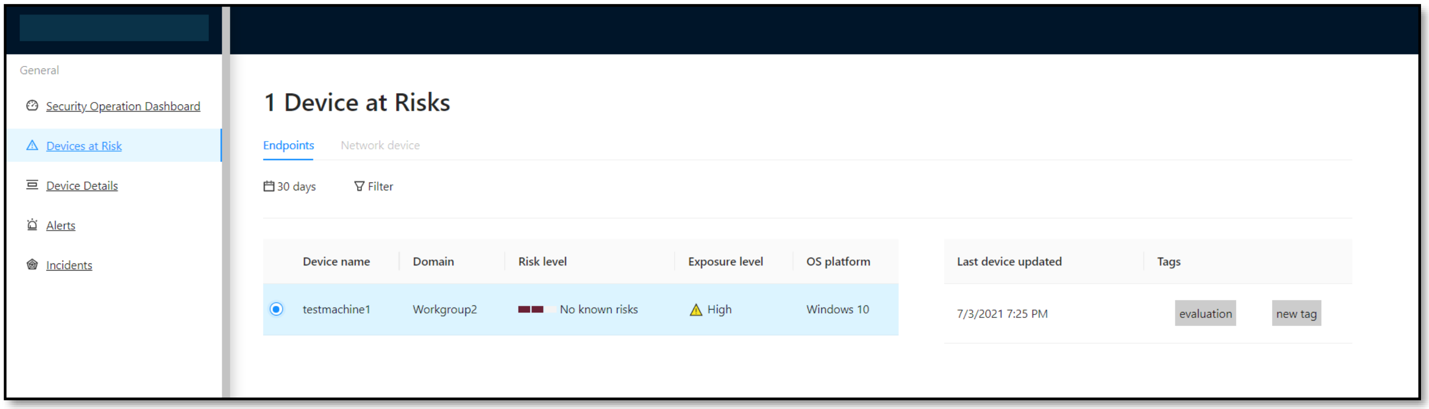
Top vulnerable software

| Software | Weaknesses |
|---|---|
| Windows Server 2016 | 14 |
| Adobe Acrobat DC | 9 |

**Figure 4: The Security Dashboard (2)**

### 4.5.2 Devices at Risk Page

This page is designed to show a list of all devices at risk, **Figure 5**. The list will contain the following information: **Device Name, Domain, Risk Level, Exposure Level, OS Platform, Last Updated, and Tags.** For the **Domain**, it will indicate the network domain to which this device belongs. The **Risk Level** represents the device's overall risk assessment based on a number of parameters, such as the number, types and severity of detected alerts and vulnerabilities. The level is represented by red (high risk), yellow (medium risk), and green (low risk). Resolving active alerts and applying the security recommendations would affect and reduce the risk level. Regarding the **Exposure Level**, it is the mean current exposure of the device, as each device will have a score based on several factors. In addition, the **Operating System** will also be illustrated and when it was **Last Updated**. **Tags** will be explained next in detail. The operator can select a device then double click on it to open its detail to take action.



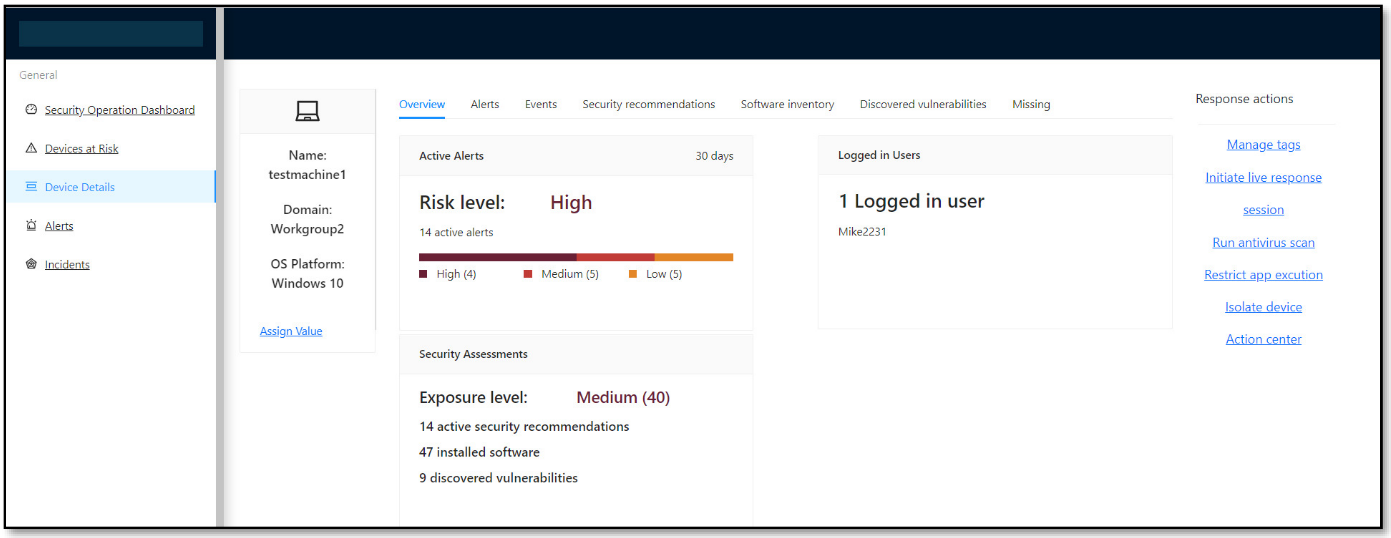
1 Device at Risks

| | Device name | Domain | Risk level | Exposure level | OS platform | Last device updated | Tags |
|---|---|---|---|---|---|---|---|
| ● | testmachine1 | Workgroup2 | 🟥🟥 No known risks | ⚠ High | Windows 10 | 7/3/2021 7:25 PM | evaluation<br>new tag |

**Figure 5: Devices at Risk Page**

### 4.5.3 Device Details Page

This page is designed to show all of the related information of the selected device, **Figure 6**. It will be divided to three sections. On the left, the **Device Details** appears with the device name, domain, operating system and tags. **Assigning a device's value** helps to differentiate between asset priorities. The device value is used to incorporate the risk appetite of an individual asset into the exposure score calculation. Device value has three options (Low, Normal, High). When devices are assigned as "high value" they receive more weight. In the middle, there are **Tabs** listed: overview, alerts, events, security recommendations, software inventory, discovered vulnerabilities and missing updates. These tabs provide all of the relevant information related to the device. On the right, the **Response Actions** are located, which includes manage tags, initiate live response session, run antivirus scan, restrict app execution, isolate device, action centre, consult a NSOC. The following paragraphs will explain **Taps** and **Response Actions** in detail.



Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

Active Alerts 30 days

Risk level: High

14 active alerts

■ High (4) ■ Medium (5) ■ Low (5)

Logged in Users

1 Logged in user

Mike2231

Security Assessments

Exposure level: Medium (40)

14 active security recommendations

47 installed software

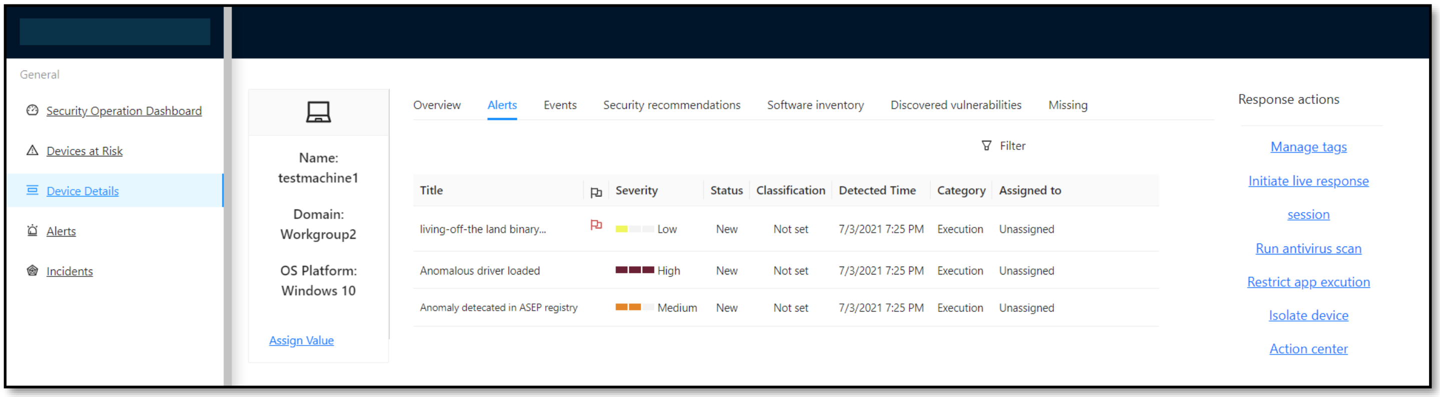
9 discovered vulnerabilities

**Figure 6: Device Details Page**

### 4.5.3.1 Device Details Tabs

The **Overview** tab displays three cards: active alerts, logged on users, and security assessment, **Figure 6**. The active alerts card displays a high-level overview of alerts related to the device and its risk level. The logged-on user’s card shows how many users have logged on with their usernames listed. The security assessments card displays the exposure levels, security recommendations, installed software, and discovered vulnerabilities.

The **Alerts** tab provides a list of alerts that are associated with the device, **Figure 7**. This list shows a short description of the alert, severity level (high, medium, low), status (new, in progress, solved), classification (not set, false alert, true alert), raised time**,** category of alert, and who is addressing the alert. All this information will be explained in detail in the Alerts page. In addition, there is the ability to flag critical alerts to indicate the need to perform further action on them. When flagging the alerts, they will appear in the Alerts page.



General

Security Operation Dashboard

Devices at Risk

Device Details

Alerts

Incidents

Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

Assign Value

Overview | Alerts | Events | Security recommendations | Software inventory | Discovered vulnerabilities | Missing

Filter

| Title | ⚑ | Severity | Status | Classification | Detected Time | Category | Assigned to |
|---|---|---|---|---|---|---|---|
| living-off-the land binary... | ⚑ | Low | New | Not set | 7/3/2021 7:25 PM | Execution | Unassigned |
| Anomalous driver loaded | | High | New | Not set | 7/3/2021 7:25 PM | Execution | Unassigned |
| Anomaly detecated in ASEP registry | | Medium | New | Not set | 7/3/2021 7:25 PM | Execution | Unassigned |

Response actions

Manage tags

Initiate live response session

Run antivirus scan

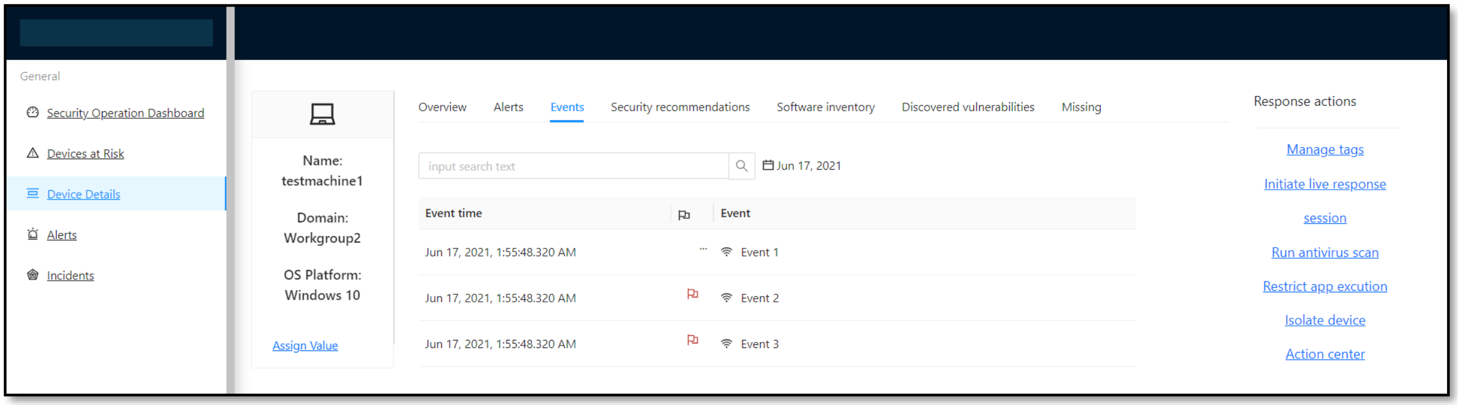
Restrict app excution

Isolate device

Action center

**Figure 7: Alerts Tab**

The **Events** tab provides a view of the events that have been observed on the device in real-time, **Figure 8**. This tab can also show events that occurred within a given time to support the investigation process by using the search bar to search for a specific event or using the calendar icon to display events on a particular day. In addition, there is the ability to flag events to help the operators in correlating, organising, and highlighting the most important events when they are investigating a potential attack.



General

Security Operation Dashboard

Devices at Risk

Device Details

Alerts

Incidents

Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

Assign Value

Overview | Alerts | Events | Security recommendations | Software inventory | Discovered vulnerabilities | Missing

input search text

Jun 17, 2021

| Event time | ⚑ | Event |
|---|---|---|
| Jun 17, 2021, 1:55:48.320 AM | ... | Event 1 |
| Jun 17, 2021, 1:55:48.320 AM | ⚑ | Event 2 |
| Jun 17, 2021, 1:55:48.320 AM | ⚑ | Event 3 |

Response actions

Manage tags

Initiate live response session

Run antivirus scan

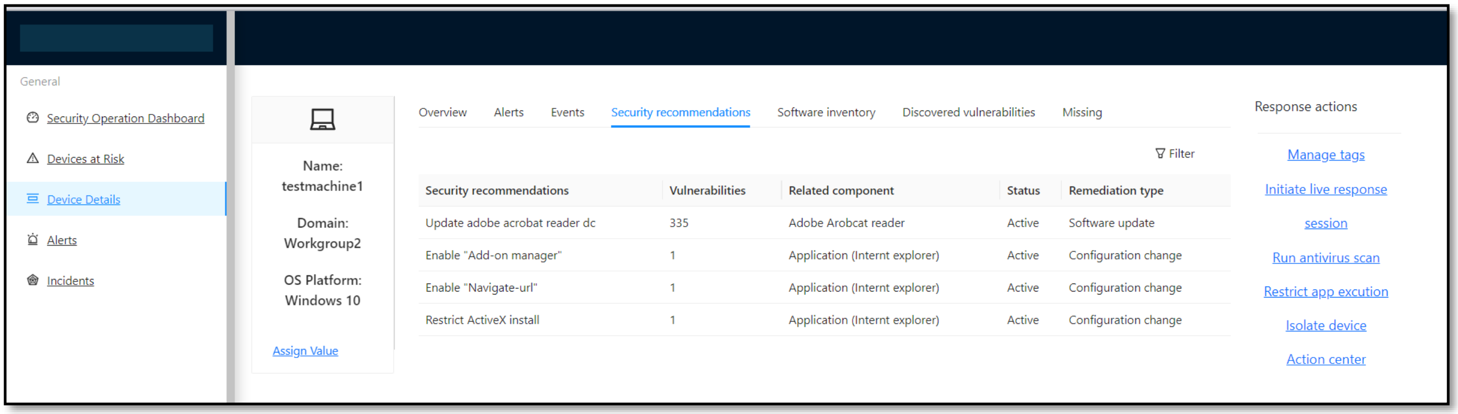
Restrict app excution

Isolate device

Action center

**Figure 8: Events Tab**

The **Security recommendations** tab lists recommendations related to the device and the connected vulnerabilities, related software, status, and remediation type, **Figure 9**.



Name:
testmachine1

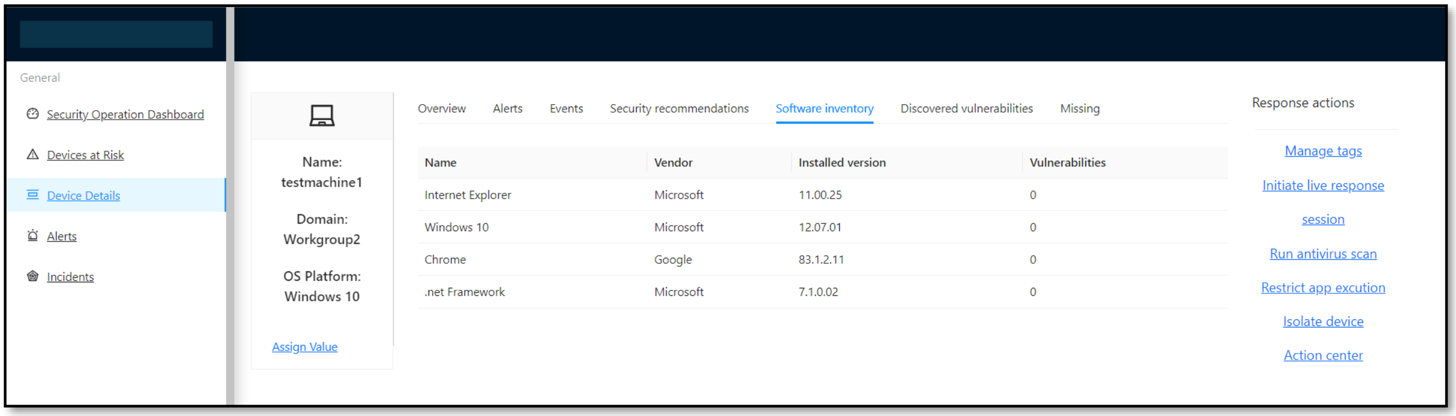
Domain:
Workgroup2

OS Platform:
Windows 10

| Security recommendations | Vulnerabilities | Related component | Status | Remediation type |
|---|---|---|---|---|
| Update adobe acrobat reader dc | 335 | Adobe Arobcat reader | Active | Software update |
| Enable "Add-on manager" | 1 | Application (Internt explorer) | Active | Configuration change |
| Enable "Navigate-url" | 1 | Application (Internt explorer) | Active | Configuration change |
| Restrict ActiveX install | 1 | Application (Internt explorer) | Active | Configuration change |

**Figure 9: Security Recommendations Tab**

The **Software inventory** tab lists all of the installed software on the device, along with their vendors, versions, and if they have some vulnerabilities, **Figure 10**.



Name:
testmachine1

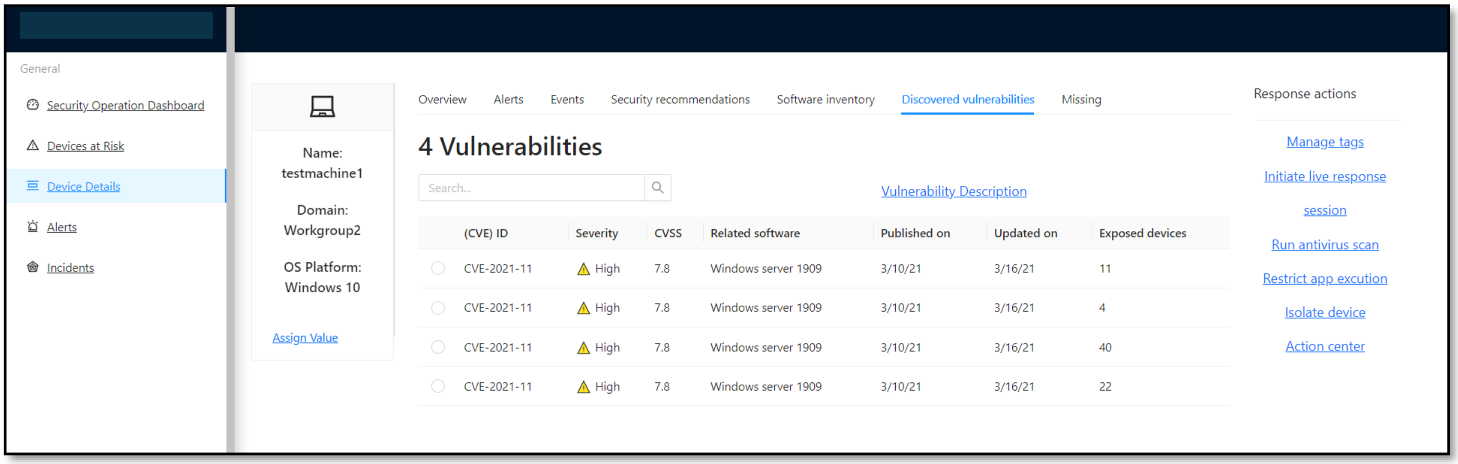
Domain:
Workgroup2

OS Platform:
Windows 10

| Name | Vendor | Installed version | Vulnerabilities |
|---|---|---|---|
| Internet Explorer | Microsoft | 11.00.25 | 0 |
| Windows 10 | Microsoft | 12.07.01 | 0 |
| Chrome | Google | 83.1.2.11 | 0 |
| .net Framework | Microsoft | 7.1.0.02 | 0 |

**Figure 10: Software Inventory Tab**

The **Discovered vulnerabilities** tab shows all the vulnerabilities that the device is exposed to with the following information: Common Vulnerabilities and Exposures (CVE) ID, the severity, Common Vulnerability Scoring System (CVSS) rating, and information on the related software, where it was published, updated and the vulnerability description, **Figure 11**.



Name: testmachine1

Domain: Workgroup2

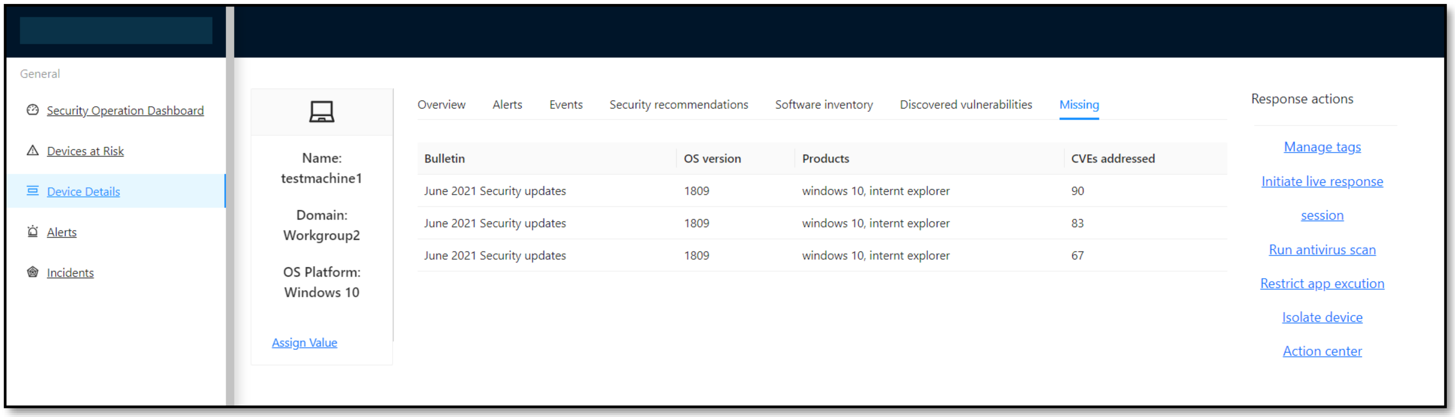
OS Platform: Windows 10

4 Vulnerabilities

| | (CVE) ID | Severity | CVSS | Related software | Published on | Updated on | Exposed devices |
|---|---|---|---|---|---|---|---|
| ○ | CVE-2021-11 | ⚠ High | 7.8 | Windows server 1909 | 3/10/21 | 3/16/21 | 11 |
| ○ | CVE-2021-11 | ⚠ High | 7.8 | Windows server 1909 | 3/10/21 | 3/16/21 | 4 |
| ○ | CVE-2021-11 | ⚠ High | 7.8 | Windows server 1909 | 3/10/21 | 3/16/21 | 40 |
| ○ | CVE-2021-11 | ⚠ High | 7.8 | Windows server 1909 | 3/10/21 | 3/16/21 | 22 |

**Figure 11: Discovered Vulnerabilities Tab**

The **Missing updates** tab is a list of the missing security updates of the device operating system, **Figure 12**.



Name: testmachine1

Domain: Workgroup2

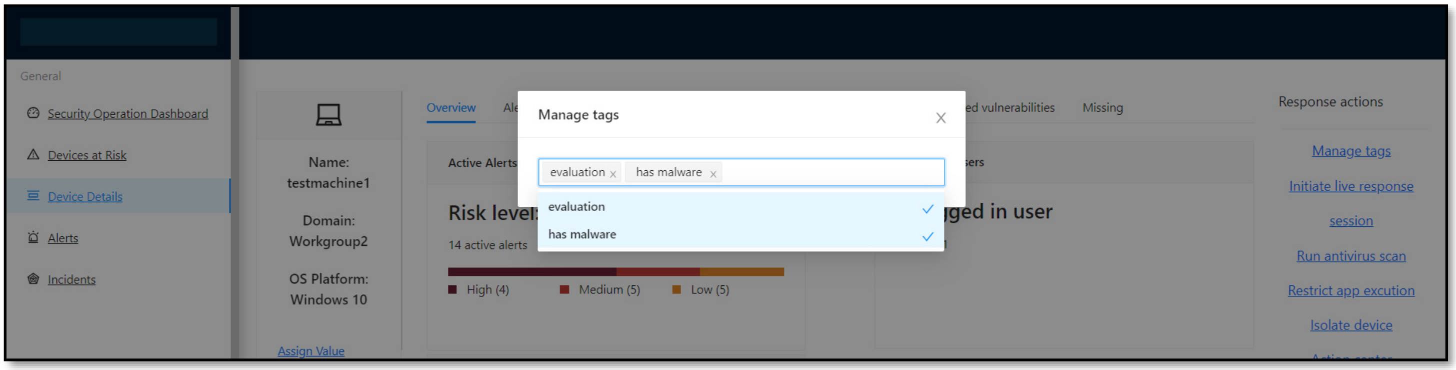
OS Platform: Windows 10

| Bulletin | OS version | Products | CVEs addressed |
|---|---|---|---|
| June 2021 Security updates | 1809 | windows 10, internt explorer | 90 |
| June 2021 Security updates | 1809 | windows 10, internt explorer | 83 |
| June 2021 Security updates | 1809 | windows 10, internt explorer | 67 |

**Figure 12: Missing Updates Tab**

### 4.5.3.2 Response Actions

The **Manage tags or Add tag** actions could improve security operations by classifying the organisation devices and sharing them with the team. Then the tag will appear with the device information list, **Figure 13**.



Manage tags

evaluation x has malware x

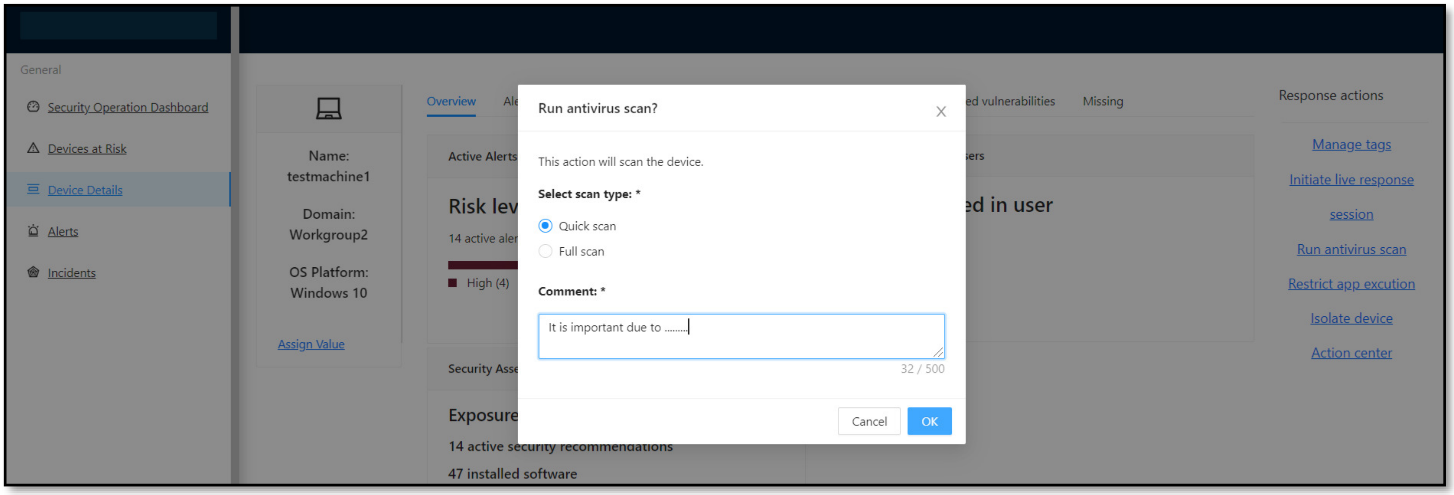
evaluation ✓

has malware ✓

**Figure 13: Manage Tags**

**Initiate live response session** is an action that allows access to a device through a remote shell connection to conduct in-depth investigations and take immediate response actions to promptly contain identified threats in real-time. Live response is a feature used to improve the security operations team in collecting forensic data, executing scripts, analysing suspicious activities, remediating threats, and proactively looking for emerging threats.

**Run antivirus scan** is a part of the response process, which could be done remotely in order to identify or remediate malware that might exist on a device, **Figure 14**.



Run antivirus scan?

This action will scan the device.

Select scan type: *

● Quick scan

○ Full scan

Comment: *

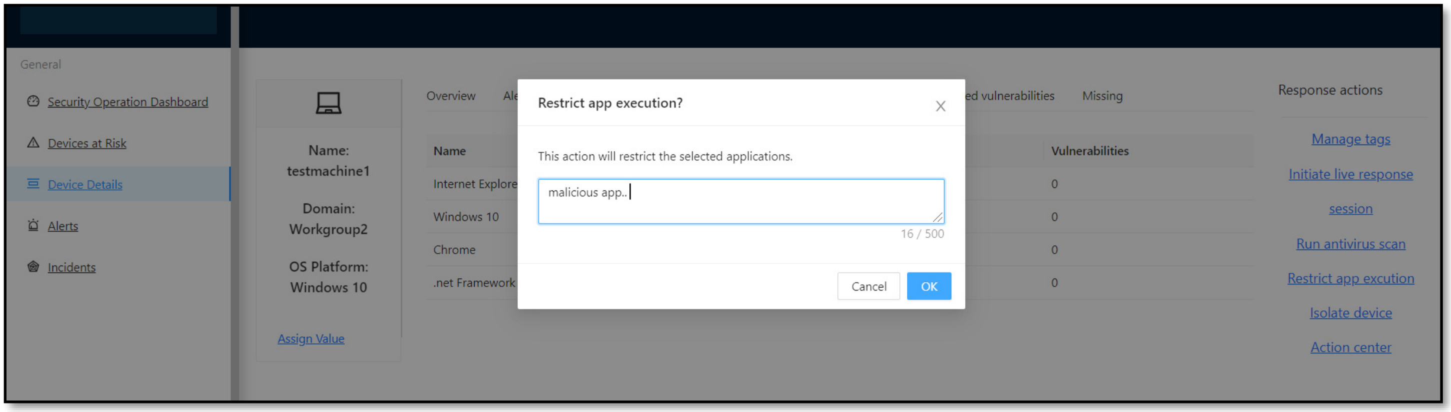
It is important due to ........

32 / 500

Cancel OK

**Figure 14: Run Antivirus Scan**

**Restrict app execution** is an action to contain an attack and terminate malicious processes. This action can prevent an attacker from gaining control of a compromised device or doing any further malicious activity, **Figure 15**.



Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

| Name | Vulnerabilities |
|---|---|
| Internet Explore | 0 |
| Windows 10 | 0 |
| Chrome | 0 |
| .net Framework | 0 |

Restrict app execution?

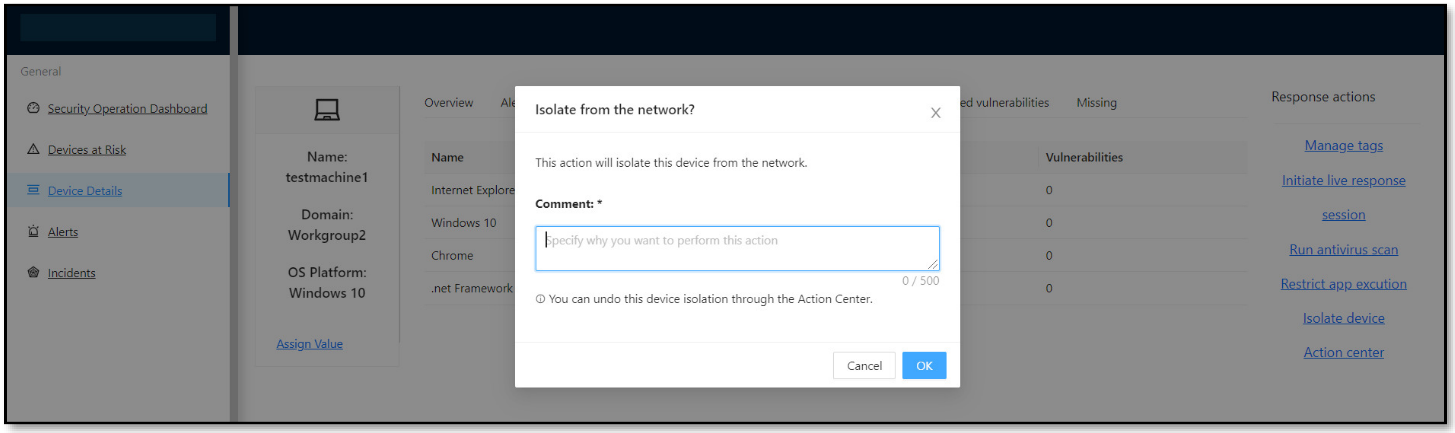
This action will restrict the selected applications.

malicious app..

16 / 500

Figure 15: Restrict App Execution

**Isolate device from the network**, depending on the device criticality and the attack severity the security operator should assess the situation then decide to do this action or not. This action also can assist in preventing the attacker from taking control of the compromised device or performing additional action, **Figure 16.**



Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

| Name | Vulnerabilities |
|---|---|
| Internet Explore | 0 |
| Windows 10 | 0 |
| Chrome | 0 |
| .net Framework | 0 |

Isolate from the network?

This action will isolate this device from the network.

Comment: *

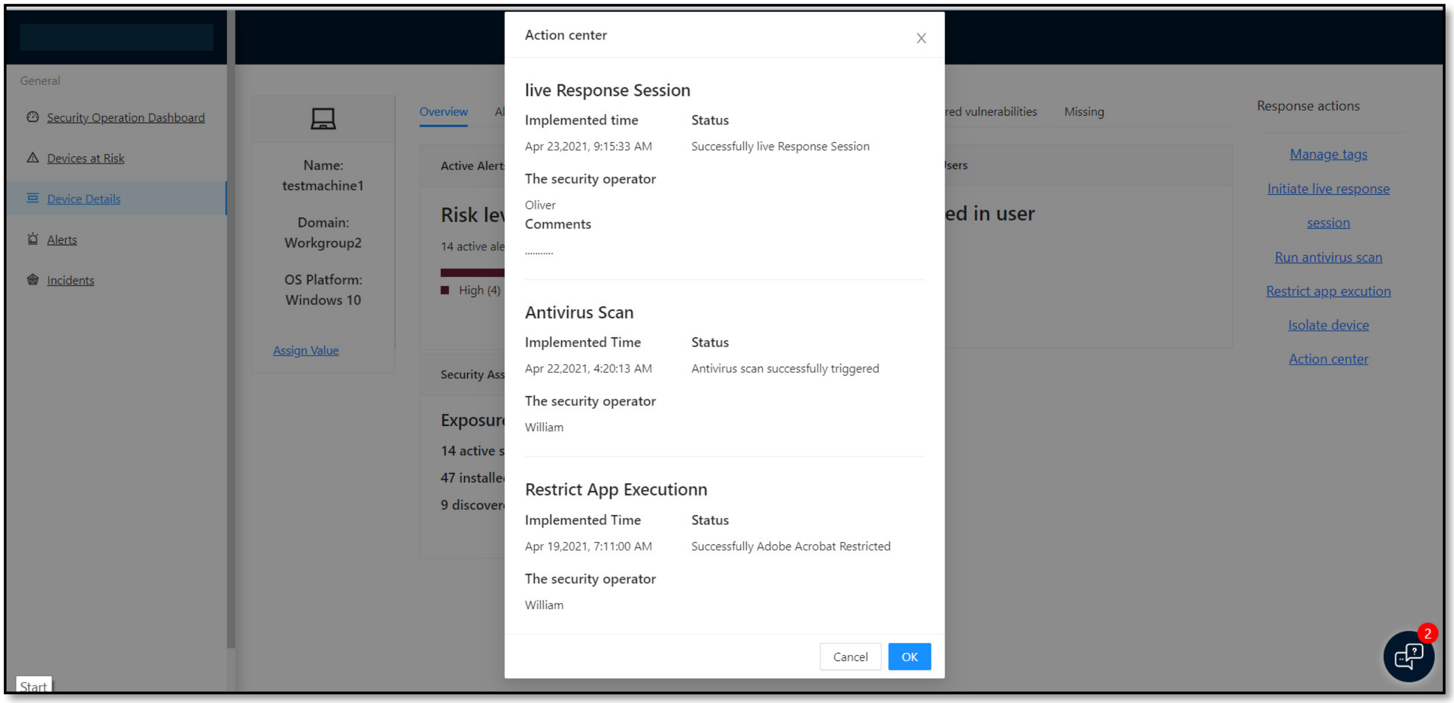
Specify why you want to perform this action

0 / 500

ⓘ You can undo this device isolation through the Action Center.

Figure 16: Isolate a Device

**Action centre** provides information on actions that were taken on the device with other related details, such as implemented date/time, the security operator, his/her comments, and if the action succeeded or failed, **Figure 17**.



Action center

live Response Session

Implemented time: Apr 23,2021, 9:15:33 AM

Status: Successfully live Response Session

The security operator: Oliver

Comments: ..........

Antivirus Scan

Implemented Time: Apr 22,2021, 4:20:13 AM

Status: Antivirus scan successfully triggered

The security operator: William

Restrict App Executionn

Implemented Time: Apr 19,2021, 7:11:00 AM

Status: Successfully Adobe Acrobat Restricted

The security operator: William

Name: testmachine1

Domain: Workgroup2

OS Platform: Windows 10

**Figure 17: Action Centre**

### 4.5.4 Alerts Page

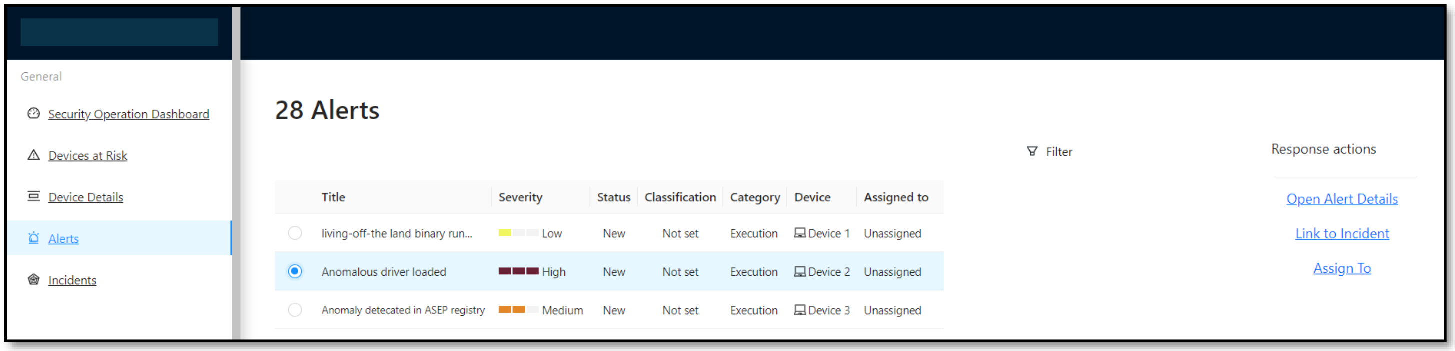
The Alerts page shows a list of the critical alerts that were flagged in the Device Details page to manage and investigate them, **Figure 18**. **Managing alert** means changing its status, assigning it to a security operations member, or classifying it. **Investigating alert** explains what it means, how to resolve it, or the device details associated with it. The alert list will contain the following information: **Alert title, Severity, Status, Classification, Categories, Related Devices, Assigned to, and time.**

- **Status** will have three options (New, In Progress, or Solved).
- **Classification** is determined by the security operator after investigating it (not set, false alert, true alert).
- **Alert category** is defined based on the enterprise attack tactics of the MITRE ATT&CK matrix; reconnaissance, initial access, execution, privilege escalation, credential access, and exfiltration.

- **Assigned to** one of the security operation team.
- **Time** indicates when it was detected.
- **Severity** determines the alert severity level with a colour coding system. High severity alerts, such as ransomware activities or credential theft tools will be highlighted in red. Medium severity alerts, such as downloaded unauthorised software or an anomalous registry change will be represented by orange. Low severity alerts, such as clearing logs or running exploration commands will be recognised in yellow.

#### 4.5.4.1 Response Actions

**Link to Incident** allows the operator to create a new incident from the selected alert or link the alert to an existing incident. It also can be used to define the incident's detected time. **Assign to** assigns the operator, or other one expert. This action can contribute to optimising cyber operations by escalating the alert to an expert as well as assessing the effort of each operator, as it helps to determine the number of alerts analysed by an operator at the end of a shift. **Open Alert Details** will be explained in the next paragraph.



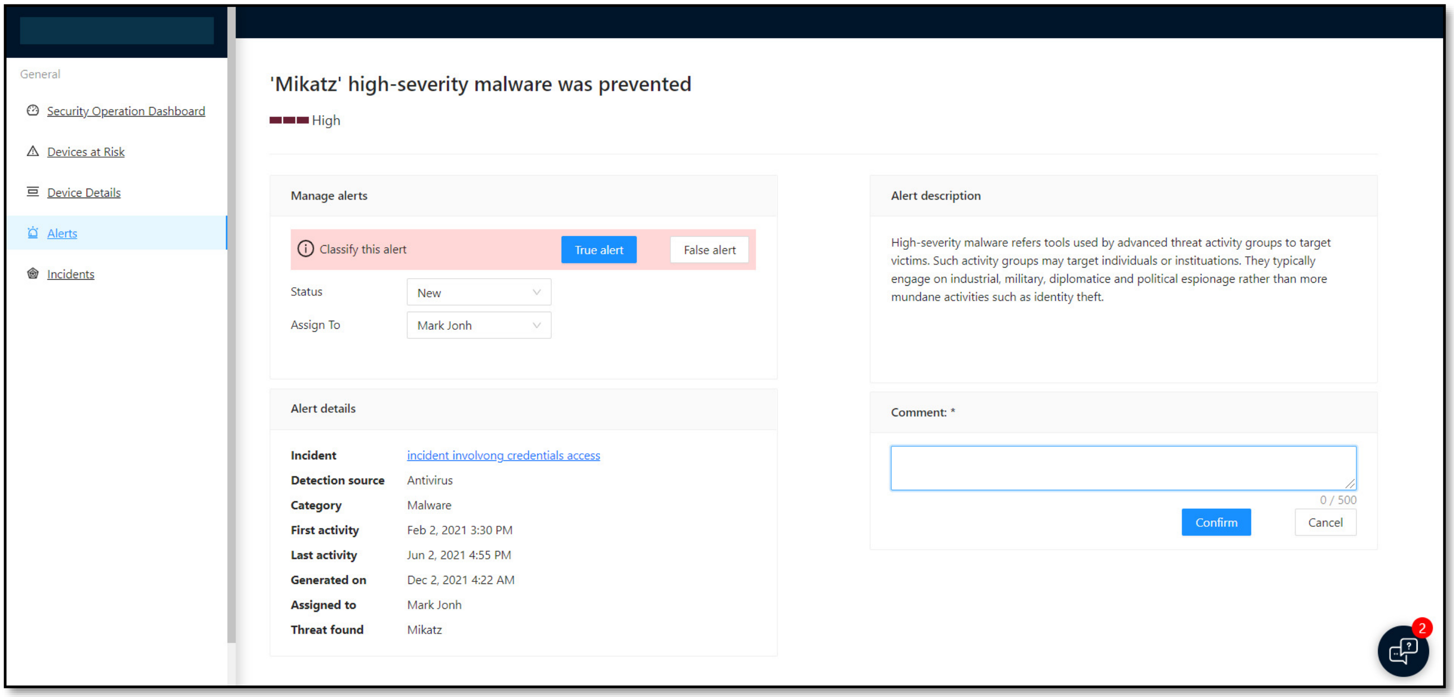
28 Alerts

| | Title | Severity | Status | Classification | Category | Device | Assigned to |
|---|---|---|---|---|---|---|---|
| ○ | living-off-the land binary run... | Low | New | Not set | Execution | Device 1 | Unassigned |
| ● | Anomalous driver loaded | High | New | Not set | Execution | Device 2 | Unassigned |
| ○ | Anomaly detecated in ASEP registry | Medium | New | Not set | Execution | Device 3 | Unassigned |

**Figure 18: Alerts Page**

### 4.5.5 Alert Details Page

This page is the result of selecting a particular alert and clicking on open alert details. This page will show the alert details, the alert's description, managing alerts, and where to add comments, **Figure 19**. Managing the alert means classifying it as either a true or false alert, changing its status (new, in progress, or solved), and assigning it either to the operator or to another expert.



'Mikatz' high-severity malware was prevented

High

Status: New

Assign To: Mark Jonh

High-severity malware refers tools used by advanced threat activity groups to target victims. Such activity groups may target individuals or institutions. They typically engage on industrial, military, diplomatice and political espionage rather than more mundane activities such as identity theft.

Alert details

| | |
|---|---|
| **Incident** | incident involvong credentials access |
| **Detection source** | Antivirus |
| **Category** | Malware |
| **First activity** | Feb 2, 2021 3:30 PM |
| **Last activity** | Jun 2, 2021 4:55 PM |
| **Generated on** | Dec 2, 2021 4:22 AM |
| **Assigned to** | Mark Jonh |
| **Threat found** | Mikatz |

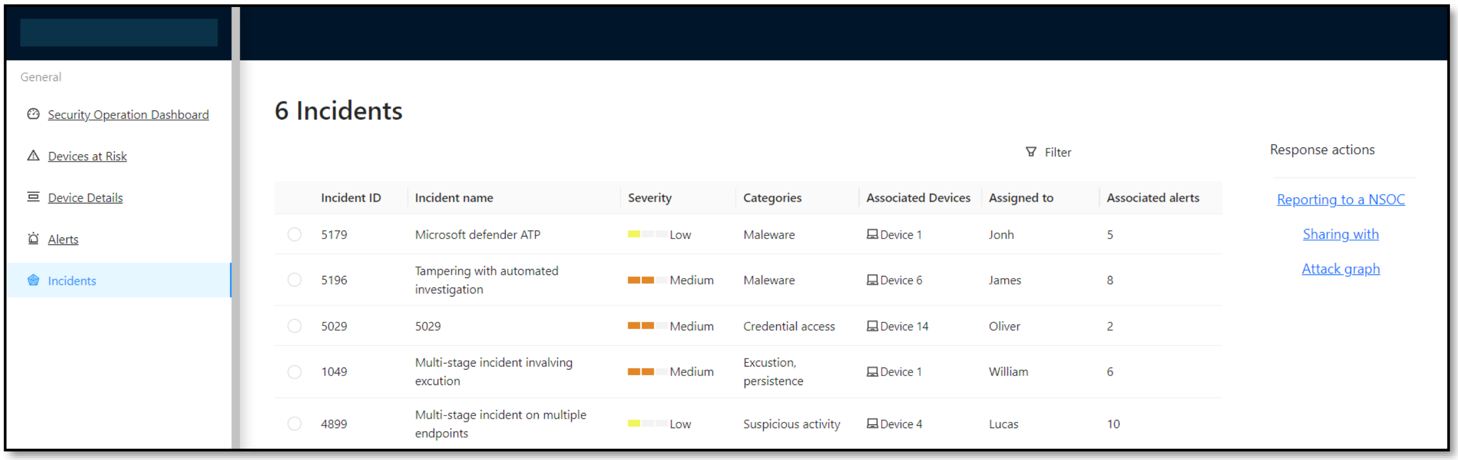
**Figure 19: Alert Details Page**

### 4.5.6 The Incidents Page

The incidents page shows a collection of alerts and events that are considered incidents. It displays the following information**: Incident ID, Incident name, Severity, Categories, Associated Devices, Assigned to, Associated alerts, Figure 20**.

#### 4.5.6.1 Response actions

**Reporting to a NSOC** would be for more insights regarding a potentially compromised device or already compromised ones. **Sharing with** shares the incident information with the trusted partner organisations, **Figure 20**.



General

- Security Operation Dashboard
- Devices at Risk
- Device Details
- Alerts
- Incidents

# 6 Incidents

Filter

| | Incident ID | Incident name | Severity | Categories | Associated Devices | Assigned to | Associated alerts |
|---|---|---|---|---|---|---|---|
| ○ | 5179 | Microsoft defender ATP | Low | Maleware | Device 1 | Jonh | 5 |
| ○ | 5196 | Tampering with automated investigation | Medium | Maleware | Device 6 | James | 8 |
| ○ | 5029 | 5029 | Medium | Credential access | Device 14 | Oliver | 2 |
| ○ | 1049 | Multi-stage incident invalving excution | Medium | Excustion, persistence | Device 1 | William | 6 |
| ○ | 4899 | Multi-stage incident on multiple endpoints | Low | Suspicious activity | Device 4 | Lucas | 10 |

Response actions

- Reporting to a NSOC
- Sharing with
- Attack graph

**Figure 20: Incidents Page**

# Chapter 5: Results and Evaluation

## 5.1 Overview

This chapter presents the research results: the proposed model (OOPDA), and various components and tools that would achieve and maintain CSA. In addition, in this chapter the recommended system was evaluated based on scenarios of common attack patterns that SOCs teams face frequently.

## 5.2 The analysis results of the CSA models

Generally, the interpretation of SA will depend on the application area. In this research, the application area that was focused on improving the SA are (SOCs). Therefore, some of the significant SA models have been selected and analysed in order to find the most efficient model for SOCs SA as well as decision-making processes. Despite SA having a wide range of applications, most SA models have one thing in common: they are all based on Endsley's general definition and most frequently referenced model. Consequently, the described components by Endsley serve as a basis for the analysis process and the selected models analysed regarding their applicability in SOCs. Each model describes the SA based on similar phases. In spite of the difference in phases names, they are compatible in meaning. **Table 5** summarises the analysis of the selected SA models and denotes the phases that correspond to Endsley's model with tick mark (✓), while the cross mark (X) indicates that the model has a softer focus on these phases.

Endsley divides SA into two main processes (SA Gaining and SA Application). First, the SA Gaining process contains three levels: perception, comprehension and projection. The perception and comprehension phases are covered in most models except NCSA. In contrast, the projection phase is described in only the CSAM and ECSA models described by Pahi et al. (2017). Although the ECSA model covers most of the phases, its scope is specified in the network, while the required SA of the SOCs should utilise a wide range of information types. Second, the SA Application, which contains the decision, performance of actions and feedback phase. In this research the decision component was focused on because SOCs are considered dynamic environments where the information flow is high and any wrong decision can result in serious consequences, particularly in defence of critical infrastructure. The models that concern the decision phase and describe it more comprehensively are the SAM, OODA and ECSA. In terms of the OODA Loop, it describes the steps for decision-making in detail, while the ECSA provides the decision-making process through predicting possible scenarios (Pahi et al. 2017). In this case, the basic model SAM is not recommended for the cyber domain according to [], and the ECSA model is only for a network. The remaining model to be selected for a SOCs environment is OODA. In fact, OODA was selected by many researchers, such as Sawilla and Wiemer (2011) and Nakhla et al. (2017), to automate cyber defence. According to Zimmerman (2014), most of the SOCs followed the OODA Loop for gaining SA, and it can serve as a solid base for SA decision-making. However, as a result of the analysis, it is missing the projection phase, and as SA is typically forward-looking, and the future projection of various situations can be taken into account during the selection of appropriate action, thus as a recommendation, the projection phase should be added to form an OOPDA-Loop (Observe, Orient, **Predict**, Decide, Act).

**Table 5: The analysis of SA Models**

| Abbrv. | Models | SA Gaining | | | SA Application | | |
|---|---|---|---|---|---|---|---|
| **SAM** | **Situation Awareness Model (1995)** | ✓<br>**Perception** | ✓<br>**Comprehension** | ✓<br>**Projection** | ✓<br>**Decision** | ✓<br>**Performance of Actions** | ✓<br>**Feedback** |
| **OODA** | **OODA Loop (1976)** | ✓<br>(Observe) | ✓<br>(Orient) | ✗ | ✓<br>(Decide) | ✓<br>(Act) | ✓ |
| **CSAM** | **Cyber Situational Awareness Model (2009)** | ✓<br>(Sense) | ✓<br>(Evaluate) | ✓<br>(Assess) | ✗ | ✗ | ✗ |
| **ECSA** | **Effective Cyber Situational Awareness (2014)** | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **NCSA** | **Cyber Situational Awareness Model for National Cyber Security Centre s (2017)** | ✓<br>( sharing information) | ✗ | ✗ | ✗ | ✗ | ✗ |
| **MIRTE-CSA** | **MIRTE-Cyber SituationalAwareness (2014)** | ✓<br>(Information) | ✓<br>(Analytics, Visualization) | ✗ | ✗ | ✗ | ✗ |

### 5.2.1 OOPDA Loop model

The proposed OOPDA model supports the concept that achieving SA in an environment must be a continuous (loop) process. In addition, it supports that SA and decision-making are not separate processes but are strictly connected. Therefore, it will consist of five phases depicted in **Figure 21**. In the first phase, **Observe**, all the related information should be collected to improve the CSA. Also, this phase will observe the feedback after acts and decisions are considered. The second phase, **Orient**, will represent the analysis and visualisation needed to understand the information provided by the observe phase. The third phase, **Predict**, will predict the future state of the environment, as it builds upon the knowledge gained in the previous two phases. According to Jirsík (2018), experienced operators rely heavily on future predictions regarding decision-making. The fourth phase, **Decide**, will select a specific action optimal for security and least optimal for attackers. While the last phase of the OOPDA loop, **Act,** will represent the actions taken in the decision phase. The loop will be continued, as the action's results will impact the environment and observation of the impact would be done in the **observe** phase.

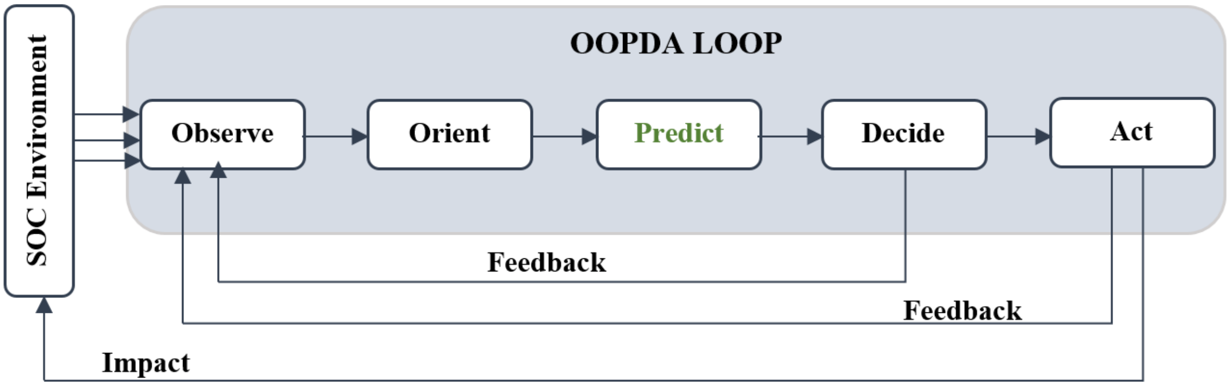


**Figure 21: The OOPDA Loop Model**

### 5.2.2 Taxonomy and Components of OOPDA-CSA Loop Model

In further contribution to improving SOCs CSA, addressing the need to identify the fundamental building blocks of any CSA tool **Data Sources** is becoming one of the objectives. This section will list various components and tools that would help achieve and maintain CSA. In addition, they will be classified based on the proposed CSA model (OOPDA). In **Figure 22** the general overview of the taxonomy will be presented, and in **Table 6** each component and tool will be described.

The taxonomies and components built on and extended the original CSA taxonomies provided by Evesti et al. (2017). Their CSA taxonomies were the only ones that consisted of data gathering (operational and strategic), analysis, and visualisation. However, Husák et al. (2020) tried to link the original taxonomy to the Endsley model, but it is noticeable that the taxonomy is still missing some of the important tools that MITRE recommend any SOC to have for maintaining cybersecurity operations (Zimmerman 2014). The **Observe** phase will match the data gathering category, which has operational and strategic subcategories. To be more convenient and reflect the different needs of handling the operations of day-to-day cybersecurity incidents, the following tools should be considered and added: Anti-Malware, AntiSpyWare Software, Intrusion Prevention Systems (IPSs), Network Scanning/Monitoring, Forensic Tools, Cyber Intelligence, SIEM, and Governance Risk Compliance (GRC) software. The **Orient** phase will cover the analysis and visualisation categories, as they both expand the comprehension of a situation. In the analysis, the original taxonomy includes anomaly detection, which is quite confusing because it can be under both observe and orient, as it can be an anomaly detection processing primary data (network traffic) or inferred data (security alerts). Therefore, it has been replaced by User and Entity Behaviour Analytics (UEBA) systems. In addition, Artificial Intelligence has been added as a method of analysis. Under visualisation, the mission dependency view is also considered a critical view that should be added. In terms of the **Predict** phase, it was nicely structured and convenient, as done by Husák et al. (2020). In the **Decide** phase, the decision-making process is either an automated process or depends on the human. For the **Act** phase, MITRE mentioned that Remote Access tools and Endpoint Detection and Response (EDR) tools could perform the decided actions.

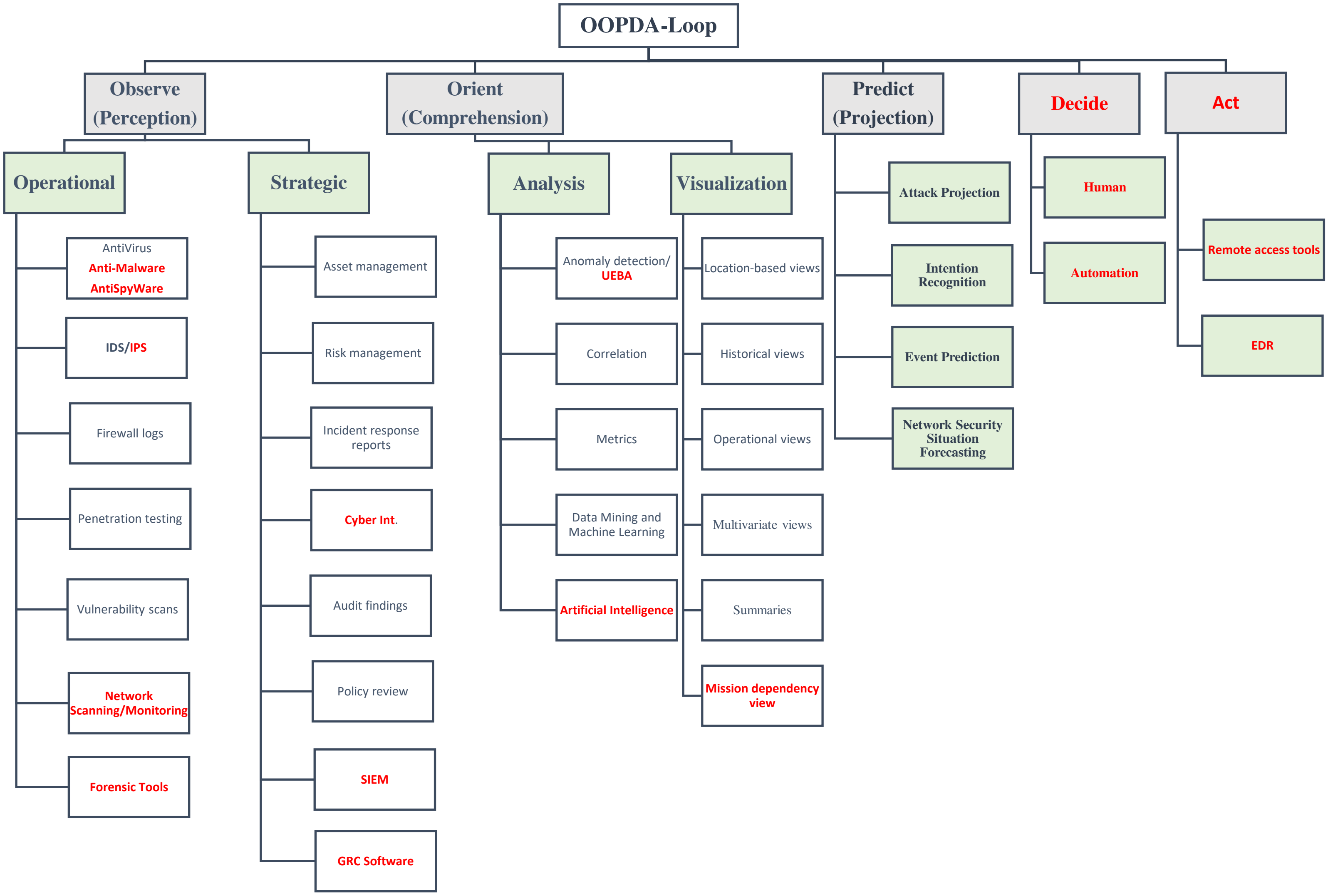


**Figure 22: Taxonomy and Components of OOPDA-CSA Loop Model**

**Table 6: The Tools and Components of OOPDA-CSA Loop Model**

| OBSERVE | |
|---|---|
| **OPERATIONAL** | |
| **Anti-Virus**<br>**Anti-Malware**<br>**AntiSpyWare** | They are known as detective and preventive security countermeasures. Briefly, they are software that scan the contents of the file system and memory, using a vast signature database and algorithms to discover malicious files or techniques. Therefore, they have the ability to produces log data about the malicious files, and they can provide indicators that a host is infected, which can be utilized for CSA (Zimmerman 2014; Evesti et al. 2017). |
| **Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)** | Intrusion detection is the process of monitoring and analysing events in a system or network for signals of potential incidents, such as security policy violations or threats. An intrusion detection system (IDS) is a piece of software that automates the detection of intrusions. An intrusion prevention system (IPS) is software that combines the capabilities of an intrusion detection system (IDS) with extra features to help prevent events (Arshad et al. 2020). |
| **Firewall** | It performs detective and preventative actions. For the CSA, it can produce huge amount of audit trail data on network and application levels, and it can monitor both incoming and outgoing traffic (Evesti et al. 2017). |
| **Vulnerability Scanner** | Vulnerability scanner is an automated tool that enables organizations to monitor their networks, systems, applications and procedures for known security vulnerabilities.<br>Further, it has the ability to create an inventory for all IT assets. It also detects operational characteristics for each asset, such as the operating system and the software installed on it, as well as other properties like open ports and user accounts. Generally, vulnerability scanner is a critical tool for CSA because it provides information about: the environment weaknesses, the risk degree of each vulnerability, and recommendations on how to mitigate the vulnerability (Roldan-Molina et al. 2017). |
| **Network Monitoring** | Network monitoring systems can be either software or hardware that track different elements of a network and its operation such as traffic, such as traffic. They can monitor and update the status of devices when connected to the network. Thus, such systems can alert about issues and generate reports via network analytics (CISCO, 2021). |
| **Penetration testing** | It is a step further from vulnerability scanning, it attacks the target system and penetrate their defenses. From the CSA, it is able to find weaknesses that are not discovered in the vulnerability scanning such as weak policies or default passwords (Evesti et al. 2017). |
| **Forensic Tools** | Digital forensics tools are important to CSA because they can provide a reliable digital evidence collection for a range of legal and industrial applications. Along the criminal investigation, they also can be used for maintenance, debugging, data recovery, and reverse engineering of computer systems (Hibshi et al. 2011). |
| **STRATEGIC** | |
| **Asset information** | For achieving CSA, each organization should collect and keep track of their assets information, such as hosts names, MAC / IP addresses, OS and versions, installed and running software, hardware details and configuration, system settings, personal owner, and so forth. Vulnerability scanners can offer comparable information, but a strong asset management and tracking database may be preferred. As many SOCs when an analyst investigated at an incident that has hit several systems across the organization, the information from a robust asset management database can be very useful to answer these questions; which are the IPs of the victim hosts. What are the physical locations of these systems? What is the running software? Is it possible that they are vulnerable because of their service pack level? , and more (Zimmerman 2014). |

| | |
|---|---|
| **Risk identification** | Risk identification is the process of determining and assessing threats to an organization, its operations, and its workforce. it could be a brainstorming session where experts documenting and communicating the concern. For example, identifying IT security risks such as malware and ransomware, accidents, natural catastrophes, and other potentially detrimental occurrences that might interrupt organization operations are all examples of risk identification (EKUonline). |
| **Incident response reports** | They can give an overview of the security landscape for the strategic level. Based on this information effective security policies and practices can be defined (Evesti et al. 2017). |
| **Audit findings** | They are an essential part in order to ensure the compliancy of selected standards or mandatory regulation. The purpose is to reveal how well organization is performing from the security point of view and to pinpoint required enhancements (ibid). |
| **Policy review** | It can reveal if current security practices are not fulfilling all security requirements derived from risk analysis results. For instance, a finding may indicate that separation of duties is not applied, which has to be resolved on the strategic level. On the other hand, policy review can elicit security practices that are not increasing security in practice (ibid). |
| **Cyber Intelligence** | It is information derived from external sources that gives insight about threats, vulnerabilities, and adversary TTPs. In addition, it could include cyber news feeds (social media), incident reports, signature updates, vulnerability alerts, and threat briefs. It is a recent emerging source of information for cybersecurity analysts (Zimmerman 2014). |
| **SIEM** | It is a critical software that combines security information management (SIM) with security event management (SEM) to increase an environment's security awareness, through the collection and analysis of real-time and historical security event data and sources, it improves threat detection, compliance, and security incident management (Mcafee). |

| **ORIENT** | |
|---|---|
| **Analysis** | |
| **Anomaly detection/ UEBA** | It is the process of recognizing abnormal behavior of users / systems through collecting and analyzing the normal events. This can improve the detection of the complex anomalies as lateral movement, malicious behavior, and compromised credentials (rapid7). |
| **Correlation** | In general, the importance of correlation analysis in cybersecurity is seen growing, as this analysis could be done on events, cyber threats, or system behavior in order to look for interested information and improve CSA (Kim et al. 2016). |
| **Machine learning** | It is a broad field, encompassing several sub-fields. Generally, machine learning can be used to target properties like recognizing advanced persistent threats (APT) or identifying trends and patterns in large historical and operational datasets which is clearly enhance CSA (Evesti et al. 2017). |
| **Metrics** | They may be used to present security in a standardized manner and to combine several raw measurements. Quantitative security metrics such as the length or age of a password, may be measured and sent more easily between systems. Qualitative security metrics are more like level or category indicators. These may be more abstract concepts, such as employee training or estimated security awareness levels. Security metrics can be used on both strategic and operational levels (Evesti et al. 2017). |
| **Visualization** | |

| | |
|---|---|
| **Statistical summaries** | They use simple visualizations like histograms and line charts to describe data like event counts over time intervals (ibid). |
| **Location** | This view focus on tying the data to specific locations. The locations can be for example geographic-locations (country/city) or organizational locations (subnets, specific workstations) (ibid). |
| **Historical** | It reveals larger trends in the data set over time, such as the number of identified attacks or malware, or number of logins over time. These may also be used to interactively display data connected to other sorts of visualizations, such as statistical summaries over time, and in an interactive way (ibid). |
| **Operational** | This view gives you real-time insight to the data and what is going on in real time, such as live connection and session counts. These are comparable to historical data, but the operational perspective's tactics are more focused on the current situation, whereas the historical view is more concerned with the long term and overall picture (ibid). |
| **Multivariate** | Multivariate views allow for visual comparison and correlation of data parameters. Scatterplots, parallel coordinate plots, and principal component projections are all examples of this. These views allow to see how different data attributes interact with one another and how they could affect one another (ibid). |
| **Mission dependency view** | It views the dependencies among mission requirements and critical assets, through visualizing how mission objectives, tasks, and information depend on cyber assets for analysis the context of mission assurance (Noel et al. 2016). |

| **PREDICT** | |
|---|---|
| **Attack Projection and Intention Recognition** | In terms of functionality, attack projection and intention recognition are quite similar, according to. They usually use attack models (attack graphs) to connect the observed events to a known scenario and predict the continuation of an attack. For example, by estimating the most likely next step of an adversary (Husák et al. 2020). |
| **Event Prediction** | It includes a variety of techniques for predicting events, such as specific attacks and exploitations (ibid). |
| **Network Security Situation Forecasting** | It includes a variety of methods for predicting the overall situation of cybersecurity as a decrease or an increase in the number of predicted attacks (ibid). |
| **Artificial Intelligence** | To further improve CSA, combining AI with human insight is required. Using AI techniques, organisations will be able to stay ahead of cybercriminals, automate threat detection, and respond more efficiently (Hai et al. 2017). Furthermore, AI enables improved predictive intelligence by scraping articles, news, and research on cyber threats to provide information on new abnormalities, cyberattacks, and protection techniques (IEEE).<br>According to Richards (2017), with AI, two of the existing problems can be solved; botnets that are used to launch Distributed Denial of Service (DDoS) attacks, and IDPS that create large numbers of false alarms and disrupt cybersecurity experts from discovering the true threats. |
| **ACT** | |
| **Remote access tools** | It is a software used to provide remotely access or control a host. It is frequently used by adversaries, but legitimately it can provide many advantages, the general using is for code execution, file access, registry management, recording key logging, screen and camera capture, password sniffing, for example (Zimmerman 2014). |
| **Endpoint Detection and Response (EDR) tools** | The main functions of an EDR security system are monitor, collect, and analyze data from endpoints that could indicate a threat, but the important function is that it can respond automatically to the identified threats though removing or containing them, then notify security operator (ibid). |

## 5.3 The Evaluation of the Recommended System

In this section two operational scenarios will be explained for giving evidence on how the recommended system would operate by providing a demonstration showing detailed screenshots of a walkthrough of each scenario.

1. **Scenario 1 will address a phishing emails campaign.**
2. **Scenario 2 will illustrate a download of unauthorised software on one of the organisation's devices.**

### 5.3.1 General Scenario Design and Background

The selected scenarios are going to focus on the detection and response actions to cyber threats through the recommended system in order to highlight the functions of the system that contributed to raising the level of the security situation. The scenarios are designed with two objectives in mind. First, they should be realistic in the sense that each scenario must point out a common attack pattern that SOCs teams face frequently and indicate a realistic threat to the critical infrastructure. Second, they should provide a basis for describing the functionalities of the recommended system.

As a general background, the scenarios describe attackers targeting a critical infrastructure (government hospital) that has around 8,000 users/IPs. It can be presumed that the attackers have a strong background, which could be criminal organisations focusing on monetary return, groups of activists, or cyber-divisions of adversarial governments. The hospital has invested in an internal centralised SOC with sixteen employees contributing to detecting and responding to the threats. Although this is considered a small SOC, it is structured into three sections, **Figure 23**:

- **Tier 1:** analysts perform routine duties such as operating a call centre, real-time monitoring, sorting alerts, and vulnerability scanning.
- **Tier 2:** analysts perform any in-depth analyses on incidents passed to them by tier 1, such as log analysis or response to sophisticated incidents.
- **System administrators:** maintain SOC systems and sensors and could include engineering and deployment of new capabilities.

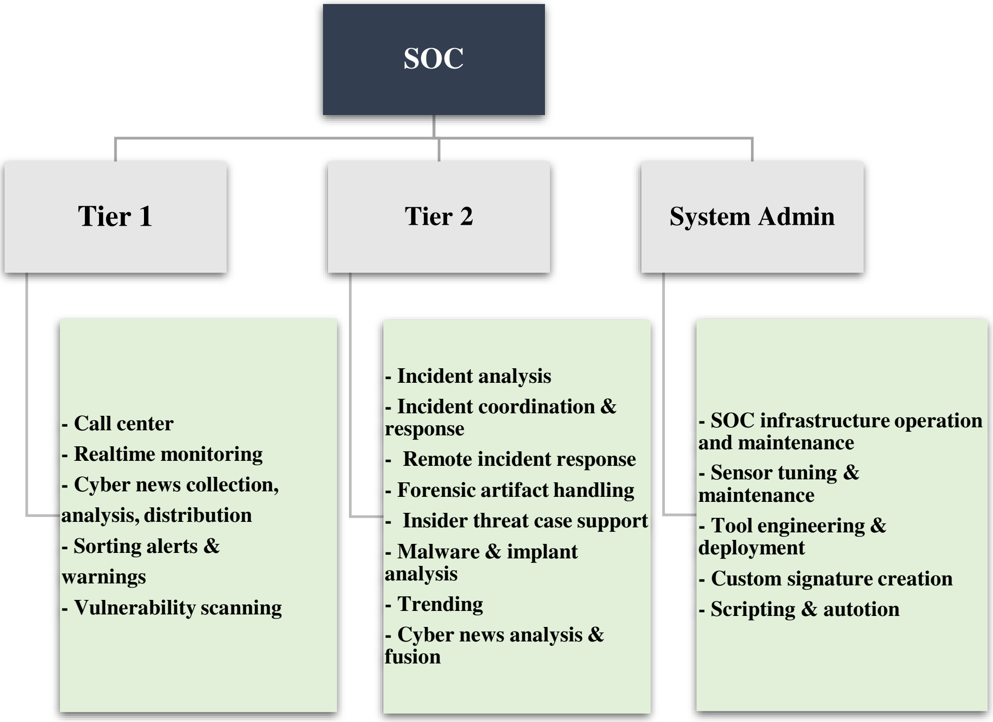

SOC
Tier 1
Tier 2
System Admin
- Call center
- Realtime monitoring
- Cyber news collection, analysis, distribution
- Sorting alerts & warnings
- Vulnerability scanning
- Incident analysis
- Incident coordination & response
- Remote incident response
- Forensic artifact handling
- Insider threat case support
- Malware & implant analysis
- Trending
- Cyber news analysis & fusion
- SOC infrastructure operation and maintenance
- Sensor tuning & maintenance
- Tool engineering & deployment
- Custom signature creation
- Scripting & autotion

**Figure 23: SOC Structure**

## 5.3.2 Scenario 1 – Phishing Emails Campaign

| | |
|---|---|
| **Scenario Background** | A hostile country has launched a campaign to attack the critical infrastructures of another country. Part of this campaign includes sending phishing emails targeted to government hospital employees with the intent of convincing the employees to click on a link to install malware on their systems, which will ultimately bring down the system and cause much damage and widespread inconvenience.<br>Unfortunately, one of the employees receives that phishing email and infects his device. As a consequence, the malware is replicating itself through the network by attaching itself to legitimate emails sent by employees of infected devices. |
| **Actors** | The actors involved in this threat scenario are:<br>• Originator of email (Foreign intelligences, Hackers, Insiders, Phishers)<br>• Initial user who received the email<br>• Other infected devices and users |

| | |
|---|---|
| | The actors involved in the handling of the incident are:<br>• Tier 1 and 2 analysts |
| **Threats** | The main threat in this scenario is: the distribution of malware. |
| **Effect** | The main effects that could result are:<br>• Disruption to systems, increased network traffic<br>• IT recovery costs<br>• Downtime<br>• Possible further implications (data corruption/loss, exfiltration, resource use, installations of other malware). |
| **The toolset used to solve the incident when not using the recommended system** | The analyst will need to change his interface many times during the resolution of the incident. They will use:<br>• SIEM to check email logs and Full Packet Capture (FPC) to see full emails<br>• Antivirus software<br>• Vulnerabilities scanning tool<br>• Common Vulnerabilities and Exposures (CVE) database<br>• IDS |

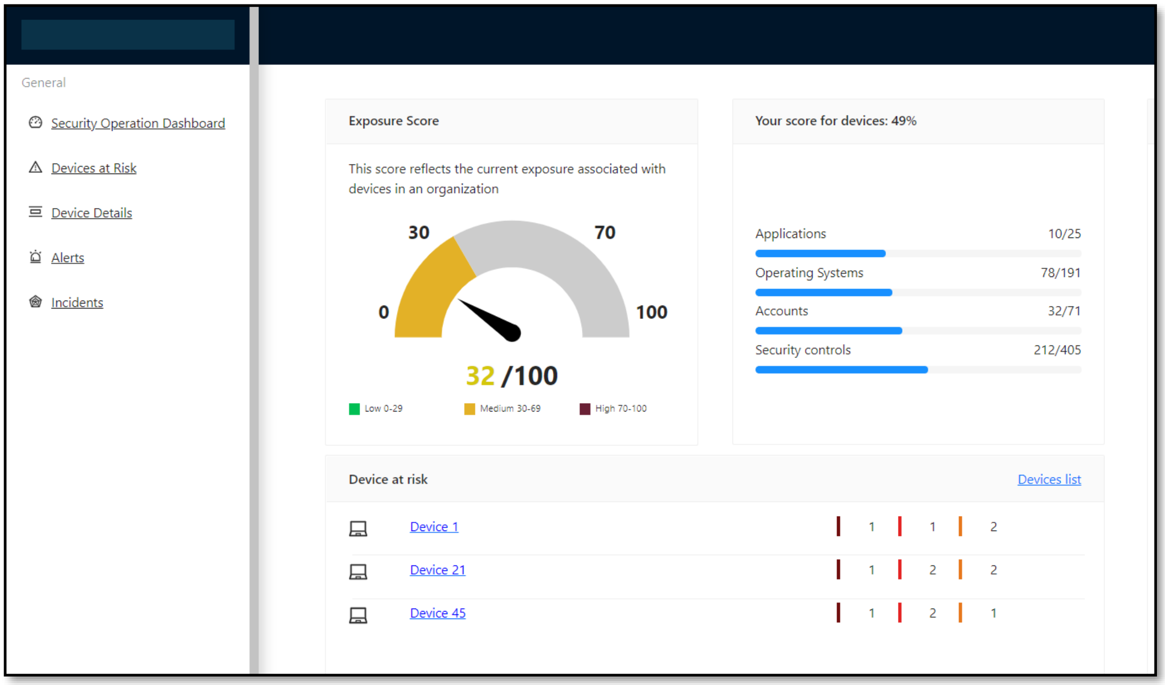
### 5.3.3 Scenario 2 – Unauthorized Software

| | |
|---|---|
| **Scenario Background** | One of the employees has noted that the required resources for effective bitcoin mining exceed what he has personally available at home. Therefore, he has decided to exploit the hospital resources and install a bitcoin mining application on his work device to continue mining for his personal gain. |
| **Actors** | The actors involved in this threat scenario are:<br>• The employee<br>• The bitcoin mining application<br>The actors involved in the incident handling are:<br>• Tier 1 analysts |
| **Threats** | The main threat in this scenario is: Unauthorised use of system resources. |
| **Effect** | The main effects that could result are:<br>• Excessive use of system resources<br>• The employee could waste work time and resources on personal activities. |
| **Impact** | The possible longer-term impacts include:<br>• Effort necessary to remove the application and assess its impact, including if it has been installed elsewhere or if it has a malicious payload.<br>• The employee who makes personal profits from the hospital resources may inspire others to do the same. Staff discipline is required; therefore, the investigation and action are necessary to prevent future employees from downloading this type of application. |

| | |
|---|---|
| **The toolset used to solve the incident when not using the recommended system** | The analyst will need to change his interface many times to address the incident. They will use:<br>- Digital Forensic Tools<br>- SIEM<br>- Antivirus software<br>- IDS |

### 5.3.4 The Application on the System

As known, the SOC operates 24 hours a day monitoring security. Suppose that on Sunday the 9th of March at 11 am during real-time monitoring, an analyst noticed on the Security Dashboard that the exposure score level began to increase until it reached the medium (yellow) level, which indicates that the organisation devices are under threat or at risk, **Figure 24**.



Exposure Score

This score reflects the current exposure associated with devices in an organization

32 /100

🟩 Low 0-29 🟨 Medium 30-69 🟥 High 70-100

Your score for devices: 49%

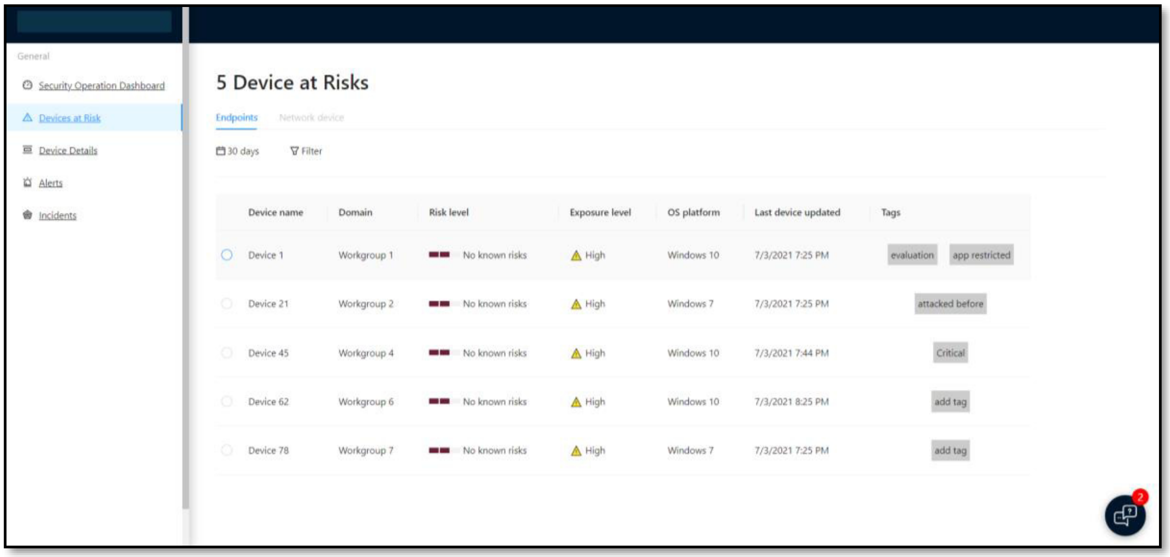
| | |
|---|---|
| Applications | 10/25 |
| Operating Systems | 78/191 |
| Accounts | 32/71 |
| Security controls | 212/405 |

Device at risk

| | | | |
|---|---|---|---|
| Device 1 | 1 | 1 | 2 |
| Device 21 | 1 | 2 | 2 |
| Device 45 | 1 | 2 | 1 |

**Figure 24: Reviewing the Dashboard**

After that, he started to figure out which devices were at risk by reviewing the Devices at Risk page. In seconds, he notices that there are five devices from several network domains, and they all have the same level of risk, **Figure 25**.

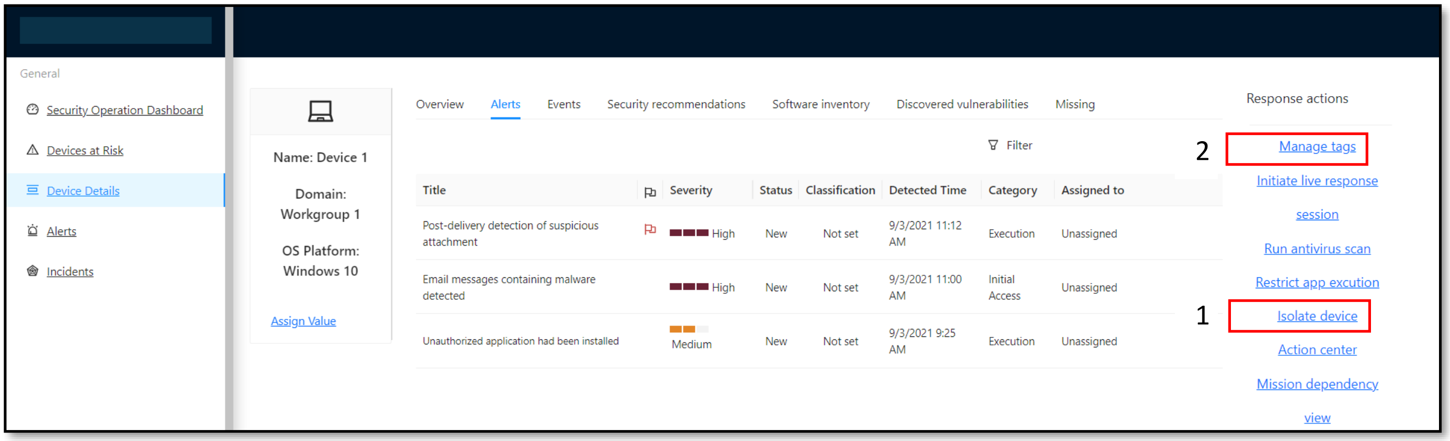


5 Device at Risks

| Device name | Domain | Risk level | Exposure level | OS platform | Last device updated | Tags |
|---|---|---|---|---|---|---|
| Device 1 | Workgroup 1 | No known risks | High | Windows 10 | 7/3/2021 7:25 PM | evaluation<br>app restricted |
| Device 21 | Workgroup 2 | No known risks | High | Windows 7 | 7/3/2021 7:25 PM | attacked before |
| Device 45 | Workgroup 4 | No known risks | High | Windows 10 | 7/3/2021 7:44 PM | Critical |
| Device 62 | Workgroup 6 | No known risks | High | Windows 10 | 7/3/2021 8:25 PM | add tag |
| Device 78 | Workgroup 7 | No known risks | High | Windows 7 | 7/3/2021 7:25 PM | add tag |

**Figure 25: Five Devices at Risk**

To investigate the devices, the alerts and security recommendations related to each device should be checked and reviewed in order to fully understand the situation and make the right decision regarding the response and mitigation actions. In the Alerts tabs of the devices, a number of alerts have been seen; email messages containing malware detected, post-delivery detection of suspicious attachment, and email reported by user as malware or phish. **Figure 26** presents the alerts that related to Device 1. In addition, another type of alert is discovered in Device 1, but with low severity level; unauthorized application had been installed.



Name: Device 1

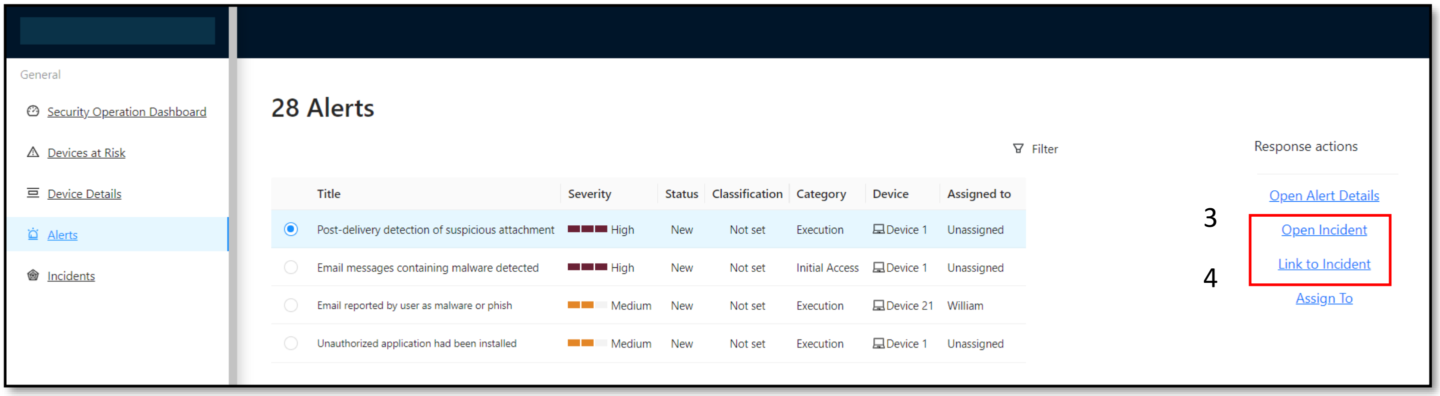
Domain: Workgroup 1

OS Platform: Windows 10

| Title | | Severity | Status | Classification | Detected Time | Category | Assigned to |
|---|---|---|---|---|---|---|---|
| Post-delivery detection of suspicious attachment | | High | New | Not set | 9/3/2021 11:12 AM | Execution | Unassigned |
| Email messages containing malware detected | | High | New | Not set | 9/3/2021 11:00 AM | Initial Access | Unassigned |
| Unauthorized application had been installed | | Medium | New | Not set | 9/3/2021 9:25 AM | Execution | Unassigned |

**Figure 26: Alerts Tab of Device 1**

In this case, the tier 1 analyst focused on: 1) isolating the five devices of the network, 2) tagging them as under phishing. These two actions could be done through the response actions of each device, **Figure 26**. After that Tier 1 analyst can 3) open an incident (ticket), then 4) linking all the related alerts from the Alerts page, **Figure 27**. In addition, Tier 1 analyst can 5) manage the alerts through Alerts Details page.

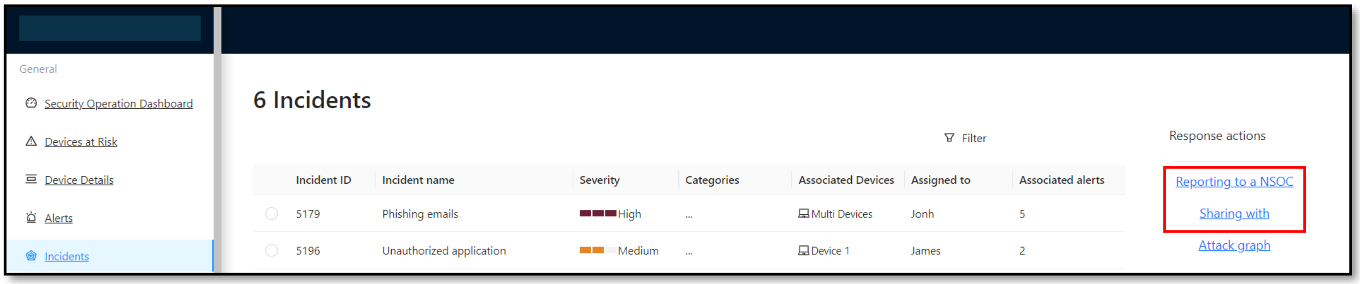


28 Alerts

| | Title | Severity | Status | Classification | Category | Device | Assigned to |
|---|---|---|---|---|---|---|---|
| ● | Post-delivery detection of suspicious attachment | High | New | Not set | Execution | Device 1 | Unassigned |
| ○ | Email messages containing malware detected | High | New | Not set | Initial Access | Device 1 | Unassigned |
| ○ | Email reported by user as malware or phish | Medium | New | Not set | Execution | Device 21 | William |
| ○ | Unauthorized application had been installed | Medium | New | Not set | Execution | Device 1 | Unassigned |

**Figure 27: Open an Incident (ticket) and Link the Alerts**

Now, the phishing emails case has been escalated to tier 2 to understand how far this threat extends and what the necessary actions to remove it, **Figure 28**.

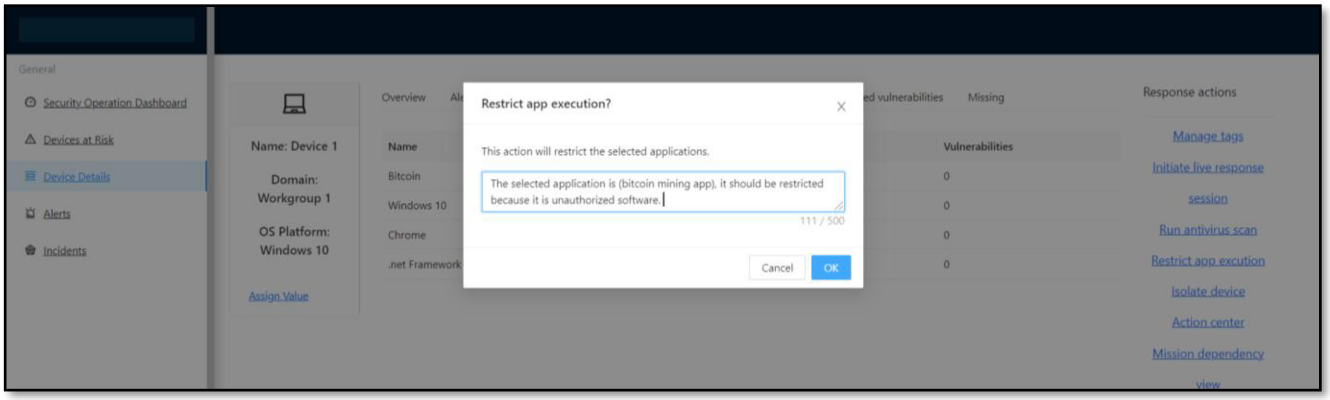


6 Incidents

| | Incident ID | Incident name | Severity | Categories | Associated Devices | Assigned to | Associated alerts |
|---|---|---|---|---|---|---|---|
| ○ | 5179 | Phishing emails | High | ... | Multi Devices | Jonh | 5 |
| ○ | 5196 | Unauthorized application | Medium | ... | Device 1 | James | 2 |

**Figure 28: Cyber Security Incidents**

In terms of the unauthorised application, the tier 1 analyst can also handle it partially by 1) reviewing the software inventory of the device, 2) selecting to restrict app execution, **Figure 29**.



| Name | Vulnerabilities |
|---|---|
| Bitcoin | 0 |
| Windows 10 | 0 |
| Chrome | 0 |
| .net Framework | 0 |

Restrict app execution?

This action will restrict the selected applications.

The selected application is (bitcoin mining app), it should be restricted because it is unauthorized software.

111 / 500

**Figure 29: Response to Unauthorized Application**

After that, he could escalate it as an incident to let a tier 2 analyst investigate more about the application that was installed, such as whether it is just on a single device, whether it is only a case of unauthorised software or if there is any malicious payload involved, **Figure 28**.

In tier 2, the analyst now can perform an in-depth analysis of the incidents through reviewing the events in the Event Tab, or through remote incident response by selecting initiate a live response session or doing malware & implant analysis by selecting run antivirus scan, **Figure 26.** After containing the threats, all data related to the incidents such as a malware sample, analysis for Indicators of Compromise (IOCs) and possible signatures must be collected, written and then shared with trusted partner organisations and National SOC, **Figure 28.**

# Chapter 6: Conclusion

## 6.1 Conclusion

This research was motivated by the growing need of efficient Cybersecurity Operation Centres (SOCs) to secure the operations of critical infrastructures. This need was the result of the increasing number of cybersecurity threats and incidents, with the dependence on cyberspace to conduct most of the operations. However, most of SOCs are facing some challenges that hinder the cybersecurity operators from achieving CSA and making an appropriate decision, e.g., the variety of toolsets, data challenges, and limited budget. Therefore, recommending an integrated system to improve the decisions by providing CSA on a unified platform and addressing the SOC operations challenges was the main objective of this research. To achieve this, there was focusing on identifying the SOCs challenges with their solutions, contributing to improve CSA for the decision-making process, determining the basic requirements to establish the system. For improve CSA, we proposed a OOPDA model that supports the concept of achieving CSA must be a continuous (loop) process as well as CSA and decision-making are not separate processes but are strictly connected. To further strengthen the proposed model, various components and tools that would help achieve and maintain CSA have been provided, defined, and classified based on the proposed model (OOPDA). In addition, we designed our recommended system based on it. The recommended system (DSS-CSA) is designed as a prototype, in order to integrate some valuable features of the existing tools to improve the cybersecurity operations. It illustrates the important of utilising multiple data sources, having a high-level overview as a security dashboard, presenting the endpoints with all the related information from alerts, vulnerabilities, and security recommendations.

## 6.2 Future Work

The cybersecurity is constantly evolving, thus the opportunities for improving CSA needs to keep up with this evolution as a future work. Further, in terms of the DSS-CSA system, it needs to be improved more based on the needs of cybersecurity teams and incident handlers. As we suggesting that visualizes the attack and mission dependency is critical for the decision making process, thus further study to implement these views is needed with different visualization techniques. In addition, the system functionalities that based on the data analysis and algorithms must be illustrated and identified. Furthermore, we noticed that there are some directions of interested future research that need to be addressed: the prediction phase of the CSA and correlation of data sources.

# References

Agyepong, E. et al. 2020. Challenges and performance metrics for security operations center analysts: a systematic review. Journal of Cyber Security Technology 4(3), pp. 125–152. Available at: https://doi.org/10.1080/23742917.2019.1698178.

Alexander, L. 2002. Decision support systems in the 21st century. doi: 10.1145/571681.571692.

ALHARBI, S.A. 2020. A qualitative study on security operations centers in saudi arabia: Challenges and research directions. Journal of Theoretical and Applied Information Technology 98(24), pp. 3972–3982.

Analytics, C. 2017. Abstract : Cybersecurity Analytics and Operations in Transition. (July)

AntDesign. Available at: https://ant.design/ [Accessed: 9 September 2021].

Andersson, J. 2010. Decision Support Systems in Small Firms Decision Making with Financial Information Decision Support Systems in Small Firms :, p. 52.

Angelini, M. and Santucci, G. 2015. Visual cyber situational awareness for critical infrastructures. ACM International Conference Proceeding Series (August), pp. 83–92. doi: 10.1145/2801040.2801052.

Arshad, J. et al. 2020. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics (Switzerland) 9(4), pp. 1–24. doi: 10.3390/electronics9040629.

Artman, H. 2000. Team situation assessment and information distribution. Ergonomics 43(8), pp. 1111–1128. doi: 10.1080/00140130050084905.

Barford, P. et al. 2010. Cyber SA: Situational awareness for cyber defense. Advances in Information Security 46, pp. 3–13. doi: 10.1007/978-1-4419-0140-8_1.

Boyd, J. 1996. The Essence of Winning and Losing. A Discourse on Winning and Losing - Unpublisched Lecture Notes. A Discourse on Winning and Losing - Unpublisched Lecture Notes (August). Available at: http://dnipogo.org/john-r-boyd/ [Accessed: 13 August 2021]

Bricata. Cybersecurity Tools in Financial Services Have Become Part of the Problem Available at: https://bricata.com/blog/cybersecurity-financial-services/ [Accessed: 1 September 2021].

Brosset, D. et al. Cr @ ck3n : a cyber alerts visualization object., pp. 8–9.

CISCO. What Is a Firewall? Available at: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html [Accessed: 20 August 2021].

CISCO. What Is Network Monitoring? Available at: https://www.cisco.com/c/en_uk/solutions/automation/what-is-network-monitoring.html [Accessed: 29 September 2021].

Chamiekara, G.W.P. et al. 2018. AutoSOC: A low budget flexible security operations platform for enterprises and organizations. 2017 National Information Technology Conference, NITC 2017 2017-Septe, pp. 100–105. doi: 10.1109/NITC.2017.8285644.

Cyber Situation Awareness via IP Flow Monitoring. 2018.

Dressler, J. et al. 2014. Operational data classes for establishing situational awareness in cyberspace. International Conference on Cyber Conflict, CYCON 2014, pp. 175–186. doi: 10.1109/CYCON.2014.6916402.

Druzdzel, M.J. and Flynn, R.R. 2011. Decision support systems. Understanding Information Retrieval Systems: Management, Types, and Standards , pp. 461–472. doi: 10.1177/0193841x8500900105.

EKU Online. Risk Identification: 7 Essentials Available at: https://safetymanagement.eku.edu/blog/risk-identification/ [Accessed: 10 August 2021].

Evesti, A. et al. 2017. Cybersecurity situational awareness taxonomy. 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA 2017 , pp. 1–8. doi: 10.1109/CyberSA.2017.8073386.

Factoring Chain International (FCI) 2020. Annual review 2020. at - Automatisierungstechnik 68(12), pp. 979–981. Available at: https://fci.nl/en/annual-review?language_content_entity=en.

Galipalli, A.K. and Madyala, H.J. 2012. Process To Build An Efficient Decision Support System – Identifying Important Aspects of A DSS. University of Boras , p. 66. Available at: https://pdfs.semanticscholar.org/c9ed/b0fd3d75e97c713fb583cfd5353bd3fd5933.pdf [Accessed: 13 August 2021]

Garc, V. 2021. Algorithms in Decision Support Systems. doi: 10.3390/books978-3-0365-0589-3.

Graf, R. et al. 2016. A decision support model for situational awareness in National Cyber Operations Centers. 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016 , pp. 1–6. doi: 10.1109/CyberSA.2016.7503281.

Gutzwiller, R. 2019. Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015. Niwc-Tr-3184 (June)

Hellesen, N. 2019. Cyber Situational Security Awareness Architecture ( CSSA ) for Industrial Control Systems. Available at: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2617748/no.ntnu%3Ainspera%3A2455111.pdf?sequence=1&isAllowed=y [Accessed: 23 August 2021]

Hevner, A. et al. 2004. Design Science in IS Research. MIS Quarterly 28(1), pp. 75–105.

Hibshi, H. et al. 2011. Usability of forensics tools: A user study. Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011 , pp. 81–91. doi: 10.1109/IMF.2011.19.

Huang, Z. et al. 2016. Fuzzy sets based team decision-making for Cyber Situation Awareness. Proceedings - IEEE Military Communications Conference MILCOM , pp. 1077–1082. doi: 10.1109/MILCOM.2016.7795473.

Husák, M. et al. 2020a. SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. ACM International Conference Proceeding Series (August). doi: 10.1145/3407023.3407062.

Husák, M. et al. 2020b. SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. ACM International Conference Proceeding Series , pp. 1–23. doi: 10.1145/3407023.3407062.

IEEE. The Use of Artificial Intelligence in Cybersecurity: A Review Available at: https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity [Accessed: 29 September 2021].

Imanimehr, F. et al. 2020. An Architecture for National Information Sharing and Alerting System. 2020 10th International Symposium on Telecommunications: Smart Communications for a Better Life, IST 2020 , pp. 217–221. doi: 10.1109/IST50524.2020.9345861.

Johannesson, P. and Perjons, E. 2012. A Design Science Primer CreateSpace.

Khodashahri, N.G. and Sarabi, M.M.H. 2013. Decision Support System ( DSS ). Singaporean Journal of Business , Economics and Management Studies 1(6), pp. 95–102. doi: 10.12816/0003780.

Kim, D. et al. 2016. 'I know what you did before': General framework for correlation analysis of cyber threat incidents. Proceedings - IEEE Military Communications Conference MILCOM , pp. 782–787. doi: 10.1109/MILCOM.2016.7795424.

Klein, G. et al. 2011. From detection to reaction - A holistic approach to cyber defense. 2011 Defense Science Research Conference and Expo, DSR 2011 . doi: 10.1109/DSR.2011.6026824.

Komárková, J. et al. 2018. CRUSOE: Data model for cyber situational awareness. ACM International Conference Proceeding Series (August). doi: 10.1145/3230833.3232798.

Matta, L. and Husak, M. 2021. A Dashboard for Cyber Situational Awareness and Decision Support in Network Security Management. Proceedings of the IM 2021 - 2021 IFIP/IEEE International Symposium on Integrated Network Management , pp. 716–717.

Mcafee. What Is Security Information and Event Management (SIEM)? Available at: https://www.mcafee.com/enterprise/en-gb/security-awareness/operations/what-is-siem.html [Accessed: 29 September 2021].

Microsoft, 2021. Exposure score - threat and vulnerability management Available at: [Accessed: 1 September 2021].

Moye, T. et al. 2015. Cyber Situational Awareness. 0044

Nakhla, N. et al. 2017. Automated computer network defence using ARMOUR: Mission-oriented decision support and vulnerability mitigation. 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA 2017 . doi: 10.1109/CyberSA.2017.8073389.

National Cybersecurity Authority (NCA), 2021. About NCA Available at: https://nca.gov.sa/en/pages/about.html [Accessed: 10 August 2021].

Noel, S. et al. 2016. CyGraph: Graph-Based Analytics and Visualization for Cybersecurity. 1st ed. Elsevier B.V. Available at: http://dx.doi.org/10.1016/bs.host.2016.07.001 [Accessed: 10 August 2021]

Oltramari, A. et al. 2013. Towards a cognitive system for decision support in cyber operations. CEUR Workshop Proceedings 1097, pp. 94–100.

Pahi, T. et al. 2017. Analysis and assessment of situational awareness models for national cyber security centers. ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy 2017-Janua(Icissp), pp. 334–345. doi: 10.5220/0006149703340345.

Rapid. User and Entity Behavior Analytics (UEBA) defined and explained Available at: https://www.rapid7.com/fundamentals/user-behavior-analytics/ [Accessed: 29 September 2021].

Richards, D. 2017. The Benefits of Artificial Intelligence on Workplace Productivity. Mavinlink . Available at: http://blog.mavenlink.com/the-benefits-of-artificial-intelligence-on-workplace-productivity [Accessed: 29 September 2021]

Roldan-Molina, G. et al. 2017. A decision support system for corporations cybersecurity management. Iberian Conference on Information Systems and Technologies, CISTI (September). doi: 10.23919/CISTI.2017.7975826.

Sawilla, R.E. and Wiemer, D.J. 2011. Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework. 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011 , pp. 167–172. doi: 10.1109/THS.2011.6107865.

Skopik, F. et al. 2015. Establishing national cyber situational awareness through incident information clustering. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015 , pp. 1–8. doi: 10.1109/CyberSA.2015.7166126.

Soralwinds. SIEM Tools Available at: https://www.solarwinds.com/security-event-manager/siem-tools [Accessed: 20 August 2021].

Tianfield, H. 2017. Cyber Security Situational Awareness. Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016 , pp. 782–787. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165.

Yuen, J. et al. 2015. Visual analytics for cyber red teaming. 2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015 , pp. 1–8. doi: 10.1109/VIZSEC.2015.7312765.

Zimmerman, C. 2014. Cybersecurity Operations Center. Available at: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf [Accessed: 16 August 2021]