SAVONIA

THESIS – BACHELOR'S DEGREE
TECHNOLOGY, COMMUNICATION AND TRANSPORT

CYBERSECURITY

Mitigating The Risk as SOC Alert Analyst and Incident Responder

AUTHOR/S Mayowa Oguntoyinbo

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology, Internet of Things	
Author Mayowa Oguntoyinbo	
Title of Thesis Mitigating the risk as SOC alert analyst and incident responder	
Date 15th April, 2025	Pages/Appendices 51
Client Organisation /Partners Savonia University of Applied Sciences	

The purpose of this thesis is to look at the key roles and challenges that Tier-1 Security Operations Center (SOC) alert analysts and incident responders deal with when managing cybersecurity risks.
The main goal was to pinpoint their duties, evaluate the risks they face, and suggest ways to make SOCs work better. The research took a hands-on approach, pulling together literature reviews, industry reports, and case studies to examine risks like alert fatigue, tricky threats, skill shortages, and problems with tool integration.
The data found that 50-72% of alerts are false alarms, which can lead to analyst burnout. At the same time, advanced threats and zero-day exploits make responding tougher. Suggested solutions included using AI to prioritize alerts, having standard incident responses, and providing ongoing training to tackle the worldwide shortage of about 4.8 million cybersecurity professionals.
These findings give practical ideas for organizations to strengthen their SOCs, reduce response times, and improve cybersecurity readiness, which can help lessen the financial and reputational impacts of cyber threats.

Keywords
Cybersecurity | SOC | Incident Responder | Zero Trust Framework | Alert Triage | False Positives

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. Background of the Study.

The emergence of a borderless society through cyberspace has altered global social and technological viewpoints. The fast-paced digitization of enterprises and the growing reliance on cloud-based technologies have increased cybercrime activities. According to a report issued by cybersecurity ventures, the global cost of cybercrime is predicted to reach $24 trillion per year by 2027as seen in Figure 1. The advent of cyberspace via the internet has resulted in economic growth without restrictions on entrepreneurship and allows people to interact and collaborate.

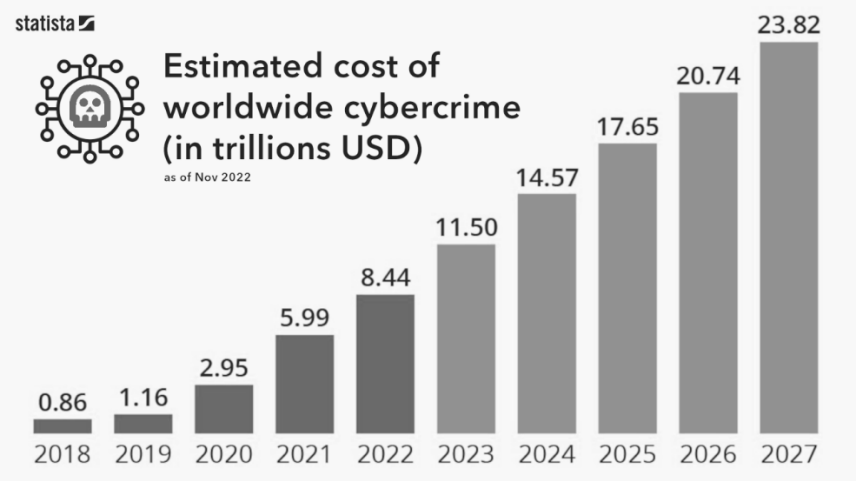

Figure 1. Global cybercrime cost forecast in trillions USD. (Morgan 2018)

Cyberspace has permeated public and private sector organizations, industries, geographical areas, and international borders. People from all around the world, whether individuals or organizations, can communicate informally or professionally through cyberspace. Indirectly, the internet has eliminated boundaries between people from various geographical regions. Public-sector entities have been tasked with developing a suite of online services to transform government service delivery, grow the national economy, and improve the people's well-being. Data and information are non-negotiable in today's digital age because they allow stakeholders to make data-driven decisions, revolutionize employment practices, and expand their business operations. The increase in cyber threats has forced the creation of Security Operations Centers (SOCs) to monitor, identify, and respond to security issues in real-time. Security Operations Centers (SOCs) are centralized units that monitor and improve an organization's security posture. It brings together people's procedures and technology to detect, evaluate, and respond to cybersecurity incidents. SOCs are a must-have for organizations to maintain compliance with regulations such as GDPR, HIPAA, and PCI-DSS. (Shackleford 2015).

1.2. Problem Statement

Today, we live in a world where cybersecurity is rapidly evolving, organizations face an increasing volume and sophistication of threats to safe cyber use. Security Operations Centers (SOCs) play a highly significant role in defending against these threats by monitoring, detecting, and responding to

security incidents in real-time. Because of this, keeping our information safe is super important. People, businesses, and even governments need to worry about cybersecurity now more than ever. Why? Because we use the internet and technology for almost everything! This also brings many dangers, like hacking, malware, scams, and data leaks. However, SOC teams, particularly SOC alert analysts (as defined in 4.2) and incident responders (as defined in 4.3), face significant challenges that hinder their ability to effectively mitigate risks.

In the overwhelming volume of alerts, SOC analysts are inundated with a large volume of security notifications, many of which are false positives, which leads to alert fatigue, where critical alerts may be overlooked, increasing the risk of undetected breaches. (Cuppens 2002).

The threat landscape keeps evolving as cybercriminals are constantly developing new attack techniques, such as advanced persistent threats (APTs) and zero-day exploits. SOC teams often struggle to keep up with the pace of these evolving threats due to limited resources and outdated tools. (MITRE 2023).

1.3. Objective of Study

This study takes a closer look at what Tier 1 Security Operations Center (SOC) alert analysts and incident responders do to help reduce cybersecurity risks. With more and more cyber threats popping up every day, it is crucial to grasp how these Tier 1 analysts play a part in keeping an organization safe. They are often in the first line of defense, working behind the scenes to spot potential issues and respond quickly. By figuring out their specific roles, we can gain insight into how they help strengthen the overall security of a business. This understanding is vital, especially nowadays when threats are constantly evolving, and organizations need to stay one step ahead of cybercriminals. The specific objectives are

- To identify the primary responsibilities of Tier 1 analysts
- To assess the risk faced by alert analysts and incident responders
- To analyze the impact of the risk on the organization’s cybersecurity posture
- How to mitigate the risk

1.4. Significance of Study

To enhance organizational resilience, effective SOC operations are critical for organizations to uncover, respond to, and recover from cyber incidents. By identifying and addressing the challenges faced by SOC teams, this study helps organizations build more resilient cybersecurity postures. This, in turn, reduces the likelihood of financial losses, reputational damage, and regulatory penalties. (National Institute of Standards and Technology 2018).

This guide emphasizes the importance of effective incident response in reducing the impact of cybercrime mishaps on organizations.

The lack of standardized processes in SOC operations often leads to inconsistent and inefficient incident handling. This study proposes the implementation of standardized incident response playbooks and workflows, which can improve the consistency and efficiency of SOC operations. Standardization also facilitates better collaboration and knowledge sharing among SOC teams. (ISC² 2021). This report highlights the need for standardized processes and training to address the skills gap in cybersecurity.

1.5. Scope and Limitations of the Study

This study may be limited by the availability of data from SOC teams, as many organizations are reluctant to share detailed information about their cybersecurity operations due to confidentiality concerns. (ISC² 2021). The findings of this study may not be universally applicable to all SOCs, as the specific challenges and solutions can vary with considerations for factors such as size, industry, and maturity level of the organization. (Cuppens 2002). Proceedings of the IEEE Symposium on Security and Privacy. New threats and attack techniques are constantly emerging, while the cybersecurity landscape is continually evolving. This study may not discuss the latest findings in the field, as the research is conducted within a specific timeframe. (Skoudis 2006). Resource constraints like time, budget, and access to advanced tools and technologies may limit the study. These constraints could impact the depth and breadth of the research. (Whitman & Mattord 2018).

2. CYBERSECURITY

Cybersecurity is about keeping digital systems, networks, and data safe from unwanted access, attacks, or damage (Cichonski 2012). The state of being protected against any criminal or unauthorized use of electronic data is also referred to as cybersecurity. It is all about protecting our computers and data from threat actors who want to steal or mess them up. It involves smart practices, tools, and rules to keep our information safe. We need to make sure that our data is secret, correct, and always ready to use. If we do not, we might lose money, our good name, and even face legal troubles.

As new cyber threats pop up, we must find new ways to fight them. Companies and governments around the world are putting money into cybersecurity plans and using strong encryption to keep important information safe. But it is not just about money. People also need to be aware and know how to stay safe online. This means understanding what not to click on and how to spot scams.

This writing will look at the basics of cybersecurity. We will focus on the common problems that digital systems face and check out the latest technologies to stay safe. We'll also offer tips on how organizations can improve their security in a world that is more connected than ever. In an age where almost everything is online, understanding these things is key to staying safe.

Figure 2. Cybersecurity Workforce Estimate. ISC^2 (Cybersecurity Workforce Study 2022)

In Figure 2. The image showcases the estimated number of cybersecurity professionals worldwide in 2022. According to the stats, about 4.65 million people are working in this field, which is up by 11.1% from last year. The United States is at the top of the list with the most cybersecurity workers, followed closely by Brazil and Mexico, which also see steady growth in this area. Countries like Japan, France, and the Netherlands are ramping up their hiring efforts too, showing that they are serious about boosting their cybersecurity teams. Unfortunately, not everyone is faring so well; Singapore and Germany experienced a drop in their cybersecurity workforce, with Singapore seeing the biggest decrease. All in all, this data shows a clear trend: countries worldwide are expanding their cybersecurity teams because they need to tackle the growing number of digital threats out there.

2.1. Overview of Cybersecurity and Security Operations Centers.

Security Operations Center SOC is a centralized function or team responsible for improving an organization’s cybersecurity posture and preventing, detecting, and responding to threats. (Microsoft 2025) SOC is a team or place in a company that keeps an eye on and responds to cybersecurity threats and incidents in real time. The SOC has the tools, processes, and people in place to keep the organization's systems, networks, and data safe from cyberattacks. SOC is the nerve center of your organization's cybersecurity and day-to-day security operations.

Cybersecurity and Security Operations Centers (SOC) go hand in hand. Think of the SOC as the main control center for all things related to cybersecurity.

Cybersecurity is a broad term. It includes everything we do to keep our digital information safe from bad actors. Meanwhile, the SOC handles the day-to-day tasks of monitoring and managing these protective actions.

As cyber threats keep changing and getting cleverer, having a strong SOC is super important. It is like having a team of guards who are always on alert. They make sure that businesses are ready to tackle any dangers that might pop up.

In simple terms, the SOC is where the action happens. They are the ones who spot issues and respond right away. This helps protect the organization from various cyber risks. Without the SOC, keeping our information safe would be a lot harder.

So, if you care about cybersecurity, you should pay attention to what SOC does. Their work is vital in today’s digital age. They help ensure that companies can operate smoothly while staying protected from constant online threats.

3. LITERATURE REVIEW

3.1. Security Operations Center (SOC)

A Security Operations Center, or SOC, is like a safety hub for many organizations. SOC is not a company or government agency, but it is a function or unit within an organization (either private or public). It keeps a constant watch over possible cybersecurity threats. Security Operations Centers (SOCs) can be set up in two main ways. Some big companies run their own SOCs with their own cybersecurity teams. Others might hire outside experts from Managed Security Service Providers.

Figure 3. SOC Network. (cyberSafeus 2022)

There is also a mix of both, where a company uses both in-house and outside help. The choice depends on what the organization needs and what it can handle. SOC is very important because it helps organizations stay safe with quick replies to any issues and keeps an eye on any helpful information about potential risks.

At the heart of a SOC, you have a log collection as shown in Figure 3, which is gathering data from a bunch of different places. This data gets sent off to various systems, where it gets analyzed to spot any potential threats. It is super important that the right people are kept in the loop when something goes wrong, and that is what reporting is all about—keeping everyone updated on incidents and the latest security trends. To keep one step ahead of hackers and other bad actors out there, the SOC engages in research and development. This means they are constantly working on new tools and strategies to address those tricky, ever-changing threats. Then you've got threat intelligence, which is all about gathering information regarding who the attackers might be and what their tactics look like. A reliable knowledge base comes in handy as well. It includes all the necessary documents and playbooks that analysts can refer to when dealing with incidents. Speaking of incidents, there is a

ticketing system that helps organize and manage how these situations are dealt with, making sure nothing slips through the cracks.

SIEM Security Information and Event Management tools are critical in connecting the dots when it comes to events and identifying real-time threats. They help analysts see what is happening across the board. Finally, aggregation and correlation are essential too. They bring together data from different platforms so patterns can be spotted. This is all about making the SOC work smoothly and efficiently to keep everything secure. (SANS 2021).

3.2. The Role of SOC in Cybersecurity

The Security Operations Center (SOC) is important in maintaining cybersecurity by constantly monitoring all traffic and security alerts. They ensure that any unusual or suspicious activity is quickly identified, allowing for an immediate response to potential threats. (Salinas 2023). The SOC springs into action in a cyber-attack to manage the incident. Their rapid response is necessary to stop the danger and understand the situation, all with the primary goal of minimizing damage to the organization. Their expertise helps mitigate risks effectively and restore normal operations as swiftly as possible. In addition to their reactive measures, the SOC also focuses on threat intelligence. They actively seek out information about emerging threats and vulnerabilities. By staying informed, they can help the organization’s defenses and proactively prepare for potential attacks before they occur.

Another major responsibility of the SOC is vulnerability management. They regularly assess systems and applications for weaknesses, ensuring that any identified issues are addressed promptly to eliminate opportunities for hackers to exploit. (Chinnasamy 2023). Furthermore, the SOC plays a key role in compliance support. Organizations must adhere to cybersecurity regulations, such as GDPR and NIST guidelines. The SOC helps companies follow these regulations and align their security practices with industry standards. This proactive method makes the organization's security much better overall.

Cybersecurity is needed today because individuals, businesses, and governments rely heavily on technology. With the right efforts to protect our networks and information, we can all enjoy a safer online experience. Organizations and individuals must stay alert and informed about how best to prepare against cyber threats. Cybersecurity entails safeguarding data, networks, and systems from internet-based risks such as malware, hacking, and illegal access.

3.3. Benefits of Security Operation Center

A Security Operations Center (SOC) offers numerous advantages for organizations seeking to strengthen their cybersecurity measures. These days, security needs to be considered in every decision your company makes. Therefore, a centralized SOC has many advantages. One of the primary

benefits is asset protection. A SOC's proactive monitoring and rapid response capabilities are important in preventing unauthorized access and mitigating the risks associated with data breaches. (Scapicchio 2025) By safeguarding major systems, sensitive information, and intellectual property, SOCs significantly enhance a company's defenses against security violations and theft. SOCs contribute to business continuity by effectively reducing the frequency and impact of security incidents. This function is beneficial in ensuring that organizations maintain uninterrupted operations, which upholds productivity levels, preserves revenue streams, and sustains customer satisfaction.

Regulatory compliance is another significant benefit that SOCs offer. (Miller 2024). Through the implementation of flexible security measures and the maintenance of thorough records of incidents and the responses that followed, these centers help firms comply with a variety of legal obligations and industry requirements regarding cybersecurity. This adherence supports a secure environment and reinforces an organization’s commitment to ethical operations. Additionally, the financial implications of investing in SOC are noteworthy. Proactive security measures can lead to substantial cost savings by averting the potentially exorbitant expenses associated with data breaches and cyberattacks. (Meisner 2017). Compared to the financial consequences and harm to one's reputation that arise from security-related incidents, the initial expenditure in such security architecture is typically far cheaper. Outsourcing a Security Operations Center (SOC) can be a smart move for many small and medium-sized businesses. Running an in-house SOC demands a lot of money for tech, skilled staff, and round-the-clock operations—resources that many smaller companies just do not have. By turning to a Managed Security Service Provider (MSSP), these businesses get expert monitoring, threat detection, and incident response without the heavy costs of building their own team. This way, they can keep costs down and gain access to better tools and skills that might be out of reach otherwise.

Building customer trust is yet another significant benefit of operating an SOC. Demonstrating a steadfast commitment to cybersecurity helps enhance the confidence of customers and those involved, establishing a sense of security in the organization’s operations. (Panditharathna 2024). SOCs improve incident response capabilities. Their rapid response frameworks are essential for reducing downtime and minimizing financial losses associated with security breaches. By effectively containing threats and expediting the restoration of normal operations, SOCs play an instrumental role in limiting disruptions.

Lastly, enhanced risk management is achieved through the diligent analysis of security events and trends by SOC teams. This analysis allows organizations to pinpoint potential vulnerabilities proactively, enabling them to implement measures that mitigate these risks before they can be exploited. Furthermore, through continuous monitoring of networks and systems, SOCs enhance proactive threat detection, allowing for the swift identification and neutralization of security threats. This proactive approach alleviates potential damage and data breaches and fortifies organizations against an

ever-evolving threat landscape. Let's review the main advantages of SOC. Your business can accomplish the following thanks to SOCs. These advantages are difficult to quantify because they essentially keep your company operating.

- Act more swiftly: The SOC offers a comprehensive, real-time, consolidated view of the security performance of the whole infrastructure, including thousands of endpoints and all locations. You can recognize, detect, stop, and fix problems before they become serious problems.
- Preserve consumer and customer confidence: Your clients are growing more concerned about privacy. Establishing a SOC to safeguard client information might contribute to increased trust in your company.
- Reduce expenses: While having SOC is not prohibitively expensive, the price of a data breach or loss is. Better still? SOC staff will make sure you make the most of the appropriate tools.

3.4. Existing Risk Mitigation Strategies

In Security Operations Center (SOC) operations, risk mitigation strategies involve proactive measures to minimize, control, or eliminate potential threats and vulnerabilities, encompassing techniques like risk avoidance, reduction, transfer, and acceptance. Most risk mitigation strategies in SOC Operations can be classified into the following:

- Risk avoidance is all about steering clear of things that might put the organization in a tough spot. (Wojno 2021). For instance, if there is a software application that is been flagged as a potential risk, the Security Operations Center (SOC) team may suggest getting rid of it or swapping it out for something safer. This can help keep the company safe from any problems that could arise from that risky software. It is about playing it safe and making smart choices to avoid any headaches down the line. If a product or process could cause issues, it is often better to just cut it out altogether rather than take the chance.

- Risk reduction is all about lowering the chances of something bad happening or at least making sure that if it does happen, it does not hit too hard. This strategy involves putting in place some smart security measures and following certain processes to keep things in check. For instance, one simple way to reduce risk is by making sure that only certain people can access sensitive information. This can be done by using strong passwords or two-factor authentication, which adds an extra layer of security. Another important step is to keep your software up to date. Regularly patching systems helps to close any holes that might be easy targets for cyber threat actors. Finally, it is a good idea to run vulnerability scans from time to time. This means checking your systems for any weaknesses that need to be addressed before someone else finds them. By sticking to these practices, businesses can create a safer environment, ultimately protecting themselves from potential issues down the line. It is all about being proactive and making sure that risks are kept at bay as much as possible. (Samson 2025).

- Risk transfer is all about passing on the responsibility for dealing with potential problems to someone else. This often happens when businesses buy insurance. It is like saying, “If something goes wrong, we are covered.” Another way to do this is by hiring a third party to handle certain tasks, like security. Instead of having their team, they let someone else manage it, which can help lessen their worries about risks. It is a smart move for many companies, as it helps them focus on what they do best while ensuring they are protected from unexpected issues.

- Risk acceptance is when you decide to go ahead with something even though there might be some dangers involved. You might choose this route if dealing with the risk feels too expensive or tough to manage. In other words, if the risk does not seem like a big deal or the downsides are not that serious, you might just roll with it instead of trying to find ways to dodge those potential problems. It is like saying, I am okay with this risk; I will take my chances. People do this all the time, whether at work, in investments, or even in everyday decisions. It is important to think carefully about what you are accepting so you are not caught off guard later.

Table 1. Summary of Risk Mitigation Strategies in Security Operations Centers

Risk Type	Mitigation Strategy	Reference
Human error	**Employee training and awareness:** conduct regular cybersecurity training to educate employees on recognizing phishing attacks, practicing strong password hygiene, and understanding social engineering tactics.	(Samson 2025)
Unauthorized access	Implement multi-factor authentication (MFA)	
Insider threats	**Establish network access controls:** implement zero-trust models and role-based access to limit access to sensitive information based on job functions.	(Insights 2024)
Malware and viruses	Deploy regularly updated firewalls and antivirus software	
Unpatched vulnerabilities	**Regular software updates and patch management:** Schedule and automate updates to ensure all systems have the latest security patches.	(Samson 2025)
Incident response delays	Create comprehensive incident response plans and conduct regular simulations to ensure preparedness.	(Yuchong and Qinghui 2021)
Weak passwords	Enforce policies requiring complex passwords and regular changes to reduce the risk of credential theft.	(Insights 2024)

Table 1. shows some important strategies for the Security Operations Center (SOC) to handle different cybersecurity threats. To deal with human error, it is a good idea to keep training employees on

spotting phishing attempts, maintaining good password habits, and understanding social engineering tricks. For weak passwords, enforcing strong password rules and changing them regularly helps. To prevent unauthorized access, using multi-factor authentication (MFA) is useful, while managing insider threats can be done through zero-trust models 7.4 and role-based access controls. To fight malware and viruses, keep firewalls and antivirus software up to date. Unpatched software problems can be fixed by scheduling regular updates, and to avoid delays in responding to incidents, having clear plans and running simulations is key.

3.5. SOC Staffing and Functional Duties

SOC's main responsibility is to defend the company from cyberattacks. The Security Operations Center (SOC) has a clear chain of command, with the SOC Lead in charge of everything.

In any organized team, there's usually someone in charge. In this case, that's the SOC Chief, who sets the game plan to tackle threats to the organization.

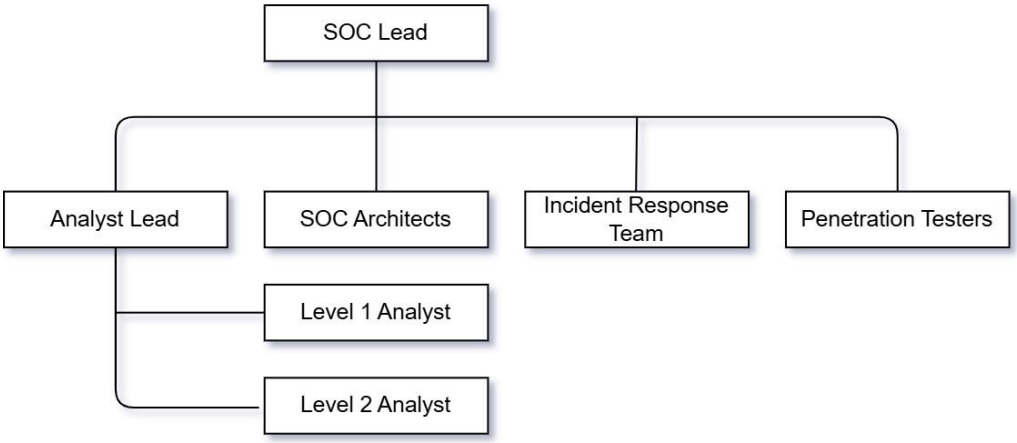

Figure 4. SOC Staffing. (W3Schools.com/cybersecurity)

Then we have the SOC Architect, who makes sure that all the systems and platforms are up to snuff for the team to do their jobs right. They also work on linking data from various sources and making sure the incoming data fits what the platform needs.

The Analyst Lead keeps things running smoothly by developing and maintaining playbooks, so analysts know how to gather the info they need to deal with alerts and possible incidents.

Level 1 Analysts are the ones who first respond to alerts. They try to resolve issues themselves and pass anything complicated up to a more experienced analyst.

Level 2 Analysts have more know-how and experience. They help sort out any problems with alerts and make sure the Analyst Lead knows about any hiccups to help improve how the SOC operates. They also work with the Analyst Lead to escalate incidents to the Incident Response Team.

The Incident Response Team (IRT) is like an extension of the SOC. They jump in to fix the problems that affect the organization.

Penetration Testers play a key role too. They understand how attackers think and can assist in figuring out how breaches happen. It's good practice to merge attack and defense teams, which is called Purple Teaming.

Additional SOC responsibilities and functions include:

- Preserving Relevance: SOC teams must be prepared to handle the most recent threats to the company because the cyber threat landscape is always changing. This entails being abreast of emerging and popular threats and making certain that security systems have a current set of rules to aid in their detection.
- Repairing Vulnerable Systems: Cybercriminals frequently use vulnerability exploitation as an attack vector. Patches for insecure enterprise software and systems must be found, applied, and tested by SOC teams.
- Technology Infrastructure Administration: New security technologies are needed as the enterprise network and the cyber threat scenario change. Their security infrastructure must be identified, deployed, configured, and managed by SOC teams.
- Resolving Support Tickets: The IT department includes numerous SOC teams. This suggests that responding to employee support tickets may be a task for SOC analysts.
- Reporting Line: SOC teams must report to management just like every other team since security is an integral component of the business. Effectively communicating security costs and return on investment to a commercial audience is necessary for this.

SOC teams, of course, have many different tasks and duties. Additionally, some of these duties might be neglected if these teams are understaffed or underfunded. The worry about SOC teams dropping the ball because of not enough staff or funding is a real issue in cybersecurity. SOCs usually have standards for response times, alert handling, and compliance with rules like NIST or ISO 27001. But without adequate resources, these standards can fall short. If teams are understaffed, analysts might get burned out, leading to slow responses or missed alerts. Similarly, not having enough money can restrict access to necessary tools and training, making it tough for a SOC to stay reliable even with existing controls in place. There is quality control and targets. Quality controls in a Security Operations Center (SOC) aim to keep performance steady and reliable. But issues like not having enough staff or budget can hurt this. SOCs set goals, like fixing high-priority alerts in 30 minutes or keeping false-positive rates low, tracking this with metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). When teams are short on staff, analysts can get overloaded and miss these goals. If they are short on funds, they might not have the right tools, like advanced SIEM systems or automation software, which can lead to missed tasks and less reliability, even with controls in place.

4. SECURITY OPERATION CENTRE ANALYST

A SOC Analyst focuses on keeping a company's digital world safe from cyber threats. Think of them as the watchful eyes in the Security Operations Center, which is the main hub where all the action happens regarding cybersecurity. Their job is to keep an eye on what's going on in the IT systems - looking out for any suspicious activity, figuring out if something's a real threat, and taking steps to deal with it when needed. They play a pretty important role in ensuring everything runs smoothly and securely. It is all about staying alert and ready to jump in when something seems off, so the organization can keep its data and systems safely guarded.

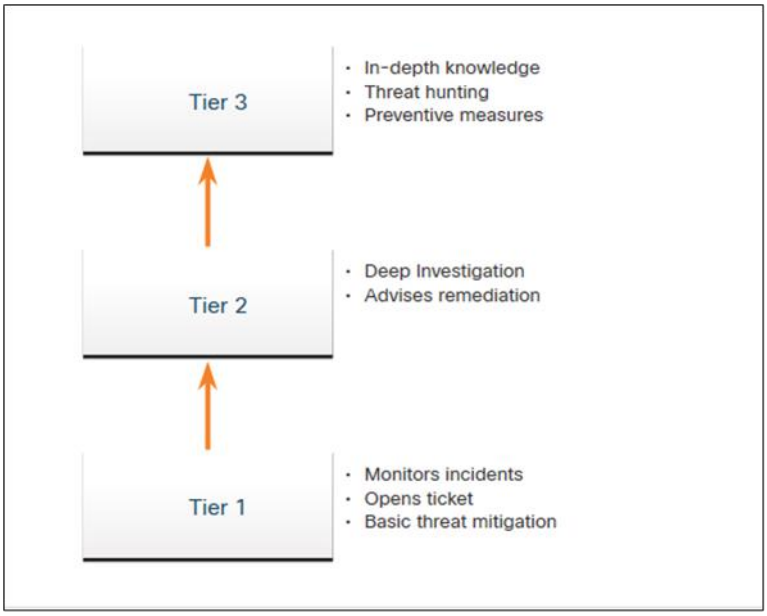

Figure 5. Security Operation Centre Analyst Categories. (ITEXAMANSWERS: CyberOps Associate: Module 2)

4.1. SOC Analysts (Tier 1, 2, 3)

Figure 5 lays out how a SOC, or Security Operations Center analyst team is organized. It starts with the first tier, where the team is mainly focused on keeping an eye on security incidents. They handle things like monitoring alerts, opening tickets for issues that pop up, and taking care of some basic tasks to deal with potential threats.

Then there is the second tier. This group steps in when a deeper investigation is needed. They take a closer look at the incidents reported by the first tier and come up with smart suggestions on how to fix those problems and keep things running smoothly.

Finally, you've got the third tier, which is the highest level in this structure. This team is faced with tougher security issues that the first two tiers might not be able to solve. They not only react to incidents but also actively look for threats before they become issues. Their job is to be a proactive force, using their experience to create plans that prevent future problems from arising. Overall, each tier is important and builds off what the previous one did, creating a layered way to manage security

operations and handle incidents effectively. This setup ensures that no matter the level of complexity, there is a well-defined process for tackling security challenges.

4.2. Role of SOC Alert Analyst

A SOC Alert Analyst, also referred to as the Tier 1 analyst, monitors and responds to security alerts, serving as the first defense against detected threats, analyzing alerts for potential security incidents, and escalating significant issues. In other words, SOC alert analysts are entrusted with surveillance, identification, and swift response to cyber threats, and they are the primary guardians of organizational networks and valuable data repositories. (Cassetto 2024). In a Security Operations Center (SOC), the job goes beyond just monitoring; it is about actively managing alerts from various security tools, understanding their significance, and developing the right strategies to address them

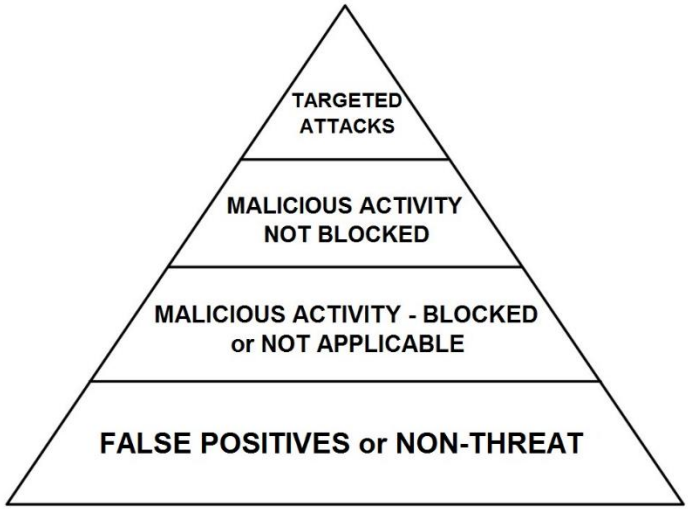

Figure 6. SOC Alert Analyst pyramid (Duncan 2015)

Figure 6 shows a pyramid that lays out how a SOC Alert Analyst sorts alerts based on their importance in spotting and dealing with threats. This model is all about making sure that the most pressing issues are addressed quickly.

At the top, we have Targeted Attacks. These alerts are the ones a SOC alert analyst needs to pay the most attention to. They signal serious, intentional attacks like Advanced Persistent Threats (APTs), which are complex cyberattacks where attackers sneak into a network and stay hidden for a long time to steal information or mess with operations. Since these can pose a big risk, analysts must dive in right away to investigate and escalate these threats to ensure everything is under control.

Next down is the second tier: Malicious Activity Not Blocked. These alerts are a little alarming because they indicate threats that somehow made it through defenses, like when a code or software designed to damage, disrupt, steal, or inflict some other bad or illegitimate action on data, hosts, or networks (malware) runs. Analysts need to figure out how this slipped past their safeguards and act quickly to contain the issue.

Moving on to the third tier, we see Malicious Activity - Blocked or Not Applicable. These alerts indicate threats that were caught by the existing security measures, like firewall rules or are just not an issue at all. In these cases, analysts do check to ensure their defenses are doing their job, but they do not need to focus on these as urgently.

Finally, at the bottom tier, there are False Positives or Non-Threat alerts. This category usually has the most alerts and mostly includes benign things or errors, like misconfigured settings. Analysts work on fine-tuning the detection systems to lessen these types of alerts, which helps prevent alert fatigue where they might miss real threats because they are overwhelmed by noise.

The bottom line is that a SOC Alert Analyst uses this pyramid model to sort through alerts, making sure to tackle the high-risk threats first while finding ways to improve the system to keep the lower-tier alerts from becoming a distraction. This approach helps keep everything running smoothly and ensures that incidents are handled promptly.

4.3. Role of an Incident Responder

Incident responders play a crucial role in the world of cybersecurity. These are the professionals who spring into action when a security breach happens in an organization. Their main goal is to stop any additional damage and keep the impact as low as possible. When a cyberattack or security issue arises, incident responders are the first to assess the situation. They not only deal with the immediate problem but also look at other potential threats that might compromise the organization’s data or systems. (Gomez 2024).

Incident responders have a key role that is different from SOC alert analysts. They jump in to handle and fix serious security issues that the SOC alert analysts cannot handle. They are part of the Incident Response Team and report to the SOC Lead. These responders use their skills to investigate and control big threats, especially during ongoing attacks or data breaches. On the other hand, SOC alert analysts keep an eye on systems and tools used by cybersecurity teams. Their job is to watch the network closely to catch any potential problems before they blow up into bigger issues.

The specific tasks for incident responders can vary depending on the organization they work for. Their duties can change quite a bit based on what’s needed in that setting. A big part of their job is also about being alert to human input, like reports of strange activities or odd emails. Such observations can be vital for catching issues early. To support their work, incident responders have access to specialized tools, including Security Information and Event Management (SIEM) systems. These tools help combine and analyze alerts coming from different parts of the organization’s security setup.

Once they identify a possible breach, incident responders conduct a thorough analysis to figure out what caused the incident, how bad it is, and what methods the attackers used, along with their pos-

sible motivations. (Yuchong and Qinghui 2021). If a system is compromised, they might need to isolate that system, block any harmful network traffic, or patch up security holes that were taken advantage of. After managing the breach, one of their key responsibilities is to get everything back to normal. This involves steps like installing the necessary software updates, changing passwords, and strengthening overall network security.

In summary, incident responders are a crisis intervention force in cybersecurity. They work tirelessly to handle breaches and keep organizations safe, using a mix of human observation and powerful technology to do their job effectively.

4.4. Threat Hunters

Threat hunters are cybersecurity professionals who proactively search for potential threats within an organization's systems and networks. Threat Hunters are a specialized team under the SOC Lead, working closely with the Incident Response Team and SOC Architects. They sometimes collaborate with Level 1 and Level 2 Analysts to investigate anomalies flagged during monitoring, but their focus is on proactive hunting rather than routine monitoring or response. Unlike reactive roles like the Incident Response Team, which responds to alerts or incidents after they occur, Threat hunters actively look for signs of malicious activity that may have gone undetected by automated security tools. Threat hunters play a key role in Security Operations Centers. Instead of just waiting for alerts to ping, these team members actively look for sneaky threats that might slip under the radar of regular detection tools. As cybercriminals get smarter, it has become even more important for organizations to have these hunters on their teams. They are like the detectives of the digital world, always on the lookout for potential problems and ready to act before anything bad happens. Their job is not just about fixing problems; it is about preventing them from happening in the first place.

In 2023, a financial security operations center (SOC) shared some interesting findings. (Picus 2024) Their threat hunters spotted 17 accounts that had been hacked and managed to sneak past the usual monitoring methods for a whole 47 days. This was a big deal because, if left unchecked, these accounts could have led to a fraud incident costing about $3 million. The team behind this crucial catch worked hard by keeping a close eye on authentication logs and studying how users typically behaved online. It is a strong reminder of how important it is to continuously watch for unusual activity to catch threats before they can do real damage.

4.5. SOC Manager

The SOC Manager plays a vital role in running the Security Operations Center, making sure that the team is ready to spot and handle threats effectively. They oversee keeping everything running smoothly and ensuring that incidents are tackled promptly. Here are some of the main responsibilities:

Strategic Leadership: The SOC Manager aligns the work of the SOC with the company's goals and makes sure everything meets necessary standards, like those from NIST. 2018. Framework for improving critical infrastructure cybersecurity Version 1.1. and ISO. 2013. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. This means understanding what the business needs in terms of security and making sure the SOC is positioned to meet those needs.

Team Management: A big part of the role is all about people. The SOC Manager is responsible for hiring and training analysts, which is crucial for building a strong team. They also focus on preventing burnout, which can be a common issue in high-pressure environments like security operations. To keep the team sharp, they run incident drills to prepare everyone for real-life situations.

Tool Management: The SOC Manager looks after various tools, including SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and EDR (Endpoint Detection and Response) explained in 4.9. Their job is to make these tools work as efficiently as possible, which includes minimizing the number of false positives that can overwhelm the team.

Incident Oversight: When a major breach happens, the SOC Manager takes the lead. They use established frameworks, to guide the team's response. This ensures that they handle incidents in a thorough and organized manner, reducing chaos and making sure all bases are covered.

Metrics & Improvement: The SOC Manager is always looking to improve. They track important metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to see how quickly the team can identify and deal with threats. After any incident, they conduct reviews to figure out what went well and what could be better, allowing the team to learn and improve their processes.

Overall, the SOC Manager's role is crucial for keeping the organization secure and ensuring that the SOC can respond quickly when needed. They blend leadership, team support, technical management, and strategic thinking to maintain a resilient security posture.

A good SOC manager knows how to mix their tech skills with strong leadership to make the Security Operations Center a real powerhouse in fighting off cyber threats. It is not just about fixing problems; it is about being one step ahead and preparing the team to handle whatever comes their way. With the right balance of know-how and the ability to inspire their team, they turn the SOC into a place that actively monitors threats and keeps everything safe. This means staying up-to-date on the latest trends in security and training the team to spot issues before they become serious. In a world where cyberattacks are constantly evolving, having someone who can lead with both skill and vision makes a difference. This can create a strong defense that not only reacts but also anticipates challenges in the digital landscape.

4.6. Elements of a SOC

SOC serves as the cognitive center for cybersecurity activities, assisting organizations in successfully reducing cyber threats. People (skilled personnel), processes (standardized procedures), and technology (tools and platforms) are the three main components of a successful Security Operations Center (SOC) as shown in Figure 7, which collaborates to identify, address, and lessen cyber threats. (IritT 2024).

Figure 7. Core Components of SOC (Rakesh 2021)

4.7. People in the SOC

The Security Operations Center (SOC) personnel represent the most relevant element in safeguarding an organization's infrastructure. Whether you bring in new hires or let current employees take on different roles, that works, if you make sure they get the training they need to handle the ever-changing threats. Working in a Security Operations Center can be tough, with a lot of specific tasks that need to be covered. Every role in a SOC matters, and for it to run smoothly, everyone needs to work well together and stick to the standard operating procedures. Keep in mind that SOCs operate all day, every day. So, it’s important to have enough staff to cover all shifts, including handovers, and account for time off, sick days, and holidays.

The SOC manager needs to lead the SOC strategy by focusing on what’s important, making smart choices to handle incidents, and keeping the business running smoothly as new attacks come up and threats change.

4.8. Process in the SOC

Processes within a Security Operations Center (SOC) involve a series of structured workflows and procedures designed to ensure effective detection, analysis, and response to potential threats. These methodologies are necessary for standardizing SOC operations, making them repeatable and reliable. The administration of security information and event management (SIEM 4.9) systems, threat tracking, incident discovery and analysis, incident handling and remediation, threat intelligence integration, and vulnerability management are some of the key procedures incorporated into SOC functionality. (Olaes 2024).

Threat monitoring involves continuously surveilling network activity, logs, and security events, which are essential for the early identification of potential security incidents. This process includes collecting data from various sources, such as firewalls, intrusion detection/prevention systems (IDS/IPS) 4.9, and other security tools contributing to a comprehensive security posture. (Insights 2024). Once anomalies or potential threats are detected, incident detection and analysis start. This phase investigates suspicious activities to check whether they constitute legitimate security incidents. It takes a sophisticated grasp of the infrastructure and threat landscape to distinguish between benign abnormalities and real threats.

Intervention and remediation are required after a security breach is discovered. This phase involves containing breaches to prevent further damage, removing threats from affected systems, and recovering compromised systems to restore normal operations. To reduce the detrimental effects of security breaches on organizational operations, these responses must be effective. Integrating threat intelligence enhances the detection capabilities of the SOC. Using both global and organizational threat information helps strengthen response strategies. (Olaes 2024). By connecting outside and inside threat data, Security Operations Center (SOC) teams can improve how they detect threats and respond to incidents.

Vulnerability management is another crucial process, characterized by regular scanning and assessment of security weaknesses. This process involves prioritizing identified vulnerabilities based on risk level and potential impact, ensuring that the most pressing threats are addressed on time. (Insights 2024). Lastly, combining, comparing, and evaluating security logs and events is a necessary part of managing Security Information and Event Management (SIEM) systems effectively. Automated alert generation based on predefined security rules enhances the SOC's ability to respond promptly to incidents.

4.9. Technologies in the SOC

SOC technologies help spot, stop, and deal with cyber incidents while making security operations run smoother. They fit right into an organization’s security setup and help quickly sort out security issues.

Check out these 7 types of SOC technologies you should know about below.

Vulnerability management is all about finding, assessing, and fixing security weaknesses in cloud systems and software. It points out small flaws that hackers might exploit to get into important networks. By checking the whole IT setup for these weaknesses, it helps to prioritize threats and reduce the chances of an attack.

An Intrusion Detection System keeps an eye on network traffic to spot any possible security issues. It can either notice when something strange happens compared to normal network activity or check against a list of known attack patterns to catch anything unusual and alert the right people. (Rajeev et al 2016)

Access Management is a security tool that helps organizations control who can access different parts of their IT systems. These tools stop unauthorized users from getting to important files, applications, and other sensitive data. They give managers better oversight and make it easier to set up and remove access to various resources.

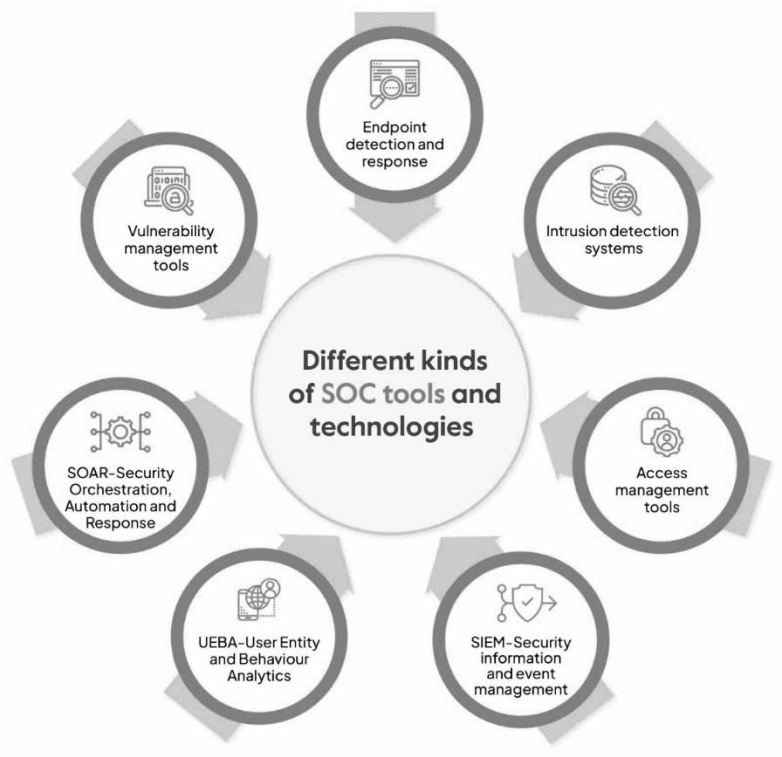

Figure 8. SOC tools and technologies (Wadhwa 2024)

SIEM technology gathers data from various sources and puts it together to help find possible security threats. It can analyze data from servers, network devices, firewalls, and more to check for any issues. Once it spots something suspicious, the SOC team gets a notification to investigate and act.

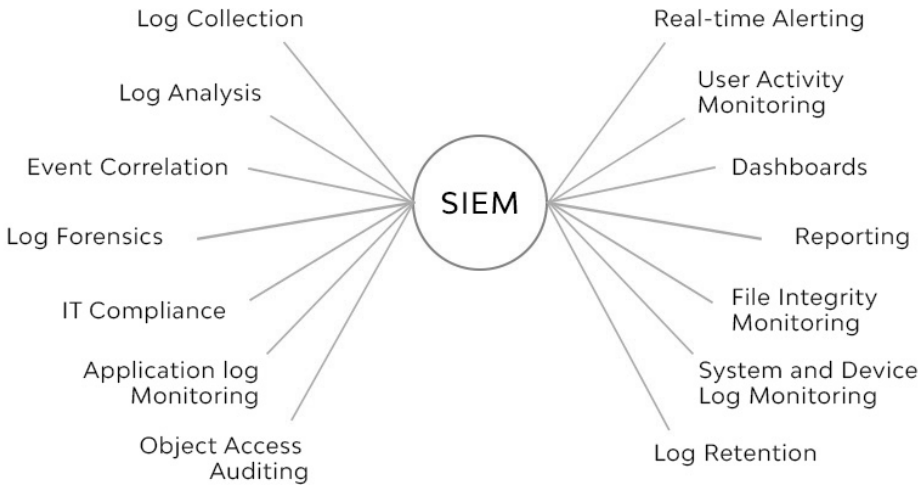

Figure 9. Components and capabilities of SIEM (Lee 2024)

SIEM systems such as Splunk Enterprise Security (http://www.splunk.com) and IBM QRadar (http://www.ibm.com) collect data and logs from a variety of sources, including intrusion detection systems, firewalls, and antivirus software on devices. Through the examination of these data, SOC analysts can spot trends and anomalous activity that might point to a security problem. SIEMs are designed to pull data from various security tools. Analyzing this information through a SIEM system allows analysts to spot potential threats. (Insights 2024). It helps guard against breaches by providing analysts with a thorough picture of network activity. The technological component of making sure a SOC can efficiently monitor networks depends on having a central repository for security data.

UEBA is a threat detection tool that spots unusual behavior in the IT environment. Instead of just looking for known attack patterns, it pays attention to how users and entities typically behave and catches any oddities that other security tools might miss. It does this by building models of what normal behavior looks like and sending alerts if something seems off.

SOAR technology helps automate incident response workflows which cut down the time it takes to handle security issues and manage risks better. It includes useful analysis and reporting features, along with ready-made playbooks for easy guidance during responses, plus it can work with other security tools. SOAR makes it easier for SOC teams to manage security incidents.

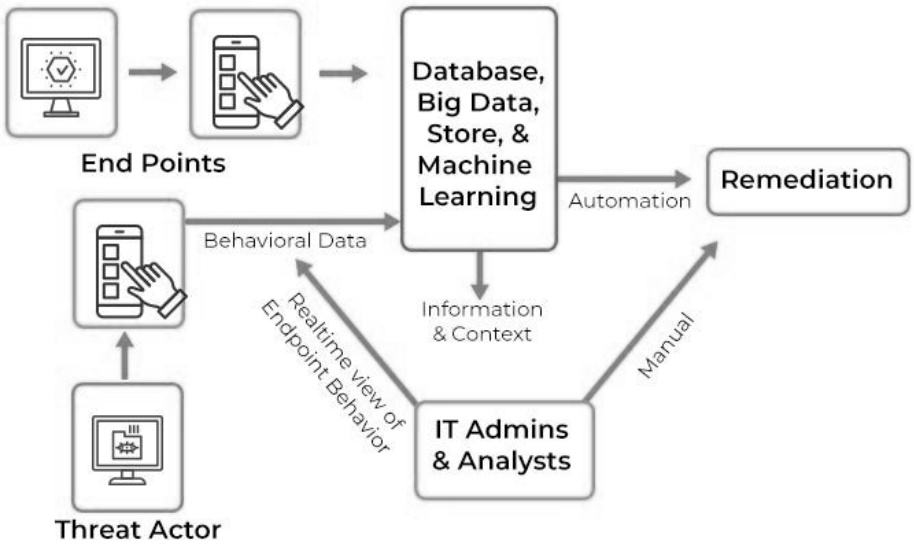

Figure 10. Workflow of endpoint detection and response. (Li and Liu 2021).

Endpoint detection and response, or EDR, are tools that help monitor and react to any suspicious activity on devices like laptops, smartphones, and servers. EDR can spot advanced attacks that might get past other security measures. These tools provide real-time insights into what's happening on endpoint devices, helping to stop potential threats before they cause damage. Figure 10 shows how cybersecurity works with endpoint devices that interact with threat actors, creating behavior data that a central system analyzes. This system uses databases, big data storage, and machine learning tools to give real-time insights into how devices behave. IT professionals can handle issues manually, and there are also automated responses to deal with threats on their own. EDR (Endpoint Detection and Response) solutions boost security by blocking bad IP addresses, stopping unauthorized access, and helping SOC analysts protect endpoints and respond quickly to threats (Li and Liu 2021).

5. PRIMARY RISKS FACED BY SOC ALERT ANALYSTS AND INCIDENT RESPONDERS

Security Operations Centers (SOCs) face big challenges because cybersecurity threats are always changing. Teams need to keep up to prevent data breaches and maintain trust (Abd Majid and Zainol Ariffin 2021). The sheer volume of alerts can cause alert fatigue for analysts, making it tough to spot real threats. High turnover and burnout add to the stress in SOCs (Wojno 2021). Also, SOCs rely on updated tools and tech; if these solutions are not good enough, it can hurt how well they detect and respond to threats, showing the need for skilled staff and reliable systems. (Wadhwa 2024).

5.1. Volume of Alerts

Security Operations Centers (SOCs) get bombarded with security alerts daily from firewalls, intrusion detection systems, antivirus software, and endpoint tools. While these alerts are meant to flag potential threats, they can overwhelm SOC staff. With so many alerts flashing on their screens, it becomes tough to determine what's urgent and what can wait, making their jobs stressful. (Safran 2019).

Analysts must constantly assess each alert's threat level. Some may be minor, while others could signal serious breaches. This balancing act can negatively impact their focus and productivity. Alert fatigue is a big issue; when analysts are flooded with notifications, they might ignore them, risking a delayed response to actual threats. (Thompson 2024).

Research shows analysts can face up to 10,000 alerts in a day, which can lower their accuracy by about 40% after 12 hours on the job. Many alerts turn out to be false alarms, wasting precious time—security teams often deal with high rates of these false positives. On average, analysts spend about 25% of their work hours chasing these false alerts, which hampers their ability to focus on real dangers. Organizations need to recognize this challenge to better support their SOC teams. (Chickowski 2019).

5.2. Complexity of Threats

Security Operations Center analysts and incident responders are facing tougher challenges these days due to the growing complexity of cyber threats. The people behind these attacks are getting smarter and are using advanced methods that can be hard to spot and deal with. Because of this, teams need to constantly adapt to new tactics and come up with stronger defensive strategies to keep systems safe. It is not just about being reactive anymore; it is about being one step ahead and ready to tackle whatever comes next. Keeping up with the evolving landscape of cyber threats requires a lot of teamwork, quick thinking, and a commitment to learning and improving all the time. The stakes are higher than ever, and embracing new technologies and methods is essential for staying in the game.

5.2.1. Advanced Persistent Threats (APTs)

APTs, or Advanced Persistent Threats 4.2, are long-term attacks where someone sneaks into a network and sticks around without anyone noticing for a long time. It is like having a burglar in your house who hides well and manages to escape detection while slowly gathering information or causing trouble. These attackers are not just in and out—they are in it for the long haul, using their time

to gather data or spread their influence quietly. It is a kind of stealthy digital invasion that can be hard to spot, and that makes it a big deal for security teams. They must stay vigilant to catch these hidden threats before they can do any serious damage. Figure 11 highlights the lifecycle of APT. Attackers know how to take advantage of security flaws, especially those zero-day vulnerabilities that haven't been patched yet. They often use a bunch of clever tricks to stay in the system without getting caught. Take that situation back in 2019 when a group thought to be linked to DarkHotel went after people involved in North Korean stuff. They managed to use at least five different zero-day vulnerabilities to pull off their attacks, which just goes to show how skilled they are. It is wild to think about how these hackers can find so many ways to breach security and how serious it can get for anyone connected to sensitive issues like that. (Greenberg, 2020).

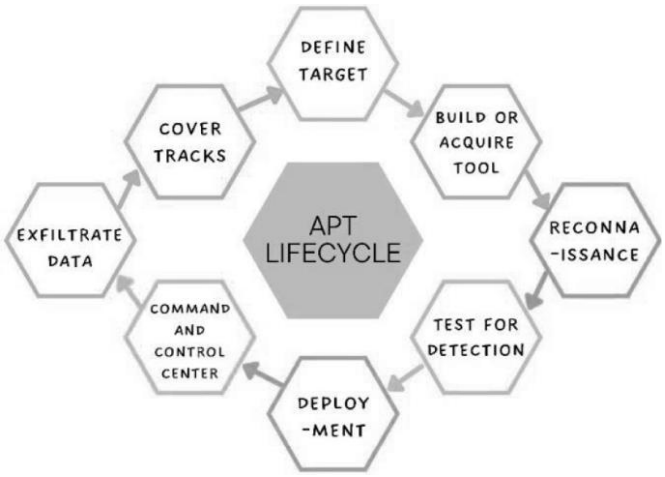

Figure 11. APT lifecycle (Bhardwaj et al. 2024)

5.2.2.Zero-Day Exploits

Zero-Day Exploits are attacks that hit software or hardware flaws that no one knew about. Attackers can use these flaws before developers get a chance to fix them, which often leads to serious security issues. Zero-day exploits are a big deal in the world of cybersecurity. They happen when hackers find weaknesses in software that the company creating it has no clue about. This means there is no time for the developers to fix the problem since they do not even know it exists—hence the term zero days. As technology gets more complicated, with all these different programs and systems working together, it is becoming easier for these exploits to occur. Hackers are cashing in on this, using these hidden weaknesses to launch attacks on valuable targets, like banking systems or important infrastructure. It is a game of cat and mouse, where the hackers are often one step ahead, and it makes protecting these systems more challenging than ever.

As systems intertwine more and more, you can see why finding and fixing these issues before they are exploited is so critical. The more connected everything is, the more opportunities cybercriminals must find these vulnerabilities. It is a stressful situation for developers and IT professionals who are working hard to keep important services up and running while staying ahead of the threat actors. (CloudOptics 2024).

5.2.3. State-sponsored and Cybercriminal Collaborations

Lately, it has become harder to tell the difference between state-sponsored groups and cybercriminals. These two types of players are starting to work together more, which is leading to some advanced and tricky attacks. For instance, you've got hackers teaming up with governments like Russia and China to spy on the U.S. and its allies. By pooling their skills and resources, they are upping the ante on how big and effective their operations can be. This kind of teamwork is making things a lot more complicated for everyone involved. It is a real concern for nations trying to protect their data and maintain security online. With these collaborations, the stakes keep getting higher, and it is clear we need to stay vigilant in tackling these threats (Klepper 2024).

5.2.4. Emerging Attack Vectors

Attackers are always coming up with new ways to sneak past basic security. For instance, there is this tactic called fileless malware. It is sneaky because it runs straight from the computer's memory and does not leave any marks on the hard drive, making it hard to spot. Then there is the living-off-the-land type of attack, where the threat actors take advantage of tools and programs that are already part of the system to do their dirty work. It is like they are using the same tools that someone might use for good but twisting them to cause harm.

On top of that, these attackers are getting smarter by using artificial intelligence to help them. This means they can run attacks faster and on a bigger scale, which adds a whole new set of challenges for those trying to defend against them. The combination of these methods makes it tougher for security teams to keep systems safe. It is like playing a game of cat and mouse where the rules keep changing, making it hard to stay one step ahead. (Fiscus 2024).

5.3. Implications of complex threats for SOC Analysts

Today's threats are complicated, and they come with a bunch of challenges for the team members working in Security Operations Centers (SOC). Analysts in these centers must deal with all sorts of issues that make their job tougher. They are constantly trying to keep up with new kinds of attacks that are popping up, and the technology behind these threats can be hard to figure out. Plus, there are so many data points to sift through to find the bad stuff. It is kind of like looking for a needle in a haystack. On top of that, the strategies that attackers use are always changing, so analysts need to stay sharp and keep learning. It is not a simple task!

1. Trouble Spotting Threats: These days, a lot of cyber threats are clever enough to slip past the usual detection systems that look for specific signals. Because of this, analysts must step up their game and start using behavioral analysis and look for odd patterns to spot these sneaky attacks.

2. Takes a Lot of Resources: When something complicated goes down, looking into the incident is not a quick or easy job. It usually takes a lot of time and expertise, which can stretch the resources of a security operations center (SOC) thin. They must juggle their limited staff and tools while dealing with serious situations.

3. Always Learning: Cybersecurity is always changing, and that is why analysts must keep their knowledge up to date. New attack methods and tools pop up all the time, so they need to get ongoing education and training to stay sharp. It can be tough to find the time, but it is necessary to keep up with the threat actors.

5.4. Mitigation Strategies on Complex Threats

Running a Security Operations Center (SOC) is all about keeping an eye on cyber threats in real-time. But adding a proactive threat hunting approach takes it up a notch. This means actively looking for threats that might have slipped under the radar, using advanced tools to spot issues before they turn into bigger problems. There are a few strategies that can help SOCs tackle their challenges. First off, they should investigate new tools for threat detection, like those powered by AI and machine learning. These can pinpoint odd activities that might indicate a serious cyber-attack. By incorporating these technologies into their routine, SOCs can catch potential threats earlier, which helps prevent chaos down the line. Think about how these tools sift through heaps of data that SOCs deal with daily. They flag anything suspicious, allowing analysts to focus on what matters instead of drowning in endless logs. It is all about making their jobs easier and more effective. Training the staff is another biggie. The tools are only as good as the people using them, so regular training can pay off. SOC teams should stay updated on the latest cybersecurity threats and trends, share experiences, and even run simulations to keep their skills sharp.

Collaboration is crucial, too! SOCs should work with other teams to share information about threats and attacks. This teamwork keeps everyone a step ahead of potential dangers. When SOCs share what they know, it strengthens the overall defense for everyone involved.

Lastly, fostering a culture of security within the organization can make a big difference. When everyone, from tech staff to management, understands the importance of security, it leads to a more vigilant environment where threats are taken seriously right from the start. By bringing in advanced tools, investing in training, collaborating with others, and promoting a security-first mindset, SOCs can manage their challenges better. It is all about being ready and proactive, especially in this ever-changing cyber world.

SOCS need to keep up with the latest threat information, though it is not just about using the latest tech. Staying informed on current threats helps them understand what attackers are up to and how they operate. When SOCs keep themselves updated on threats, they can recognize different strategies hackers might use. This knowledge helps organizations figure out what they might face next. Instead of just reacting, they can set up defenses smartly. Think of it like anticipating a rival’s moves in a game; you can adjust your strategy to counter theirs. By knowing potential hacker tactics in advance, companies can devise plans to protect their systems before an attack occurs, which gives them a better shot at keeping everything secure and running smoothly.

5.5. Skill Gaps

There is a big problem in the world of cybersecurity right now, especially for Security Operations Centers, or SOCs. There are simply not enough qualified people out there who have the skills needed to spot, analyze, and handle the complex cyber threats we are seeing more and more often. This lack of skilled professionals is a real challenge. Because of this shortage, many SOCs struggle to run smoothly and stay strong against these threats. They just cannot operate at their best when they do not have enough trained staff to support them. This creates a kind of domino effect that impacts everything from response times to overall security measures, which can lead to bigger issues. Addressing this skills gap is crucial for boosting the effectiveness of SOCs and keeping organizations safe from cyberattacks. Without more trained experts stepping up, the fight against cybercrime gets tougher every day (Ismail *et al* 2024).

5.5.1. Magnitude of the Skills Gap

Recent studies show that the situation in cybersecurity is quite serious right now. It is estimated that about 5.5 million people are working in this field worldwide. This number demonstrates just how critical cybersecurity has become, with many team members stepping up to protect us from various online threats. As technology keeps advancing, more skilled workers are needed to keep everything secure. With the internet being such a big part of our lives, the demand for cybersecurity experts is only going to grow. It is an important job, and the people in it play a crucial role in helping to keep our personal information and businesses safe from attacks (Kapko 2024).

Figure 2 and Figure 12 show trends in the global cybersecurity workforce and reveal a big gap between how many people are currently working in the field and what's needed. In 2022, there were about 4.66 million cybersecurity professionals worldwide, which is an 11.1% increase from the previous year. The U.S. had the most workers at around 1.2 million, but some places like Singapore and Germany saw a drop in numbers. Fast forward to 2023, and we see growth, with North America reaching nearly 1.5 million workers (up 11.3%) and Asia-Pacific at about 960,000 (up 11.8%). Still, we need 4.8 million more skilled workers to keep up with rising digital threats, as pointed out by Meisner back in 2017. This shortage shows that we need more trained professionals in cybersecurity.

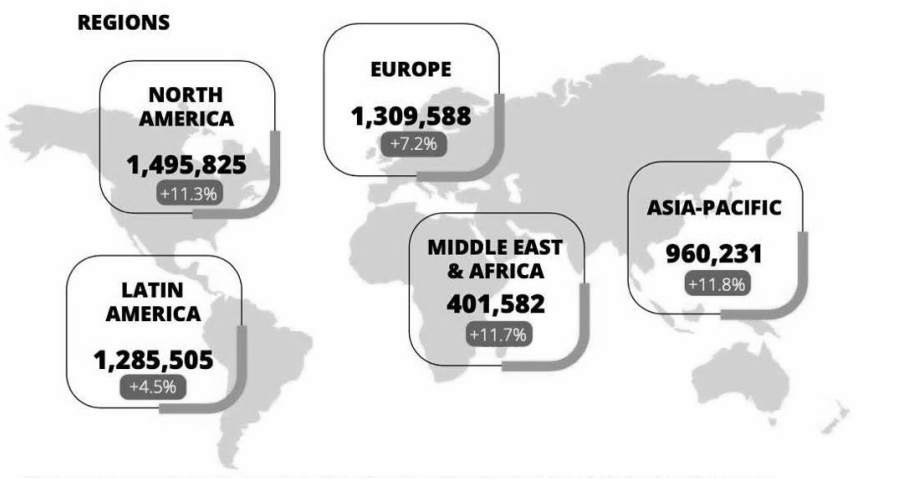

Figure 12. Global cybersecurity workforce as of 2023. (Orszula 2024).

5.5.2. Factors Contributing to Skill Gap

A lot is going on when it comes to the skills gap in today's job market. Let’s break down a few reasons why this is becoming such a big issue.

First off, technology is moving at lightning speed. It seems like every day, some new tool or threat is popping up that tech workers need to be aware of. Because of this crazy pace, team members in many professions are expected to keep learning and adapting constantly. Unfortunately, the schools and training programs that are supposed to prepare them for this just cannot keep up. They often do not cover the latest topics or give people the hands-on experience they need. (CompTIA. 2023).

Next, there is the problem of getting your feet in the door. A lot of companies want to hire candidates with tons of experience and specific certifications. This makes it tough for newcomers who are just starting out. They often find themselves stuck in a position where they cannot get a job because they do not have the experience needed, and they cannot gain experience because no one will hire them. It is a frustrating cycle that makes it hard to bring fresh talent into the field.

And then there is the issue of burnout. Working in cybersecurity, for example, is no walk in the park. The job often comes with serious stress, long hours, and the fear of constant threats. Over time, this can bring people down. When seasoned professionals start feeling this way, many decide to leave the field altogether. This exodus means there are even fewer experienced workers around, which only compounds the problems we are seeing with finding qualified applicants.

In a nutshell, these factors—like rapid changes in technology, high barriers to entry positions, and the tough nature of the work—are really piling up and creating a huge challenge for industries trying to fill positions. If we want to change this, we need to rethink our approach to training, hiring, and keeping talent engaged in their careers.

5.5.3. Impact of Skill Gap on SOC Operations

The skills gap is creating some challenges for Security Operations Centers (SOCs) in several ways.

First off, there is the issue of increased workload. With not enough skilled analysts on hand, the ones that are there are being asked to do more. This can lead to people feeling overwhelmed, which might result in mistakes or missing important details. Then there is the impact on response times. When you do not have enough knowledgeable people, it takes longer to spot threats and deal with them. This delay can make things riskier, as it gives potential attackers more time to cause harm.

Lastly, there is the effect on team morale. When a team is always short-staffed and team members are working too hard, it can bring down spirits. People might start to feel burnt out, and this can hurt how well the team functions and even how much they enjoy their work. All these factors combined make it a tough situation for SOCs, and it is something that needs addressing. (Cybersecurity Ventures 2024).

5.6. Tool Integration

Bringing different security tools together is important for spotting threats quickly and responding to them in a security operations center (SOC). But this process is not without its issues. Trying to mesh all these tools can create some challenges that might make it tough for the SOC to operate smoothly and do its job effectively.

For example, you might run into problems with compatibility between different systems. If some tools do not play well together, it can slow things down. There is also the issue of training staff to understand how to use this mix of tools. If team members are not on the same page, it can lead to confusion and longer response times when a threat does show up.

So, while getting everything integrated is crucial, it also means that SOC teams need to put in a bit more effort to iron out these kinks. Finding ways to make tools work together, getting the team trained upright, and keeping everything running smoothly are all parts of making sure the SOC can do its job well.

5.6.1. Challenges in Tool Integration

A lot of organizations find themselves dealing with an odd mix of old systems and newer security tools. This can create real issues when it comes to getting everything to work together smoothly. Older systems often do not support the latest technology, like modern APIs or new ways of sharing data, which can be frustrating. To fix this, companies usually must invest time and effort into custom solutions or use middleware to help their old systems talk to the new tools. It can take a lot of resources and creativity to make it all work as it should. (Orszula 2024).

When we bring in new tools, sometimes things can go a bit haywire. Take security tools, for example. They often need a certain level of access to the systems or the data flowing through the network. This can lead to some of the current tools not working properly anymore. It is a common issue, especially with those endpoint security tools that need to be installed directly on devices. If you are not careful, it can mess things up, causing headaches for the people trying to manage everything. (Violino 2022).

When it comes to keeping an eye on the network for any possible threats, having a complete view of the traffic is super important. If the tools we are using can only see part of what's happening, they might not get the whole story. This can mess things up because models based on incomplete data might not work right, which means they could miss spotting real threats. So, you can see how crucial it is to analyze all the traffic, not just a piece of it, to ensure that we are catching anything that could cause problems in our systems. (Violino 2022).

False alarms are becoming more common, especially with the introduction of new security tools. When these tools start sending out alerts, there is a chance that many of them will be mistakes, known as false positives. This can create a bit of a mess for analysts who are trying to do their job. Instead of being able to focus on real threats, they can get bogged down by all these unnecessary

alerts. It is like trying to find a needle in a haystack when the haystack keeps getting bigger and messier. Instead of helping to catch the threat actors, these false alarms can make it harder to spot what's going on.

In today's cybersecurity world, many organizations use a ton of different security tools and management platforms. While having various tools can seem like a good idea, it can also create a bit of a mess. When these tools are not set up to work together smoothly, it leads to what we call tool sprawl. This situation can make life hard for Security Operations Center (SOC) teams, who are responsible for keeping everything secure. They end up with way too many tools to juggle, and it is tough for them to make sense of all the data coming from different sources. Instead of getting a clear picture of what's going on, they might find themselves struggling to connect the dots. So, while the goal is to stay safe, sometimes having too many tools just makes things more complicated than they need to be. (SafeBreach 2022).

5.6.2. Strategies for Effective Tool Integration

Security Operations Centers, or SOCs, face a lot of challenges in keeping our systems safe. To handle these issues better, there are some smart strategies they can use. One important move is to bring in smart tech tools. Take Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) systems, for example. It is important to set these tools upright so that they do not bombard analysts with too much data. Instead, they should help make sense of security events and find connections between them. Another big piece of the puzzle is making sure there is clear communication among the team. It is all about having straightforward channels and protocols for raising alerts. When everyone knows how things work and what to do in response to alerts, it helps tackle issues quickly and allows the team to work together more smoothly. By focusing on these strategies, SOCs can better manage their workload and keep everything running safely. Overall, staying organized and utilizing the right tools and communication practices makes a world of difference in the fight against security threats. (Uriel 2024).

Keeping SOC teams trained and sharing knowledge regularly is important for getting everyone up to speed with the latest tools. When teams create an environment where learning is valued, it not only helps improve the systems they work with but also makes it easier for them to spot threats. Offering chances to learn together can boost their confidence and ensure they are always ready to tackle challenges that come their way. It is about building a team that feels good about what they know and can work together smoothly to protect against any potential issues. (SafeBreach 2022).

5.7. Incident Response Time

In the world of cybersecurity, there is something called Incident Response Time. It is the time it takes from when a security issue is spotted to when the team takes action to fix it. This time frame matters because it can determine how much damage is done, whether data gets lost, the financial hit a company might take, and even how people see the organization overall. If they can act quickly, they can minimize the fallout. If there is a delay, it could mean serious trouble, both losing valuable

information and hurting their reputation in the process. So, having a swift response is essential for businesses to protect themselves and maintain trust with their customers.

5.7.1. Components of Incident Response Time

1. Mean Time to Detect (MTTD): This is all about how long it takes to catch a security breach after it happens. The quicker we can spot these issues, the better we can deal with them and lessen the chances for attackers to make a move. Many businesses these days aim to get their response times down to under 15 minutes for serious incidents, but this can change depending on what type of incident we are dealing with and the tools they are using to spot these threats. So, companies must have systems in place that help them detect these problems as fast as they can. (Rahman 2022); (Morin 2024).

2. Mean Time to Respond, or MTTR, basically looks at how long it takes from spotting a problem to getting to work on fixing it. When things go wrong, acting quickly is crucial to stop any threats from getting worse. Those in the know aim to keep their MTTR under 30 minutes for important incidents. They do this by setting up solid response plans and using automated systems to help speed things along. This way, they are ready to jump into action and tackle the issue before it spirals out of control. (Morin 2024).

3. Mean Time to Handle, or MTTH for short, refers to the total time it takes to deal with an incident, starting from when it is first spotted to when it is fully resolved. This measure gives us a good idea of how well a team responds to issues and how effective their solutions are.

In many top companies, the goal is to keep the MTTH for common incidents under two hours. How do they manage to achieve this? A big part of it is keeping thorough documentation of each incident. They also make use of knowledge bases, which are collections of information and past experiences that can guide the team on how to handle similar problems in the future.

After an incident is resolved, a lot of organizations make sure to do a post-mortem analysis, where they look back on what happened, what was done, and how things could be improved next time. All these steps help keep the incident handling time low, which ultimately aids in maintaining smoother operations and happier customers. (Morin 2024).

5.7.2. Significance of Reducing Incident Response Time

Companies need to keep their data safe, especially when it comes to sensitive information. They need to make sure they are not putting too much of it out there where it could be seen or accessed by the wrong people. Quick action is key when it comes to security issues. If something goes wrong, being able to spot it right away and respond quickly can make a big difference. This way, they can help prevent any unauthorized access and keep everything secure. Keeping a tight grip on data is just part of the job, but it is one of the most important things they can do to protect themselves and their users. (Insights 2024)..

Long stretches where attacks go unnoticed can raise the chances of big data breaches happening. It is super important to tackle security threats quickly because it stops attackers from getting comfortable and holding onto access to the network. Being proactive like this helps lower the chances of facing the same issues repeatedly and boosts the overall safety of the network. Plus, taking care of incidents promptly is crucial for making sure we keep vital forensic evidence intact. That evidence is key for detailed investigations and can play a big role in legal cases later. The whole process is about staying one step ahead so that when something does happen, we are ready to deal with it without letting things spiral out of control. If we can keep a tight grip on the situation, we shield ourselves from a lot of headaches down the line and ensure that we follow through on any necessary legal steps with solid support. (Zamfiroiu and Sharma 2022).

When it comes to handling incidents effectively, you can see how much a company cares about keeping things secure. This shows customers that they can trust the organization, which is super important. By taking good care of their data, companies not only keep their customers feeling safe but also make sure their good name stays intact. We all know that in today's world, a solid reputation can make or break a business, so protecting info is not just a nice-to-have; it is a must. Keeping customers happy and confident means, they are likely to stay loyal, which is what every business wants.

5.7.3. Challenges Affecting Incident Response Time

1. One big issue that security teams deal with is the sheer number of alerts they receive. Sometimes it feels like they are drowning in alerts, which can slow them down when trying to spot and focus on real threats. It can be tricky to sift through all that noise and figure out what's worth their attention and what's not.

2. Then there is the problem of how complicated some threats can be. Nowadays, attackers use clever methods that can take a lot of time to investigate. When a threat pops up, it does not just get flagged and handled quickly. The teams have to take a careful look, analyze it, and make sure they contain it properly, which can stretch out the response time.

3. Lastly, many security teams are dealing with limited resources. They might not have enough staff or the right level of expertise on hand. This shortage can make it hard for them to react to threats as fast as they'd like. If there are not enough people or knowledge in the team, it can lead to delays when something important happens.

5.7.4. Ways to Improve Incident Response Time

Let's talk about automating workflows. When we set up systems that can automatically spot issues and act, it can cut down the time it takes to find and tackle problems. We are seeing that by automating these processes, security operations centers (SOC) can speed up their response times by as

much as half. This is great news because it means that if there is a security breach, the damage or impact can be greatly minimized. By taking some of the routine tasks off human shoulders, we free them to focus on more complex and important issues, which just makes everything run smoother. Overall, automating these workflows is not just a tech upgrade; it is a smart way to keep things secure and efficient. (Zamfiroiu and Sharma 2022).

It is important to have regular training and practice sessions for incident response. When you do these drills often, it helps the team stay sharp and ready for any real situations that might come up. They'll know what to do and can jump into action without hesitation when something serious happens. Plus, it builds teamwork and improves communication, which is vital during a crisis. Keeping everyone in the loop through these ongoing practices means that when the time comes, they'll feel more confident and capable of handling the situation effectively. So, setting aside time for these exercises can make all the difference when a real incident rolls around. (Abusix Marketing 2024).

Setting up clear ways for people to talk with each other is important, especially when something goes wrong. It helps make sure that everyone involved knows what's going on without confusion. When everyone is on the same page, it makes it easier to make decisions quickly. So, if an issue pops up, you can get through it faster by having those communication lines open and defined. (Zamfiroiu and Sharma 2022).

When something goes wrong, it is super important to look back and see what happened. By checking out past incidents, we can figure out where things might have slowed down or where we could do better next time. This way, we can change our game plan and react faster if something like that happens again in the future. It is all about learning from our mistakes and making our responses quicker and more efficient.

5.8. Impact of These Risks on SOC Operations Effectiveness

Existing Risk Mitigation Strategies

In a Security Operations Center, the main goal is to keep everything safe. This means taking steps to deal with potential risks before they turn into big problems. There are several ways to handle threats and vulnerabilities. For instance, sometimes you might just avoid a risky situation altogether. Other times, you may choose to reduce the risk by putting in better security measures. If it is not possible to avoid or reduce the threat, you might decide to transfer risk, which often means getting insurance or something similar. Lastly, you may accept the risk if you think the potential impact is not too severe. Each of these strategies plays an important role in keeping operations running smoothly and ensuring that the team can respond effectively to any issues that come up. Overall, managing risk is a continuous process and requires a lot of teamwork and vigilance. (Wojno 2021). Most risk mitigation strategies in SOC Operations can be classified into the following:

1. Risk Avoidance: This strategy involves eliminating activities or processes that expose the organization to specific risks. (Wojno 2021). For example, if a software application is identified as a high-risk vulnerability, the SOC team might recommend its removal or replacement.
2. Risk Reduction: This strategy focuses on minimizing the likelihood or impact of a risk by implementing security controls and procedures. Examples include implementing strong access controls, regularly patching systems, and conducting vulnerability scans. (Samson 2025).
3. Risk Transfer: This strategy involves transferring the risk to a third party, such as through insurance or outsourcing security functions.
4. Risk Acceptance: This strategy involves accepting the risk and its potential consequences, often when the cost of mitigation is deemed too high or the risk is deemed low enough to be tolerated.

6. MITIGATING THE RISKS IN SOC ALERT ANALYSIS AND INCIDENT RESPONSE

A Security Operations Center, or SOC for short, is like your organization's shield against cyber threat actors. It is super important for these centers to manage risks well because if they do not, they start running into some major problems. Think about alert fatigue, where team members are overwhelmed by too many notifications, or they might take too long to respond to incidents. There is also the risk of falling out of line with regulations, which can lead to penalties. Plus, nobody wants to lose money or damage their reputation.

When SOC does a good job managing risks, it stops potential breaches from getting worse. Right now, it is taking an average of 277 days for organizations to spot an attack, which is way too long (IBM 2023). When they cut down on false alarms—like those annoying alerts that turn out not to be threats (and make up over half of SOC alerts, according to SANS Institute in 2022)—it helps the team focus on real issues they need to tackle.

Keeping in line with regulations like NIST, ISO 27001, and GDPR is another big bonus. Staying compliant helps businesses steer clear of hefty fines and legal headaches.

But risk management is not just about protection; it is also key for keeping the business running smoothly. There have been some high-profile cyberattacks recently, like the one at MGM Resorts in 2023, that showed just how disruptive these breaches can be and how they can lead to big financial hits.

On top of all that, using threat intelligence—like the MITRE ATT&CK framework and various threat feeds—can really beef up how well a SOC can detect and respond to potential threats. By staying on top of these tools and practices, SOCs can keep their organizations safer and more prepared for whatever might come their way.

6.1. Key Risk Mitigation Strategies

Improving Alert Triage & Reducing False Positives

Security Operations Centers (SOCs) have a tough time dealing with a flood of alerts, and studies show that a whopping 50-72% of these alerts turn out to be false alarms (SANS 2023). This problem not only wastes valuable time for analysts but also means that real threats could slip through the cracks. To manage this mess, SOCs need a solid plan that pulls together technology, processes, and a constant push for improvement.

To start tackling this issue, one effective strategy is to refine SIEM (Security Information and Event Management) rules. By using contextual filtering and adjusting thresholds on the fly, SOCs can boost their efficiency and reduce the noise that analysts must sift through. Adding threat intelligence feeds into the mix helps too, as shown by one financial SOC, which slashed false positives by a remarkable 38% just by incorporating commercial threat intel. Then there is machine learning, which can offer some impressive results, too. According to a 2023 study by Darktrace, using methods like behavioral baselining and anomaly detection can cut down false positives by 40-60%.

Another big piece of the puzzle is automation. SOAR (Security Orchestration, Automation, and Response) platforms come in handy here. They can take care of the first steps, like validating alerts, checking reputations, and even closing out known benign issues without needing a human touch right away. When rolling out such systems, it is important to have a structured plan that includes assessing problems, carefully fine-tuning the processes based on the specific environment, and making sure everything works smoothly during testing before it goes live.

When it comes to measuring success, SOCs should keep an eye on some key metrics. A goal should be to have a False Positive Rate that stays below 30%, and aiming for a Mean Time to Triage of under 5 minutes is also smart. Keeping the Alert-to-Investigation Ratio above 25% can show how effectively alerts are managed. A real-world example can be found in the healthcare sector, where one SOC cut its false positives by an impressive 52% in just six months. They did this by regularly prioritizing alerts every day, tuning their rules each week, and implementing smart automation strategies.

Structured Incident Response (IR) Framework

A solid Incident Response (IR) 4.3 plan gives the Security Operations Center (SOC) analysts a straightforward way to handle security issues when they pop up. It lays out a clear path for identifying problems, dealing with them promptly, and getting things back to normal afterward. When organizations stick to these tried-and-true methods, they can tackle incidents more quickly, reduce the impact of those incidents, and bounce back better afterward. In simpler terms, having a structured approach helps everyone involved know what to do and how to do it when things go wrong, making it easier to keep everything secure.

Figure 13. Incident Response Framework. (Kontseva 2024)

Picking an incident response model, the team members at NIST suggest you take a good look at a few important things. See NIST Special Publication 800-61, "Computer Security Incident Handling Guide," which outlines considerations for choosing an effective incident response framework. It is not just a checklist; these factors help to ensure you choose the right model for your needs. Think

about what your organization specifically requires, what kind of threats you might face, and how prepared your team is to handle those situations. It is also wise to look at how quickly you need to respond to incidents and what resources you have available. Taking time to consider these points can steer you in the right direction and help you build a solid response plan.

When it comes to having a solid plan for handling incidents, there are a few key things to think about. First up is availability. Do you need someone ready to jump into action 24/7? And what about having someone physically present at your location for those quick responses?

Then, there is staffing. Are you thinking about having full-time people on your incident response team, or would part-time workers do the job? Another option could be having a virtual team that steps in when needed. Often, the IT help desk can be the first point of contact when things go wrong, with part-timers ready to back them up if needed.

Next on the list is expertise. What level of security knowledge do you think is necessary for your team? Can your current staff handle it, or should you investigate hiring an outside team? Indeed, outside teams often come with strong security skills, but do not forget that your in-house people know your systems inside and out, which can be just as valuable.

Furthermore, let’s talk about money. What does it cost to keep an incident response team running? You must consider everything from salaries and tools to the space you need and how your team communicates. And do not overlook Managed Security Service Providers (MSSPs) because while they bring their own set of skills, they can also hit your budget hard. So, as you think through these points, you'll get a clearer picture of what approach works best for your organization when it comes to responding to incidents effectively.

The Figure 13 above is the pictorial breakdown of the core components of an Incident Response Framework, which I will further explain briefly.

To get ready for cyber threats, you need a solid plan. Start by creating guides for common attacks like ransomware, phishing, or DDoS. These guides will help your team know exactly what to do if something happens, making sure everyone acts quickly and works together. Keep an updated contact list that includes legal and PR teams, so you can communicate fast during a crisis without delays. It is also smart to run practice drills, where your team can act out different attack scenarios. This helps them know their roles, check how prepared they are, and find areas to improve. The more you practice, the stronger your team will be in dealing with threats.

For spotting and investigating issues, look at alerts and check various sources like logs and network data to understand what’s going on. Once you collect this info, rank incidents based on how serious they are. This way, the team knows how urgent each situation is. If something might lead to legal trouble, make sure you document everything carefully to back yourselves up later. When a system gets compromised, you need to act fast. First, isolate the affected systems to stop the spread. Lock down any related accounts to keep unauthorized users out. After containing the issue, focus on fixing it for the long run. Apply patches for any weak spots that let the attack happen, and dig deep to

remove any malware or backdoors that could let the attackers back in. When getting systems back up, use clean backups and check they are safe before going online again.

Once everything is back to normal, it is important to review what happened to avoid it in the future. Do a root cause analysis to find out why the attack happened, using tools like the 5 Whys or fish-bone diagrams. Update your guides with what you learned so you can handle these situations better next time. To track how you are doing, keep an eye on metrics like Mean Time to Respond (MTTR) to see how quickly your team handles incidents. Watching MTTR over time helps you see improvements and strengthen your response skills.

7. ADAPTIVE APPROACHES IN ENSURING RELIABILITY AND VALIDITY

Adaptive cybersecurity approaches ensure reliability and validity by dynamically adjusting to evolving threats, using techniques like AI, machine learning, and behavioral analytics. This includes creating a feedback loop of threat visibility, detection, and prevention that consistently improves. A major aspect of these approaches includes prevention, detection, responsiveness, and prediction. Adaptive cybersecurity also involves validating models against parameters like adaptive optimization, configuration, healing, and protection.

7.1. Continuous Threat Landscape Monitoring

Adaptive systems are required in cybersecurity by continuously monitoring user sessions and network traffic for any suspicious activities. This vigilant act is essential in this technological age, where cyber threats are becoming increasingly sophisticated. These systems analyze data in real time to proactively tackle potential security threats before they develop into significant breaches. (CloudOptics 2024).

The integration of AI and machine learning algorithms has also significantly enhanced the capabilities of adaptive systems. These algorithms swiftly detect potential threats by analyzing different data patterns. (Wafula 2021). This level of analysis helps in discerning unusual patterns that might escape human detection, enabling organizations to respond effectively to threats as they arise.

Furthermore, the application of behavioral analytics serves as a vital tool in tracking user behavior over time. These analytics identify anomalies indicating malicious intent by establishing a normal activity baseline. Such proactive detection not only aids in safeguarding sensitive information but also fosters a more secure environment for users. Generally, the synergy between adaptive systems, AI technologies, and behavioral analytics underscores an evolving approach to cybersecurity that is both reactive and proactive. (Scapicchio, Downie and Finio 2025).

7.2. Dynamic Threat Response

Adaptive security is a changing concept that emphasizes the importance of dynamically adjusting security measures in response to varying threat levels. But even when the threat level seems low, it might still attract some attackers. A smart security system should be able to recognize this risk and not leave any easy openings. This adaptability enables organizations to effectively counteract emerging cyber threats and safeguard sensitive information. Using advanced technologies, systems can automatically adjust their security protocols, keeping protective measures strong and relevant against emerging threats. (Chickowski 2019).

One significant aspect of adaptive security is its capability to implement changes, such as altering encryption technologies, which enhance data protection. Additionally, it can involve refining access controls, either by introducing new controls or modifying existing ones, to ensure that only authorized personnel have access to critical systems and data. These ongoing adjustments foster a proactive rather than reactive security posture.

Moreover, real-time threat responses play a critical role in maintaining the effectiveness of security strategies. (Chickowski 2019). Adaptive security systems continuously monitor the environment for

potential threats, enabling them to quickly trigger alerts and notifications. This allows teams to respond rapidly to incidents. This not only enhances overall security resilience but also empowers organizations to stay ahead of potential breaches. Consequently, the implementation of adaptive security measures becomes indispensable for organizations seeking to fortify their defenses in an increasingly complex digital landscape. (Bhardwaj et al. 2024).

7.3. Predictive Security

Adaptive systems play a pivotal role in enhancing security measures by leveraging the power of historical data analysis. By analyzing historical events and identifying patterns, these systems allow organizations to predict potential threats before they occur. (Chickowski 2019). This predictive capability is not merely a reactive approach; instead, it equips businesses with the foresight needed to implement proactive strategies. (CloudOptics 2024). In an environment where cyber threats are continuously evolving, the ability to anticipate incidents is invaluable.

Moreover, by engaging in the proactive identification of security threats, organizations can significantly reduce the likelihood of costly incidents. The financial repercussions of security breaches can be devastating, affecting not only the organization's bottom line but also its reputation among stakeholders. (Cichonski et al. 2012). Consequently, the integration of adaptive systems can serve as a safeguard, helping to maintain robust security protocols and instill confidence among clients and employees alike. Therefore, the significance of adaptive systems in security cannot be overstated. Their ability to analyze historical data and recognize trends fosters a proactive approach to threat management. Such capabilities not only help organizations avoid potential attacks but also ensure the upkeep of a high level of security, contributing to overall operational resilience in an increasingly complex digital landscape. (Abusix Marketing, 2024).

7.4. Zero Trust Framework

Adaptive security plays a pivotal role within the architecture of a zero-trust framework, fundamentally challenging the traditional notions of trust in the digital landscape. (CloudOptics, 2024). In this model, no user or device is presumed to be trustworthy by default; instead, a rigorous verification process is mandated. This approach ensures that every user and device must pass through stringent checks of verification and authorization before being granted access to any resources. (Kapko 2024).

Through the application of these principles, zero trust significantly reduces the attack surface organizations need to protect, thereby strengthening their overall security stance. Adopting adaptive security measures not only enhances defenses against potential threats but also creates a more resilient atmosphere where security is consistently evaluated and enhanced in response to emerging risks. (CloudOptics 2024).

7.5. Security Lifecycle Integration

Adaptive security represents a significant evolution in the landscape of cybersecurity, integrating seamlessly with the entire cybersecurity lifecycle. (CloudOptics 2024). This lifecycle encompasses five critical stages: identification, protection, detection, response, and recovery. Integrating adaptive security within this framework enables organizations to create a strong defense system that tackles each stage while simultaneously boosting resilience against cyber threats.

The holistic nature of adaptive security is particularly important in today's digital environment, where cyber incidents can occur unexpectedly and with devastating effects. Organizations that adopt this approach are better equipped to handle the complexities of cybersecurity and can devise strategies to prevent, detect, and respond to threats effectively. (Wafula 2021). This thorough preparedness reinforces their ability to recover from incidents, thus minimizing potential damage and downtime resulting from security breaches.

Moreover, adaptive security embodies both proactive and reactive strategies, making it an invaluable aspect of contemporary cybersecurity. Organizations can detect and resolve vulnerabilities by emphasizing proactive measures before they are exploited. Concurrently, the responsive element ensures that if a cyber incident does occur, there are established protocols and resources in place to mitigate the impact. (Chinnasamy 2023). This duality is essential for fostering a culture of security that adapts to evolving threats while continuously learning from past incidents to improve future responses.

7.6. Adaptive Learning and Optimization

Adaptive systems are designed to continuously learn from new data and adjust their security measures in response. This dynamic capability is crucial in an increasingly complex threat landscape, where security vulnerabilities can evolve rapidly. The continuous improvement and refinement of security policies and procedures is another significant advantage of adaptive systems. (Zamfiroiu and Sharma 2022). As they gather more information from various data sources, these systems can identify patterns and make informed adjustments to policies, thereby enhancing the security posture. This iterative process not only strengthens defenses but also fosters resilience in security frameworks. (IritT 2024).

8. CONCLUSION

This thesis looks into the important roles of Tier-1 Security Operations Center (SOC) alert analysts and incident responders in tackling cybersecurity risks, especially as cyber threats become more common and advanced. SOC alert analysts are the first line of defense. They:

* Handle thousands of alerts each day.

* Spot possible threats

* Push critical incidents up the chain.

Incident responders follow up with thorough investigations and work on containment and fixes. These jobs are crucial for quick threat detection and response, which is the backbone of SOC operations.

That said, some challenges slow things down. A lot of alerts, anywhere from 50-72%, turn out to be false. There are tough threats out there, like advanced persistent threats (APTs) and zero-day exploits. Plus, we are facing a global shortage of around 4.8 million cybersecurity pros. Disconnected tools and slower response times also hurt SOC efficiency, leading to missed threats, burnout among analysts, high turnover, and increased risks for organizations.

This study is based on risk management ideas and adaptive security principles, like Zero Trust 7.4, using a qualitative method that pulls together literature, industry reports, and case studies. It connects with earlier research on quick alert assessment, alert fatigue, and adaptive systems. Suggested fixes include using AI for alert prioritization, automating processes, integrating threat intelligence, standardizing incident response procedures, and providing regular training to fill the skills gap. Shifting to a Zero Trust framework and continuous threat monitoring can boost resilience, with some real cases showing up to a 52% drop in false positives.

This research stresses the need for a well-coordinated SOC with skilled staff, effective processes, and modern technologies, measuring success through metrics like Mean Time to Detect and Respond. While it mainly addresses Tier-1 roles, these findings might not apply to advanced positions or threat hunting. Future studies could look at how generative AI affects SOC practices, different industry needs, and strategies to reduce burnout in the long run to strengthen cybersecurity defenses.

REFERENCES

Abd Majid M. & Zainol Ariffin K. A., 2021. Model for Successful Development and Implementation of Cyber Security Operations Centre (SOC). s.l.:PloS one.

Abusix Marketing 2024. Racing Against the Clock in Incident Response Times, Cybersecurity Solutions | Email & Network Security. https://abusix.com/blog/optimizing-incident-response-cybersecurity/ Accessed 9 April 2025.

Bejtlich R. 2005. The Tao of Network Security Monitoring: Beyond Intrusion Detection https://archive.org/details/taoofnetworksecu0000bejt/mode/2up Accessed 30 March 2025.

Bhardwaj R. e. a. 2024. Analysis of Advanced Persistent Threat Attacks, Lifecycle, and Counter Measures: A Comprehensive Review. Singapore: Springer Nature Singapore.

Breaker-Rolfe J. 2024. Strategies to Manage and Reduce Alert Fatigue in SOCs. https://www.itsecurityguru.org/2024/06/11/strategies-to-manage-and-reduce-alert-fatigue-in-socs/ Accessed 30 March 2025.

Cassetto O. 2024. What is a SOC Analyst? Role & Responsibilities Explained https://radiantsecurity.ai/learn/soc-analyst/ Accessed 24 March 2025.

Chickowski E. 2019. Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives. Accessed 7 April 2025.

Chinnasamy V. 2023. Vulnerability Assessment Types and Methodology. https://www.indusface.com/blog/explore-vulnerability-assessment-types-and-methodology/ Accessed 29 March 2025.

Cichonski P. e. a. 2012. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-61r2 Accessed 30 April 2025.

Cichonski P. M. T. G. T. &. S. K. 2012. Computer Security Incident Handling Guide. Special Publication 800-61, Rev. 2 ed. s.l.:National Institute of Standards and Technology NIST.

CloudOptics 2024. The Growing Threat of Zero-Day Exploits: Why Traditional Security Measures May Not Be Enough. https://cloudoptics.ai/cybersecurity-updates/he-growing-threat-of-zero-day-exploits-why-traditional-security-measures-may-not-be-enough/ Accessed 7 April 2025.

Colin, M., 2024. The Essential Role of a SOC Manager in Cybersecurity Operations Centre. https://nicyberguy.com/the-essential-role-of-a-soc-manager-in-cybersecurity-operations-centre/ Accessed 29 March 2025.

CompTIA 2023. State of the tech workforce 2023. https://www.comptia.org/content/research/state-of-the-tech-workforce Accessed 28 March 2025.

Cuppens F. &. M. A. 2002. Alert Correlation in a Cooperative Intrusion Detection Framework. https://ieeexplore.ieee.org/document/1012423 Accessed 26 April 2025.

Duncan B. 2015. SOC Analyst Pyramid.https://isc.sans.edu/diary/19677 [Accessed 11 April 2025.

Fiscus D. 2024. CISO’s Guide: Using AI for Cyber Defense. https://deloitte.wsj.com/riskandcompliance/cisos-guide-using-ai-for-cyber-defense-d6e06cfc Accessed 30 April 2025.

Folorunso A. e. a. 2024. Security Compliance and Its Implication for Cybersecurity. s.l.:World Journal of Advanced Research and Reviews.

Gomez A. 2024. What Is an Incident Responder? Everything You Need to Know. https://www.ollusa.edu/blog/what-is-an-incident-responder.html Accessed 24 March 2025.

Greenberg A. 2020. An Elite Spy Group Used 5 Zero-Days to Hack North Koreans. https://www.wired.com/story/north-korea-hacking-zero-days-google/ Accessed 7 April 2025.

Gurkok C. 2014. Cyber Forensics and Incident Response. In: Managing Information Security. s.l.:Elsevier, p. 275–311.

Insights D. 2024. How Intrusion Detection Systems Help Identify Cyber Threats in Real-Time. https://www.dataguard.com/blog/how-intrusion-detection-systems-help-identify-cyber-threats/ Accessed 29 March 2025.

IritT 2024. SOC Fundamentals– Cyber Security 101-Defensive Security -TryHackMe Walkthrough. https://iritt.medium.com/soc-fundamentals-cyber-security-101-defensive-security-tryhackme-walkthrough-82b1093bea59 Accessed 27 March 2025.

ISC² 2021. Cybersecurity Workforce Study. https://www.isc2.org/Research/Workforce-Study Accessed 10 April 2025.

Ismail M. et al. 2024. Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16(100501), p. 100501.

ISO I. O. f. S. 2013. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html Accessed 21 March 2025.

Kapko M. 2024. Global cybersecurity workforce growth flatlines, stalling at 5.5M pros. https://www.cybersecuritydive.com/news/global-cyber-workforce-flatlines-isc2/726667/ Accessed 8 April 2025.

Kasa C. 2024. Major Challenges facing by SOC operations. https://www.linkedin.com/pulse/major-challenges-facing-soc-operations-chethan-kumar-reddy-kasa-fgnff Accessed 29 March 2025.

Klepper D. 2024. Cyber criminals are increasingly helping Russia and China target the US and allies, Microsoft says. https://apnews.com/article/microsoft-russia-china-iran-israel-cyberespionage-cyber-d3a22dd2dcea32615ac15ed4fb951541 Accessed 7 April 2025.

Mansi 2022. Key Components of a Security Operations Centre. https://atech.cloud/resources/key-components-of-a-security-operations-centre/ Accessed 11 April 2025.

Meisner M. 2017. Financial Consequences of Cyber Attacks Leading to Data Breaches in Healthcare Sector. s.l.:Copernican Journal of Finance & Accounting.

Michael Scapicchio A. D. M. F., 2025. What Is a Security Operations Center (SOC)?. https://www.ibm.com/think/topics/security-operations-center Accessed 23 March 2025.

Miller J. 2024. The Benefits of a Security Operations Center for Financial Institutions. https://www.bitlyft.com/resources/the-benefits-of-a-security-operations-center-for-financial-institutions Accessed 23 March 2025.

MITRE ATT&CK 2025. A Knowledge Base of Adversarial Techniques Based on Real-World Observations. https://attack.mitre.org/resources/ Accessed 10 April 2025.

MITRE C. 2023. MITRE ATT&CK. https://attack.mitre.org/ Accessed 27 April 2025.

Mitton L. 2025. Preventing Alert Fatigue in Cybersecurity: How To Recognize & Combat Alert Fatigue. https://www.splunk.com/en_us/blog/learn/alert-fatigue.html Accessed 7 April 2025.

Morgan S. 2018. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ Accessed 23 March 2025.

Morgan S. 2020. Cybercrime To Cost the World $10.5 Trillion Annually By 2025. https://www.scirp.org/reference/referencespapers?referenceid=3646578 Accessed 29 March 2025.

Morin C. 2024. How to Cut Your Incident Response Time in Half. https://qohash.com/incident-response-time/ Accessed 9 April 2025.

National Institute of Standards and Technology, N., 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf Accessed 30 April 2025.

NIST 2012. Computer Security Incident Handling Guide. https://www.nist.gov/news-events/news/2012/02/nist-requests-comments-updated-guide-handling-computer-security-incidents Accessed 23 March 2025.

Olaes T. 2024. Building an Intelligent Security Operations Center. https://www.balbix.com/insights/introduction-to-security-operations-center/ Accessed 29 March 2025.

Orszula B. 2024. Integrating GenAI with Legacy Infrastructure. https://intervision.com/blog-integrating-genai-with-legacy-infrastructure/ Accessed 9 April 2025.

Picus S. 2024. Financial Services Cybersecurity: 2024 Performance in Banking, Financial Services, and Insurance (BFSI). https://www.picussecurity.com/ Accessed 30 April 2025.

Rakesh E. 2021. SECURITY OPERATIONS CENTER — SOC https://medium.com/predict/security-operations-center-soc-e5f47e277a35 Accessed 27 April 2025.

Roshan Panditharathna et al. 2024. How Cyber Security Enhances Trust and Commitment to Customer Retention: The Mediating Role of Robotic Service Quality. s.l.Big Data and Cognitive Computing.

SafeBreach 2022. Best Practices for SOC Success. https://securityboulevard.com/2022/06/best-practices-for-soc-success/ Accessed 9 April 2025.

Salinas S. 2023. What Is a Security Operations Center? Complete Guide. https://www.exabeam.com/blog/security-operations-center/security-operations-center-ultimate-soc-quick-start-guide/ Accessed 29 March 2025.

Samson R. 2025. SOC Risk Management: Best Practices for Effective Threat Mitigation. https://www.clearnetwork.com/soc-risk-management-best-practices-for-effective-threat-mitigation/ Accessed 25 March 2025.

SANS I. 2021. SIEM Solutions Guide and Best Practices. s.l.:SANS Institute.

Scapicchio M., Downie A. & Finio M. 2025. What Is a Security Operations Center SOC?. https://www.ibm.com/think/topics/security-operations-center Accessed 23 March 2025.

Shackleford D. 2015. Building a World-Class Security Operations Center: A Roadmap. https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-36230 Accessed 26 May 2025.

Skoudis E. &. L. T. 2006. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 2nd ed. Upper Saddle River, NJ: Prentice Hall.

Thompson L. 2024. A guide to SOC Alert fatigue. https://www.infosecpeople.co.uk/a-guide-to-soc-alert-fatigue/ Accessed 7 April 2025.

Uriel 2024. SIEM and SOC Best Practices for Integration. https://cybool.com/siem-and-soc-best-practices-for-integration/ Accessed 9 April 2025.

Violino B. 2022. 7 top challenges of security tool integration. https://www.csoonline.com/article/572023/7-top-challenges-of-security-tool-integration.html Accessed 9 April 2025.

Wadhwa P. 2024. Key Risk Mitigation Strategies to Reduce Business Risks. https://sprinto.com/blog/risk-mitigation-strategies/ Accessed 25 March 2025.

Wadhwa P. 2024. Top SOC Tools for Threat Monitoring and Response. https://sprinto.com/blog/soc-tools/ Accessed 2 May 2025.

Wafula I. 2021. 6 Strategies to Reduce Cybersecurity Alert Fatigue in Your SOC. https://www.microsoft.com/en-us/security/blog/2021/02/17/6-strategies-to-reduce-cybersecurity-alert-fatigue-in-your-soc/ Accessed 10 April 2025.

Whitman M. E. & Mattord H. J. 2018. Principles of Incident Response and Disaster Recovery. 6th ed. Boston, MA: Cengage Learning.

Wojno R. 2021. What is Risk Mitigation? 4 Useful Strategies to Mitigate Risk. https://monday.com/blog/project-management/risk-mitigation/ Accessed 25 March 2025.

Yuchong L. & Qinghui L. 2021. A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. s.l.:Elsevier.

Zamfiroiu A. & Sharma R. C. 2022. Cybersecurity Management for Incident Response. Romanian Cyber Security Journal, 4(1), p. 69–75.

APPENDIX 1: CREATIVE COMMONS LICENCES – IMAGE COPYRIGHT

Image copyright can be ensured by setting search criteria in the image search that allow the image to be used and edited. An image taken from a source can be edited, but you need to check with the copyright whether this can be done. For example, cropping an image or annotating an image is editing. If a finished map is used to mark off an area, it is regarded as editing.

This is how to check image copyright: If you search for an image using Google's Image Search tool, then use the Searching Tools and select Access. Select one of the following options: A derivative work means that you have edited the image in question.

Attribution (BY) The work may be copied, distributed, shown and performed in public and derivative works may be created, provided that the name of the author or copyright holder is duly mentioned.

Non-Commercial (NC) The work may be copied, distributed, shown and performed in public and derivative works may be created only when they are not used for commercial purposes.

No Derivative Works (ND) The work may be copied, distributed, shown and performed in public, but no derivative works may be created from it.

Share Alike (SA) Derivative works may only be distributed under the same license as the original work.

Indicating CC licenses in combinations

The licenses are written with the letter combination CC first. This is followed by a space and a dashed list of abbreviations for license terms. The first of the conditions is always BY, followed by a possible NC and followed by a possible third condition.

The licenses obtained by combining the terms are:

- Attribution (CC BY)
- Attribution – Share-alike (CC BY-SA)
- Attribution – No Derivative Works (CC BY-ND)
- Attribution – Non-Commercial (CC BY-NC)
- Attribution – Non-Commercial – Share-alike (CC BY-NC-SA)
- Attribution –Non-commercial – No Derivative Works (CC BY-NC-ND)

In addition, there is a special CC0 license, which allows the author to waive all rights to the work to the extent permitted by law. In Finland, the author cannot waive his moral rights, thus the name of the author / photographer must always be mentioned.

Example: FIGURE 1. A detail of the Colosseum in Rome (Laamanen 2015, CC BY-SA)

The image may be edited and shared, but the original creator must be mentioned. A modified image may only be shared under the same license as the original image.