International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

IMPROVING INCIDENT RESPONSE TIMES THROUGH EFFICIENT SECURITY OPERATIONS CENTER (SOC) MANAGEMENT: TECHNIQUES TO REDUCE THE MEAN TIME TO DETECT AND RESPOND (MTTD/MTTR)

Wasif Khan
wasif.khan.271195@gmail.com

Abstract

This paper analyzes best practices and tools that can be deployed to optimize SOCs to decrease the MTTD and the MTTR. It speaks to the growing complexity and sheer numbers of cyber threats and how these affect SOC operations. Specific steps discussed in the paper include the process of automation through SOAR platforms, the incorporation of Artificial Intelligence and Machine Learning to identify, real-time monitoring using next-generation SIEM systems, and threat-hunting techniques. It also encompasses the SOC teams' training and the functioning of the Threat Intelligence Platforms (TIPs). The applied or implemented advanced approaches and solutions shall help organizations optimize the productive efficiency of their SOC, enhance cybersecurity situations, and offer new threats.

Keywords: Security Operations Center (SOC), Incident Response Time, Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Security Orchestration, Automation, and Response (SOAR), Artificial Intelligence (AI), Machine Learning (ML), Real-Time Monitoring, Threat Hunting, Threat Intelligence Platforms (TIPs)

I. INTRODUCTION

As the corporate world moves forward towards the future of work, the speed of generating and escalating incidents cannot be overemphasized. In recent years, as organizations turned to digital infrastructure for answers, the threat turned too, and cybercrime became more frequent, diverse and intelligent (Johnson, 2016). These threats are executive entities monitoring, analyzing, and responding to organizations. By meaning effectiveness and efficiency, a SOC can sometimes be a make or determinant of how much an organization can contain an attack or how much it will lose.One of the critical parameters of SOC performance is the speed of reaction to incidents. Two of these regarding the same are the Mean Time to Detect (MTTD) and the Mean Time to Respond (MTTR). MTTD computes the average time taken before a SOC realizes an occurrence of an incident, while MTTR calculates the time taken to contain the incident from the time it was realized. These are not only the performance indicators of SOC efficiency but also instrumental in addressing the impact of threats. The smaller the MTTD and MTTR, the lower the chances of an organization suffering prolonged exposure to threats that will negatively impact its systems, data, and reputation.

1.1 Challenges in SOC Operations

An essential source of the challenge is the constant growth of the number and complexity of cyber threats. New specific threats like ransomware attacks, APTs, and threats from the inside are more

common now, and each is different from the others in terms of detection and prevention (Hudson, 2014). An excellent example of an advancing threat is ransomware, which may randomly encrypt essential data and require a fast intervention lest the data is lost for good. APTs, in contrast, are sneakier, more challenging to get rid of, and can lie dormant for extended periods. Consequently, better detection resources are needed. Insider threats are equally complex because they emanate from within the organization; therefore, it becomes difficult to stop them from using standard security technologies. Apart from threat diversification, SOCs are also challenged by a high alert rate contributed by security systems. This is always characterized by alert fatigue, where the SOC team receives many alerts in their inboxes, which makes it tiresome to filter through them, which might cause a delay in response or even total missing out on vital threats in the organization. High alertness can also demoralize and cause screen fatigue among SOC personnel, which adequately alters their response capacity.

1.2 Purpose of the Article

Based on these challenges, it becomes imperative for this article to discuss several strategies and technologies that can help improve the functioning of SOCs in terms of MTTD and MTTR. The discussion will be centered on adopting modern technologies, machine learning, and artificial intelligence, which can help automate detection and response, eliminating the reliance on the SOC team. Furthermore, the article will discuss ways of enhancing organizational identity management and how real-time data can increase the speed and efficiency of identifying an incident. By considering these aspects, the article offers practical recommendations that can assist organizations in enhancing the effectiveness of SOC and, therefore, enhance the protection against continually emerging cyber threats. Thus, organizations' position in the contemporary cybersecurity landscape is unchallenged. Since threat actors are also constantly innovating, SOCS must adapt quickly by changing the processes and tools used to mitigate these threats; by employing the best practices of MTTD and MTTR, the organization protects its assets from threats that may exist in the present world.

II. IMPLEMENT AUTOMATION WITH SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

2.1 Overview of SOAR

Day-to-day SOAR platforms have become a critical architecture piece in today's emerging Security Operations Center (SOC). SOAR platforms integrate various cybersecurity tools into a single system where the various processes can be coordinated to automate some processes (Bolton et al, 2015). They help handle such incidents through the ability to automate interactions with security incidents, therefore reducing the workload placed on the SOC teams. The primary purpose of SOAR platforms is to pull information from several security systems, process it, and trigger reactions to security threats. This orchestration improves SOC efficiency by raising the speed of timely and effective responses to potential threats. Today's SOC is incomplete without SOAR platforms like Splunk Phantom, Cortex XSOAR, and IBM Resilient, especially when dealing with the threat landscape the world faces today.

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

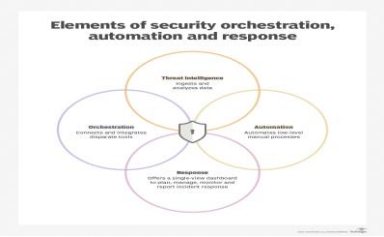

Figure 1: Security Orchestration, Automation and Response (SOAR)

2.2 Automating Incident Response

The other considerable benefit of deploying SOAR platforms is the increase and overall optimization or elimination of recurring actions during the incident handling workflows. Of course, by reducing the amount of intervention required to manage incidents, SOAR platforms ensure that SOC teams are likely to avoid becoming bogged down by routine work. For example, alert classification, data preparation, and the first threat identification can be performed entirely by automated systems, increasing the time. They also noted that this automation is better than manual work since it reduces the likelihood of errors when accomplishing routine work.Furthermore, the SOAR platforms also reduce the response to the incident process by integrating security tools and data sources. This integration ensures that threat data is acquired and then associated with other data, thus improving threat knowledge and analysis of security incidents. The SOAR solution automation means that all the products on the market contain templates for incident handling called playbooks that help follow the rules for each type of event (Sokolowski& Banks, 2012). These books ensure that incidents are performed or handled appropriately, benchmark with others, and increase the SOC's efficiency and effectiveness.

2.3 Key Technologies

Several SOAR platforms, which are market leaders, are presently in the market with different features and capabilities tailored to address various organizational requirements. Praise for Splunk Phantom, which has been exceptionally terrific regarding automation, where it has a rich collection of reusable playbooks that SOC can adapt. Based on the findings, the flexibility of incorporating Phantom into various other security applications is evident, thereby making Phantom a valuable solution for organizations hoping to improve their response to security incidents.

Figure 2: A Splunk Phantom Playbook for Masking Sensitive Data

Cortex XSOAR by Palo Alto Networks was observed to have packed orchestration features and comprehensive threat intelligence coverage. XSOAR is very helpful when threat identification

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

must be efficient and accurate because it tries to automate even complicated workflows and mainly highlights threat intelligence. The second favorite and most highly ranked SOAR platform is IBM Resilient, which focuses on case management as a primary function. It enables SOC teams to record and contain all the incidents and their progress as they go through various phases of the incident management process.

Figure 3: Palo Alto Networks Cortex XSOAR

2.4 Outcome: Outcome of Improving SOAR on SOC Efficiency

Utilization forms transform most providers' Mean Time to Respond (MTTR) to security occurrences (Jhawar&Piuri, 2013). As a concept, SOAR platforms allow for quick initial reactions of SOC teams, for example, through alert filtering, enrichment of the initial data received, and other tasks. Reducing this MTTR is essential because the ability to respond quickly to these security threats means the effect of the incident on the organization.The SOC efficiency enhancements achievable through SOAR implementation. For instance, Splunk Phantom and a major financial services organization decreased the average MTTR of the analysts on the organization Splunk Phantom by 60%, meaning the SOC analysts could manage more rather than fewer incidents per analyst with the same workforce. Likewise, an organization that led Cortex XSOAR experienced a significant decrease in the TTR of responding to phishing attacks, cut down from hours to a few minutes, and helped SOC analysts perform more value-added tasks.

The increased consolidation, coordination, and optimization because of SOAR implementation improves the organization (Newell, 1992). Because SOAR tools further enhance the functionality of ticketing systems by automating repetitive tasks and coordinating intricate processes, SOC teams can actually be more proactive in threat identification and mitigation. Such a strategy does more than lower the threat of securitization; tips to prepare the organization's organization. For the current paper, integrating SOAR platforms into SOC plans enhances cybersecurity management. Regarding practical applications, SOAR platforms enhance the SOC teams' ability to handle incidents by eliminating or reducing the need for a workforce (Schnellbacher, 2017). Some of the market's most popular and widely-used SOAR technologies, such as Splunk Phantom, Cortex XSOAR, and IBM Resilient, have a combination of features that can meet the needs of organizations' MTTR reduction and enhanced security visibility and protection. That way, as threats increase, the SOC environment, through SOAR platforms, shall greatly help ensure organizations are organized against any threats.

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

III. UTILIZE AI AND MACHINE LEARNING FOR THREAT DETECTION

Deploying AI and ML for SOCs also showed many opportunities for threat intelligence and management in diverse organizations (Watson et al, 2018). Consequently, SOCs of the past mainly employed many manual processes and signature-based detection to identify threats. This was highly ineffective due to the increasing sophistication of threats. These shortcomings have, however, been tackled by the current advances in AI and ML to improve the capability in terms of the detection, analysis, and response of threats, hence reforming the entire threat detection procedure.

3.1 AI and ML in SOCs

AI and ML are critical to the modern SOC, and they identify threats after parsing vast amounts of data in real time. These technologies draw experience from previous occurrences, knowledge of new threats, and likely occurrences of security violations. Today, AI and ML used in SOCs permit the automation of the process, which includes the analysis of skeletal traffic and security logs, so that analysts can take up complex threat analysis (Tschider, 2018). This automation improves the effectiveness of SOCs in promptly investigating and mitigating expected security threats to large extents.Risk identification, where the application of AI in this context, means that algorithms can identify signatures and changes within a network or even the network users. These algorithms use big data of normal and unwanted behaviors to distinguish between normal and unwanted behaviors. For example, in the case of regular traffic pattern identification, machine learning techniques are vital for noting anomalies resulting from security threats.

Figure 4: AI detectors: Use cases and technologies

Several new AI-based threat detection tools have become stars in improving SOC operations. For instance, the Darktrace, Microsoft Sentinel, and CrowdStrike Falcon security systems use AI and machine learning to analyze and counter threats in real time.Darktrace is the only AI-driven method to autonomously detect, respond to, and prevent threats in an organization's digital ecosystem (Hall &Pesenti, 2017). It uses machine learning to learn how an organization's network looks and can identify deviations from the usual that could portend an attack. The self-learning technology explained here will enable Darktrace to 'learn' and 'observe' threats in an organization's network and mitigate them without defined rules or forms of signature.

Microsoft Sentinel, a cloud-native SIEM solution, provides features such as strength and deep learning that will assist the tool in identifying threats much sooner (Balaganski, 2015). It gathers data about threats from diverse sources, processes them by applying artificial Intelligence, and coordinates actions to counter them. Compared to a traditional SIEM solution, Microsoft Sentinel

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

uses Artificial Intelligence to identify threats that the typical SIEM tools cannot, which makes it more helpful in bolstering security.Another example of an AI-based tool will be called CrowdStrike Falcon, which applies machine learning mechanisms to threats, including malware. AI helps to improve its EDR to identify advanced threats such as fileless malware and advanced persistent threats (APTs). With real-time analysis of endpoint data, CrowdStrikeFalcon can identify deviations in the path, give notice, and respond to threats.

3.2 Behavioral Analytics

Behavioral analytics can be defined as a subfield of analytical AI primarily aimed at recognizing security threats by observing the users' or the network's behavior patterns, respectively. An ML algorithm's role is to help draw prototypes of normal behavior for users and systems (Poshyvanyk et al, 2018). Once such baselines are set, the algorithms look for anomalies that denote the possibility of carving out an attack.For instance, behavior analysis can alert the analytical system to a user's sudden access to restricted data at odd hours or from an unknown geolocation. This approach helps SOCs detect threats that may not be seen by rule-based systems based on well-known attack patterns.This way, ML's contribution to behavioral analytics is central to minimizing false positives, a wrong facet in traditional threat detection techniques. By making more fine-grained understandings of traffic and properly distinguishing between 'good' and 'bad' activities, the ML algorithms reduce the number of so-called 'false positives', which is helpful for security teams to concentrate on.

Figure 5: Machine Learning Algorithm Overview

3.3 Outcome

When using AI and ML in the threat detection processes, the speeds of threat detection have improved, and the accuracy of threats detected has also increased. One of the most significant benefits of using such technology is that false favorable rates have significantly decreased, which has long been a problem for SOCs. The concept of using AI-driven tools is to consider subjecting and isolating most activities to allow security teams to work on what is more accurate to contribute to the SOC's efficiency (Srinivas, 2018).Furthermore, with the help of AI and ML concepts, quick identification of threats and a response to them are possible. This frees the technologies from having to work on the data step by step, and since it takes a shorter time to detect a threat and the needed responses, it is faster than doing it manually. Such fast detection and response are primarily possible to prevent or at least reduce the impact of cyber threats. Integrating AI and ML in SOCs is progress towards improving threat detection in organizations. These technologies allow for better handling of routine tasks, improved behavior-based analysis, and minimized edited

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

signals to give organizations a better security position against escalating cyber-medium-level threats.

IV. ADOPT REAL-TIME MONITORING WITHNEXT-GENERATION SIEM SYSTEMS

4.1 Evolution of SIEM Systems

SIEM systems have developed significantly since their inception. Current SIEM solutions mainly concern themselves with gathering and storing log information, with end analysis informed by past occurrences (Johansen, 2017). These systems were usually not very effective in generating real-time data. Thus, they were only effective in responding to events rather than anticipating them. Traditional solutions were analytical based on rules and correlation engines and could not provide a deeper understanding of more advanced threats or the methods used for their delivery.The limitations mentioned above have been refined in the next-generation SIEM systems that use other advanced technologies such as machine learning, behavioral analytics and AI. These systems are intended to operate in today's IT environments and can process the enormous volume of data produced in today's data centers; the systems can monitor and detect threats in real-time. New generation SIEMs such as Splunk Enterprise Security and Azure Sentinel are not just real-time data collectors and analyzers but also predictive, enabling, and organized to detect threats that are yet to occur. These systems can learn from past occurrences, making them perfect examples of how AI and machine learning function as they improve on existing detection and response processes.

Figure 6: Understanding SIEM: Strengthening Your Cybersecurity Defenses

4.2 Real-Time Monitoring capabilities

Another significant facet of next-generation structures in SIEM systems is the visibility of network activities. This differs from the first generations of SIEM, which were designed to store data about security events but could not be processed in real-time. This real-time monitoring is essential today as threats can come in quickly and, if not detected on time, can severely compromise an enterprise (Ni et al, 2018).

Splunk Enterprise Security and Azure Sentinel are examples of next-generation SIEM solutions providing accurate and effective real-time monitoring. For instance, Splunk Enterprise Security has a robust search processing language called SPL that will enable real-time query processing on massive datasets. It can look at and draw connections between events from several sources that can offer a broader picture of the security state of an organization. On the other hand, Azure Sentinel takes advantage of Microsoft's Microsoft structure to provide real-time monitoring and threat detection (Bashir et al, 2013). It is fully interoperable with other Microsoft services; it offers a

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

single window view of security incidents in the cloud and on-premise infrastructures. These SIEMs let the security teams know, understand, and respond to threats promptly, limiting the time the adversary takes to attack the system.

4.3 Key Technologies

New-generation SIEM systems differ from traditional ones in that they apply superior technologies to their monitoring and detection processes. Of all these technologies, advanced analytics, contextual alerts, and dashboards are the most essential features, as they will serve as the backbone of the implementation of the proposed Information Services.The advanced analytics about SIEM systems utilize deep and extensive data analysis options along with machine learning algorithms to look for potential signals that may represent a security threat (Jaeger, 2018). These analytics can stay working on significant amounts of data and pick up low-level signs of a breach that a conventional system could overlook. For instance, anomaly detection algorithms can detect or instead recognize some specific levels of network traffic activities that have deviated from the usual trend and alter the trend negatively or negatively by alerting the security team.

Contextual alerts are another vital concept used in next-generation SIEMs (Bezas&Filippidou, 2023). Unlike simple alarms associated with a set of rules, these alerts contain context information about the environment where a security event occurred. For instance, a timeout may be based on current time, user privileges, or an event's general location to determine the possible danger level. This contextual awareness results in better and more relevant alerts since fake alerts are minimized, giving the security teams real threats.Modern SIEMs consist of customizable dashboards that give security teams a specific perspective of their business's position. These dashboards can be configured to display quantities of current threats, the status of current investigations, real-time notifications, etc. This allows organizations to work on valuable data to enhance situation awareness and hasten decision-making.

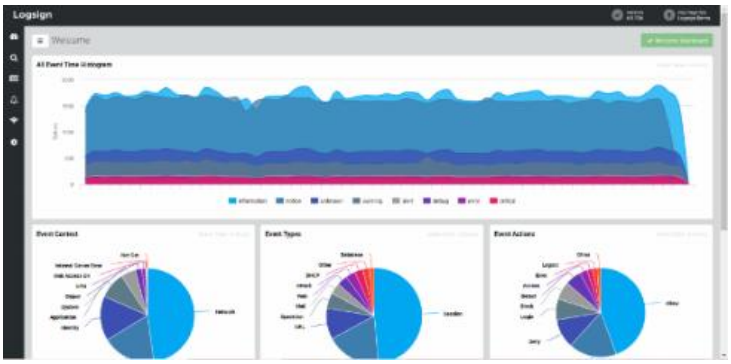

Figure 7: The Types of Dashboards in a SIEM Solution

4.4 Outcome

Next-generation SIEM systems, which support real-time monitoring, positively correlated with MTTD and MTTR to security threats. Unlike traditional SIEMs, these systems include high levels of alerts and real-time dashboards, allowing security and teams to threats much faster in MTTD, which is even more important because they decrease the time available for an attacker within a network undetected. In turn, this reduces the degree of losses resulting from security incidents.Finally, next-generation SIEM systems are a significant advancement in the cybersecurity

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

world. Real-time monitoring tools, supplemented with machine learning and contextual alerts, have become imperative in organizations today. With these systems in place, organizations could elevate their security levels considerably and shorter response times to threats; thus, reducing t those threats will fully exploit the vulnerabilities in the organizations.

V. DEVELOP A PROACTIVE THREAT HUNTING PROGRAM

5.1 Proactive vs. Reactive SOCs

In the past decade, security operations centers (SOCs) have been working primarily in the reactive mode, analyzing incidents (Lindström, 2018). This reactive type includes closely watching systems for alerts caused by potentially anomalous activity or a breach and then containing it. One of the adverse effects is that it depends on predefined patterns (signature) of the threats; therefore, it cannot detect newly emerging and sophisticated threats (Nyati, 2018). Since investigations are started later, the reactive SOC model usually provides the client with a higher MTTD and a higher MTTR.Conversely, as we know, a proactive SOC integrates threat hunting as one of its primary functions, seeking out threats that still need to produce alarms. Threat hunting is the proactive and ongoing methodology of forming hypotheses about threats, outlining indicators of compromise (IoCs) and using tools and techniques to discover threats before they become significant. This approach reduces MTTD by a considerable margin, helping organizations pick threats in their early stages and neutralize them. Threat hunting changes the approach from just having to wait for alerts, which will be analyzed, to using the human brain and enhanced analytics to look for and combat threats, making it a more effective strategy against a constantly growing number of cyber threats (Gill, 2018).

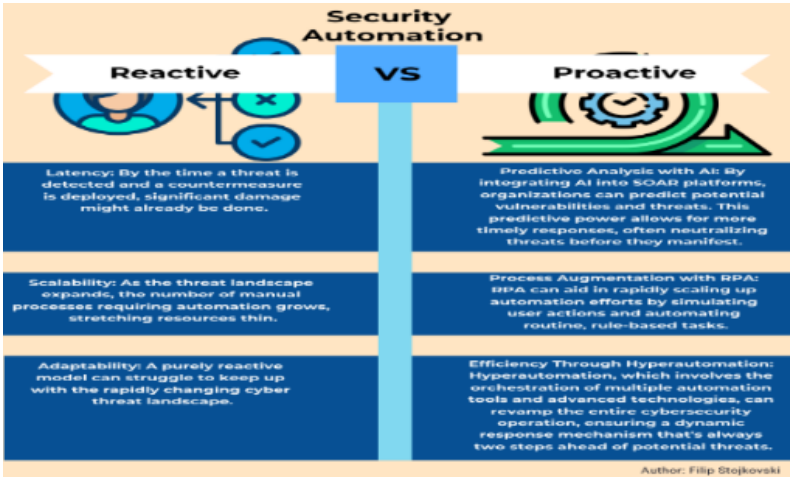

Figure 8: Reactive vs. Proactive Approach of Security Automation and Orchestration (SOAR)

5.2 Threat Hunting Tools

Traditional analysis cannot achieve threat hunting; it requires specific tools that scan big data and possible signs of threat activities. Some of the many solutions that provide advanced threat hunting are CrowdStrike Threat Graph and Carbon Black.Instead, CrowdStrike Threat Graph uses big data analytics to compare billions of events across different sources and determine if they paint a picture of an impending threat. Its real-time analysis and data correlation capabilities make it a

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

great tool for revealing intricate threats that are otherwise hard to identify using standard means. This tool employs machine learning, so it constantly develops a system based on new data to predict and mitigate future threats.

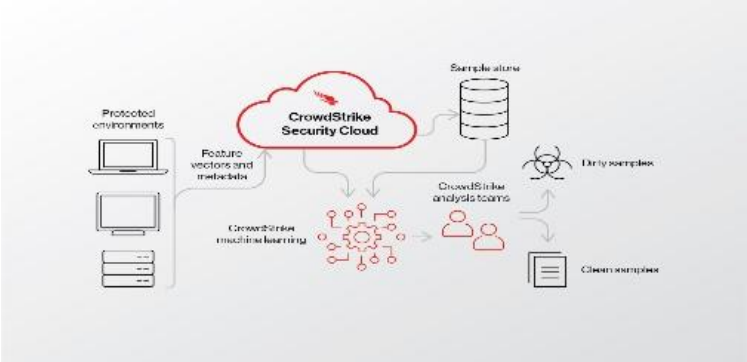

Figure 9: crowd strike threat graph

Carbon Black offers endpoint detection and response (EDR) features through which threat-hunting processes can closely track and analyze endpoint activities' inaccurate timelines (De Fusco, 2023). With stunning telemetry data and fast search and query to different data layers, Cribl allows security analysts to investigate intricate actions and possible breaches in detail. This is because Carbon Black enhances other security solutions and technologies through integrations to function as a valuable tool for a proactive SOC to share and exchange information with other security sectors closely.

5.3 Indicators of Compromise (IoCs).

They include indicators that can turn this theory into simple practice, called Indicators of Compromise (IoCs), which point in the direction of hostile actions within a system or a network. IoCs can refer to activity regarding the flow of network traffic, file changes, or user behaviour that may signal a breach or an attack. In threat hunting, this preeminent candidate, IoCs, is crucial. These components define the threats that threat hunters use to generate hypotheses during their investigations. IoCs are a tool that the security teams use to notice that an adversary is in the network, distinguish his actions, locate him, and potentially apprehend him before he can cause much harm (Cornwell, 2017). In addition, they participate in the development and put procedures in place to enhance the rules and signature framework used for detection, helping advance the capability of the SOC. In a proactive SOC, IoCs are constantly watched and examined to identify any emerging signs of a threat at an early attack stage. This early detection ability is very important to reduce the time that the attacker spends in the network before being detected and promptly ejected, which would reduce the chances of data theft and other unfavourable consequences.

5.4 Outcome: Benefits of Threat Hunting

The main benefit of establishing a proactive threat-hunting programme is the reduction in MTTD, an aspect well associated with improved security performance. Thus, threats are reduced to a minimum in regard to actual incidents that may harm the company or organization's operations

and compromise data. Threat hunting also improves an organization's security posture in other ways because it reveals blind spots that regular surveillance may not uncover (Cole, 2012). Such a proactive approach allows for keeping up the defensive on every step and strengthening it while adversaries constantly develop new tactics. In addition, it should also be said that the intelligence gathered during threat hunting can be used at other stages, for instance, during incident response and threat intelligence, thereby creating linkages and an integrated security operations environment. Proactive threat hunting is an essential process for an organization that wants to enhance its protection from cyber threats. When done in a proactive manner that differs from the traditional SOC model, implementing CrowdStrike advanced tools such as Threat Graph and Carbon Black, as well as the proper usage of IoCs, can help minimize early threat identification and lessen the likelihood of cyber threats.

VI. STREAMLINE COLLABORATION WITH INTEGRATED INCIDENT RESPONSE PLAYBOOKS

6.1 Importance of Standardizes Processes

Playbooks are essential in ensuring a standardized practice across many teams in a security incident (Valites et al, 2015). They also offer the main blueprints for outlining how incidents are investigated and mitigated to minimize such impacts or prevent them from reoccurring within the shortest time possible. In the ever-changing threat landscape, organizations face new threats, so it is crucial to have procedures to work with. Playbooks assist an organization in managing the organization's detection, isolation, and address of incidents, as well as limiting the negative impact of an adverse event. One of the strategic benefits of developing incident response playbooks is that they can help avoid confusion and miscommunications between teams. When IT teams are introduced, when a security incident occurs, other related groups, such as legal, communication, and managerial, must work cooperatively to find the solution. Playing books in incidents prepares all the teams to work in a given manner and does not allow a loose end to be created for one team to misunderstand the rest (Runde& Flanagan, 2008). This is mainly because large organizations have many teams of organizations, leading to inadequate standard processes consequent to etherealized efficiency in therealized incidents.

6.2 SOAR Integration

In their recent forms, SOAR platforms have extensively upgraded traditional approaches to performing and documenting playbooks that organizations need for inside organizations. OAR platforms enable organizations to continue beyond manual action, optimizing reaction time. For a centralized reason, organizations use forms to meet organizational needs and accommodate new threats (King, 1983). This flexibility is essential in today's threat environment, where relatively few threats can always be identified ahead of time. The ability to respond quickly to new challenges can mean the difference between a minor hiccup and a full-blown breach. In addition, SOAR platforms also involve handling and managing multiple responses to incidents in one location, where all the data can be aggregated and analyzed in accurate real-life situations. This helps improve the analyzed response since the teams get all the information, communication, and actions required to manage the situation. The capability to send pre-scheduled notices to the concerned functional parties, collate data, and perform hard-coded operations spars the incident response teams valuable time to address tasks requiring human intervention.

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

6.3 Collaboration Tools

Today, these communication platforms are part of standard practices when handling incidents, with many teams using platforms such as Slack, Microsoft, and Atlassian'sOpsgenie. They support cross-silo work by enabling teams to have real-time communication and exchange of ideas and plans for operations. In an incident, the necessity of sharing particular information and coordinating the activities is valuable. Tools for communication make it possible for the teams to create specific channels for the management of incidents, and everyone who needs to be informed, updated and included in the decision-making process can be informed. These tools would be even more efficient in collaboration with these SOAR platforms because they notify the teams, share information, and coordinate the work. For example, when an event is detected, a SOAR platform can open a channel in either Slack or Microsoft Teams and notify or pull the members of the corresponding teams and reveal the correct information for handling the event. This integration means that all the other teams are instantly notified, which means they can quickly resolve the incident.

Figure 10: Opsgenie - Slack integration | Atlassian

6.4 Outcome

The result of following structured incident response playbooks in time cuts Mean Time to Respond (MTTR), i.e., time required to contain and remediate an incident. Therefore, organizations can operate more efficiently when an incident occurs by centralizing, decentralizing, and improving team cooperation (Lauver&Trank, 2012). It also reduces the legal responsibility for the extent of the consequences after the event and a comprehensive outline of all the company's exposures, operational, reputational and financial losses, presuming that the issue will not interfere with business processes (Nyati, 2018). The integrated incident response playbooks are an essential part of the cybersecurity solution. Because they guarantee standardization activities by the SOAR platforms and foster cross-functional work, these playbooks allow organizations to minimize security incidents, thus lowering the overall level of risk from those incidents.

VII. CONTINUOUS TRAINING AND SIMULATION WITH CYBER RANGES

Such characteristics as activity and the constant appearance of new threats characteristic of cyberspace make it necessary for the SOCs to train their teams. A significant highlight learned from the submitted reports is this: the threat of cyberattacks is dynamic, and SOC teams must, therefore, strive to enhance their bench strength. In its four editions, this continuous training is not just a nice to have but a must-have for SOC teams to detect, respond and neutralize threats in real-time.

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

7.1 Need for Continuous Training

Training the SOC teams is also necessary because threats are not constant and continually transform or move. Unlike training that would be held every time, continuous training ensures that SOC teams are always up to date with the newest threat information and protection methods (Carnevale, 1990). This is important due to cyberspace's dynamic nature, which is why the adversary constantly changes their TTPs; thus, SOC teams should employ strong responses. That is why, with daily training, SOC teams can be more effective and experience timely responses, which is critical.Continuous training can best be achieved whenever an organization embraces cyber ranges as training tools.

7.2 Cyber Ranges and Red Team/Beam Team Exercises

A cyber range is nearly a computerized imitation of actual cyberspace environments utilized to train SOC teams on different threats (Huhtakangas, 2022). A few of the mentioned platforms have adopted Range Force or Immersive Labs, designed to offer realistic and scenario-based learning. These enable the SOC teams to face various elemental and compound challenges, such as phishing, APTs, etc. Such an approach lets teams improve their abilities to mitigate incidents, comprehend the depth of various types of attacks, and plan ways to prevent breaches.Cyber ranges also help Red Team/Blue Team activities since they are the only way to enhance SOC performance. In such exercises, the Red Team attacks to breach through an organization's defences, and the Blue Team's role is defence. These exercises are essential to apply to live scenarios, control SOC teams, and provide them with a fully adversarial environment to think as attackers and learn how to defend. Participation in Red Team/Blue Team activities also benefits the SOC team from the technical level of learning when practicing during incidents. Furthermore, undertaking these exercises makes identification of any gaps in the organization's security structure to enable rectification possible.

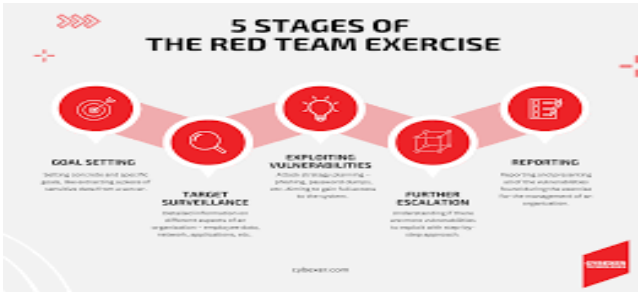

Figure 11: Red Team Exercise in Cyber Security

7.3 Outcome

The result of continuous training for cyber ranges is combining the SOC team into practice incidents (Zimmerman, 2014). The benefits of skills and knowledge enamel established through received coaching and simulation practice lead to enhanced occasions for managing incidents. SOA teams, for instance, can detect actual attacks, understand where and how they originate, the type of impact they will make, and finally, how to mitigate them. This level of preparation is essential in order to minimize the effect of cyber threats and the capability to safeguard the organization's IS. Further, it guarantees that SOC teams change frequently on diverse trends and advanced technologies in cyberspace and practices. Hence, from the given discussion, it can be concluded that with the introduction of new and even more advanced tools and techniques for

International Journal of Core Engineering & Management
Volume-7, Issue-06, 2023 ISSN No: 2348-9510

attacking systems, SOC teams must use them to support defence sustainably. Cyber ranges give a perfect opportunity to use these tools for the first time and adapt them to the SOC processes.

Ongoing training and exercises with cyber ranges working for the success of an efficient cybersecurity measures solution (Yamin&Katt, 2022). Having trained SOC teams that are ready and active in real-time against threat analysis gives an organization more potential to be ready in the event of a cyber attack. The critical advantage found with Range ForceImm, erosive Labs, and Red Team/Blue Team practice is that the growing threat evolution is successfully trained and replicated in a realistic, controlled environment that enhances organizational security effectiveness and constantly lowers SIG Risks.

VIII. LEVERAGE THREAT INTELLIGENCE PLATFORMS (TIPS)

8.1 Role of Threat Intelligence

Threat intelligence is traditionally used in cybersecurity as it offers the information required to prevent and counteract organizational organization.(Jasper, 2017) opines that threat intelligence offers guidance and a framework for a security operation, reducing the time an organization would otherwise spend responding to Threats. This predictive capability is precious in the modern threat environment when a high rate of innovation and growth of new threats affects everyone. Other ways of doing this include threat intelligence, where an organization discovers more vulnerable areas, allowing the right resources to be used in the right areas and improving an organization.

8.2 Key Technologies

Other tools referred to as Threat Intelligence Platforms (TIPs) like ThreatConnect, Anomalies, Recorded Future, and many more are critical tools for organizations using threat intelligence. These sites compile and often sort and broadcast threat information gathered from diverse sources to offer organizations single sources of valuable information. One such tool is ThreatConnect, an application for exchanging threat data and computing threat analysis results for organizational security among organizations that deal with threat intelligence management, including ingestion into an organization's security stack. Recorded Future relies on machine learning and natural language processing for threat intelligence that comes in real-time and will give an analyst a holistic perspective.

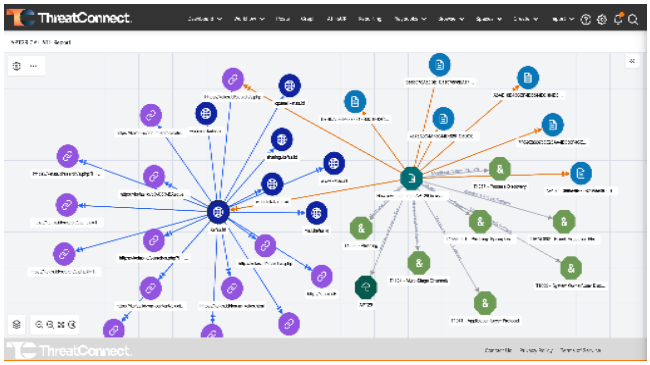

Figure 12: Threat Connect TI Ops Platform Pricing, Cost & Reviews

TIPs' primary advantage is their potential to complement solutions that create alerts, such as SIEM or SOAR systems. When TIPs are connected to SIEM and SOAR, alerts become more refined, and the noise level is lowered, which, in turn, provides security personnel with context to deal with (Nichols & Scanlon, 2018). For instance, when a SIEM system produces an alert, a TIP can add context, create new or extend existing IOCs, detail threat actors or define attack patterns. Consequently, this enriched information leads to better decisions by security analysts, efficient response prioritization timely counteracting threats.

8.3 Enriched Alerts

Adding TIPs with SIEM and SOAR systems also increases identification and reduces MTTD (Bussa et al, 2020). MTTD is reduced to cybersecurity and measures the average time an organization takes to identify a threat once it has emerged. With the use of TIPs, one of the benefits that can be derived is that they provide detailed information on actions taken and, therefore, alert an organization earlier than when there will be no intelligence provided at all. However, this capability is very relevant, especially in APT and other advanced forms of attack that often go undetected for a long time and cause considerable damage if not detected on time.

8.4 Outcome

Threat Intelligence Platforms (TIPs) are critical to improving an organization's platforms. They help prepare and respond to threats by supplying precise and valuable data. The interaction with SIEM and SOAR stereotypes enhances the value of TIPs by providing rich alerts that enhance threat identification and minimize D. Threats are getting more complex with time; utilizing will remain crucial for organizations that want to stand a better chance against them.

IX. CONCLUSION

The development of Management of Security Operation Centers (SOC) in the field of cybersecurity has highlighted advanced techniques and strategies as indispensable components of organizational security (Paans et al, 2015). This report depicts several approaches, such as real-time monitoring, using machine learning in threat identification, and incorporating automation technologies to increase the bang response. SIEM systems are showcased alongside sophisticated threat intelligence platforms and intrusion detection systems as critical technologies that lower the time to detect threats and take action against them.The industry for SOC management is expected to evolve since organizations have started embracing early measures of cybersecurity. One significant implication of defining cyber threats this way is that because they are constantly changing, so must the technologies and the strategies used to guard against them be changing regularly (Gunduz& Das, 2020). Sources say that over time, artificial intelligence (AI) and machine learning (ML) will be incorporated to allow for advancing cautionary measures against probable threats. Also, the current trends of automation tools will continue to decrease the workload of cybersecurity professionals. This evolution will be critical given that, as it must be expected, the volume and the sophistication of the cyber threats will rise.

Organizations should adopt the strategies and technologies discussed in this paper as soon as possible to continue to foster the efficiency of SOCs. Real-time monitoring and threat detection systems are not novelties that can be considered helpful, but they could be considered necessary in the present world (Mishra & Pandya, 2021). Companies that must embrace these technologies will

likely be hamstrung in their capability to defend their assets from new IT threats. Moreover, the need to adopt automation tools and interfaces to achieve better SOC operation efficiency and ensure a shorter response time for incidents, thus significantly decreasing the level of threats from cyber-attacks (Conroy et al, 2017).Therefore, applying the most complex technologies and strategies in the management of SOC is fundamental for organizations desiring to better the position of organizational cybersecurity. Organizations need to immediately get information on the latest threats as this information is provided through mechanisms like real-time monitoring, machine learning-based threat detection and automated tools. Considering trends observed in the present, it can be stated that the future SOC management will rely even more on AI and automation. Thus, organizations either should employ them now.

REFERENCES

1. Balaganski, A. (2015). API Security Management. KuppingerCole Report, (70958), 20-27.
2. Bezas, K., &Filippidou, F. (2023). Comparative analysis of open source security information & event management systems (SIEMs). The Indonesian Journal of Computer Science, 12(2), 443-468.
3. Bollinger, J., Enright, B., &Valites, M. (2015). Crafting the InfoSec playbook: security monitoring and incident response master plan. " O'Reilly Media, Inc.".
4. Carnevale, A. P. (1990). Training in America: The organization and strategic role of training. ASTD best practices series: Training for a changing work force. Jossey-Bass Inc., Publishers, 350 Sansome Street, San Francisco, CA 94104.
5. Cole, E. (2012). Advanced persistent threat: understanding the danger and how to protect your organization. Newnes.
6. Cornwell, J. (2017). Online Anonymization Relating to Cyber Attacks (Master's thesis, Utica College).
7. De Fusco, L. (2023). Advanced C2 Fingerprinting (Doctoral dissertation, Politecnico di Torino).
8. Gill, A. (2018). Developing a real-time electronic funds transfer system for credit unions. International Journal of Advanced Research in Engineering and Technology (IJARET), 9(1), 162-184. https://iaeme.com/Home/issue/IJARET?Volume=9&Issue=1
9. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.
10. Hall, W., &Pesenti, J. (2017). Growing the artificial intelligence industry in the UK. Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy. Part of the Industrial Strategy UK and the Commonwealth.
11. Hudson, B. (2014). Advanced persistent threats: Detection, protection and prevention. Sophos Ltd., US February.
12. Huhtakangas, T. (2022). Xamk cyber range: design of concept for cyber training environment.
13. Jaeger, D. (2018). Enabling Big Data security analytics for advanced network attack detection (Doctoral dissertation, Dissertation, Potsdam, Universität Potsdam, 2019).
14. Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. International Journal of Intelligence and CounterIntelligence, 30(1), 53-65.
15. Jhawar, R., &Piuri, V. (2013, July). Adaptive resource management for balancing

availability and performance in cloud computing. In 2013 International Conference on Security and Cryptography (SECRYPT) (pp. 1-11). IEEE.
16. Johansen, G. (2017). Digital forensics and incident response. Packt Publishing Ltd.
17. Johnson, M. (2016). Cyber crime, security and digital intelligence. Routledge.
18. Jones, R. M., O'Grady, R., Nicholson, D., Hoffman, R., Bunch, L., Bradshaw, J., & Bolton, A. (2015). Modeling and integrating cognitive agents within the emerging cyber domain. In Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) (Vol. 20). Pennsylvania State University.
19. Kesan, J. P., Hayes, C. M., &Bashir, M. N. (2013). Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency. Wash. & Lee L. Rev., 70, 341.
20. King, J. L. (1983). Centralized versus decentralized computing: Organizational considerations and management options. ACM Computing Surveys (CSUR), 15(4), 319-349.
21. Lauver, K. J., &Trank, C. Q. (2012). Safety and organizational design factors: Decentralization and alignment. Journal of Business and Management, 18(1), 61-80.
22. Lindström, O. (2018). Next generation security operations center.
23. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., &Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.
24. Masombuka, M., Grobler, M., & Watson, B. (2018, June). Towards an artificial intelligence framework to actively defend cyberspace. In European Conference on Cyber Warfare and Security (pp. 589-XIII). Academic Conferences International Limited.
25. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377.
26. Moran, K., Bernal-Cárdenas, C., Curcio, M., Bonett, R., &Poshyvanyk, D. (2018). Machine learning-based prototyping of graphical user interfaces for mobile apps. IEEE Transactions on Software Engineering, 46(2), 196-221.
27. Newell, A. (1992). SOAR as a unified theory of cognition: Issues and explanations. Behavioral and Brain Sciences, 15(3), 464-492.
28. Nichols, W. R., & Scanlon, T. (2018). DoD developer's guidebook for software assurance. SpecialReport/2018_003_001_538761. pdf.
29. Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. https://www.ijsr.net/getabstract.php?paperid=SR24203184230
30. Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666https://www.ijsr.net/getabstract.php?paperid=SR24203183637
31. Runde, C. E., & Flanagan, T. A. (2008). Building conflict competent teams (Vol. 116). John Wiley & Sons.
32. Sadowski, G., Kavanagh, K., &Bussa, T. (2020). Critical capabilities for security information and event management. Gartner Group Research Note, 1.
33. Schinagl, S., Schoon, K., &Paans, R. (2015, January). A framework for designing a security operations centre (SOC). In 2015 48th Hawaii International Conference on System Sciences (pp. 2253-2262). IEEE.
34. Schnellbacher, E. J. (2017). New Product Development: The Role of Best Practices and

SOAR in Predicting New Product Success. Lawrence Technological University.
35. Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., ...& Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. Journal of Information Security and Applications, 34, 166-182.
36. Sokolowski, J. A., & Banks, C. M. (Eds.). (2012). Handbook of real-world applications in modeling and simulation (Vol. 2). John Wiley & Sons.
37. Srinivas, S. K. (2018). Security analytics tools and implementation success factors: Instrument development using Delphi approach and exploratory factor analysis (Doctoral dissertation, Capella University).
38. Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. Denv. L. Rev., 96, 87.
39. Yamin, M. M., &Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. Computers & Security, 116, 102635.
40. Zimmerman, C. (2014). Cybersecurity operations center. The MITRE Corporation.