SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 5.1, (2026), pp. 1233-1246
Open Access. Online & Print

10.5281/zenodo.22818107

SCALABLE ADAPTIVE SOAR FRAMEWORK FOR THREAT INTELLIGENCE–BASED CYBER THREAT DETECTION AND AUTOMATED INCIDENT RESPONSE

Shunmugam U[1*] and Rajesh D[2]

[1]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, Email: shunmugamshunmu0@gmail.com
[2]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, Email: drrajeshd@veltech.edu.in

Received: 15/05/2026
Accepted: 22/06/2026

Corresponding Author: Shunmugam U (shunmugamshunmu0@gmail.com)

ABSTRACT

Cyber threats are evolving and growing rapidly and require intelligent automation in the contemporary security operations. In this paper, a proposal will be made on adaptive Security Orchestration, Automation, and Response (SOAR) framework to improve information-driven detection and incident response by cyber threat intelligence (CTI). The structure incorporates the heterogeneous security tools and multisource threat information to be automated to identify, prioritize, and mitigate the threats through advanced orchestration. The machine learning techniques are applied to continuously consume, correlate and process real-time threat intelligence in order to detect potential attacks and execute predefined playbooks to respond to them automatically. The proposed architecture ensures that the detection accuracy and efficiency are improved significantly by minimizing staff involvement and enhancing the latency of the responses. The findings of the evaluation show that the adaptive SOAR framework improves the situational awareness, increases the effectiveness of incident response, and provides a scalable support of the emerging cyber defense processes.

KEYWORDS: SOAR Architecture, Cyber Threat Intelligence, Automated Incident Response, Machine Learning, Security Automation, Threat Detection, Cybersecurity Analytics.

1. INTRODUCTION

Security Orchestration Automation and Response (SOAR) is a collection of unique technologies, which enables businesses to aggregate data and security alerts from diverse sources based on the definition of Gartner [1]. Industries can establish their response processes and conduct threat assessments using SOAR technologies in a comprehensive digital workflow structure, which paves the way for the mechanisation of numerous machine-driven tasks. SOAR incorporates three technology areas which are security orchestration and automation, threat intelligence and incident response. The anticipated value of the worldwide SOAR market is predicted to increase from USD 1.1 billion from 2022 to USD 2.3 billion in 2027, with a Compound Annual Growth Rate (CAGR) of 15.8% between 2022 to 2027 [2].

Solutions and services are the two core SOAR components. SOAR solutions are digital aids that help businesses defend themselves from cyberattacks, which can have a severe impact on their operations by causing application outages, confidential data breaches, reputational harm, compliance penalties, and other issues. Small, medium-sized businesses as well as big businesses employ them, which are installed in the cloud or on-site. It is applicable in various areas like threat intelligence, incident management, network forensics, workflow management, compliance management, and others. Various end users of BFSI (Banking, Financial Services, and Insurance), healthcare, retail, government, energy and utilities, IT and telecommunications, and others are taken in. The key players in the SOAR market are IBM, Cisco, FireEye, Palo Alto Networks, Swimlane, Rapid7, LogRhythm, Splunk and others.

COVID-19 had a favourable effect on the market because of the development of the IT and telecom sectors and the digital transformation of economies. As a result of the pandemic's widespread effects, the industrial sector is becoming more modern and digital. Automation raised the demand for better Internet connectivity, cloud-based applications, connected devices, and IoT services in order to transport data files in real time with great reliability. SOAR utilization has considerably risen in the last few months, and solution suppliers are investing a significant amount of cash in R&D to develop and improve SoCs (Security Operations Centre).

The amount, velocity, and wide range of data present today among firewalls, IDS, and SIEM devices is becoming more and more challenging for SOC analysts to successfully track and handle. This is worsened by the reality that the majority of medium-sized and big businesses use a wide range of security tools and products to protect their data, network, endpoints, and other vital infrastructure. Also, companies often end up installing a variety of products and tools from various vendors that offer various levels of security services and solutions because they lack a particular security tool that can handle all the security operations demands. It is very uncommon for a business to be using over twenty security tools at once to detect and stop cyberattacks. Because of this, SOC organisations must deal with more complicated security stacks that require more time and money to manage. Existing cyber protection systems and solutions have uneven processes, their own data formats and interpretive methods, and a non-integrated design [3]. There is also no standardisation for data interchange among tools. As a result, SOC analysts may find it challenging to properly conFigure____ure and integrate the operations of multi-vendor security products and tools, as well as to obtain a comprehensive understanding of their organisational security posture using specific security tools operating independently. This difficulty typically requires ongoing human involvement (HITL) throughout the whole security incident response process, placing a significant strain on human expertise and producing complex, ineffective, and subpar incident response systems. Furthermore, because of the intricacy of security stacks as well as the variety of security solutions, threats continue to grow at an exponential rate and worsen the issue. Another problem in this difficult effort is the regrettable shortage of security specialists [4-6].

The following list includes the main contributions of the research.

- Automation of Security Orchestration, Automation and Response (SOAR) architecture, which eliminates the need for human involvement and improves response times to threats.
- Integration of multiple data sources, including cyber threat intelligence feeds and internal event logs, to create a comprehensive view of the threat landscape and improve threat detection.
- Development of automated playbooks to handle millions of regular indicators and de-duplicate data to reduce false positives, freeing up security analysts' time for more critical tasks.
- Utilization of machine learning algorithms to provide insights and risk assessments by overlaying internal occurrences with external threat intelligence, improving prioritization of threats and allowing for more informed decisions.

- Possibility of sharing threat intelligence with internal and external trusted organizations, expanding the investigation scope and enabling the development of a community defence against cyber threats.
- Integration with existing security infrastructure, such as firewalls and intrusion detection systems, to provide automated actions to stop threats from spreading throughout the enterprise.
- Continuous monitoring and improvement of the SOAR architecture to adapt to evolving threats and improve overall security posture.

The remaining sections of the research work are separated as the following sections: In Section, a literature review of recent research works on SOAR and cyber threat intelligence is presented, highlighting the current state of the field and identifying gaps in existing research. In Section III, the preliminaries related to SOAR are discussed, providing a foundation for understanding the automated SOAR architecture presented in the following sections. In Section IV, the automated SOAR architecture is presented and explained in detail. Section V discusses about the design and implementation of automated playbooks, the integration of threat intelligence, and the use of machine learning for decision-making. Finally, In Section VI, the conclusion is presented, summarizing the key contributions of the research and outlining directions for future work.

2. RELATED WORK

It is essential for a SOC team to automate security requirements for network connectivity and device compliance operations. Montesino et al. [7] reviewed various enterprise-level security software and hardware options placed special attention on those that provide centralised automation of operations and controls. According to the researchers, a Security Content Automation Protocol (SCAP) may be employed to verify information security management procedures and offer an automated way to make specific operations possible. It has been determined that a security control could be automated if its operation can be carried out with no need for human interaction during the playbook process. According to the researchers, around 30% of security controls could be mechanized. By supplying a single operational environment that allows security personnel to handle security incidence response issues more properly, SOAR will play a significant role in a scenario like it. Thankfully, these controls can provide realistic strategies with prioritised advice on how to apply orchestration and automation tailored specifically for SOAR in incident response needs, serving as a guide for lowering risk and controlling compliance.

A taxonomy of security orchestration is offered based on execution environment, automation approach, deployment category, mode of job, and type of resource analogous to network service orchestration [5]. The main objectives of security orchestration is to close the gap between the identification and correction of security incidents, which increases the task-level flexibility, robustness, dynamicity, and intelligence of orchestration for applications. According to a research study [8] of network service orchestration, integrating network operations and services will adapt pro-actively to alterations in network circumstances to develop resilient and fault - tolerant abilities without human intervention, much as that in a SOAR system. Furthermore, By advancing standard interfaces and creating a data-driven orchestration engine, Wang et al. presented the Security Device Orchestration Framework (SDOF) with the goal of achieving real-time dynamic orchestration [9]. According to the researchers, orchestration is one of the fundamental components of Software-Defined Security (SDS), that not only makes it possible for open services to exist but also permits devices from multiple vendors to use SDS's application layer. Ahmad and Kim presented modular and adaptable task-level orchestration [10], which is made possible by automation at a finer level. By utilising security automation to accomplish real-time threat detection, incident response, and risk-based decision-making skills, AlSadham and Park suggested a framework to improve Information Security Continuous Monitoring (ISCM) capabilities [11].

AI/ML emerges as a remedy for the problem of managing incidence response activities to limit the ever-increasing number of cybersecurity threats due to the quick speed of growth and demand for more robust cybersecurity defence methods [12]. By quickly recognizing and tackling possible ways to enhance, utilizing trackable metrics by SOAR gives cybersecurity analysts a greater understanding of the efficacy of workflows [13]. The researcher identifies the important SOAR indicators as mean time to detect (MTTD), mean time to respond (MTTR), time to qualify (TTQ), and time to investigate (TTI), which enable the SOC management to assess the overall organizational value generated by the team. Those indicators are essential components to reducing security incidents since many security breaches go unnoticed for longer than anticipated, allowing attackers additional time to switch networks and increasing the risk that sensitive data will be

accessed. Less harm is done to organisational claims as a result of quicker notice and response times.

By using ML models as well as other analytical approaches to examine network traffic, network detection and response (NDR) companies continue to integrate cutting-edge manual and automated response capabilities in their products [14]. This method works a lot better than other security solutions at helping businesses identify questionable traffic. In order to create models that accurately represent typical network activity, NDR can also monitor network traffic that crosses the enterprise perimeter and evaluate actual traffic and/or flow data from strategically positioned network sensors.

As per Shoard [15], a crucial component of any threat mitigation strategies is the aggregation of security operations capabilities, such as the incorporation of user and entity behaviour analytics (UEBA) capability in numerous security information and event management (SIEM) platforms. In fact, SIEM providers have added automated response features to different levels of the systems as a result of SOAR's strong alignment with security incident response and general operations processes [16]. According to authors, security teams are required to manually compile and assemble all triaging components into manual playbooks for tasks relating to the severity of events due to the SOC solutions' lack of centralized capabilities. One cannot underscore enough the importance of artificial intelligence.

From the literature, it is observed that there is a need for a robust solution to tackle the problem of automation in CTI. Therefore, an automated SOAR architecture is needed for CTI because it can provide a more efficient and effective approach to managing incident response activities, leveraging AI/ML, trackable metrics, and advanced NDR capabilities to enhance CTI, reduce the need for manual playbooks, and enable SOC teams to evaluate the overall organizational value generated by their efforts.

3. SOAR PRELIMINARIES

Advanced security operations teams at larger organizations include plenty of dynamic components. SOC analysts, security incident responders, and threat intelligence analysts are the three primary parts of modern security operations. Figure 1 provides the different phases of SOAR.

SOC analysts review thousands of internal alerts each day that are generated by endpoint detection and response (EDR) systems, security information and event management (SIEM) technologies, and occasionally hundreds of additional internal security tools. Their role as the enterprise's eyes is to spot security incidents, investigate them, ascertain the cause, and act swiftly. They constantly scan the network with detection instruments to look for and research possible threats. Analysts must also report their results and communicate suggested steps with other stakeholders after identifying an imminent threat.

SOC analysts frequently battle issues like alert exhaustion, a shortage of time, and context limitations. To overcome those issues, SOC analysts require automation, real time collaboration and threat intelligence. Automation to handle daily activities so they can concentrate upon what concerns most. Real-time interaction with all members of the team will keep everyone on the same page and able to share knowledge. They can better appreciate the significance and possible effects of a threat with the use of contextual threat intelligence.

Damage control is a concern for incident responders. They search for potential violations, and if they discover proof of one, it becomes their responsibility to check into it and stop it from propagating. Due to the serious aspect of incidents, all available evidence must be carefully recorded and distributed to all relevant parties. The ability to use EDR tools to destroy the end host is a technique available to incident responders that aids in the containment of vulnerabilities. To implement policies that obstruct dissemination at the network level, they cooperate with firewall administrators. They depend greatly on outsider intelligence to learn about the characteristics and typical tactics of attackers, enabling them to react with assurance and accuracy.

Figure 1: Soar Phases.

Knowledge transfer, case management and limited threat intelligence are considered as major

challenges for security incident responders. To overcome the challenges, complete security case management and threat intelligence are required for them. Complete security case management enables them to properly record their results, interact in real time with other parties involved, and give protective and quarantine precautions for the entire company. Threat intelligence offers more background on attackers and their objectives.

Analysts of threats discover prospective risks to companies that are yet to be noticed in the network. By merging personal intelligence with outside intelligence inputs from various sources, they offer contextuality around possible risks. A recent SANS Institute survey found that 49.5% of organisations have some kind of threat intelligence team or programme with a separate budget and people [17]. This demonstrates the increasing value of threat intelligence analysts, who aid in the identification of attackers by revealing their objectives, methods, and processes. In order to develop stronger preventive measures, threat intelligence teams share their results on specific assaults in addition to reports about the overall threat environment with SOC and incident response teams. Threat intelligence analysts face various challenges like inadequate oversight of threat intelligence streams, secluded processes and acting with difficulty. Complete command of the threat intelligence stream indications is required for the threat intelligence analysts to develop their own reasoning and credibility depending on the circumstances and business requirements. Threat intelligence analysts also need to work with different groups in order to quickly empower them by providing detailed context, current research, and comprehensive records to record their findings.

- Security orchestration, Security automation and Security response are frequently found elements in SOAR systems. SOAR utilization has various advantages which follow as
- Efficiency gains: SOAR solutions can make security teams more effective and efficient by optimising redundant and human security processes.
- Quicker reaction times: Because of automated detection, evaluation, and response processes, SOAR systems can assist organisations in responding to security problems more swiftly.
- Better visibility: SOAR technologies can offer instantaneous insight into security problems, allowing security professionals to spot risks earlier and react more skillfully.
- Improved flexibility: SOAR systems assist organisations in scaling their safety procedures without adding staff members by automating security duties.
- Increased compliance: Through offering an auditable log of security incidents and response actions, SOAR systems assist organisations in meeting the demands of compliance.

4. THE PROPOSED AUTOMATED SOAR ARCHITECTURE

An automated SAOR architecture is presented in Figure 2. A variety of tools and systems, including intrusion detection systems (IDS), networking devices, surveillance tools, and scanners for vulnerabilities produce threat alerts. The risk level, immediacy, and possible impact on the organisation are used to classify and prioritize the alerts. As a whole The SOAR system will immediately carry out a series of specified actions in response to a threat alert, such as banning traffic from a suspect IP address, isolation a compromised endpoint, or alerting the security team. In the incident management system, the platform can additionally generate a ticket or case for additional inquiry and solution.

The real time collaboration component necessitates the recording of workflows or procedures, however once set up, it will assist security teams in applying thorough workflows continuously. The workflows are then organised and standardised to ensure all required personnel, such as SOC analysts, IT analysts, as well as quality control personnel, are given their role at the right moment with the right context. This is a significant advance over earlier approaches to managing workflows and cooperation, like unrecorded knowledge, which can result in loopholes in research and team sloppiness.

Case management component reveals SOAR's capacity to deal with event case management. Security teams can monitor cases, record processes, handle data, and identify violations of compliance using this component's SIRP capability. The fact of the case management is integrated with each of the SOAR components is advantageous compared to employing an independent non-SOAR SIRP. The knowledge stored inside the case-management component can help other components by offering data or procedures accessible however it will additionally benefit from data from other sections to enlarge case-relevant data. Then differentiation of security-incident-based data derived from less dangerous IT information is made possible by more separation from customary IT service management (ITSM) systems like JIRA or ServiceNow.

To increase productivity and effectiveness for

security teams alongside additional users, automation and orchestration are connected in a SOAR system. As was previously indicated, SOAR will integrate with additional technologies, like firewalls or SIEMS, to orchestrate and, with that orchestration, automate. It is significant to remember that not all SOAR providers utilise the identical connection or are compatible with the exact same application. While connected, SOAR may automate security-related tasks in different security network products or offer an abstraction layer to ensure the security professional interacts with SOAR rather than the tool where it is ingesting knowledge. The abstraction layer may assist security teams in streamlining training and procedures since more capability is included within the sole SOAR graphical user interface, necessitating the learning of just one tool rather than a variety of applications.

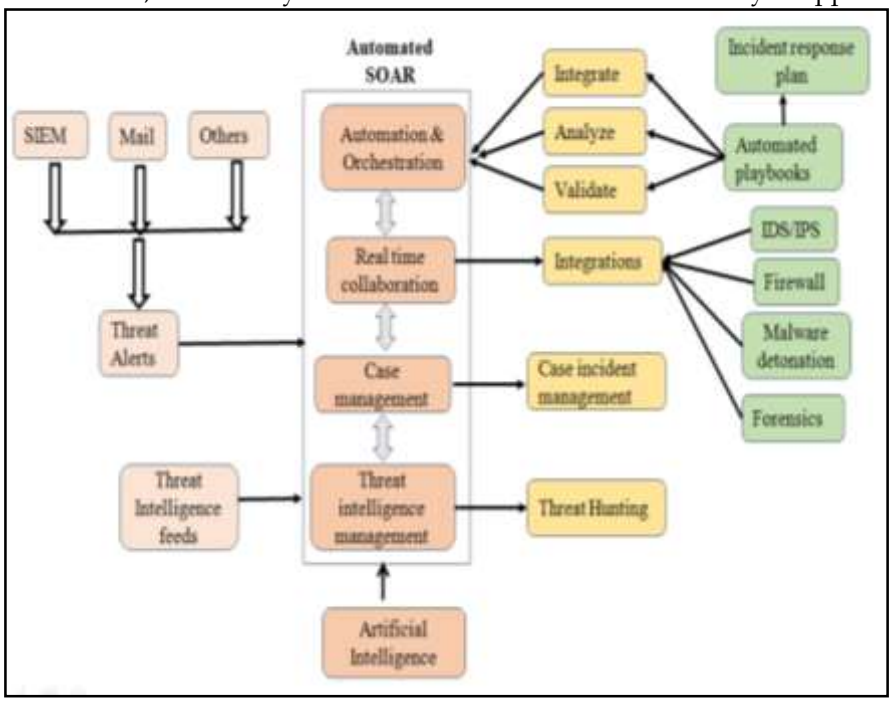

Figure 2: The Proposed Automated SOAR Architecture.

In terms regarding the way machine-readable threat intelligence is utilised, threat-intelligence management does numerous of the similar tasks as standard threat-intelligence platforms (TIPs). By enabling the collection, deduplication, and dissemination of threat-intelligence inputs, SOARs connectivity is once more an impact multiplier. Threat information is able to quickly forwarded downstream to a SIEM or firewall thanks to SOAR's connections with additional security technologies.

Solutions based on artificial intelligence (AI) compile data to automate and analyse IT tasks. Although such solutions extend above the level of automation offered by SOAR systems, the integration that SOAR platforms offer eventually helps. A company has a better chance of utilising true machine learning as well as more advanced forms of automation which are inherent in AI when a SOAR platform is implemented. Given this connection, it's feasible that, like SOAR, AI will be slapped onto the security platform lineup of major manufacturers like IBM, Splunk, and others. If the vendors continue to develop solutions that complement and feed one another, the dependencies necessary for achieving automated processes and machine learning for this domain can be strengthened.

Internal and outside TI are incorporated into the incident response processes by the automated SOAR security solution. Every SOAR security system must have the capacity to automate, and automation is accomplished via playbooks as well as runbooks [18]. A playbook is a series of procedures (workflows) that must be followed in a linear fashion in order to react effectively to a particular event kind or risk. Incident response playbooks offer a straightforward, top-down, step-by-step method of orchestration. Versatility and usability are equally crucial since workflows are the foundation for the automation and orchestration processes inside a SOAR solution. A runbook, on the other hand, is a set of conditional processes that are automatically performed as a component of the incident response or protection operations workflow to carry out tasks including indicator enhancement, threat protection, and

notification issuing.

In automated SOAR, an incident response plan is a written, methodical strategy for handling cybersecurity issues. The plan explains the duties and obligations of every member of the team as well as the precautions that the security team is taking as a result of an incident of security.

The following essential elements are often included in the incident response plan in SOAR:

- Identification and classification of security incidents: The strategy specifies the standards for determining and categorising various security incident types according to their seriousness and potential consequences for the organisation.
- Response procedures: This plan defines the sequential steps that should be taken in the case of an attack, includes ways to control the incident, look into the cause, and repair the harm.
- Procedures for reporting and sloppiness: This plan outlines whom needs to be notified if there is any such an attack on security, comprising employees, law enforcement authorities, and various outside service providers. Additionally, it outlines how to escalate processes for issues that call for immediate action.
- Communication protocols: It specifies the routes and standards that must be utilised to interact with stakeholders at all levels, as well as ways to exchange data across the security team, throughout the incident response process.
- Procedures for testing and reviewing: The strategy contains steps for frequently evaluating the incident response strategy to assess its efficacy as well as regularly reviewing and revising the strategy to account for shifts in the threat environment or the security posture of the company.

By connecting with different security products, automating response activities, and offering real-time analytics and reporting capabilities, automated SOAR systems assist organisations in automating and streamlining their incident response process. Organisations can enhance their capacity to promptly identify and address security events by utilising the incident response plan in SOAR.

5. EXPERIMENTAL SETUP AND RESULTS ANALYSIS

The entire experimentation is performed in two phases. A deeper insight with respect to open-source tool and splunk phantom is compared. The experimental setup involved the use of open-source technologies for CTI and SOAR. For CTI, the experimental environment utilized MISP (Malware Information Sharing Platform) as the main threat intelligence-sharing platform. MISP provides a collaborative platform for sharing, storing, and correlating threat information among the different security teams. In addition to MISP, OpenCTI was also used as an open-source CTI platform to store and visualize threat intelligence data. For SOAR, the experimental environment utilized The Hive and Splunk Phantom as the main orchestration and automation platform. The Hive provides a centralized platform for handling security incident response tasks and integrates with other open-source tools such as Cortex, which provides automated responses to incidents. Splunk Phantom provides a powerful automation and orchestration solution for security operations. It enables security teams to automate repetitive tasks and create playbooks for different security incidents. Splunk Phantom also provides various integrations with security tools, including threat intelligence feeds, vulnerability scanners, and SIEM platforms. The SOAR environment was further enhanced with the integration of WAZUH (Elasticsearch and Kibana) for log management and analysis.

5.1 Testing & Validating The Experimental Setup

To test the effectiveness of the experimental setup, a series of simulated attacks were conducted. Threat intelligence data was ingested into MISP and OpenCTI, and rules were created to trigger automated responses in Splunk Phantom & The Hive through Cortex. The logs generated by the different tools were collected and analyzed using Elasticsearch and Kibana. To test the CTI & SOAR setup, we created a use case for detecting and responding to a phishing email. We used the following components to implement the use case followed below.

5.1.1 *Splunk Phantom*

We created a playbook in Splunk Phantom that included the following actions:

- Receiving an email alert from the SIEM platform
- Extracting email headers and content
- Checking the email headers against a list of known malicious indicators in MISP
- Generating an incident in Splunk Phantom if the email is found to be malicious
- Notifying the security team via email and a

messaging platform
- Quarantining the email in the email gateway

5.1.2 *Thehive*

We developed a playbook in The Hive that included the following actions:
- Automatically triaging the alert based on predefined severity levels
- Parsing and analyzing the metadata of the alert to identify the source, type, and scope of the incident
- Correlating the incident data with threat intelligence feeds to determine if it matches any known indicators of compromise (IOCs)
- Generating an incident report with all relevant information for further investigation by the security team
- Assigning the incident to a specific analyst or team based on their area of expertise
- Updating the incident status and priority based on the investigation progress
- Notifying the security team via email and a messaging platform
- Quarantining any suspicious files or emails associated with the incident to prevent further damage

5.1.3 *Misp*

We configured MISP to receive and store threat intelligence feeds from various sources, including open-source feeds and commercial feeds. We also created a list of known malicious indicators, including domains, IP addresses, and hashes.

5.1.4 *Email Gateway*

We configured the email gateway to quarantine any emails that are found to be malicious by Splunk Phantom.

5.1.5 *Messaging Platform*

We configured a messaging platform to notify the security team of any incidents generated by Splunk Phantom.

We simulated a phishing attack by sending a malicious email to one of the email addresses monitored by the email gateway. The email was detected by the SIEM platform, which triggered both the playbooks. Both the SOAR platforms extracted the email headers and content, checked them against the list of known malicious indicators in MISP, and generated an incident when it found a match. Further escalation was notified via email and the messaging platform, and the email was quarantined in the email gateway.

5.2 *Attack Simulation Using Splunk Phantom & Thehive*

5.2.1 *Splunk Phantom*

The playbook in Splunk Phantom was designed to detect and respond to a phishing attack. It consisted of several actions, including receiving an email alert from the SIEM platform, extracting email headers and content, checking the email headers against a list of known malicious indicators in MISP, generating an incident in Splunk Phantom if the email is found to be malicious, notifying the security team via email and a messaging platform, and quarantining the email in the email gateway.

To further test the effectiveness of the playbook, we simulated a phishing attack by sending a malicious email to one of the email addresses monitored by the email gateway. The email was detected by the SIEM platform, which triggered the Splunk Phantom playbook. Splunk Phantom extracted the email headers and content, checked them against the list of known malicious indicators in MISP, and generated an incident when it found a match. The security team was notified via email and the messaging platform, and the email was quarantined in the email gateway.

5.2.2 *Thehive*

The Hive was used to create a playbook for detecting and responding to a ransomware attack. The playbook consisted of several actions, including receiving an alert from the SIEM platform, analyzing network traffic, identifying the source of the attack, isolating the affected systems, and notifying the security team. To test the effectiveness of the playbook, we simulated a ransomware attack by creating a malware sample and executing it on one of the systems on the network. The SIEM platform detected the attack and triggered the playbook in The Hive. The Hive analyzed the network traffic, identified the source of the attack, and isolated the affected system. The security team was notified of the incident and took further action to mitigate the damage caused by the attack.

5.2.3 *Deploying Machine Learning Model For Missing Alert Classification*

The ability of ML models to identify patterns and anomalies in large datasets can significantly enhance the accuracy and speed of detecting cyber-attacks. In this study, we employed five popular ML algorithms, namely Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, Random Forest, and Support Vector Machine (SVM), to validate the alert and traffic

data generated by our proposed system.

5.2.4 *Phishing URL Detection*

The collected alert and traffic data were preprocessed to extract relevant features, including URL length, domain age, and presence of suspicious keywords. The processed data was then split into training and testing sets to train and evaluate the performance of the machine learning models. The dataset was splitted into training and testing sets, with a 70/30 ratio, respectively.

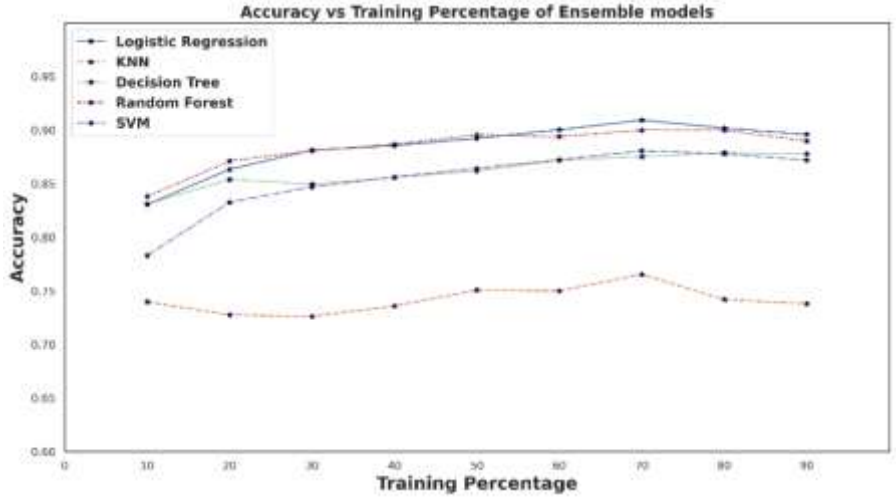

Figure 3: Accuracy Vs Training (Malicious URL).

In Figure 3 indicates that the Random Forest model outperformed the other models with an accuracy of 90.8%, precision of 95.2%, and recall of 66.7%. The SVM model also performed well, with an accuracy of 89.7%, precision of 95.3%, and recall of 65.3%. The other models achieved accuracies between 55% to 90%. From the results of our experiments, it is clearly demonstrated that machine learning models can effectively classify URLs alerts and traffic data, providing an additional layer of security in detecting potential threats. The findings of this study can be utilized to enhance the performance of SOAR and SIEM modules and improve the overall cybersecurity posture of an organization.

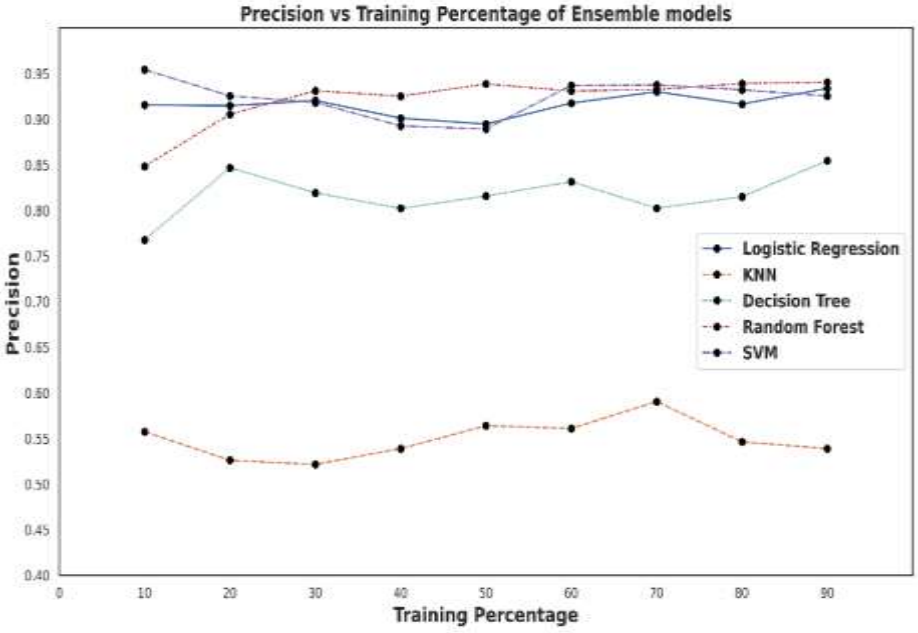

Figure 4: Precision Vs Training (Malicious URL).

In Figure 4 represent for phishing classification, our results showed an accuracy of 91%, precision of 95%, and recall of 72%. This means that out of all the phishing traffic data we tested, 91% were classified correctly by our model. Additionally, when our model classified traffic data as phishing, it was correct

85% of the time. Finally, when phishing traffic data was present, our model was able to identify it 96% of the time.

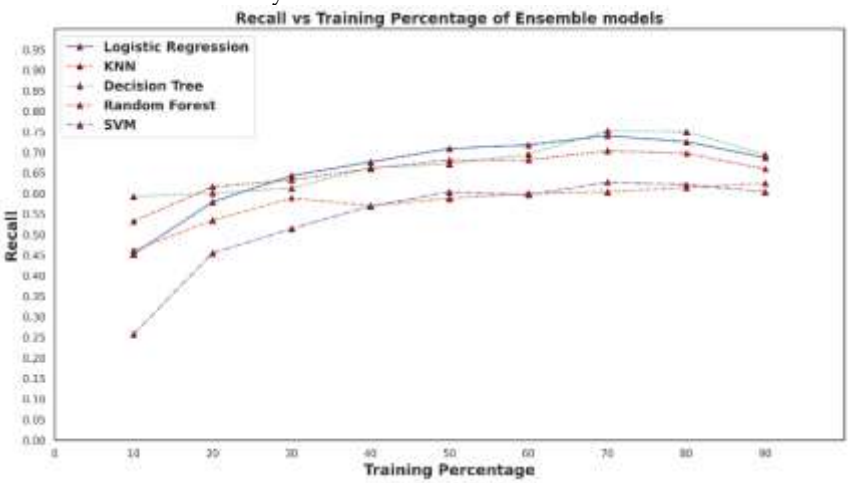

Figure 5: Recall Vs Training (Malicious RL).

The results showed that KNN performed poorly for both phishing and ransomware data, with accuracy (Figure 3) and precision values below 0.80 (Figure 4) and recall values below 0.60 (Figure 5). On the other hand, Logistic Regression and Random Forest showed higher accuracy, precision, and recall values for both phishing and ransomware data, with accuracy values above 0.85 (Figure 3), precision values above 0.90 (Figure 4), and recall values above 0.60 (Refer Figure 5).

5.2.5 *Ransomware Traffic Detection*

For the ransomware network traffic data, we collected various network traffic logs from the SIEM and SOAR modules. These logs contained information about network connections, packet data, and other relevant traffic metadata. We then used a set of ML models including Logistic Regression, KNN, Decision Tree, Random Forest, and SVM to classify this traffic data and identify any potential ransomware attacks. The ML models were trained on a labeled dataset that contained both normal network traffic and traffic associated with known ransomware attacks. We used various feature engineering techniques (here we used statistical moments) to extract meaningful features from the network traffic data, such as packet size, source and destination IP addresses, and protocol types. These features were then used as input to the ML models, which were able to learn patterns and correlations in the data to make accurate predictions about the presence of ransomware in the network traffic indicates in Figure 6.

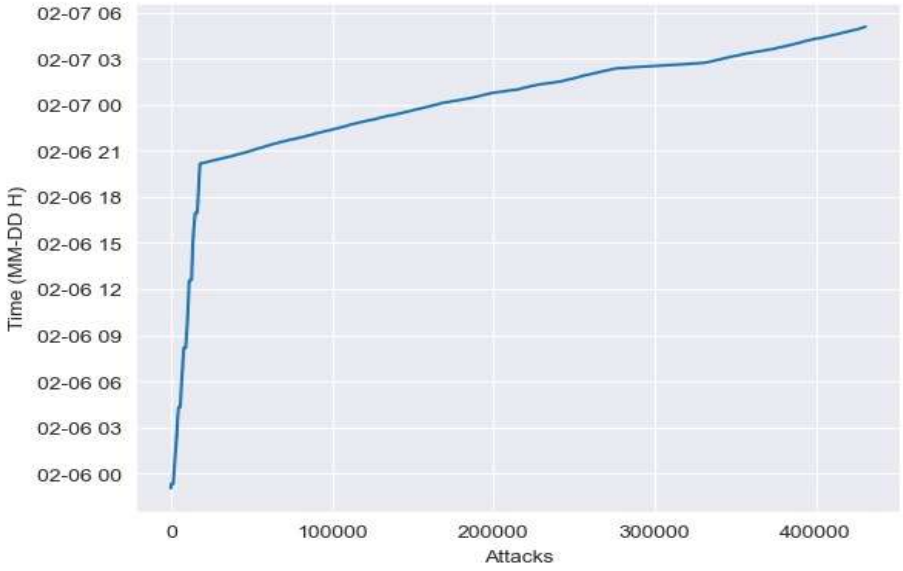

Figure 6: Ransomware Attack – Network Traffic Data.

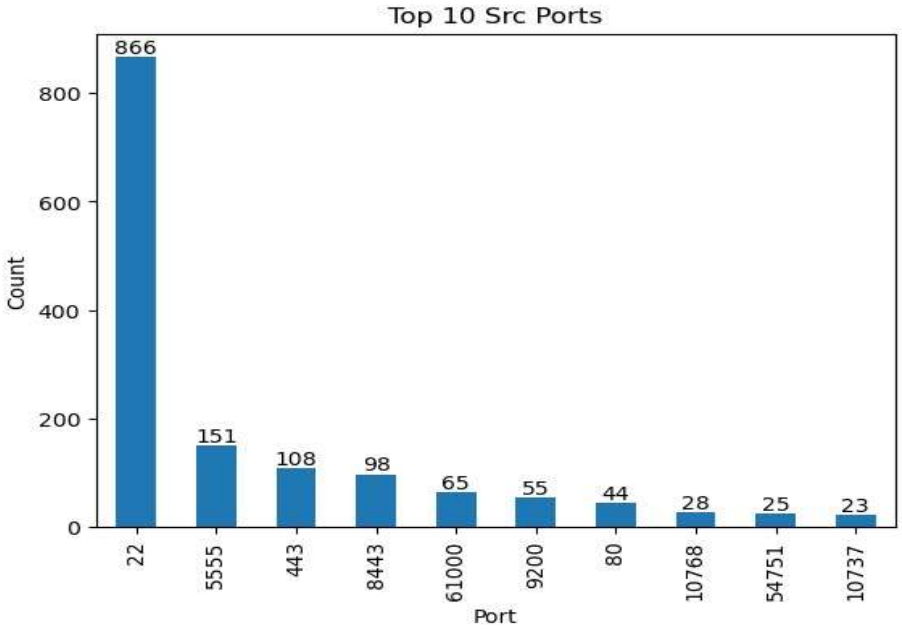

Figure 7: Frequency Of Port Access (Top 10 Source Ports).

Figure 7 shows the Frequency of port accessed which displays the top 10 source ports accessed in the network traffic captured during the ransomware attack. The x-axis represents the source port number and the y-axis represents the frequency of access. Each bar on the plot corresponds to a particular source port number and its height indicates the frequency of access. From the plot, we can see that the most frequently accessed source port is 22, 5555, 443, which is typically used for SSH traffic, followed by port 5555, which is used for malicious traffic. This suggests that the ransomware may be using the standard HTTPS and HTTP traffic to communicate with its command-and-control (C2) server, possibly to exfiltrate data or receive commands. Figure 7 also shows that some other ports, such as 8443 and 61000, were accessed relatively frequently, which could indicate that the ransomware was attempting to spread laterally across the network or exploiting vulnerabilities associated with these ports. Overall, Figure 7 provides insights into the network traffic patterns associated with the ransomware attack and can be useful for developing detection and mitigation strategies.

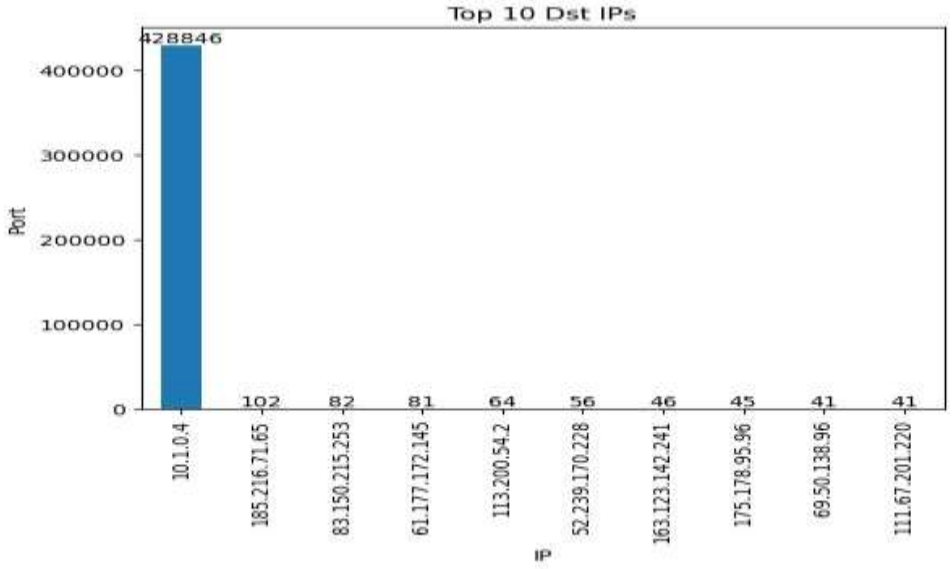

Figure 8: Frequency Of Destination IP.

Figure 8 shows Frequency of destination IP where it displays the top 10 destination IP addresses that were accessed in the captured network traffic during the ransomware attack. The x-axis represents the IP

addresses, while the y-axis represents the count of times each IP address was accessed. Figure 8 also provides insights into the top destinations of the ransomware attack, which could potentially be the command and control (C2) servers used by the attackers to control the malware. The security analysts can investigate these IP addresses further to determine if they are associated with any malicious activities or known threat actors. It can also be used to identify any potentially compromised machines that were communicating with these IPs and could be used to further propagate the ransomware attack.

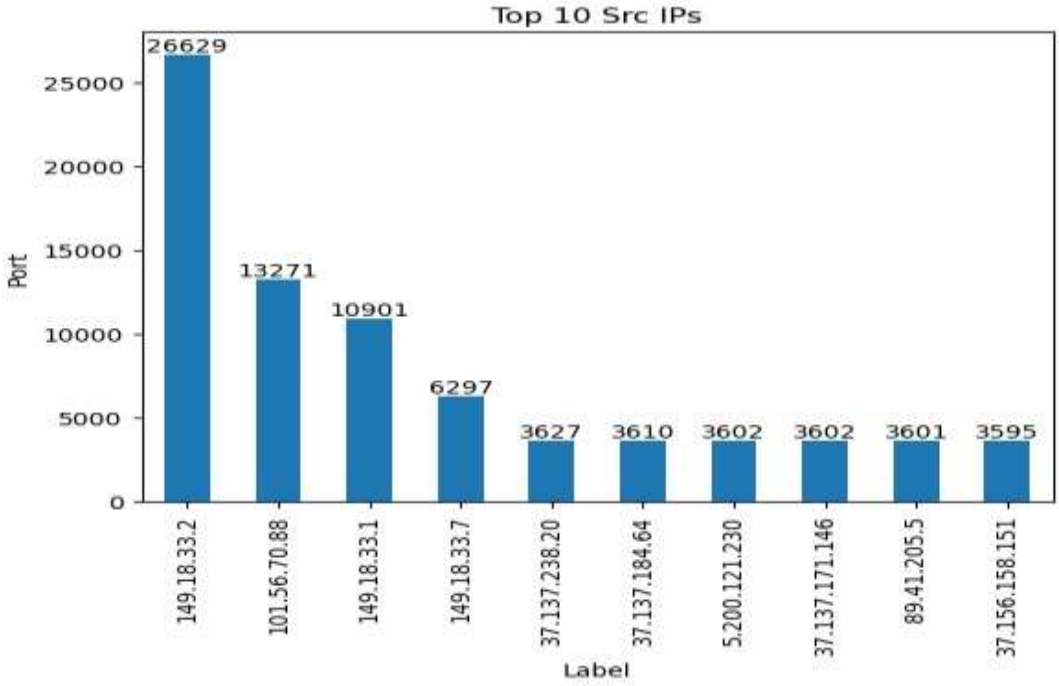

Figure 9: Frequency Of Source Ips.

Figure 9 shows the Frequency of source IP where it displays the distribution of the top 10 source IP addresses that accessed the network during the observed time period. Each bar in the plot represents the number of times a particular source IP accessed the network. The height of the bar indicates the frequency or count of that source IP in the network traffic data. By analyzing this plot, we can identify the top 10 source IP addresses that accessed the network most frequently during the observed time period. This information can help in identifying the origin of the ransomware attack, as well as in designing and implementing preventive measures to block access from those source IPs. Additionally, this plot can provide insights into potential vulnerabilities or weaknesses in the network, such as outdated software or misconfigured firewalls, that may have enabled access from these source IPs.

6. CONCLUSION AND FUTURE RESEARCH

The results of the experiment showed that the proposed SOAR architecture used in the experimental setup were effective in detecting and responding to simulated attacks. In both experiments, we used the accuracy metric to evaluate the performance of the machine learning models. The results showed that Random Forest outperformed the other models with an average accuracy of 92% for the phishing traffic data and 88% for the ransomware network traffic data. This indicates that our feature engineering techniques were effective in capturing the relevant characteristics of the data and that the Random Forest algorithm was able to learn these patterns and classify the data accurately. Overall, this approach allowed us to effectively classify ransomware network traffic and identify potential attacks in real-time. By integrating these ML models into the SOAR and SIEM modules, we were able to automate the detection and response process and improve the overall security posture of the organization. In addition, the collaborative nature of MISP and OpenCTI allowed for the sharing and correlation of threat intelligence data, while TheHive provided a centralized platform for handling incident response tasks. The use of Cortex for automated responses, Elasticsearch, and Kibana for log analysis further enhanced the effectiveness of the SOAR environment. In order to support cyber defence activities effectively and efficiently in the modern

sophisticated and evolving cyber threat landscape, sophisticated orchestration and automation expertise are urgently required. An automated SOAR architecture will employ information gathered from threat intelligence to increase the precision and quickness of threat identification and response in the overall picture of cyber threats. Security teams today face numerous issues due to the overabundance of data and tool sets, which can be addressed by automated SOAR. Along with orchestrating and automating warnings, it aids security personnel in reducing alert fatigue to some extent. Overall, automated SOAR system assist organizations in strengthening their defence posture through allowing individuals to swiftly and efficiently identify, explore, and react to security issues.

The proposed SOAR architecture, used in the experimental setup, demonstrated its effectiveness in detecting and responding to simulated attacks. However, there are still several areas of research that can be explored to enhance its capabilities. One potential research direction is to investigate the use of deep learning models, such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), for network traffic classification. Another promising research direction is to incorporate explainable AI (XAI) techniques to enhance the interpretability of the classification results, which can help in building trust and confidence in the automated system. Moreover, the use of automation and orchestration in cyber defence is still in its early stages, and further research is required to develop more sophisticated and intelligent automated response mechanisms. Additionally, there is a need for the development of more efficient and effective methods for sharing threat intelligence data among different organizations to improve the overall security posture of the cyber ecosystem.

Overall, the results of this research provided a solid foundation for the development of more advanced and effective automated SOAR architectures in the future. These architectures will play a crucial role in improving the overall security posture of organisations by enabling the swift and efficient identification, exploration, and response to security issues.

Data Availability Statement: The data generated and analyzed during the current study are available from the corresponding author upon reasonable request.

Conflict of Interest: The authors declare to have no conflict of interest.

Funding: No funding

Author contribution: Shunmugam U [1,*]: Conceptualization, Data collection, Methodology, writing- original draft, Validation, Resources.

Rajesh D [2]: writing- review and editing, Formal Analysis, Supervision, Investigation, Vizualization.

REFERENCES

1. https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
2. https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=176584778&utm_source=Email&utm_medium=Acoustic_ICT_APAC&utm_campaign=Acoustic_Security_Orchestration_Automation_and%20_Response_Market_12_July_2022 0
3. C. Islam, M. A. Babar and S. Nepal, "A multi-vocal review of security orchestration," ACM Computing Surveys, vol. 52, no. 2, pp. 1–45, 2019.
4. NIST, "Cybersecurity workforce demand," 2020. [Online].Available:https://www.nist.gov/system/files/documents/2017/10/26/nice_workforce_demand_pdf.pdf.
5. Cyberseek, "Hack the gap: Close the cybersecurity talent gap with interactive tools and data," 2020. [Online]. Available: https://www.cyberseek.org/index.html.
6. S. Morgan, "Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021," 2019. [Online]. Available: https://cybersecurityventures.com/jobs/.
7. R. Montesino and S. Fenz, "Automation possibilities in information security management," in Proc. of the European Intelligence and Security Informatics Conf. (EISIC), Athens, Greece, pp. 259–262, 2011.
8. N. F. Saraiva de Sousa, D. A. L. Perez, R. V. Rosa, M. A. S. Santos and C. E. Rothenberg, "Network service

orchestration: A survey," Computer Communications, vol. 142-143, no. 1, pp. 69–94, 2019.
9. W. Wang, X. Qiu, L. Sun and R. Zhao, "A data driven orchestration framework in software defined security," in Proc. of 2016 5th International Conf. on Network Infrastructure and Digital Content, IEEE IC-NIDC, Beijing, China, pp. 34–39, 2017.
10. S. Ahmad and D. H. Kim, "A multi-device multi-tasks management and orchestration architecture for the design of enterprise IoT applications," Future Generation Computer Systems, vol. 106, pp. 482–500, 2020.
11. T. AlSadhan and J. S. Park, "Security automation for information security continuous monitoring: Research framework," in Proc. IEEE World Congress on Services, SERVICES, pp. 130–131, 2016.
12. R. Trifonov, O. Nakov and V. Mladenov, "Artificial intelligence in cyber threats intelligence," in Proc. ICONIC: 6th & 7th Dec 2018, Holiday Inn, Plaine Magnien, Mauritius, 2018.
13. R. Brewer, "Could SOAR save skills-short SOCs?," Computer Fraud & Security, vol. 2019, no. 10, pp. 8–11, 2019.
14. L. Orans, J. D'Hoinne and J. Chessman, "Market guide for network detection and response," 2020. [Online]. Available: https://www.gartner.com.
15. P. Shoard, "Hype cycle for security operations," 2020. [Online]. Available: https://www.gartner.com.
16. C. Neiva, C. Lawson, T. Bussa and G. Sadowski, "Innovation insight for security orchestration, automation and response," 2017. [Online]. Available: https://www.gartner.com/en/documents/3834578/innovation-insight-forsecurity- orchestration-automation.
17. "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 11, 2020, https://www.sans.org/reading-room/whitepapers/threats/paper/39395.
18. DFLabs, "The difference between playbooks and runbooks in incident response," 2019. [Online]. Available: https://www.dflabs.com/resources/blog/the-difference-between-playbooks-and-runbooks-in-incident-response/.