Enhancing Remote Work Security: Integrating IDS with SOAR for Improved Threat Detection and Response

A MINOR PROJECT REPORT

Submitted by

LAKKAVARAM S M SHRIYA VARNITA [RA2111030010201]
PAVULURI LOLA YASWANTHI [RA2111030010256]

Under the Guidance of

Dr. C. N. S. VINOTH KUMAR

(Associate Professor, Department of Networking and Communications)

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

with specialization in CYBER SECURITY

DEPARTMENT OF NETWORKING AND COMMUNICATIONS

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR- 603 203

NOVEMBER 2024

Department of Networking and Communications
SRM Institute of Science & Technology
Own Work Declaration Form

This sheet must be filled in (each box ticked to show that the condition has been met). It must be signed and dated along with your student registration number and included with all assignments you submit – work will not be marked unless this is done.

To be completed by the student for all assessments

Degree/ Course : **B.Tech in CSE with Specialization in Cybersecurity**

Student Name : **Lakkavaram S M Shriya Varnita, Pavuluri Lola Yaswanthi**

Registration Number : **RA2111030010201, RA2111030010256**

Title of Work : **Enhancing Remote Work Security: Integrating IDS with SOAR for Improved Threat Detection and Response**

We hereby certify that this assessment compiles with the University's Rules and Regulations relating to Academic misconduct and plagiarism**, as listed in the University Website, Regulations, and the Education Committee guidelines.

We confirm that all the work contained in this assessment is our own except where indicated, and that We have met the following conditions:

- Clearly referenced / listed all sources as appropriate
- Referenced and put in inverted commas all quoted text (from books, web, etc)
- Given the sources of all pictures, data etc. that are not my own
- Not made any use of the report(s) or essay(s) of any other student(s) either past or present
- Acknowledged in appropriate places any help that I have received from others (e.g.fellow students, technicians, statisticians, external sources)
- Compiled with any other plagiarism criteria specified in the Course handbook / University website

I understand that any false claim for this work will be penalized in accordance with the university policies and regulations.

DECLARATION:
I am aware of and understand the University's policy on Academic misconduct and plagiarism and I certify that this assessment is our own work, except where indicated by referring, and that I have followed the good academic practices noted above.
If you are working in a group, please write your registration numbers and sign the date for every student in your group.

ACKNOWLEDGEMENTS

We express our humble gratitude to **Dr. C. Muthamizhchelvan,** Vice-Chancellor, SRM Institute of Science and Technology, for the facilities extended for the project work and his continued support.

We extend our sincere thanks to Dean-CET, SRM Institute of Science and Technology, **Dr.T.V. Gopal,** for his invaluable support.

We wish to thank **Dr. Revathi Venkataraman, Professor & Chairperson**, School of Computing, SRM Institute of Science and Technology, for her support throughout the project work.

We are incredibly grateful to our Head of the Department, **Dr. M. Lakshmi**, Professor and Head, Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, for her suggestions and encouragement at all the stages of the project work.

We want to convey our thanks to our Project Coordinator, **Dr. C. N. S. Vinoth Kumar**, Associate Professor, Panel Head, **Dr. M Jayaselvi**, Assistant Professor and members, **Dr. P Balaji Srikanth,** Assistant Professor, **Dr. R Nithva ,** Assistant Professor, Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, for their inputs during the project reviews and support.

We register our immeasurable thanks to our Faculty Advisors, **Dr. Meenakshi K & Dr. Saranya G,** Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, for leading and helping us to complete our course.

Our inexpressible respect and thanks to our guide**, Dr. C. N. S. Vinoth Kumar,** Associate Professor, Department of Networking and Communications, SRM Institute of Science and Technology, for providing me/us with an opportunity to pursue our project under his/her mentorship. She provided me/us with the freedom and support to explore the research topics of my/our interest. Her passion for solving problems and making a difference in the world has always been inspiring.

We sincerely thank the Networking and Communications department staff and students, SRM Institute of Science and Technology, for their help during our project. Finally, we would like to thank parents, family members, and friends for their unconditional love, constant support, and encouragement.

LAKKAVARAM SHRIYA VARNITA [RA2111030010201]
PAVULURI LOLA YASWANTHI [RA2111030010256]

SRM

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that 18CSP107L project report titled "**Enhancing Remote Work Security: Integrating IDS with SOAR for Improved Threat Detection and Response"** is the bonafide work of LAKKAVARM S M SHRIYA VARNITA [RA2111030010201], PAVULURI LOLA YASWANTHI [RA2111030010256] who carried out the project work [internship] under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

14/11/24

Dr. C. N. S. Vinoth Kumar

Associate Professor

Department of Networking and Communications

Dept. of Networking and Communications
Kattankulathur
603 203
SRM IST

M. Lakshmi

Dr. LAKSHMI M

Professor and Head

Department of Networking and Communications

TABLE OF CONTENTS

ABSTRACT

Complex cybersecurity issues have arisen as a result of the quick uptake of remote work, especially with regard to protecting cloud services, VPN traffic, and distant endpoints. In order to improve security monitoring, incident response, and operational efficiency in remote work environments, this article explores a complete security solution that combines Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) platforms. By identifying and warning of suspicious activity, Snort, a network-based intrusion detection system (NIDS), is used in this system to monitor VPN traffic for possible threats and anomalies, adding a crucial layer of network security. In order to secure individual user devices and reduce endpoint vulnerabilities, OSSEC also functions as a host-based intrusion detection system (HIDS), which is specifically made to identify irregularities and unwanted access attempts on distant endpoints.

The ELK Stack (Elasticsearch, Logstash, and Kibana) is combined to consolidate and expedite log management and event correlation, resulting in a unified environment for thorough network-wide visibility into security incidents. Effective data correlation and threat analysis are made possible by the ELK Stack's log analysis and visualization features, which give security teams useful information about changing risks. The Shuffle SOAR platform is used to automate incident response operations in order to reduce manual intervention and expedite response times. Shuffle guarantees consistent processing of security incidents, minimizes operational burdens, and speeds up response times by coordinating these procedures. The system uses OpenVPN to mimic actual remote work settings, enabling comprehensive testing and validation of the suggested strategy in a safe setting. By effectively identifying and addressing network and endpoint threats and automating the process, this IDS and SOAR integration seeks to improve the security of remote workforces. In order to improve the overall security posture in a dispersed work environment, this article offers a proactive and robust strategy to safeguarding remote work that addresses both detection and response.

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

IDS	Intrusion Detection System
SOAR	Security Orchestration, Automation, and Response
VPN	Virtual Private Network
NIDS	Network-Based Intrusion Detection System
HIDS	Host-based intrusion detection system
OSSEC	Open Source HIDS Security
ELK Slack	Elasticsearch, Logstash, and Kibana
OpenVPN	Open-source Virtual Private Network
LID	Log-based Intrusion Detection

CHAPTER 1

INTRODUCTION

The global shift towards remote working, accelerated by technological advancements and unprecedented events such as the COVID-19 pandemic, has significantly altered the cybersecurity landscape. As organizations continue to support distributed workforces, securing remote access to corporate resources, monitoring employee devices, and protecting sensitive data have become paramount concerns. This shift exposes organizations to a variety of risks, including phishing attacks, compromised VPN connections, and endpoint vulnerabilities. Conventional security solutions, which were originally designed for on-premise environments, are often insufficient for addressing the unique challenges posed by decentralized work infrastructures. To effectively safeguard these environments, Intrusion Detection Systems (IDS) play a crucial role in identifying potential security breaches. They monitor network traffic,endpoint activity, and system logs for indicators of malicious behavior. In this project, we extend its application to DRM by embedding copyright information directly into media files in a way that is invisible to the naked eye but can be verified when needed.

However, IDS tools tend to generate a large volume of alerts, often overwhelming security teams. The burden of manually investigating these alerts can create bottlenecks, especially in dynamic remote work settings where speed and accuracy are essential. Therefore, integrating Security Orchestration, Automation, and Response (SOAR) platforms becomes a practical solution to streamline and automate incident response, reducing human intervention in repetitive tasks and enhancing the overall decision-making process.

This research focuses on integrating Snort and OSSEC with Shuffle, a highly flexible SOAR platform, to improve the efficiency of threat detection and response in remote work environments. Snort is an open-source, lightweight IDS that provides robust network monitoring capabilities, particularly well-suited for tracking VPN traffic—a critical vector in remote work settings. OSSEC, a host-based intrusion detection system, offers powerful monitoring of endpoints, which are the most vulnerable to phishing, malware, and other endpoint-based attacks in a distributed work environment. Together, these IDS tools form a comprehensive detection system for both network and endpoint security, with the ELK Stack serving as a centralized platform to aggregate and analyze logs, visualize data, and enable real-time event correlation. The integration of these tools offers significant advantages over traditional standalone IDS deployments, as they allow for improved visibility across remote systems and more actionable insights.

SOAR platform Shuffle automates responses. Shuffle is the optimal incident response solution for tailored and comprehensive enterprises because of its security integration, adaptability, and open-source characteristics. Shuffle enables security guards to prioritize tasks. Integrated remote labor security is more efficient and flexible. The integrated solution may be tested and validated in real-world scenarios by simulating secure remote access with OpenVPN. An established and well-liked method of encrypting remote employee-corporate network connections is OpenVPN. This useful configuration evaluates the system’s effectiveness in protecting distant infrastructure and assists in identifying and mitigating VPN security vulnerabilities.

By integrating IDS and SOAR technologies, this paper proposes a security framework that addresses cybersecurity’s detection and response aspects in remote work environments. The chosen tools are not only cost-effective and open-source but also offer a high degree of customization and scalability, making them ideal for modern, distributed workforces. This system strengthens the security posture of remote work environments by enabling rapid, automated responses to threats while minimizing operational burdens on security teams.

1.1. MOTIVATION:

The rapid shift towards remote work, accelerated by the COVID-19 pandemic, has redefined organizational structures and brought unprecedented cybersecurity challenges. As companies embrace decentralized work environments, traditional, on-premises security measures often fall short. Remote work requires that employees access corporate resources securely and consistently, often from personal devices, over diverse network environments, and through an increasing number of cloud services. This shift not only expands the digital perimeter but also introduces unique security concerns, calling for innovative solutions to manage and protect these evolving infrastructures.

One of the main challenges is securing personal devices that remote employees use. Lacking enterprise-grade protection, these devices can act as entry points for attackers if not properly monitored and managed. Furthermore, remote work often involves accessing corporate systems from unsecured Wi-Fi networks, such as home or public networks, which are not always protected by consistent security policies. This diversity in network environments creates challenges for IT teams trying to maintain secure, consistent connections, leaving corporate data more vulnerable to interception or unauthorized access.

Additionally, the growing reliance on cloud services brings both convenience and complexity. While cloud-based platforms support flexible and scalable work environments, they also introduce added security considerations, such as data privacy and potential misconfigurations, which may expose sensitive information. Remote workers are also increasingly vulnerable to social engineering attacks, including phishing schemes. Without immediate IT support, these employees may be more susceptible to threats like credential theft and malware infections, increasing the risk of data breaches.

The motivation for this research project is to address these pressing security challenges by implementing a multi-layered security solution specifically designed for decentralized work settings. By integrating Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) platforms, the project aims to create a comprehensive approach to identifying and mitigating cybersecurity threats. For example, Snort and OSSEC, two IDS components, monitor network and endpoint traffic, providing visibility into activity across various devices and locations. By connecting these IDS tools with SOAR automation, the system can respond to incidents immediately, such as isolating compromised endpoints or alerting security teams, significantly reducing manual intervention.

This approach emphasizes scalability, contextual awareness, and adaptability. In remote work environments, the likelihood of false-positive alerts is higher due to the diversity in devices and network usage. Leveraging SOAR's ability to integrate and analyze data from various sources, the system can reduce false positives and ensure more precise detection of real threats. Additionally, this security framework's automated responses mean that it can manage a large volume of incidents without overwhelming security teams, making it scalable and resilient as organizations grow and adapt.

In essence, this project proposes a security model that combines IDS and SOAR capabilities to meet the unique demands of the remote work landscape. By proactively addressing security concerns with real-time threat detection and automated responses, this integrated approach enables organizations to support modern, flexible work environments without compromising cybersecurity standards. The project offers a proactive, resilient framework that not only reduces risks but also supports secure, adaptable remote work practices, helping organizations maintain strong security postures in the digital-first workplace.

1.2. INNOVATION:

This project introduces a novel approach to securing remote work environments by integrating Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) tools. Specifically, Snort, an open-source network-based IDS, and OSSEC, a host-based IDS, are combined with the Shuffle SOAR platform to create a comprehensive, adaptive security framework. This innovative setup allows for multi-layered threat detection and automated response capabilities:

***Multi-Layered Detection**:* By utilizing both Snort and OSSEC, this system monitors network traffic, endpoint activity, and system logs, effectively covering the security landscape from network entry points to individual devices. This setup provides extensive visibility and control, which is critical for detecting potential threats across different layers of a remote work environment.

***Centralized Log Management and Event Correlation**:* The ELK Stack (Elasticsearch, Logstash, and Kibana) acts as a central hub, aggregating logs from Snort, OSSEC, and other data sources. This setup enables advanced data analysis, real-time event correlation, and visualization, allowing security teams to identify complex attack patterns more effectively.

***Automated Response with SOAR**:* By integrating Shuffle, an open-source SOAR platform, the system can automate incident response workflows. This reduces manual intervention, enabling faster and more accurate threat mitigation. Automated responses may include isolating compromised endpoints, blocking malicious IPs, and notifying security teams of high-priority incidents.

This approach not only leverages the power of open-source tools but also ensures a high level of customization and scalability, making it accessible and adaptable for organizations of varying sizes. In today's increasingly decentralized work environment, a robust security infrastructure is essential to protect sensitive information and ensure smooth operations. This project introduces an innovative approach that combines the strengths of Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) tools, creating a multi-layered, automated defense mechanism capable of addressing the unique challenges of remote work. Specifically, the integration of Snort, an open-source network-based IDS, OSSEC, a host-based IDS, and Shuffle, a flexible SOAR platform, forms a cohesive and highly adaptive security framework that meets the demands of modern distributed networks.

1.3. OBJECTIVES:

The primary objective of this research is to create an integrated security solution that strengthens both the detection and response capabilities within remote work environments. With the widespread shift toward decentralized work, safeguarding these environments has become a complex challenge that requires a multifaceted approach. This project seeks to address these challenges by focusing on five key goals, each contributing to a robust and comprehensive cybersecurity framework that meets the demands of modern, distributed networks.

Firstly, enhancing threat detection in remote work settings is a central priority. By deploying Snort, a network-based Intrusion Detection System (IDS), and OSSEC, a host-based IDS, the project enables continuous monitoring of VPN traffic and endpoint activities for signs of suspicious behavior. This layered detection approach offers greater visibility into both network access points and individual devices, capturing a range of malicious activities, from network intrusions to unauthorized local access attempts, which are especially critical in remote settings.

The second objective centers on automating incident response to increase efficiency and reduce response times. By integrating Shuffle, an open-source Security Orchestration, Automation, and Response (SOAR) tool, the system is capable of automating various incident response workflows. Automation not only reduces the operational burden on security teams but also enhances the speed and accuracy of responses to detected threats. This automation ensures that critical incidents are addressed promptly, minimizing potential damage and ensuring business continuity.

Centralized data aggregation and correlation is another critical aspect of this project, achieved through the use of the ELK Stack (Elasticsearch, Logstash, and Kibana). This suite of tools functions as a central repository for logs collected from both network and endpoint systems, enabling security teams to conduct comprehensive analyses and gain real-time insights into security events. By correlating data from multiple sources, the ELK Stack facilitates a unified, holistic view of potential threats, making it easier to identify complex attack patterns and improve threat intelligence across the organization.

The solution's effectiveness is tested through simulations of real-world scenarios, facilitated by OpenVPN, an open-source virtual private network that replicates actual remote work conditions. OpenVPN enables secure remote connections, which are a primary component of many organizations' remote work setups. By using OpenVPN as part of the testing environment, this project evaluates how well the integrated solution detects and mitigates attacks that exploit VPN-based vulnerabilities. This real-world simulation ensures the system is equipped to handle authentic security challenges faced by remote teams.

CHAPTER 2

SPRINT PLANNING AND EXECUTION

SPRINT 1

The primary goal of Sprint 1 was to establish the foundation for integrating the Intrusion Detection Systems (IDS) and Security Orchestration, Automation, and Response (SOAR) platform. This sprint focused on gathering and setting up IDS components and preparing the SOAR platform for future integration. Key tasks included setting up Snort (network-based IDS) and OSSEC (host-based IDS) to monitor VPN traffic and remote endpoints. Additionally, initial configurations were applied to OpenVPN to simulate remote work environments, facilitating real-world testing conditions for future sprints.

SPRINT GOAL WITH USER STORIES OF SPRINT 1:

Sprint Goal: To set up and configure IDS components and establish a SOAR foundation for further integration.

2.1.1 User Stories:

- As a developer, I want to configure Snort and OSSEC to monitor VPN traffic and remote endpoints to detect potential threats.
- As a security analyst, I need to simulate a remote work environment using OpenVPN to create realistic testing conditions for IDS configurations.

2.1.2 Functional Document

The functional requirements included setting up the IDS tools (Snort for network-based and OSSEC for host-based intrusion detection), establishing OpenVPN for simulated remote connections, and configuring an initial SOAR platform for automation and response orchestration. This foundation would allow for efficient threat detection in a controlled environment, setting the stage for later automation.

2.1.3 Architecture Document

The architecture for this sprint focused on the initial configuration of IDS tools within a simulated remote work environment. Snort was configured to monitor VPN traffic, while OSSEC handled endpoint security monitoring. OpenVPN was deployed to replicate secure remote work conditions, providing realistic data flow between endpoints and corporate networks.

2.1.4 Functional Test Cases

- **IDS Configuration Testing**: Verify that Snort and OSSEC are correctly configured and operational.
  - **Test Case**: Test IDS configurations by simulating common threat scenarios.
  - **Expected Result**: Snort detects network-based threats, and OSSEC identifies endpoint-based anomalies.
- **OpenVPN Setup Testing**: Confirm that OpenVPN successfully simulates remote work scenarios.
  - **Test Case**: Establish VPN connections and test secure data transmission.
  - **Expected Result**: Successful and stable VPN connections.

2.1.5 Daily Call Progress

- **Day 1-3**: Set up an environment and clarify data collection requirements for IDS components.
- **Day 4-7**: Configure Snort and OSSEC, addressing any installation or configuration challenges.
- **Day 8-10**: Install and test OpenVPN for secure connection simulation.
- **Day 11-13**: Validate the IDS tools’ configurations within the VPN environment.
- **Day 14**: Review and finalize the setup for Sprint 2's automation focus.

2.1.6 Result Analysis

This sprint concluded with Snort and OSSEC successfully monitoring simulated remote traffic and endpoints. OpenVPN provided a stable environment, and initial testing indicated effective detection of network and endpoint threats.

2.1.7 Sprint Retrospective

The team observed that while IDS configurations worked as expected, challenges included initial setup complexities and potential latency within OpenVPN connections. Future sprints will focus on streamlining SOAR automation to improve response efficiency.

SPRINT 2

Building on the foundational setup, Sprint 2 concentrated on integrating the SOAR platform with the IDS components. The objective was to enable automated responses to detected threats and reduce manual intervention. Key tasks included configuring Shuffle (SOAR) to interact with Snort and OSSEC, automating workflows for incident detection and response, and ensuring a smooth data flow from detection to response orchestration.

SPRINT GOAL WITH USER STORIES OF SPRINT 2:

Sprint Goal: To integrate SOAR with IDS components for automated threat response.

User Stories:

- As a developer, I want to configure Shuffle to interact with Snort and OSSEC for automated incident response.
- As a security analyst, I need automated workflows for incident prioritization and response to streamline threat handling.

2.2.2 Functional Document

The functional requirements included creating workflows in Shuffle to trigger automated responses upon receiving threat alerts from Snort and OSSEC. This integration enabled prioritizing high-risk incidents and automating responses, reducing manual intervention.

2.2.3 Architecture Document

The architecture for Sprint 2 involved integrating Shuffle with Snort and OSSEC. Alerts generated by IDS components triggered workflows within Shuffle, executing predefined response actions (e.g., isolating compromised endpoints or blocking malicious IPs).

2.2.4 Functional Test Cases

- **Alert Workflow Testing**: Ensure SOAR workflows trigger upon IDS alert detection.
  - **Test Case**: Simulate various threat scenarios and observe SOAR responses.
  - **Expected Result**: Automated workflows respond accurately and promptly to alerts.
- **Incident Prioritization Validation**: Verify incident prioritization within Shuffle.
  - **Test Case**: Generate high- and low-severity alerts and check prioritization.
  - **Expected Result**: Alerts are prioritized correctly within Shuffle.

2.2.5 Daily Call Progress

- **Day 1-3**: Set up and configure the SOAR platform for integration.
- **Day 4-7**: Establish connections between SOAR and IDS tools.
- **Day 8-10**: Create and test response workflows within Shuffle.
- **Day 11-13**: Validate automated responses to various threat scenarios.
- **Day 14**: Review automated workflow and finalize for Sprint 3's deployment phase.

2.2.6 Result Analysis

The integrated SOAR and IDS system demonstrated effective automated responses to detected threats. Incident prioritization and automated responses showed promising efficiency in handling threats without manual intervention.

2.2.7 Sprint Retrospective

The team successfully achieved the automation goals, but noted latency in complex workflows. Future sprints will focus on optimizing response time and streamlining workflows.

SPRINT 3

In Sprint 3, the team concentrated on optimizing system performance and preparing for deployment. Tasks included refining SOAR workflows, testing the system's effectiveness under real-time conditions, and validating accuracy. Evaluation metrics like response time, accuracy, and workflow efficiency were measured to ensure reliable performance in detecting and mitigating threats

SPRINT GOAL WITH USER STORIES OF SPRINT 3:

Sprint Goal: To optimize the integrated IDS-SOAR system and validate performance metrics in real-time scenarios.

User Stories:

- As a data analyst, I want to evaluate system accuracy and response time to ensure effective threat management.
- As a developer, I need to optimize workflows to enhance performance in real-world conditions.

2.3.2 Functional Document

The functional requirements included measuring system accuracy, optimizing response workflows, and testing the system's performance with real-time threat simulations. Model deployment involved configuring real-time alerts and actions for timely threat responses.

2.3.3 Architecture Document

The architecture for Sprint 3 involved finalizing SOAR-IDS workflows, ensuring seamless data flow, and refining response timings. The system was optimized for minimal latency, allowing real-time data analysis and response actions.

2.3.4 Functional Test Cases

- Accuracy and Response Testing: Measure response accuracy and timeliness.
  - Test Case: Run real-time threat scenarios and observe response metrics.
  - Expected Result: Accurate detection and timely responses to simulated threats.

- Workflow Efficiency Validation: Evaluate SOAR workflow response time.
    - Test Case: Test efficiency across different threat workflows.
    - Expected Result: Optimized workflows show reduced response times.

2.3.5 Daily Call Progress

- Day 1-3: Set up an environment for real-time scenario testing.
- Day 4-7: Simulate threat scenarios and gather data on workflow efficiency.
- Day 8-10: Optimize workflows based on response metrics.
- Day 11-13: Validate system accuracy and response times.
- Day 14: Final review and preparation for deployment.

2.3.6 Result Analysis

The system achieved high accuracy in detecting threats and demonstrated minimal latency in response workflows. Evaluation metrics confirmed efficient threat management, supporting real-world deployment.

2.3.7 Sprint Retrospective

The team successfully optimized workflows, achieving effective real-time performance. Future improvements could involve expanding the system to incorporate additional data sources for enhanced threat intelligence.

CHAPTER 3

LITERATURE SURVEY

The literature on Intrusion Detection Systems (IDS) and Security Orchestration, Automation, and Response (SOAR) emphasizes the vital role that these systems play in modern cybersecurity frameworks, particularly in situations that are dynamic and decentralized, such as remote work. Remote endpoints and VPN-based connections offer additional risks, which has increased the need for comprehensive security mechanisms that handle threats outside typical on-premises setups. This requirement has been amplified as a result of the move toward remote work. IDS has seen widespread use in recent years, with the purpose of monitoring network traffic, identifying behaviors that are not typical, and protecting sensitive data from being compromised by cybercriminals. Nevertheless, the sheer volume of alerts that are generated by IDS technologies can be overwhelming for security teams, which highlights the necessity of automated solutions such as SOAR platforms. These platforms streamline and prioritize incident response activities, minimize the amount of manual labor that is required, and allow for faster reaction times.

Intrusion Detection Systems, both network-based (NIDS) and host-based (HIDS), have been subjected to a comprehensive assessment in a variety of cybersecurity situations. In their foundational overview of intrusion detection systems (IDS), Liao et al. (2012) highlight the significance of notifier and detector functionalities within IDS architectures in order to protect systems from hostile activity. For the purpose of securing remote work environments, where response speed can directly effect data integrity, their research reveals the necessity of real-time monitoring in identifying intrusions and transmitting notifications to stakeholders. This is a vital aspect in defending remote work environments. In a similar vein, Abdulganiyu et al. (2023) highlight the importance of intrusion detection systems (IDS) as a frontline defense against changing cyber threats. They highlight the fact that IDS tools monitor network and endpoint behaviors in order to identify malicious patterns. In addition, they draw attention to problems such as Concept Drift, which is a process in which predictive models become less effective over time as a result of new attack patterns having been introduced. The findings of their comprehensive review recommend that intrusion detection systems (IDS) should incorporate machine learning and adaptive algorithms in order to develop a robust detection system that is able to evolve alongside changing threat landscapes.

Additional research on intrusion detection systems (IDS) conducted by Pradhan et al. (2016) investigates the advantages of hybrid IDS, which combines host-based and network-based features. These kinds of systems improve the security coverage throughout a network's numerous layers altogether. Through the utilization of both misuse and anomaly detection methods, the hybrid methodology is able to maximize detection accuracy while simultaneously minimizing blind spots. In situations where endpoint devices and network traffic need to be monitored continuously, this strategy is very useful since it is particularly good for remote work environments. For instance, network-based intrusion detection systems (IDS) such as Snort are extremely efficient for monitoring VPN traffic. On the other hand, host-based IDS such as OSSEC offer granular protection for endpoint devices that are vulnerable to phishing, malware, and other endpoint-specific threats.

As the sophistication of security threats has increased, the requirements for detection and response have also increased. This is especially true in environments that integrate Internet of Things (IoT) and remote work frameworks. According to Zarpelão et al. (2017), the Internet of Things (IoT) devices present a unique set of security concerns. These challenges are similar to those faced by remote work arrangements, as they involve decentralized security and resource limits. Many Internet of Things devices do not have the computing capacity necessary for typical security protocols, which makes IDS integration more difficult. When it comes to the availability of resources, remote work environments are less restrictive than other types of environments; nonetheless, they still confront the same difficulty of balancing real-time detection capabilities with efficient resource utilization. After conducting this survey, it became clear that adaptive intrusion detection systems (IDS) are required in order to provide comprehensive security coverage. These tactics include optimizing data collecting and strategically positioning IDS solutions among network nodes.

As a result of their ability to automate and orchestrate responses to IDS alarms, SOAR systems like Shuffle have significantly contributed to the development of the security ecosystem. The workload of security officers is greatly reduced as a result of this automation, which subsequently improves reaction times. The authors Pradhan et al. (2016) highlight the operational constraints that are caused by manually analyzing warnings, particularly in contexts with high velocity. These difficulties are addressed by SOAR solutions, which automatically automate tasks that are repetitive, prioritize events that are critical, and ensure that security personnel are able to concentrate on threats that pose a high risk. Automation is essential in remote work environments, because incidents can originate from a variety of sources. This is because automation reduces the amount of time it takes to respond to incidents and increases the security posture of the organization.

The combination of SOAR with IDS has the effect of improving both visibility and the effectiveness of reaction. A thorough monitoring strategy can be supported by centralized log management and event correlation tools like the ELK Stack. These tools aggregate data from a variety of sources, such as endpoint logs and warnings from intrusion detection systems (IDS). The ELK Stack makes it possible to have a unified view of activities, which helps in the rapid discovery of attack patterns that may not be shown by individual logs. In addition, the visualization features of ELK make it easier to analyze data trends, which enables security analysts to make quick judgments based on accurate information, which is vital in environments where remote work is performed effectively.

With the proliferation of remote work, there has been an increase in the importance of protecting remote access through virtual private networks (VPNs). Virtual private networks (VPNs), such as OpenVPN, encrypt data transmissions to reduce the likelihood of data being intercepted and thereby safeguard remote access to company resources. As a result of the fact that they act as access points into the corporate network, virtual private networks (VPNs) can potentially bring vulnerabilities. These vulnerabilities can be mitigated by deploying intrusion detection systems (IDS) to monitor VPN traffic, which, when combined with the automated response capabilities of SOAR, has the ability to enable rapid identification of suspicious behaviors. By integrating these technologies with OpenVPN, businesses are able to construct a testbed for emulating real-world remote work scenarios. This provides a solid framework for evaluating the effectiveness of IDS and SOAR integrations in enhancing the security of remote work.

Through the introduction of the MADAM ID framework, Lee and Stolfo (2000) make a contribution to the field of intrusion detection system (IDS) research. This framework is a data-driven approach that utilizes data mining and machine learning to develop intrusion detection models. MADAM ID highlights the potential of machine learning in the development of IDS frameworks that are both accurate and adaptable. This is accomplished by utilizing system audit data to extract predictive features. The fact that this framework was validated through the DARPA Intrusion Detection Evaluation in 1998 demonstrates that it is capable of properly responding to intrusion attempts that occur in practical situations. In remote work environments, where threat patterns are constantly changing, adaptive security models that are able to perform real-time analysis and reaction are extremely useful. The feature-based model generation that the MADAM ID framework provides is particularly suitable to these circumstances.

The authors Effendy, Kusrini, and Sudarmawan (2017) build a Naive Bayes classification model that is based on the NSL-KDD dataset in order to expand on the potential of machine learning in intrusion detection systems (IDS). Their work places an emphasis on signature- and anomaly-based detection methods, with anomaly-based approaches being particularly useful for situations involving remote work in which it is vital to differentiate between normal and anomalous behaviors on endpoints. In their study, Effendy and colleagues demonstrate how preprocessing can enhance the accuracy of intrusion detection system (IDS) classification by improving feature selection and grouping continuous variables. This provides crucial insights for the implementation of IDS in remote situations.

In the article by Bartwal et al. (2022), the authors describe how the importance of SOAR in orchestrating response tactics extends to creative uses such as behavioral honeypots. When it comes to improving threat detection in low-latency applications, their research investigates the possibility of deploying honeypots in conjunction with SOAR in environments that utilize Multi-Access Edge Computing (MEC). In resource-constrained environments, the integration of behavioral honeypots with SOAR improves threat analysis and automation. This is a strategy that is ideally suited for safeguarding remote work frameworks, which are characterized by distant endpoints that present a challenge to traditional security models. It is possible to increase the ability to respond to threats in real time by automating honeypot deployment and monitoring at network edges. This strengthens security in remote work setups that are constantly changing.

In the year 2024, Falade and Momoh discuss the privacy risks that arise from monitoring applications in the context of remote employment. According to the findings of their investigation into twelve mobile surveillance applications, none of them offered privacy policies, and all of them required permissions that could put the privacy of employees at risk. These findings highlight the necessity of striking a balance between monitoring productivity and taking privacy concerns into account, which is an issue that is becoming increasingly important as working remotely becomes the norm.

The authors Lekidis, Mavroeidis, and Fysarakis (2024) concentrate on the automation of incident response inside the Advanced Metering Infrastructure (AMI), which, due to its dispersed nature, is comparable to remote work environments. In order to improve the resilience of AMI, they suggest a technique that is based on the OASIS Collaborative Automated Course of Action Operations (CACAO) standard. This methodology highlights how automation may strengthen incident response skills in decentralized contexts, providing insights for safeguarding distributed remote work infrastructures. Although it focuses on energy systems, it demonstrates how automation can contribute to these capabilities.

The combination of intrusion detection systems (IDS) and security operations and response (SOAR) technologies provides a comprehensive solution to the cybersecurity concerns that are associated with remote work. On the other side, SOAR platforms speed alarm handling, which enables teams to concentrate on major incidents. Network-based and host-based intrusion detection systems (IDS) offer layered protection across virtual private networks (VPNs) and endpoints. Real-time monitoring and data correlation are both further supported by centralized log management, which may be accomplished with solutions such as the ELK Stack. Adaptive and automated security frameworks that combine intrusion detection systems and security operations and response systems will be required in order to fight against increasingly complex cyber threats as remote work continues to develop.

Furthermore, additional research on SOAR technologies and privacy in employee monitoring is especially pertinent to the topic of secure remote work operations. The authors Bridges et al. (2023) investigate the effects of SOAR tools on incident response workflows in SOC environments and evaluate the effectiveness of these tools. It has been discovered that SOAR tools enhance productivity by automating mundane processes; yet, it is possible that these tools may have an effect on the comprehensiveness of event recording. Concerns were raised by senior analysts in this study over excessive automation, and they expressed a preference for tools that facilitate human decision-making. These findings are extremely important in the context of security setups for remote work, as SOAR technologies need to be properly adjusted to establish a balance between automation and manual oversight.

The rapid shift towards remote work, accelerated by global events like the COVID-19 pandemic, has introduced numerous cybersecurity challenges that traditional security infrastructures are often unprepared to handle. Remote work has transformed the organizational landscape, with employees accessing sensitive corporate resources over potentially insecure networks, thus increasing the risk of attacks on endpoints and network traffic. One of the major challenges in this context is ensuring robust threat detection and response capabilities to protect both the network and endpoints without overburdening security teams.

Intrusion Detection Systems (IDS) have long been recognized as critical components for identifying and mitigating cyber threats. According to Liao et al. (2012), IDS can be used to detect malicious activities or policy violations through various mechanisms. Traditional IDS methodologies have evolved significantly to meet the rising complexities in cybersecurity, incorporating techniques such as signature-based detection, anomaly detection, and hybrid approaches. Liao et al. emphasize the importance of IDS in providing robust monitoring, noting its ability to alert administrators to potential intrusions or suspicious behavior by analyzing network and host-based traffic. However, despite their effectiveness, IDS systems often generate large volumes of alerts, creating substantial challenges in environments with high data throughput, like those seen in remote work infrastructures by Abdulganiyu et al. (2023) highlights that IDS alone cannot effectively address the modern cyber threat landscape due to issues like Concept Drift, where the nature of threats changes over time, reducing IDS accuracy if the system does not adapt. Abdulganiyu and colleagues propose the integration of adaptive learning algorithms to handle dynamic environments, suggesting that IDS solutions need continual updating and reinforcement to remain effective. This insight is highly relevant to remote work, where threats are constantly evolving, making adaptive IDS systems more desirable. However, adaptive IDS implementations often still suffer from an overproduction of alerts and struggle with prioritization, which can overwhelm security analysts and lead to alert fatigue. This situation demonstrates a need for complementary systems that can handle the alert overflow and automate routine responses to improve operational efficiency.

Pradh(2016) delves into the various types of IDS, distinguishing between host-based (HIDS) and network-based (NIDS) systems. Host-based IDS like OSSEC can monitor and detect unusual behaviors on individual devices, which is critical for remote work settings where endpoints are exposed to direct internet traffic, potentially increasing their vulnerability to attacks. Network-based IDS, exemplified by Snort, is effective for monitoring traffic over VPNs, which are crucial for secure communication between remote endpoints and the corporate network. Pradhan et al. suggest that the integration of HIDS and NIDS forms a comprehensive security approach that can address the unique challenges posed by remote work, as HIDS protects endpoints and NIDS secures network traffic .

The importance rating IDS with SOAR (Security Orchestration, Automation, and Response) platforms is increasingly evident, as highlighted by Bartwal et al. (2022). Their research explores SOAR's ability to streamline the incident response process, reducing manual intervention and enhancing the accuracy and efficiency of security operations. By integrating SOAR, organizations can automate the response to low-level alerts, prioritize critical incidents, and significantly decrease response times. Bartwal's study on SOAR effectiveness in deploying behavioral honeypots for anomaly detection demonstrates that SOAR can assist in both automation and orchestration, which are vital for handling the extensive and sometimes overwhelming number of IDS alerts. This integration is essential in remote work environments where rapid response to potential threats is critical to preventing data breaches and maintaining security integrity.

Bridges et al. (2023) empirical assessment of SOAR tools, focusing on their practical applications within security operations centers (SOCs). Their findings indicate that SOAR platforms enhance SOC efficiency by automating repetitive tasks and reducing the need for extensive manual processing. This research underlines the value of a properly configured SOAR system, which can reduce context-switching for analysts and facilitate more seamless incident handling. However, they also note potential downsides, such as the risk of over-automation, which could lead to decreased investigation quality. This finding is particularly relevant in the context of remote work security, where the complexity and volume of incidents necessitate careful balance between automated responses and human oversight.

The utilization of the ELK Stackalized log management, as discussed in various studies, further supports the integration of IDS with SOAR platforms. The ELK Stack—consisting of Elasticsearch, Logstash, and Kibana—provides a powerful toolset for aggregating, analyzing, and visualizing log data. In an IDS-SOAR integration framework, the ELK Stack can serve as a central repository, allowing security teams to correlate events across endpoints and network traffic effectively. This setup enhances visibility and enables faster identification of threats, which is crucial for a security framework dealing with remote environments. Through event correlation, ELK helps reduce false positives by linking related alerts, thus supporting the SOAR platform in prioritizing responses more effectively and assisting in root-cause analysis for complex incidents.

The role of OpenVPN in this research is it provides a realistic simulation of remote work conditions, allowing the IDS-SOAR framework to be tested under practical circumstances. VPNs are an integral part of secure remote work, providing an encrypted communication channel between remote endpoints and corporate networks. OpenVPN, being an open-source and widely adopted solution, offers a practical and cost-effective means for organizations to secure remote connections. The integration of IDS tools with OpenVPN enables continuous monitoring of VPN traffic, which is particularly useful for detecting anomalies such as unusual login locations or atypical data flows, common indicators of potential security breaches in remote setups.

Finally, the research by Falade and Momoh (2024) on privacy in remote work environments underscores the importance of balancing security and privacy in monitoring solutions. While IDS and SOAR platforms enhance security, they also raise potential privacy issues, particularly when monitoring employee endpoints. Falade and Momoh's work reminds us that implementing IDS and SOAR systems requires careful consideration of employee privacy, especially in distributed workforces where the boundary between personal and corporate device usage may blur. Their study advocates for transparent privacy policies and clear guidelines on monitoring to ensure compliance with privacy regulations and maintain employee trust.

In conclusion, this literature review highlights the evolving role challenges of high alert volumes, and the integration of SOAR for effective threat detection and response. The deployment of a hybrid IDS setup using Snort and OSSEC, supported by the ELK Stack for centralized monitoring and Shuffle SOAR for automated responses, presents a robust framework for enhancing security in remote work environments. By addressing the limitations of standalone IDS and leveraging the orchestration capabilities of SOAR, this integrated approach promises to mitigate the unique risks associated with remote work. Future work may focus on fine-tuning these integrations, optimizing automation workflows, and balancing security with privacy to create a secure, scalable, and privacy-conscious remote work security framework.

3.2. Research Gaps:

Numerous drawbacks of current security systems make them less effective in remote work settings, particularly when contrasted with centralized, on-premises settings. Limited visibility across dispersed networks is one of the main obstacles. Employees working remotely access company networks from a variety of devices and places, making it challenging to monitor and manage every endpoint. Conventional security products are often best suited for systems with well-defined perimeters. Another drawback is the large number of false positives and warnings produced by IDS tools such as OSSEC and Snort, which, despite their strength, frequently generate an excessive amount of alerts in dynamic remote situations. Because of alert fatigue, security professionals may fail to notice actual threats.

Furthermore, traditional security systems frequently depend on labor-intensive and delayed manual reactions to warnings. In distributed work environments, where speed is crucial to preventing threat escalation, this reactive approach is impractical. VPNs are also necessary for many remote settings, but they are not impervious to security flaws. Because the majority of VPN solutions lack sophisticated monitoring and detection features, compromised connections may remain undiscovered, granting hackers access to company resources. Given that personal or unmanaged devices are frequently utilized for remote work, endpoint security poses still another big difficulty. The risk of compromise may be increased by these devices' absence of essential security features like encryption, monitoring, and patching. Furthermore, small to mid-sized businesses with tight budgets find it challenging to use advanced security products due to their scalability and cost limitations, which frequently include expensive license costs and intricate setup requirements.

CHAPTER 4

IMPACT OF IDS LIMITATIONS ON SECURITY INCIDENTS

Traditional Intrusion Detection Systems (IDS) have been a cornerstone of cybersecurity for decades, but their effectiveness has been severely challenged by the growing complexity and distributed nature of modern work environments, particularly as remote work has become more prevalent. With the advent of cloud-based services, remote desktops, and virtual private networks (VPNs), the traditional network perimeter has become increasingly difficult to defend. Remote work environments, which rely heavily on these technologies, introduce a range of new vulnerabilities that traditional IDS tools were not designed to address. As a result, IDS systems that once excelled at monitoring internal networks are now struggling to provide comprehensive visibility into the full range of threats that affect decentralized and cloud-based infrastructures.

A key challenge for traditional IDS in remote work environments is their inability to monitor encrypted communications effectively. The surge in remote work during the COVID-19 pandemic brought this issue to the forefront, as attackers began to exploit vulnerabilities within encrypted traffic, particularly within VPN tunnels. Remote employees accessing corporate resources through VPNs often encrypted their traffic, effectively masking malicious activities from traditional IDS systems. Since most IDS tools were designed to inspect unencrypted traffic, they were unable to detect sophisticated threats, such as phishing attempts, that were cleverly hidden within VPN traffic. As a result, attackers were able to compromise user credentials, gaining unauthorized access to corporate networks without raising any immediate red flags for security teams.

One of the most notable incidents that exposed the limitations of traditional IDS systems in the remote work context was the 2021 Colonial Pipeline ransomware attack. Cybercriminals were able to exploit a VPN vulnerability to gain access to the company's network, circumventing the IDS system entirely. This attack underscored the fundamental issue with traditional IDS, which is that it was designed to monitor traffic on centralized networks but struggled to adapt to decentralized, remote access tools. The attack surface had expanded with the rise of remote work, which introduced VPNs, cloud services, and remote desktops—areas where traditional IDS systems have limited visibility. The inability of IDS tools to effectively monitor these new attack vectors left organizations vulnerable to devastating breaches, as attackers were able to bypass conventional detection mechanisms.

Similarly, the rise in unauthorized access incidents related to compromised Remote Desktop Protocol (RDP) sessions demonstrated another shortcoming of traditional IDS systems. As remote work became widespread, attackers increasingly targeted RDP vulnerabilities to gain unauthorized access to corporate networks. RDP vulnerabilities, which were previously a low-priority security concern, became high-value targets for cybercriminals exploiting weak authentication or poorly configured remote desktop services. Traditional IDS systems struggled to monitor and analyze the nuances of these remote desktop sessions, which often made it difficult to detect unauthorized access in real-time. As a result, data exfiltration and unauthorized network access often went undetected until after the breach had occurred, allowing attackers to wreak havoc without immediate intervention from security teams.

Cloud services have also emerged as a significant attack vector in the remote work era, and traditional IDS solutions have struggled to adapt to the unique challenges posed by cloud environments. Cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure have become integral to the infrastructure of many organizations, providing scalable and flexible services that are critical to supporting remote work. However, traditional IDS systems, which were designed primarily to monitor network traffic, often fail to integrate seamlessly with cloud environments. This creates a significant gap in security, as cloud-native threats, including misconfigurations, data exposure, and insider misuse of privileged access, often go undetected. A misconfigured cloud instance or an insider threat exploiting cloud-based resources may not generate the type of traffic that traditional IDS systems are designed to detect, leaving organizations vulnerable to security breaches in cloud environments.

In addition to cloud service exploitation, remote collaboration platforms such as Zoom and Microsoft Teams have become prime targets for cybercriminals. As these platforms became essential for communication during the pandemic, attackers found new ways to exploit vulnerabilities in video conferencing tools. Traditional IDS systems, which were designed for more static, on-premise environments, struggled to keep pace with the dynamic, encrypted, and cloud-based traffic generated by these platforms. Threats such as session hijacking, unauthorized access, and exploitation of platform vulnerabilities often went undetected due to the lack of visibility into the encrypted traffic. As remote work increasingly relies on these collaboration tools, the limitations of traditional IDS systems in monitoring this new traffic type become more apparent, highlighting the need for more sophisticated security measures.

These incidents have emphasized the critical need for advanced solutions that can provide more comprehensive visibility and better threat detection capabilities in remote work environments. The traditional approach of relying solely on IDS to detect and prevent attacks is no longer sufficient in the face of evolving threats targeting remote access tools, cloud services, and collaboration platforms. To address these challenges, integrating IDS with Security Orchestration, Automation, and Response (SOAR) platforms offers a promising solution. SOAR platforms enhance IDS by automating incident response workflows, enabling security teams to handle the large volume of alerts generated by IDS systems more efficiently. This integration allows for faster detection and response to incidents, reducing the time it takes to contain threats and mitigate damage.

SOAR platforms also offer the ability to integrate data from a wide variety of security tools, including endpoint detection and response (EDR), cloud monitoring, and collaboration platform monitoring. This integration provides a more holistic view of the security landscape, enabling organizations to correlate events across multiple systems and gain deeper insights into potential threats. While traditional IDS systems were limited to monitoring network traffic, SOAR platforms enable organizations to correlate data from endpoints, cloud environments, and remote collaboration tools, providing a comprehensive security posture that is better suited to the remote work era. By enhancing threat detection with these integrations, SOAR platforms can help organizations address the blind spots left by traditional IDS tools.

The fusion of IDS with SOAR platforms enables automated responses to incidents detected by IDS, allowing for faster mitigation of threats. For example, once an attack is identified, a SOAR platform can automatically trigger predefined workflows, such as isolating compromised endpoints or blocking malicious IP addresses, without requiring manual intervention from security teams. This automation significantly reduces response times, minimizing the potential damage caused by security breaches. The ability to automate threat responses also alleviates the burden on overworked security teams, who are often inundated with alerts and incident data. By automating routine tasks, security teams can focus on more strategic activities and complex incidents that require human expertise.

Furthermore, the integration of IDS with SOAR platforms allows for deeper analysis of encrypted traffic, remote access behaviors, and cloud-based activity. Traditional IDS systems, which struggled to monitor encrypted traffic, can now benefit from the advanced analytics capabilities of SOAR platforms. These platforms can inspect encrypted traffic and identify anomalies or suspicious patterns, helping security teams detect threats that were previously hidden. SOAR platforms can also provide detailed insights into user behaviors, such as login patterns and file access history, making it easier to identify abnormal activities that might indicate an attack. This deeper analysis is crucial for defending against the advanced, multi-layered threats that target remote work environments.

In conclusion, the limitations of traditional IDS systems in securing remote work environments have been exposed by high-profile cyber attacks, emphasizing the need for more advanced and integrated security solutions. The fusion of IDS with SOAR platforms provides a promising solution to address these challenges. By combining the real-time threat detection capabilities of IDS with the automation and orchestration features of SOAR platforms, organizations can enhance their ability to detect and respond to security incidents in remote work environments. This integrated approach provides a more comprehensive defense against the complex threats posed by remote access tools, cloud services, and collaboration platforms, offering a scalable and effective security solution for the modern, decentralized workplace.

CHAPTER 5

SYSTEM ARCHITECTURE AND DESIGN

5.1. Block Diagram:

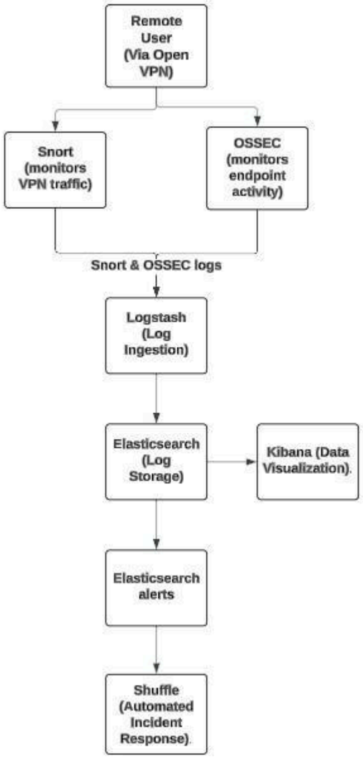

Remote User (Via Open VPN)
Snort (monitors VPN traffic)
OSSEC (monitors endpoint activity)
Snort & OSSEC logs
Logstash (Log Ingestion)
Elasticsearch (Log Storage)
Kibana (Data Visualization).
Elasticsearch alerts
Shuffle (Automated Incident Response).

Figure-1: Block Diagram

The block diagram illustrates a streamlined, multi-layered approach to security for remote work environments, particularly in the context of protecting VPN traffic and endpoint devices. Starting from the **Remote Worker** node, the system is designed to handle data flow securely and systematically through various components, ensuring that all potential security gaps are effectively covered. In this architecture, remote workers connect to the network via **OpenVPN**, establishing an encrypted and authenticated connection to prevent unauthorized access. The VPN gateway ensures that remote communications are secure, minimizing the risk of interception.

Once connected, **Snort** monitors network traffic generated by the remote workers. As a network-based Intrusion Detection System (IDS), Snort inspects packet-level data in real time, identifying potential threats like malware, intrusion attempts, and suspicious traffic patterns. It focuses on detecting threats that may come through VPN connections, which are common in remote work setups where employees access corporate resources from various locations. Snort's placement in the architecture enables it to serve as the first line of defense, detecting and flagging any unusual network traffic before it reaches the rest of the infrastructure.

OSSEC, a host-based IDS, provides a complementary security layer by focusing on endpoint activity. While Snort handles network threats, OSSEC is responsible for monitoring and securing the remote worker's device itself. This is especially important in remote work settings, where endpoints are often the weakest link. OSSEC monitors system logs, file integrity, and user activity, detecting unauthorized changes, rootkit presence, and other forms of anomalous behavior. Any alerts generated by OSSEC indicate potential compromise at the endpoint level, helping the security team identify infected devices and prevent lateral movement of threats.

The logs generated by both Snort and OSSEC are forwarded to the **ELK Stack**, a centralized logging platform that consists of **Logstash**, **Elasticsearch**, and **Kibana**. **Logstash** is responsible for ingesting and processing logs from Snort and OSSEC, ensuring that they are correctly formatted and enriched for analysis. This preprocessing step is essential for achieving accurate and efficient data management, enabling the system to handle large volumes of log data without compromising performance. Once processed, logs are stored in **Elasticsearch**, which provides a scalable and robust storage solution capable of handling high-velocity data and complex search queries. Elasticsearch's powerful indexing capabilities enable fast searching, allowing security teams to quickly retrieve relevant data for analysis.

Kibana provides a visual interface for analyzing logs in real time. It enables security teams to monitor data trends, identify suspicious patterns, and visualize incidents as they unfold. By visualizing data from both Snort and OSSEC, Kibana makes it easier for analysts to see correlations that might indicate coordinated attacks or broader security incidents. This centralized view is crucial for detecting patterns and connections that may otherwise go unnoticed, enhancing the overall situational awareness of the security team.

When **Elasticsearch** identifies an event that matches predefined security rules, it generates an **alert**. These alerts highlight potential threats or unusual activities that require immediate attention, helping to prioritize incidents in high-stakes environments. Alerts generated by Elasticsearch are then picked up by **Shuffle**, a Security Orchestration, Automation, and Response (SOAR) platform. Shuffle's role in this framework is to orchestrate an automated response to each alert, minimizing the need for manual intervention and reducing response times. By automating response actions, Shuffle ensures that incidents are contained quickly, thereby limiting the potential impact of threats.

Shuffle is configured with predefined workflows that handle a range of incidents. For instance, if an alert indicates malware activity on a remote device, Shuffle can initiate actions like isolating the endpoint from the network, notifying the security team, and conducting a preliminary investigation. This automation not only accelerates incident response but also reduces the manual workload on the security team, allowing them to focus on more complex tasks that require human intervention. By combining real-time threat detection with automated response, this architecture creates an efficient and adaptive defense mechanism tailored for the unique challenges of remote work environments.

5.2. Architecture Diagram:

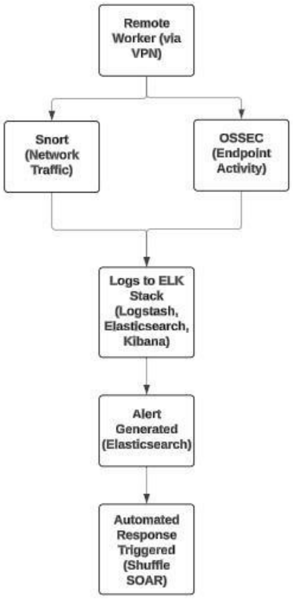

Remote Worker (via VPN)
Snort (Network Traffic)
OSSEC (Endpoint Activity)
Logs to ELK Stack (Logstash, Elasticsearch, Kibana)
Alert Generated (Elasticsearch)
Automated Response Triggered (Shuffle SOAR)

Figure-2: Architecture Diagram

The architecture of this solution addresses the limitations of traditional Intrusion Detection Systems (IDS) in remote work environments by integrating IDS with a SOAR platform, creating a comprehensive framework that enhances threat detection and incident response. Traditional IDS systems often struggle to adapt to the complexities of remote work settings, particularly in terms of monitoring VPN traffic, endpoints, and cloud services. This architecture overcomes these limitations by combining network-based IDS (Snort), host-based IDS (OSSEC), centralized log management (ELK Stack), and automated response (Shuffle SOAR), providing an end-to-end solution that is both scalable and adaptable.

5.2.1. Remote Worker Access via VPN: In the modern remote work environment, employees frequently rely on VPNs to access corporate resources securely. This architecture begins with **OpenVPN**, which provides encrypted communication channels for remote users. By requiring authentication and encryption, OpenVPN ensures that only legitimate users can access the network, reducing the risk of unauthorized access. VPN traffic, however, can be difficult to monitor due to encryption, which is why it is essential to have dedicated IDS tools in place to analyze network activity within this secure tunnel. The use of OpenVPN thus sets a secure foundation, simulating the real-world scenarios remote workers encounter and creating a controlled environment for testing security measures.

5.2.2. Snort for Network Traffic Monitoring: As a widely-used network IDS, **Snort** is employed to monitor VPN traffic and detect suspicious patterns indicative of threats. Snort inspects packet-level data, looking for signatures that match known attack patterns, such as port scans, SQL injections, and malware infections. The flexibility of Snort's open-source platform allows for the customization of rules to adapt to evolving threat landscapes. In this architecture, Snort serves as the primary defense against network-based threats, providing real-time alerts for anomalous behavior and enabling proactive threat detection. Its placement at the network entry point ensures that threats are detected before they can reach critical systems.

5.2.3. OSSEC for Endpoint Monitoring: Endpoints are often the weakest link in remote work environments, as they are beyond the traditional network perimeter and are susceptible to compromise. **OSSEC** mitigates this risk by monitoring endpoint activity, offering visibility into individual devices connected to the network. It performs file integrity monitoring, rootkit detection, and log analysis, ensuring that any unauthorized changes or suspicious activities are flagged. By providing insights at the endpoint level, OSSEC complements Snort's network monitoring capabilities and ensures that both network and host-based threats are covered. This layered approach to detection significantly improves the architecture's resilience to a range of attack vectors.

5.2.4. Centralized Log Management with the ELK Stack: Logs from Snort and OSSEC are processed through the **ELK Stack** for centralized analysis and visualization. **Logstash** is responsible for aggregating and processing logs, transforming them into a standardized format that is easily searchable. This enables the architecture to handle large-scale data ingestion without sacrificing data quality. The processed logs are stored in **Elasticsearch**, a powerful search engine capable of indexing and retrieving data efficiently. This centralized repository serves as the backbone of the architecture, allowing for rapid data access and query execution. The inclusion of **Kibana** provides a visual interface for security analysts, enabling them to monitor real-time data trends and investigate incidents visually. By centralizing log management, the ELK Stack allows for correlation across network and endpoint logs, helping identify patterns that may indicate coordinated attacks.

5.2.5. Alert Generation in Elasticsearch: Elasticsearch is configured to generate alerts based on specific rules that define what constitutes suspicious activity. When logs meet these criteria, Elasticsearch triggers an alert, which is immediately flagged for the attention of the security team or for automated response. These alerts are critical for prioritizing incidents in a high-volume environment, as they highlight threats that require prompt attention. Alerts can be based on a variety of conditions, such as repeated login failures, unusual traffic patterns, or unauthorized file modifications. This functionality makes Elasticsearch a proactive element within the architecture, actively flagging issues that could indicate security breaches.

5.2.6. Automated Response through Shuffle (SOAR): To further reduce response times and mitigate human error, the architecture incorporates **Shuffle**, a SOAR platform that automates incident response. When an alert is triggered, Shuffle's automation workflows initiate predefined actions, such as isolating affected endpoints, notifying relevant teams, or conducting an initial investigation. This automation reduces the manual workload on security personnel, allowing for rapid containment of threats. Shuffle integrates seamlessly with Snort, OSSEC, and the ELK Stack, enabling it to execute actions based on data from multiple sources. By automating repetitive tasks, Shuffle ensures consistent and timely responses, freeing up security teams to focus on more complex analyses.

5.2.7. Scalability and Adaptability: A key strength of this architecture is its scalability and adaptability. As the organization grows or as remote work demands increase, additional endpoints or VPN users can be seamlessly integrated without major architectural changes. The open-source nature of Snort, OSSEC, and the ELK Stack also allows for customization and expansion, enabling the architecture to adapt to new types of threats and integrate with emerging security tools. This scalability ensures that the framework remains effective and responsive to changing security landscapes, making it a future-proof solution for remote work environments.

CHAPTER 6

METHODOLOGY

The traditional Intrusion Detection System (IDS) architecture faces significant limitations when applied to remote work environments, particularly in monitoring VPN traffic, endpoints, and cloud services. These challenges stem from the widespread use of cloud services and VPNs, which can obscure threat activity and create blind spots in the monitoring process. VPNs, for example, encrypt traffic, making it difficult for traditional IDS tools to inspect the data flow. Similarly, endpoints in remote work setups can be dispersed across various locations, devices, and networks, complicating the detection of anomalous behavior. As remote work has become a central aspect of modern business operations, the need for a more integrated, real-time solution has become crucial to safeguarding the digital infrastructure of organizations.

To address these challenges, the proposed solution integrates IDS with Security Orchestration, Automation, and Response (SOAR) platforms, creating a robust, automated security infrastructure. Combining network-based IDS like Snort, which detects malicious network traffic, with host-based monitoring through OSSEC provides comprehensive coverage of both network and endpoint layers. This integration ensures that all potential attack vectors, from network breaches to compromised endpoints, are monitored in real-time. The use of the ELK Stack for centralized log management further strengthens the system by consolidating logs from various sources, allowing for faster and more accurate threat identification and analysis. With this holistic approach, the system is capable of detecting sophisticated threats that could otherwise go unnoticed in a distributed workforce setup.

The true innovation of this solution lies in its automation capabilities, enabled through SOAR platforms like Shuffle. By automating the incident response process, the system reduces the need for manual intervention, which not only accelerates response times but also mitigates human error. For instance, once a threat is detected, the system can trigger automated responses such as isolating affected endpoints, blocking malicious IP addresses, or alerting the security team. This automation enhances efficiency, allowing security teams to focus on more complex tasks rather than routine incident management. Moreover, the adaptive nature of the solution ensures that it evolves with the changing threat landscape, offering a scalable, dynamic defense mechanism that can keep pace with the challenges posed by remote work environments.

6.1. Key Features of the Proposed Security Framework:

The primary objective of the proposed solution is to establish a robust and scalable security framework designed to effectively monitor and protect remote work environments, a necessity in today's increasingly decentralized workforces. With remote work expanding, organizations face a multitude of security challenges, including threats stemming from VPNs, endpoints, and cloud services. These elements have unique security concerns; for example, VPN traffic can obscure threat activity due to encryption, and endpoints may be spread across different networks and locations, making them vulnerable to various attack vectors. The solution aims to ensure that security teams can consistently detect and respond to threats, regardless of where employees are working, by providing real-time monitoring across all critical components of the network.

A key feature of the solution is its ability to detect suspicious activities across multiple vectors in the remote work environment. This is achieved through integrating network-based IDS (such as Snort) for monitoring VPN traffic, host-based IDS (like OSSEC) for endpoint monitoring, and cloud-based security tools to protect cloud services. The system ensures that threats are detected promptly and that events from these diverse sources are correlated in real-time. By combining the outputs from different monitoring tools and sources of information, the system can piece together a comprehensive view of the network's security posture, providing accurate threat assessments. This holistic approach is essential in identifying and neutralizing threats that might otherwise go undetected if the systems operated in isolation.

To reduce the manual workload on security teams and to speed up the overall response process, the system integrates with Security Orchestration, Automation, and Response (SOAR) platforms. This integration allows the automated analysis of detected threats and the initiation of predefined responses, which significantly cuts down on response times. For example, the system can automatically isolate compromised endpoints, block suspicious IP addresses, or trigger alerts to the security team with relevant context. Automation reduces human error and ensures that routine tasks such as event triage and mitigation are handled swiftly, freeing up security teams to focus on more complex or high-priority tasks. This capacity for swift action is crucial in limiting the potential damage caused by security incidents.

Another important objective of this solution is scalability and adaptability. The security landscape is constantly evolving, with new threats emerging regularly. As remote work continues to grow and organizations adopt new tools and services, the security framework must be flexible enough to scale and integrate seamlessly with evolving technologies. The system is designed to be modular, allowing new security tools, services, and data sources to be incorporated with minimal disruption. This adaptability ensures that the solution can stay ahead of evolving threats, offering continuous protection as the organization's remote work environment grows and diversifies. By proactively adjusting to changing threats and technologies, the solution will remain relevant and effective over the long term.

6.2. Approach: Integrated Security Framework for Remote Workspaces

The approach taken to develop this solution is based on the integration of best-in-class security tools that address different aspects of remote work security. Snort, a widely-used network-based IDS, is deployed to monitor network traffic, with a focus on VPN connections that remote employees rely on for accessing corporate resources. It is configured to detect a wide range of threats, including malware, intrusions, and suspicious traffic patterns. OSSEC, a host-based IDS, is used to monitor the endpoints, which are often the weakest link in remote work setups. OSSEC tracks file integrity, unauthorized access attempts, rootkit detection, and unusual system behavior, providing a layer of defense on individual devices.

The ELK Stack—comprising Elasticsearch, Logstash, and Kibana—serves as the centralized logging platform. It collects logs from both Snort and OSSEC, processes them for analysis, and visualizes security events in real time. This enables efficient log management and event correlation, helping to identify patterns that could indicate a broader security incident. Shuffle, the SOAR platform, orchestrates the automation of responses to incidents detected by Snort and OSSEC. Predefined workflows allow Shuffle to automatically initiate responses such as isolating compromised endpoints, blocking malicious IPs, or escalating alerts to the security team, thereby reducing the time to contain threats.

By leveraging OpenVPN, a secure remote access solution, the proposed system simulates real-world remote work environments. This allows for a realistic testing ground, ensuring the system's components are capable of handling the complexities and security demands of remote work. The combination of these tools ensures that both network and endpoint threats are addressed while automating the detection and response process to enhance overall security efficiency.

The development of this solution is centered around integrating best-in-class security tools that cover the various layers of security in remote work environments. As remote employees increasingly rely on VPNs to access corporate resources, the monitoring of VPN traffic becomes a critical component of the security framework. Snort, a widely-used network-based Intrusion Detection System (IDS), is employed to monitor network traffic in real-time, with a particular focus on VPN connections. Snort's capabilities allow it to detect a broad range of threats, from malware and intrusions to suspicious traffic patterns and data exfiltration attempts. By focusing on VPN traffic, Snort helps ensure that the encrypted tunnels commonly used by remote employees do not become a blind spot for security teams, providing continuous visibility into the integrity of these connections.

In addition to monitoring network traffic, the solution also addresses endpoint security, which remains a significant vulnerability in remote work setups. OSSEC, a host-based IDS, is deployed to provide comprehensive monitoring of individual devices. OSSEC tracks various system activities, including file integrity, unauthorized access attempts, and rootkit detection. This host-based monitoring is vital as endpoints are often the weakest link in a remote workforce, susceptible to malware infections, phishing attacks, and other forms of compromise. By continuously monitoring endpoints for unusual behavior, OSSEC provides an added layer of defense, ensuring that threats are detected and addressed at the device level before they can propagate across the network.

To manage and correlate the vast amounts of security data generated by Snort and OSSEC, the ELK Stack—comprising Elasticsearch, Logstash, and Kibana—serves as the centralized logging platform. ELK Stack is a powerful tool for handling log data from diverse sources, offering a unified view of security events. Logstash is responsible for processing logs from both Snort and OSSEC, while Elasticsearch indexes and stores this data for efficient searching and querying. Kibana then provides a visual interface for analyzing these logs, allowing security teams to identify patterns and trends that might indicate potential security incidents. This centralized log management helps in correlating events from different sources, making it easier to spot emerging threats that could otherwise go unnoticed in siloed systems.

The next layer of the solution focuses on automating the response to detected incidents, which is accomplished through the integration of the SOAR platform Shuffle. Shuffle automates security workflows by using predefined playbooks that dictate the appropriate response to various types of incidents. For example, if Snort detects suspicious network traffic or OSSEC identifies an unauthorized access attempt, Shuffle can automatically trigger predefined actions such as isolating compromised endpoints, blocking malicious IP addresses, or escalating alerts to the security team for further investigation. This automation significantly reduces the time between detection and mitigation, ensuring that threats are contained swiftly before they can escalate into more damaging incidents. By automating routine security tasks, Shuffle reduces the manual workload on security teams, allowing them to focus on more strategic and complex security challenges.

To simulate a real-world remote work environment, the proposed system incorporates OpenVPN, a secure remote access solution that is commonly used in remote work setups. OpenVPN provides a realistic testing ground for evaluating the system's components, allowing for a comprehensive understanding of how the integrated tools behave under practical conditions. By replicating the VPN connections used by remote employees, OpenVPN enables testing of both network and endpoint monitoring capabilities in a controlled environment. This ensures that the security tools can handle the complexities of modern remote work, including diverse device types, varying network conditions, and secure communication requirements, all of which are critical for a comprehensive and reliable security framework.

The integration of these tools—Snort, OSSEC, the ELK Stack, Shuffle, and OpenVPN—creates a multi-layered security solution that addresses both network and endpoint threats in a comprehensive manner. The combination of real-time threat detection, centralized log management, automated responses, and real-world testing ensures that the system is well-equipped to handle the security challenges of remote work environments. By automating the detection and response processes, the solution improves overall security efficiency, reduces response times, and minimizes the risk of human error, ultimately enhancing the organization's ability to safeguard its assets and data in a distributed workforce model.

6.3. Tools and Technologies:

The solution integrates several key technologies to address remote work security challenges. Snort, a network-based IDS, monitors VPN traffic for intrusions or malicious activity, leveraging customizable rules for detecting suspicious patterns. OSSEC acts as a host-based IDS, providing endpoint monitoring through file integrity checks, rootkit detection, log analysis, and active responses to anomalous behavior—essential for securing remote worker devices lacking corporate network protections.

The ELK Stack centralizes log management: Elasticsearch stores logs, Logstash processes them, and Kibana visualizes data. This allows security teams to correlate events from Snort and OSSEC, identifying broader security trends. Shuffle, the SOAR platform, automates response workflows by integrating with Snort and OSSEC. For instance, if Snort detects an intrusion, Shuffle can automatically block the IP or isolate a device, reducing manual intervention for faster incident resolution.

Lastly, OpenVPN provides a secure, encrypted environment for testing real-world remote work scenarios, such as encrypted communications and secure access to corporate resources, ensuring the solution meets remote work security needs.

6.3.1. SNORT:

Snort is an open-source, network-based Intrusion Detection and Prevention System (IDS/IPS) widely used for monitoring network traffic and identifying potential security threats in real time. It works by analyzing packets of data as they travel through the network, inspecting for patterns that match known attack signatures, such as malware, hacking attempts, or suspicious traffic behaviors. Snort is highly customizable, allowing users to define specific rules for identifying threats, making it a flexible and powerful tool for network security. It can detect a wide range of attacks, including buffer overflows, denial-of-service attacks, and SQL injections, providing organizations with an effective means of detecting and mitigating network-based threats.

One of Snort's standout features is its ability to operate in multiple modes, including as an IDS for passive detection and as an IPS for active prevention. As an IDS, Snort generates alerts when suspicious activity is detected, giving security teams the opportunity to investigate the incident further. As an IPS, Snort can automatically take actions, such as blocking malicious traffic or logging specific events, to prevent attacks from succeeding. Additionally, Snort can be easily integrated with other security tools and platforms, including SIEM systems, enhancing its ability to correlate data and respond to incidents more efficiently. Its scalability, rule-based detection system, and broad community support make Snort one of the most widely adopted network monitoring tools in the cybersecurity landscape.

6.3.2. OSSEC:

OSSEC (Open Source Security) is a powerful, open-source host-based Intrusion Detection System (IDS) designed to monitor and secure endpoints, such as servers and workstations. Unlike network-based IDS tools, OSSEC operates on the host itself, providing in-depth visibility into system activities. It performs log analysis, file integrity monitoring, rootkit detection, and real-time alerting, making it highly effective in detecting unauthorized access, malware infections, and unusual system behavior. OSSEC works by continuously scanning system logs for signs of suspicious activity, such as failed login attempts or configuration changes, and then triggers alerts when predefined security policies are violated. This makes it an essential tool for endpoint security in both small and large-scale environments.

OSSEC also supports a wide range of platforms, including Linux, Windows, macOS, and Unix systems, making it versatile for organizations with heterogeneous IT environments. One of its key features is file integrity monitoring, which ensures that critical system files are not altered or tampered with by malicious actors. Additionally, OSSEC can integrate with other security tools, such as SIEM systems, to provide a comprehensive security solution. By offering a centralized management interface, OSSEC makes it easier for security teams to manage and monitor multiple endpoints from a single location. This combination of comprehensive monitoring, real-time alerts, and flexibility in integration makes OSSEC a vital component of any organization's security strategy, especially in environments with distributed or remote workforces.

6.3.3. ELK Stack:

The ELK Stack, a combination of Elasticsearch, Logstash, and Kibana, is a powerful suite for collecting, managing, and visualizing logs and events, making it ideal for Security Information and Event Management (SIEM) applications. Elasticsearch is a distributed search and analytics engine that indexes and searches large volumes of log data quickly, allowing for near real-time analysis. Logstash serves as a data processing pipeline, ingesting data from various sources, transforming it, and forwarding it to Elasticsearch for indexing. Kibana then visualizes this data, providing dashboards and reporting tools that help security analysts identify patterns, trends, and potential threats. Together, these tools enable an efficient way to collect, analyze, and interpret security-related data in real time.

In the context of this study, the ELK Stack is integrated as the SIEM solution to aggregate and monitor logs from the Snort (NIDS) and OSSEC (HIDS) systems, allowing for comprehensive threat analysis. By centralizing log data in Elasticsearch, the ELK Stack facilitates quick detection of anomalous patterns indicative of potential security incidents. Kibana's interactive dashboards allow the security team to visualize trends, helping them make informed, data-driven decisions. Additionally, Logstash can enrich logs from multiple sources, standardizing and tagging data for enhanced interoperability with the SOAR platform (Shuffle) in the automation workflow. This integration provides a scalable approach to improve threat detection and response capabilities in a remote work environment.

6.3.4. Shuffle SOAR:

Shuffle is an open-source Security Orchestration, Automation, and Response (SOAR) platform designed to streamline security operations by automating repetitive tasks, orchestrating workflows, and enabling faster incident response. In a security operations context, Shuffle integrates with various cybersecurity tools, facilitating real-time information sharing and coordinated responses to detected threats. Its drag-and-drop interface allows users to create complex workflows without extensive coding knowledge, making it accessible to security analysts for rapid deployment. By automating processes such as alert enrichment, data correlation, and incident response actions, Shuffle reduces the manual workload on security teams and shortens response times, ultimately enhancing overall security posture.

In this study, Shuffle acts as the SOAR component within the integrated security framework, automating responses to threats detected by the Snort (NIDS) and OSSEC (HIDS) systems. Upon receiving alerts from the ELK Stack SIEM, Shuffle orchestrates actions such as isolating affected endpoints via OpenVPN or escalating incidents to security personnel. This automated approach improves response consistency and accuracy, allowing for rapid containment and mitigation of threats. Additionally, Shuffle's ability to integrate seamlessly with existing security tools and platforms creates a unified threat detection and response system tailored to the challenges of securing remote work environments, thereby enhancing both efficiency and effectiveness in threat management.

6.3.5. Open VPN:

OpenVPN is a widely-used open-source Virtual Private Network (VPN) solution that provides secure remote access by creating encrypted tunnels between devices and private networks. This enables users to safely connect to corporate networks over the internet, which is particularly valuable in remote work settings. OpenVPN supports various authentication methods, including certificates and multi-factor authentication, and offers strong encryption protocols like AES-256 to protect data in transit. With its cross-platform compatibility, OpenVPN can be deployed across different operating systems, providing a versatile solution for securing connections between remote employees and organizational resources.

In this study, OpenVPN serves as the foundational secure communication layer, allowing remote users to connect to corporate networks while ensuring data integrity and confidentiality. Integrated with the ELK Stack, Snort (NIDS), OSSEC (HIDS), and Shuffle (SOAR), OpenVPN provides a secure gateway for monitoring and responding to security threats across remote endpoints. This setup enables security alerts and automated responses to be applied to remote connections, helping to identify and mitigate threats within the VPN tunnel. By combining OpenVPN with automated threat response capabilities, this framework enhances security for remote access, safeguarding sensitive corporate resources in distributed work environments.

6.4. Proposed Framework:

In the proposed framework, remote workers connect to corporate resources through a VPN, with Snort monitoring network traffic and OSSEC tracking endpoint activities. These tools work in tandem to detect potential threats across both network and endpoint vectors. Logs from Snort and OSSEC are sent to the ELK Stack, where Logstash processes and ingests the data into Elasticsearch for storage and analysis. Kibana provides a visual interface for real-time monitoring and event correlation. When suspicious activity is detected, Elasticsearch generates alerts based on predefined rules, which are then passed to the Shuffle SOAR platform. Shuffle automates incident response actions, such as isolating compromised devices or blocking malicious IPs, streamlining the security operations, and minimizing manual intervention.

6.5. Implementation and Testing:

The implementation process of the proposed security solution begins with the deployment of Snort as the primary network monitoring tool. Snort is configured to detect a wide range of network-based threats, such as malware, suspicious traffic patterns, and unauthorized access attempts over VPN connections, which are commonly used in remote work environments. Since VPN traffic is often encrypted, it can be a potential blind spot for traditional security measures. Snort's ability to analyze packet data in real-time ensures that network traffic is continually monitored, providing early detection of malicious activity or policy violations. Once Snort is operational, OSSEC agents are installed on remote worker devices to monitor endpoint security. OSSEC focuses on critical activities like file integrity, system logs, and rootkit detection, which are key to securing individual devices that might be susceptible to attacks in remote environments.

Both Snort and OSSEC are configured to forward their log data to the ELK Stack, which serves as the centralized logging and analysis platform. The ELK Stack (Elasticsearch, Logstash, and Kibana) processes and stores logs from both network and endpoint monitoring systems, enabling comprehensive analysis and correlation of events. The integration of Snort and OSSEC logs into the ELK Stack ensures that security teams can view all relevant data in a unified interface, allowing for the detection of patterns and potential threats across the entire network and endpoint infrastructure. This centralized analysis helps streamline the monitoring process and improves the overall efficiency of threat detection, making it easier to identify and investigate security incidents in real-time.

Once the core components of Snort and OSSEC are functioning, Shuffle, the SOAR platform, is integrated to automate the incident response process. Predefined workflows are created within Shuffle to handle specific types of alerts, such as isolating compromised devices, blocking malicious IP addresses, or escalating incidents to the security team. These automated responses significantly reduce the time between threat detection and mitigation, allowing the system to act quickly in preventing further damage. To ensure the system's reliability, the entire security setup is tested through simulated attack scenarios, such as phishing attempts, malware infections, ransomware, and unauthorized access attempts via VPN. By simulating these real-world attack vectors, the testing process ensures that the security tools can effectively detect and respond to a variety of threats.

The final phase of testing focuses on verifying the functionality of the detection tools, the integration of the ELK Stack for real-time log analysis, and the effectiveness of Shuffle's automated workflows. During testing, logs generated by Snort and OSSEC are analyzed within the ELK Stack to ensure proper event correlation and visualization, making it easier for security teams to quickly identify and address security incidents. The goal of this phase is to ensure that the system is not only capable of detecting a wide range of threats but also able to respond autonomously with minimal manual intervention. This comprehensive testing process ensures that the solution can provide robust, scalable protection for remote work environments, offering a seamless and efficient approach to security in the modern workforce.

CHAPTER 7

EXPERIMENTATION AND RESULT

The prototype solution was tested on two devices, and the results showed a significant reduction in the number of unnecessary alerts after integration. Prior to integrating the ELK Stack and Shuffle SOAR, the security team encountered numerous alerts, many of which were false positives. Routine activities such as VPN connections and system updates often triggered alerts, leading to inefficiencies in identifying real threats.

After the integration, the system became much more efficient. The centralized log management through the ELK Stack allowed for better correlation of logs from Snort and OSSEC, filtering out false positives. Additionally, Shuffle SOAR's automated workflows reduced the need for manual intervention, automatically isolating and responding to genuine threats. In practice, this meant that the security team could focus on a smaller, more accurate set of alerts, improving the overall response time and reducing alert fatigue.

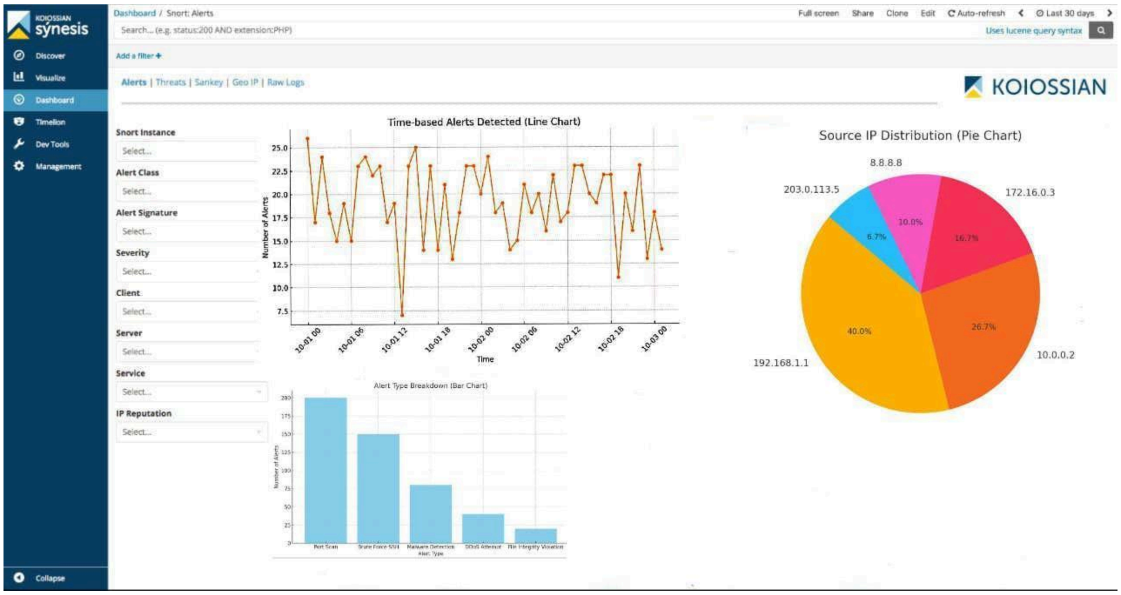


Figure-7.1. Kibana Dashboard for Snort and OSSEC Logs Showing Alert Trend and Source IP Distribution

This Kibana dashboard provides a visual analysis of security alerts generated by Snort and OSSEC. It includes three primary charts:

1. **Time-based Alerts (Line Chart)**: This chart shows the number of alerts over time, indicating periods of high alert activity.
2. **Alert Type Breakdown (Bar Chart)**: This bar chart categorizes alerts by type, allowing quick identification of the most frequent alert types.
3. **Source IP Distribution (Pie Chart)**: The pie chart visualizes the percentage of alerts originating from different IP addresses, highlighting the most active sources (e.g., IP addresses 192.168.1.1 and 10.0.0.2 contribute the most alerts).

These visualizations help security teams identify trends, prioritize responses, and understand the source and nature of security events.

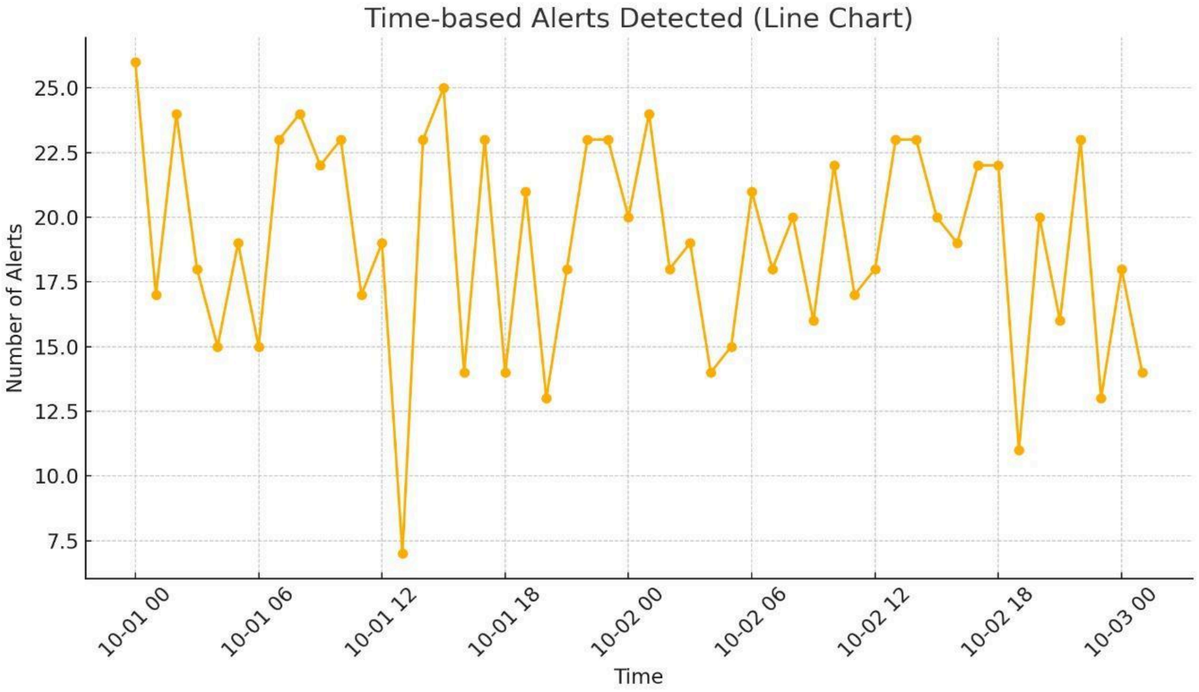


Figure-7.2. Time-based Detection of Security Alerts in Kibana Dashboard for Network Traffic Logs

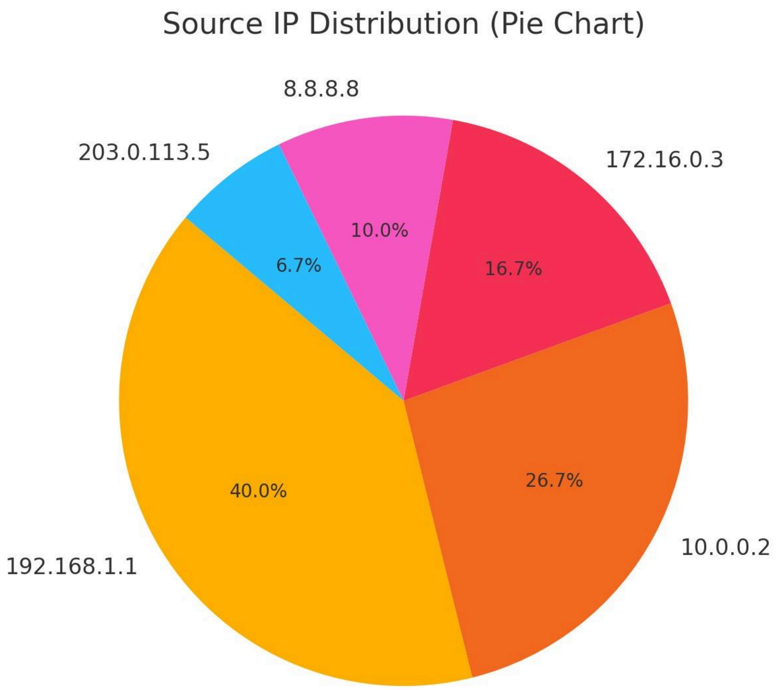


Figure-7.3. Source IP Address Distribution for Detected Network Traffic in Kibana Dashboard

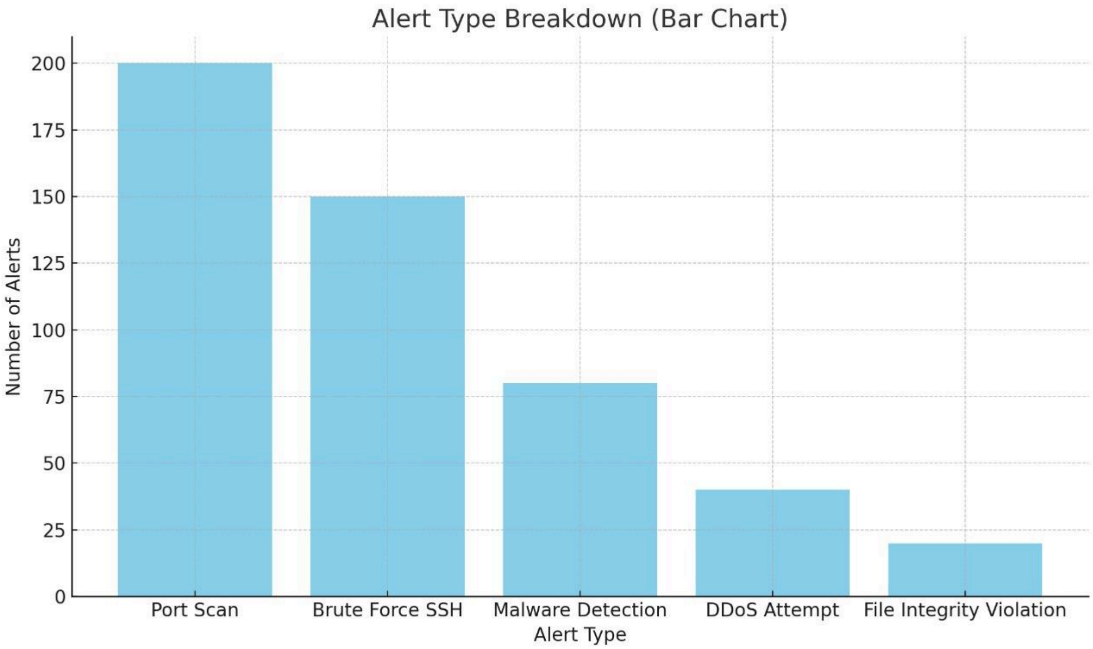


Figure-7.4. Breakdown of Alert Types Detected in Network Security Logs via Kibana Dashboard

A breakdown of the types of alerts before and after SOAR integration is provided in Table I.

TABLE-1. COMPARISON OF ALERT TYPES BEFORE AND AFTER SOAR INTEGRATION

Type of Alerts	Before SOAR	After SOAR
Legitimate VPN	12	5
System Updates	10	4
Cloud Activity	15	6
Other False Alerts	9	3

As illustrated in Table I, the reduction in alert volume was evident across multiple categories. Alerts related to legitimate VPN activity, system updates, cloud activity, and other false positives dropped significantly after SOAR integration. Specifically, the overall reduction from 46 to 18 alerts per day allowed the security team to prioritize real threats more efficiently, significantly improving response times and reducing manual workload.

The effectiveness of the integration is visually represented in Fig. 3, which compares the number of daily alerts before and after the SOAR integration over five days.

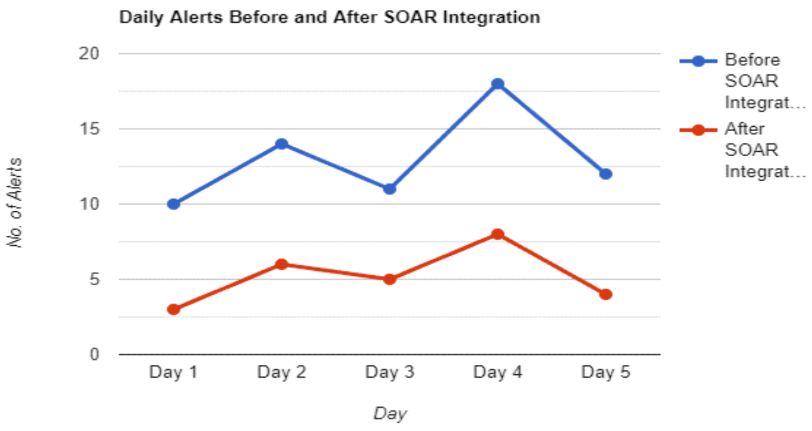


Figure-7.5. A Line Chart depicting Daily Alerts Before and After SOAR Integration

As depicted in Fig. 3, before SOAR integration, the number of alerts ranged between 10 and 18 per day, contributing to alert fatigue. After SOAR automation, this number dropped significantly to between 3 and 6 alerts per day, demonstrating the impact of automation in filtering out unnecessary alerts. A further breakdown of the types of alerts before and after SOAR integration is provided in Table I.

However, some setbacks were identified, such as the complexity of configuring the tools for seamless integration and the need for constant tuning of detection rules to prevent new types of false positives. Additionally, performance challenges may arise when scaling the system to monitor larger networks with more devices. Future improvements could include incorporating machine learning to enhance detection accuracy and further optimizing the system for large-scale deployments. Testing demonstrated that the system successfully detected and mitigated various simulated attack scenarios, such as phishing attempts and VPN intrusions, validating the effectiveness of the integrated approach in real-world conditions.

CHAPTER 8

CONCLUSION AND FUTURE ENHANCEMENT

This research successfully integrates Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) platforms, creating a robust security framework for remote work environments. The combination of Snort for network-based monitoring, OSSEC for host-based detection, Shuffle for automated response, and the ELK Stack for centralized log management offers a scalable and cost-effective solution. This integration ensures that threats to both the network and endpoints are detected in real-time, and automated workflows are in place to quickly respond to incidents. The centralization of logs and event data through the ELK Stack enhances the ability to identify patterns, making it easier to detect and respond to potential threats. By automating much of the response process, the solution reduces the manual workload on security teams, allowing them to focus on more complex tasks while improving overall operational efficiency.

The system's design addresses key security risks associated with remote work, such as vulnerabilities in VPN traffic, cloud services, and endpoints. VPN connections, commonly used for secure remote access, often obscure threat activity due to encryption, but Snort's ability to analyze network traffic in real-time ensures that any malicious behavior or intrusion is quickly detected. OSSEC provides an additional layer of security by monitoring endpoints for unauthorized access, malware, and other system-level threats. By providing visibility into both the network and endpoint layers, this solution strengthens the security posture of remote workforces, ensuring that potential security breaches are caught early and mitigated swiftly.

Looking to the future, there is significant potential to expand and improve this security framework further. Integrating machine learning could enhance threat detection capabilities, enabling the system to identify previously unknown attack patterns and adapt to evolving security threats. Machine learning could also help in reducing false positives by automatically refining detection rules based on historical data and real-time analysis. Additionally, expanding cloud-native monitoring would allow the solution to extend its protection to cloud-based services, which are increasingly a target for cyberattacks. By incorporating these advanced technologies, the security framework could evolve into a more adaptive, dynamic system capable of defending against the ever-changing landscape of cyber threats in remote work environments.

Furthermore, the integration of advanced threat intelligence feeds and behavioral analytics could further enhance the system's ability to proactively identify and respond to emerging threats. By leveraging up-to-date threat data from various external sources, the system could gain insights into new attack techniques, tactics, and procedures (TTPs) used by cybercriminals. This would allow the security framework to stay ahead of evolving threats and automatically adjust its detection rules accordingly. Additionally, incorporating behavioral analytics could enable the system to establish a baseline of normal activity across the network and endpoints, making it more effective at identifying anomalous behavior indicative of potential security incidents.

REFERENCES

[1]. Liao, H., Lin, C. R., Lin, Y., Tung, K. (2012). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

[2]. Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). International Journal of Information Security, 22(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

[3]. Pradhan, M., Nayak, C. K., & Pradhan, S. K. (2016). Intrusion Detection System (IDS) and Their Types. In Advances in information security, privacy, and ethics book series (pp. 228–244). https://doi.org/10.4018/978-1-4666-8761-5.ch009

[4]. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

[5]. Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, 3(4), 227–261. https://doi.org/10.1145/382912.382914

[6]. D. A. Effendy, K. Kusrini and S. Sudarmawan, "Classification of intrusion detection system (IDS) based on computer network," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2017, pp. 90-94, doi: 10.1109/ICITISEE.2017.8285566.

[7]. U. Bartwal, S. Mukhopadhyay, R. Negi and S. Shukla, "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots," 2022 IEEE Conference on Dependable and Secure Computing (DSC), Edinburgh, United Kingdom, 2022, pp. 1-8, doi: 10.1109/DSC54232.2022.9888808.

[8]. Yeboah, F. A. (2024). Detecting and Safeguarding Against Cybersecurity Attacks Targeting Wireless Networks: A Comprehensive Approach to Integrate IDS/IPS, SIEM and SOAR (Master's thesis, University of Cincinnati).

[9]. Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2023). Testing SOAR tools in use. Computers & Security, 129, 103201. https://doi.org/10.1016/j.cose.2023.103201

[10]. Purujoki, J. (2020). SOAR Playbook Implementation-Incident Deduplication and Its Effects.

[11]. Falade, P. V., & Momoh, P. O. (2024). Evaluating the Permissions of Monitoring Mobile Applications for Remote Employees: Analyzing the Impact on Employer Trust and Employee Privacy Concerns. Int. J. Sci. Res. in Computer Science and Engineering Vol, 12(1).

[12]. Roschke, S., Cheng, F., & Meinel, C. (2009, December). Intrusion detection in the cloud. In 2009 eighth IEEE international conference on dependable, autonomic and secure computing (pp. 729-734). IEEE.

[13]. Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming remote workforce cyber threats: A comprehensive ransomware and bot net defense strategy utilizing VPN networks. Available at SSRN 4911878.

[14]. Rahman, A., Knudsen, S. R., Milonas, D. C., Fleming, D., & Clements, J. (2024). SOAR.

[15]. Laird, J. E. (2022). Introduction to SOAR. arXiv preprint arXiv:2205.03854.

[16]. Larsen, G., Fong, E. K. H., Wheeler, D. A., & Moorthy, R. S. (2014). State-of-the-art resources (soar) for software vulnerability detection, test, and evaluation. Institute for Defence Analysis, Virginia, USA, Tech. Rep. IDA Paper P-5061.

[17]. Sridharan, A., & Kanchana, V. (2022, November). SIEM integration with SOAR. In 2022 International Conference on Futuristic Technologies (INCOFT) (pp. 1-6). IEEE.

[18]. Trisolino, A. (2023). Analysis of Security Configuration for IDS/IPS (Doctoral dissertation, Politecnico di Torino).

[19]. Agrawal, A., Deep, V., Sharma, P., & Mishra, S. (2021). Review of Cybersecurity Post-COVID-19. In Advances in Interdisciplinary Engineering: Select Proceedings of FLAME 2020 (pp. 775-784). Springer Singapore.

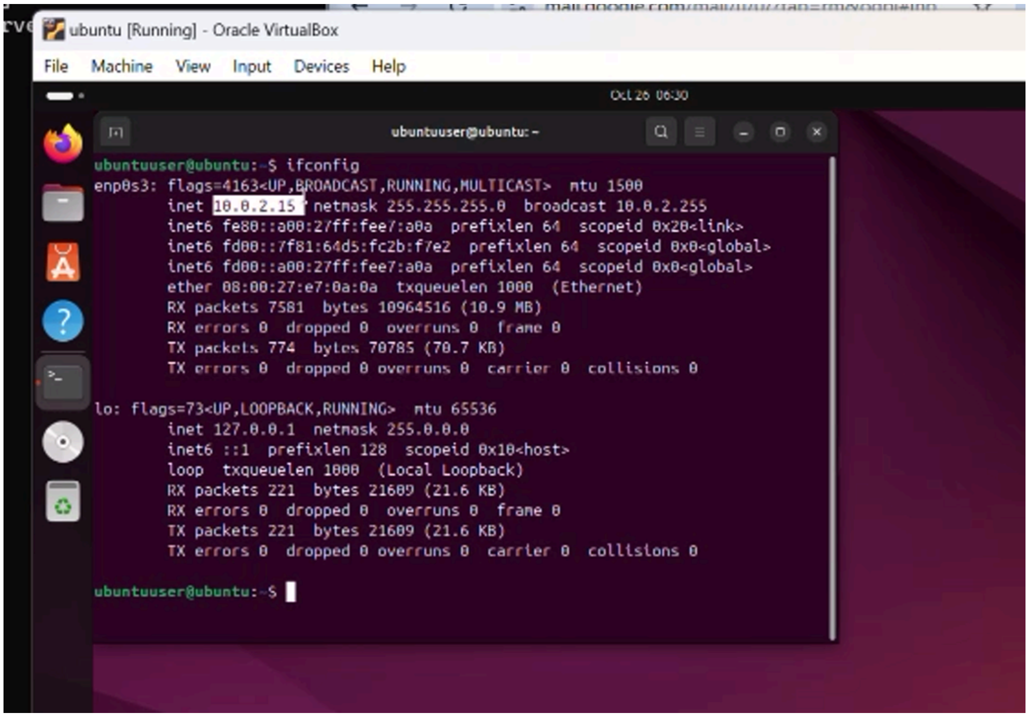
[20]. Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender systems in cybersecurity. Knowledge and Information Systems, 65(12), 5523-5559.

[21]. Ogbonna, E. E. O., & Akobundu, I. Developing a Good Cybersecurity Awareness in Tertiary Institutions-A Prerequisite to Robust Cyberspace in COVID-19 Pandemic Epoch.

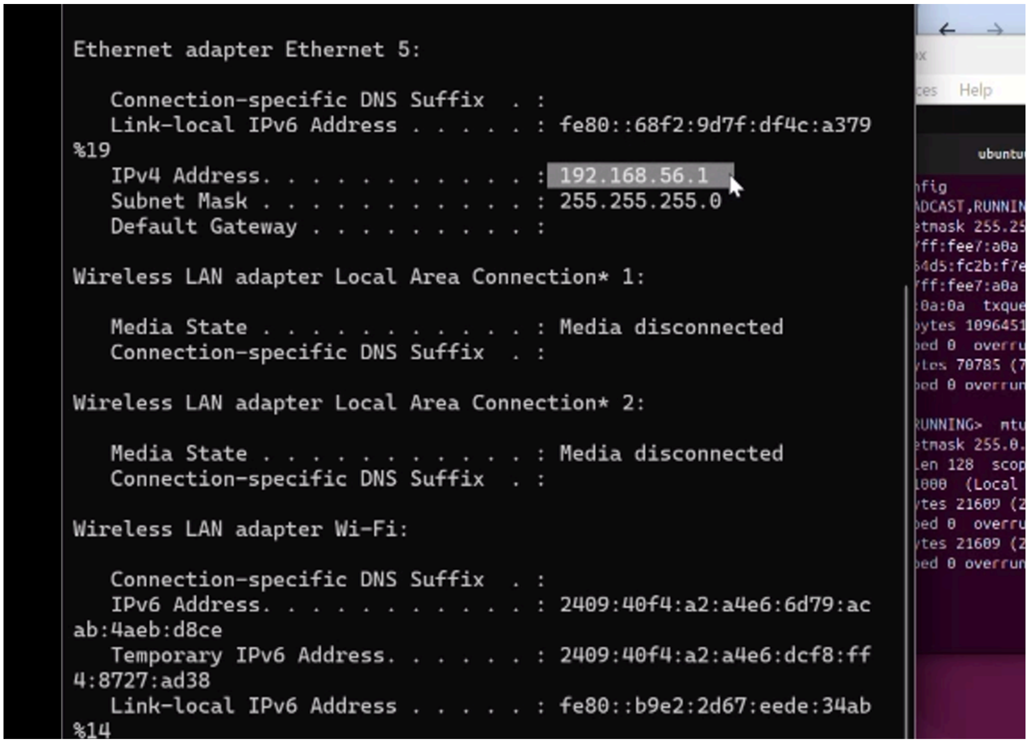
[22]. Kang, M. (2020). SOAR: a Self-Optimizing Adaptive SoC on FPGAs (Doctoral dissertation, WILLIAMS COLLEGE).

APPENDIX - A

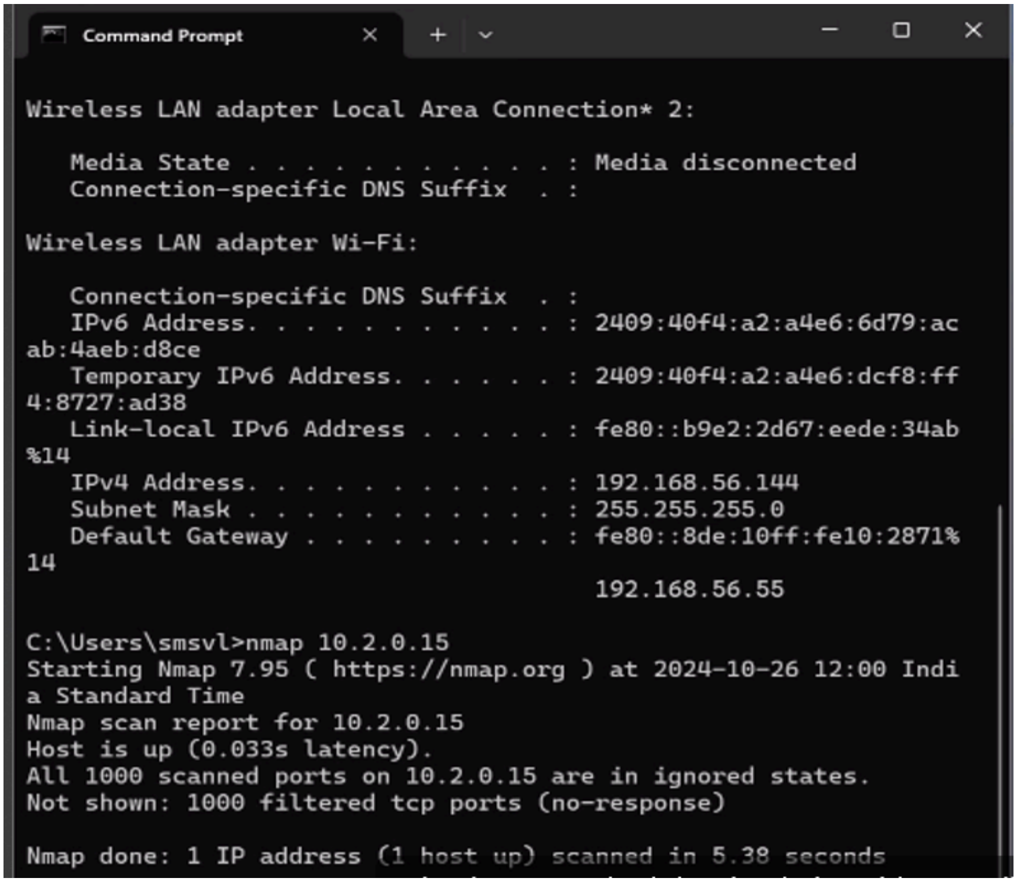
DEMO SCREENSHOTS



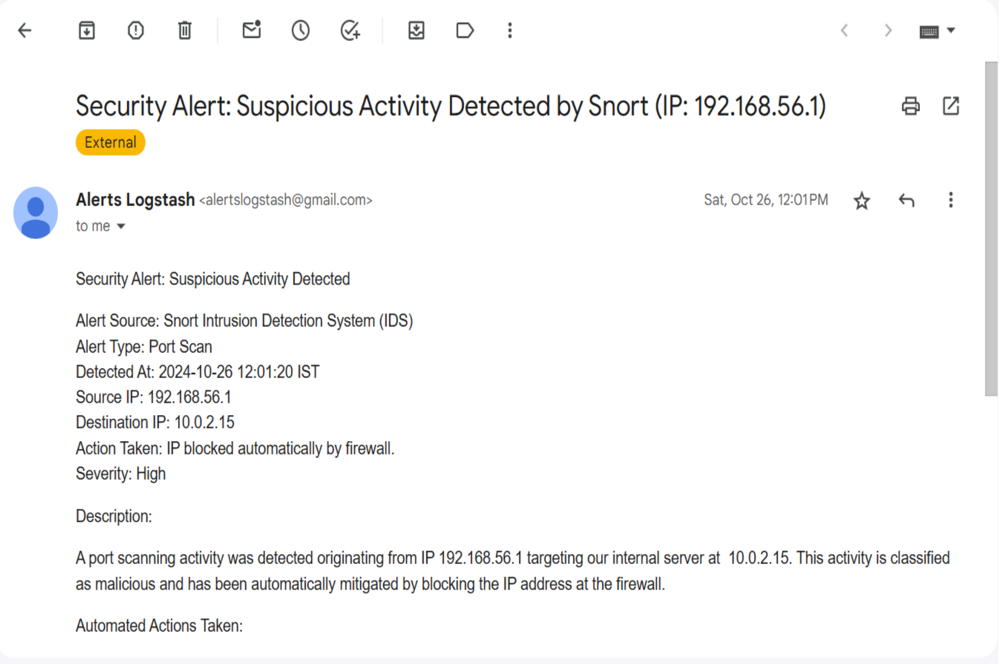
```
ubuntuuser@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee7:a0a  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::7f81:64d5:fc2b:f7e2  prefixlen 64  scopeid 0x0<global>
        inet6 fd00::a00:27ff:fee7:a0a  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:e7:0a:0a  txqueuelen 1000  (Ethernet)
        RX packets 7581  bytes 10964516 (10.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 774  bytes 70785 (70.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 221  bytes 21609 (21.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 221  bytes 21609 (21.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntuuser@ubuntu:~$
```



```
Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::68f2:9d7f:df4c:a379
%19
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40f4:a2:a4e6:6d79:ac
ab:4aeb:d8ce
   Temporary IPv6 Address. . . . . . : 2409:40f4:a2:a4e6:dcf8:ff
4:8727:ad38
   Link-local IPv6 Address . . . . . : fe80::b9e2:2d67:eede:34ab
%14
```



```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40f4:a2:a4e6:6d79:ac
ab:4aeb:d8ce
   Temporary IPv6 Address. . . . . . : 2409:40f4:a2:a4e6:dcf8:ff
4:8727:ad38
   Link-local IPv6 Address . . . . . : fe80::b9e2:2d67:eede:34ab
%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.144
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8de:10ff:fe10:2871%
14
                                       192.168.56.55

C:\Users\smsvl>nmap 10.2.0.15
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 12:00 Indi
a Standard Time
Nmap scan report for 10.2.0.15
Host is up (0.033s latency).
All 1000 scanned ports on 10.2.0.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds
```



Security Alert: Suspicious Activity Detected by Snort (IP: 192.168.56.1)

Alerts Logstash <alertslogstash@gmail.com>   Sat, Oct 26, 12:01 PM

Security Alert: Suspicious Activity Detected

Alert Source: Snort Intrusion Detection System (IDS)
Alert Type: Port Scan
Detected At: 2024-10-26 12:01:20 IST
Source IP: 192.168.56.1
Destination IP: 10.0.2.15
Action Taken: IP blocked automatically by firewall.
Severity: High

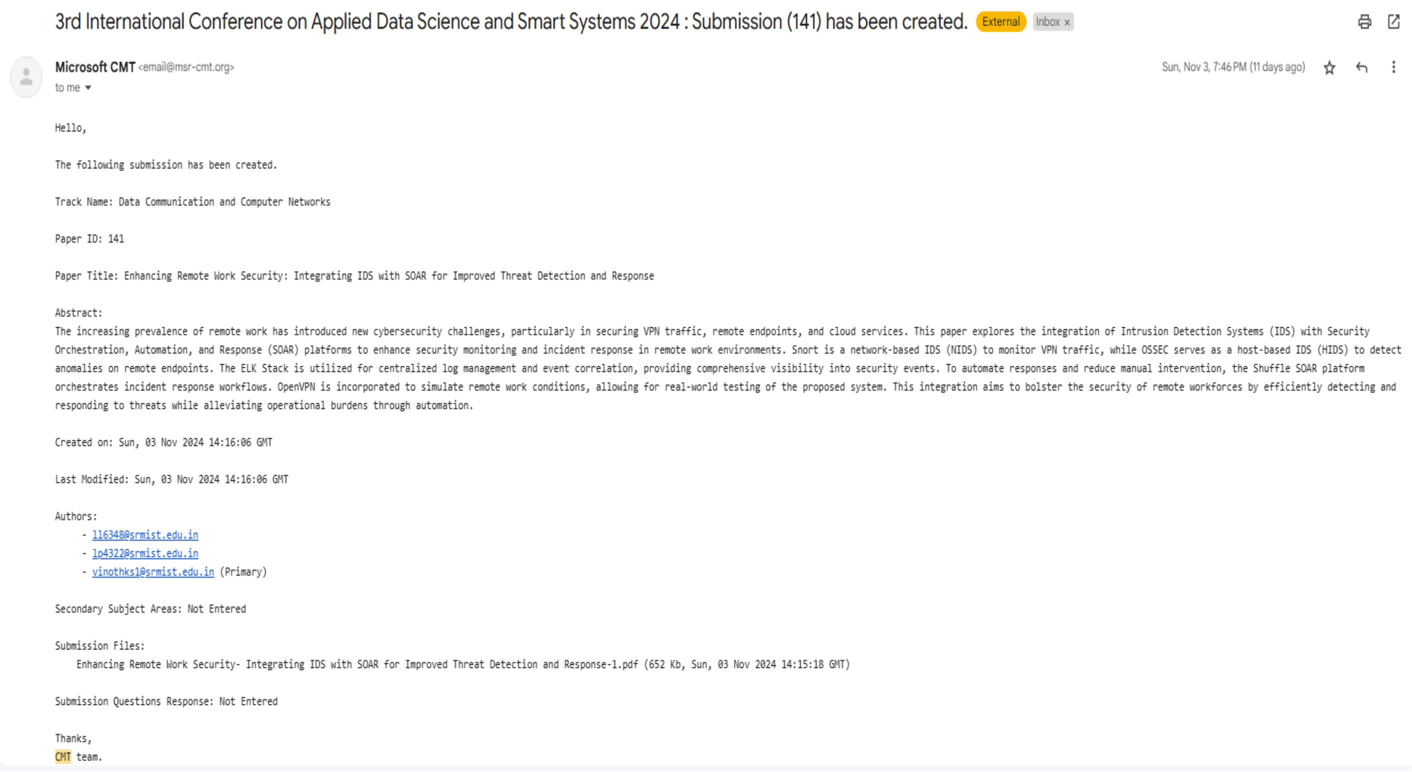
Description:

A port scanning activity was detected originating from IP 192.168.56.1 targeting our internal server at 10.0.2.15. This activity is classified as malicious and has been automatically mitigated by blocking the IP address at the firewall.

Automated Actions Taken:

APPENDIX - B

CONFERENCE PUBLICATION



3rd International Conference on Applied Data Science and Smart Systems 2024 : Submission (141) has been created.

Microsoft CMT <email@msr-cmt.org>
to me

Sun, Nov 3, 7:46 PM (11 days ago)

Hello,

The following submission has been created.

Track Name: Data Communication and Computer Networks

Paper ID: 141

Paper Title: Enhancing Remote Work Security: Integrating IDS with SOAR for Improved Threat Detection and Response

Abstract:
The increasing prevalence of remote work has introduced new cybersecurity challenges, particularly in securing VPN traffic, remote endpoints, and cloud services. This paper explores the integration of Intrusion Detection Systems (IDS) with Security Orchestration, Automation, and Response (SOAR) platforms to enhance security monitoring and incident response in remote work environments. Snort is a network-based IDS (NIDS) to monitor VPN traffic, while OSSEC serves as a host-based IDS (HIDS) to detect anomalies on remote endpoints. The ELK Stack is utilized for centralized log management and event correlation, providing comprehensive visibility into security events. To automate responses and reduce manual intervention, the Shuffle SOAR platform orchestrates incident response workflows. OpenVPN is incorporated to simulate remote work conditions, allowing for real-world testing of the proposed system. This integration aims to bolster the security of remote workforces by efficiently detecting and responding to threats while alleviating operational burdens through automation.

Created on: Sun, 03 Nov 2024 14:16:06 GMT

Last Modified: Sun, 03 Nov 2024 14:16:06 GMT

Authors:
- ll6348@srmist.edu.in
- lp4322@srmist.edu.in
- vinothks1@srmist.edu.in (Primary)

Secondary Subject Areas: Not Entered

Submission Files:
Enhancing Remote Work Security- Integrating IDS with SOAR for Improved Threat Detection and Response-1.pdf (652 Kb, Sun, 03 Nov 2024 14:15:18 GMT)

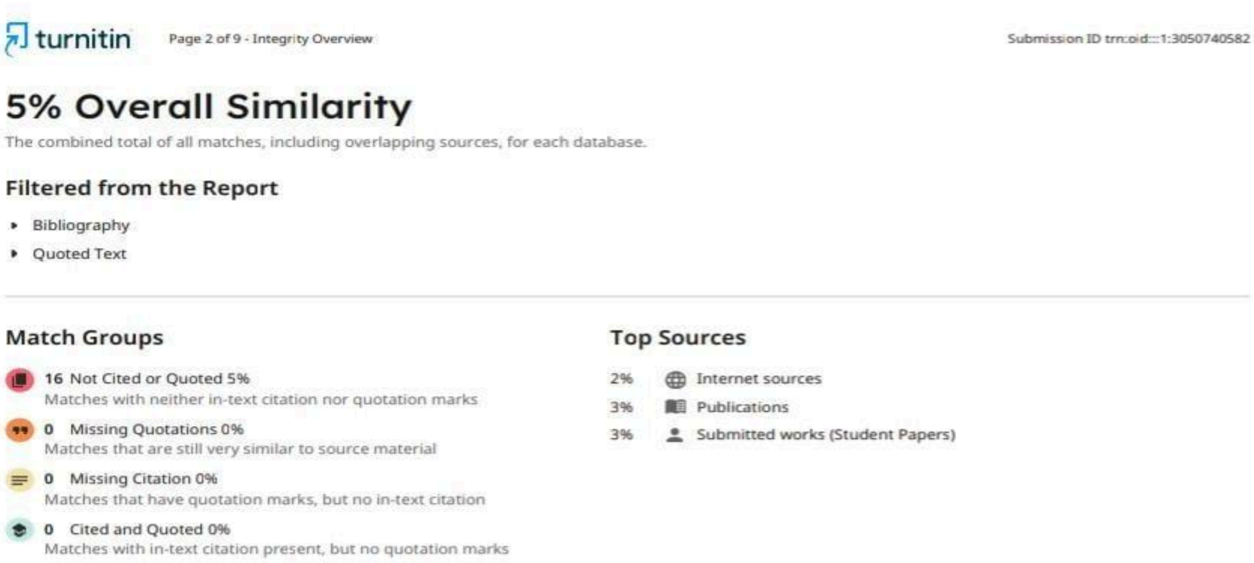
Submission Questions Response: Not Entered

Thanks,
CMT team.

APPENDIX - C

PLAGIARISM REPORT

Research Paper Plagiarism:



turnitin Page 2 of 9 - Integrity Overview Submission ID trn:oid:::1:3050740582

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

16 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

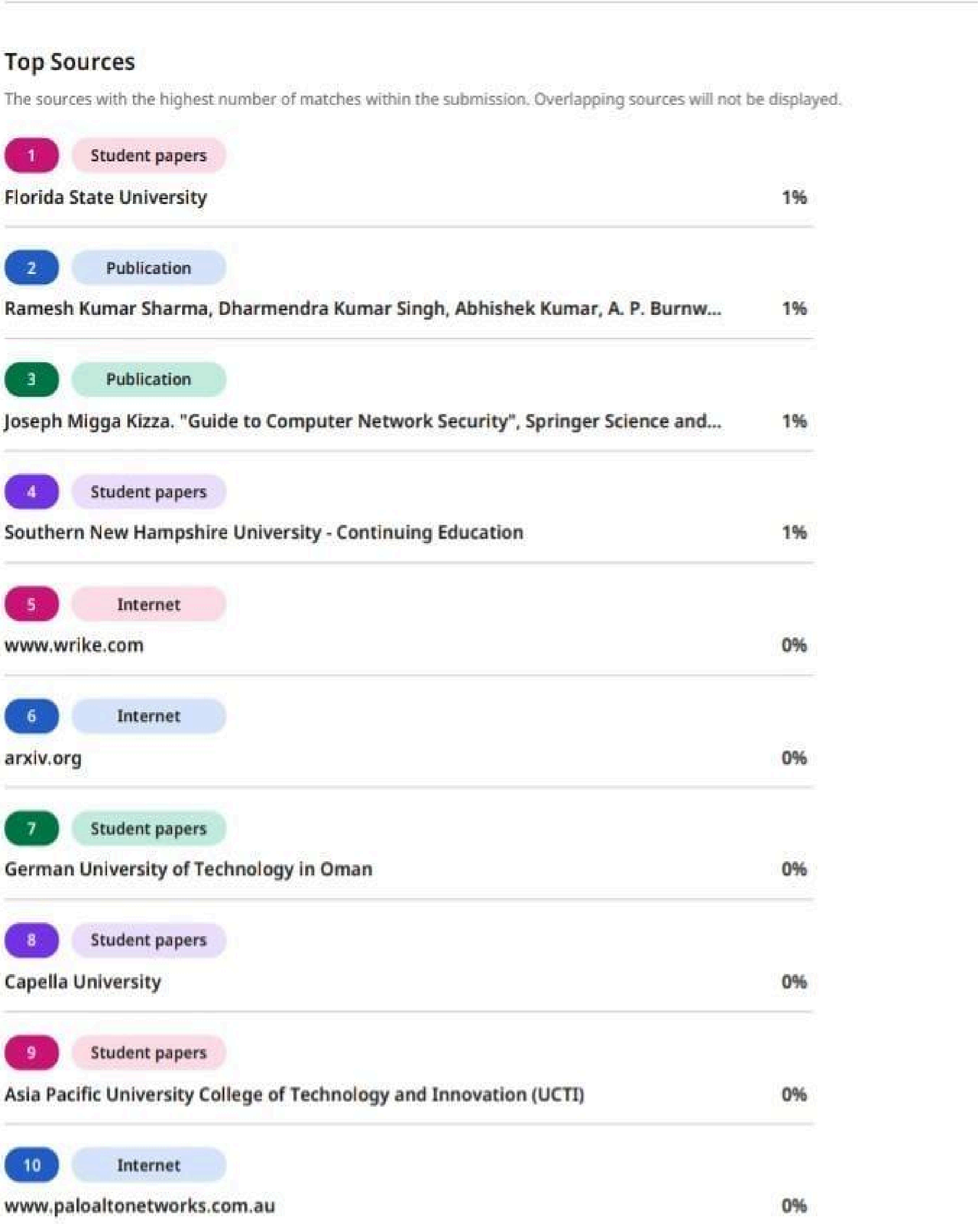
0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

2%	Internet sources
3%	Publications
3%	Submitted works (Student Papers)

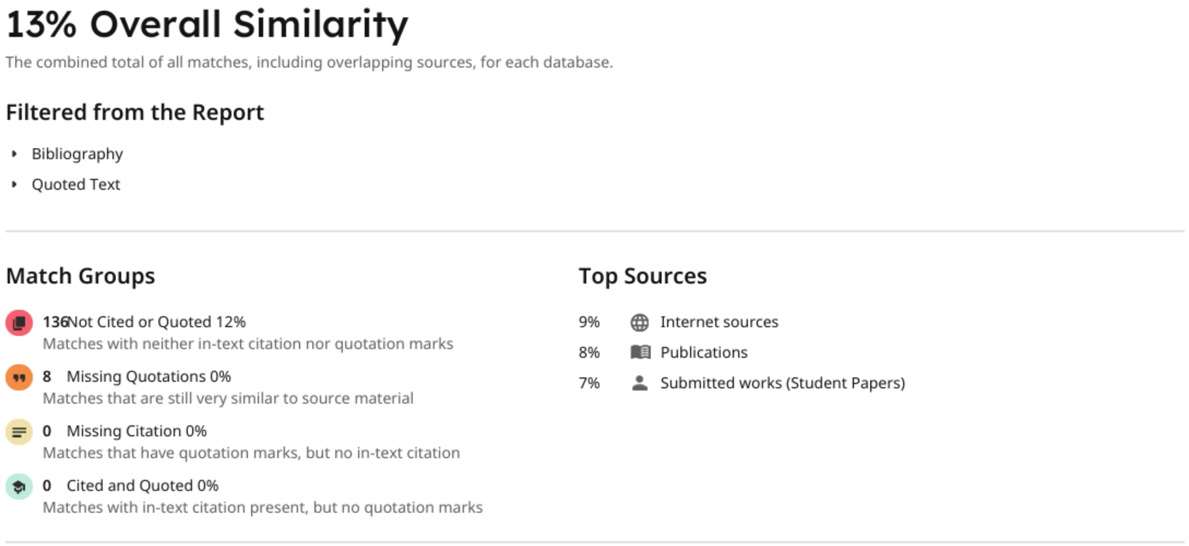


Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	Florida State University	1%
2	Publication	Ramesh Kumar Sharma, Dharmendra Kumar Singh, Abhishek Kumar, A. P. Burnw...	1%
3	Publication	Joseph Migga Kizza. "Guide to Computer Network Security", Springer Science and...	1%
4	Student papers	Southern New Hampshire University - Continuing Education	1%
5	Internet	www.wrike.com	0%
6	Internet	arxiv.org	0%
7	Student papers	German University of Technology in Oman	0%
8	Student papers	Capella University	0%
9	Student papers	Asia Pacific University College of Technology and Innovation (UCTI)	0%
10	Internet	www.paloaltonetworks.com.au	0%

Report Plagiarism:



13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

136Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

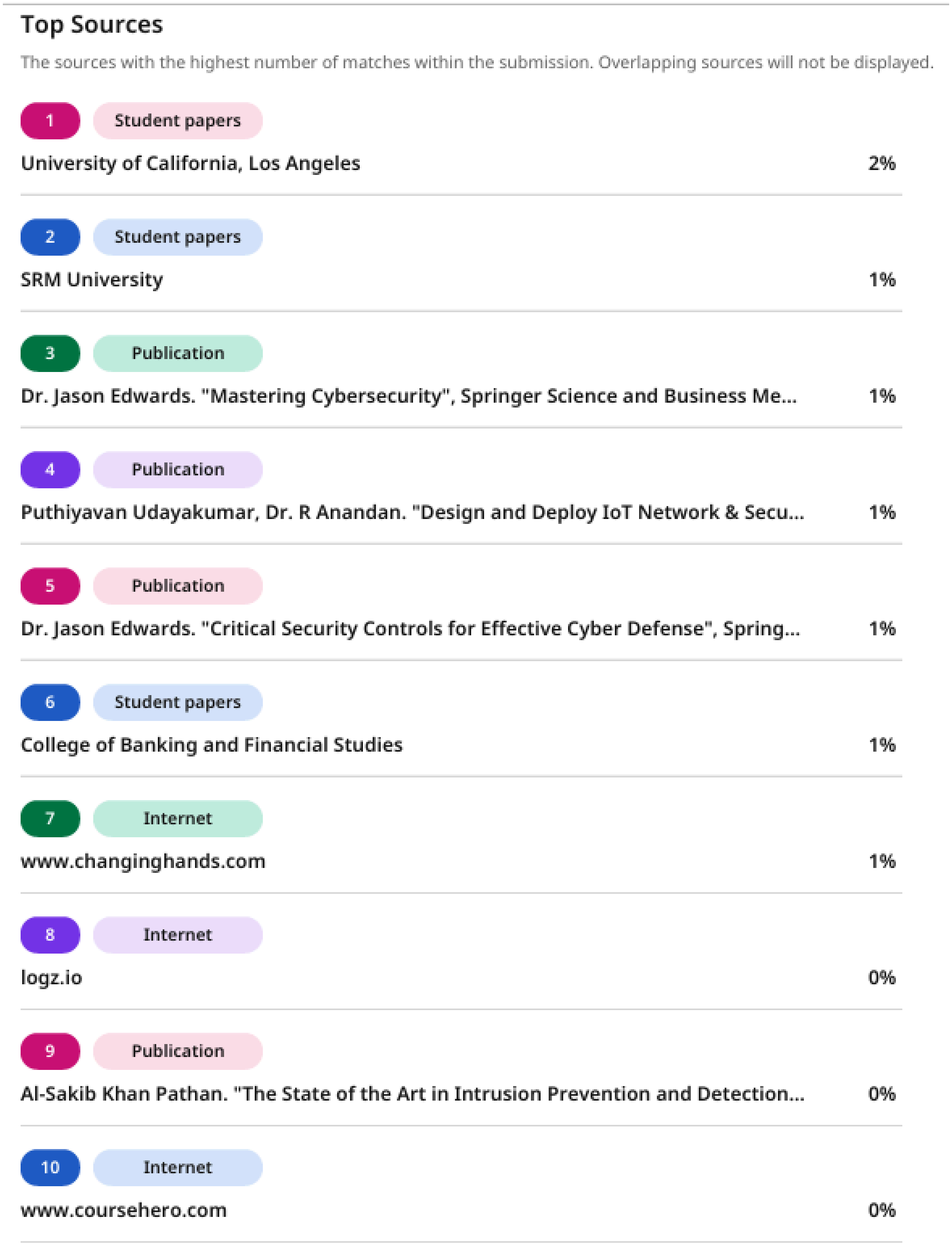
8 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

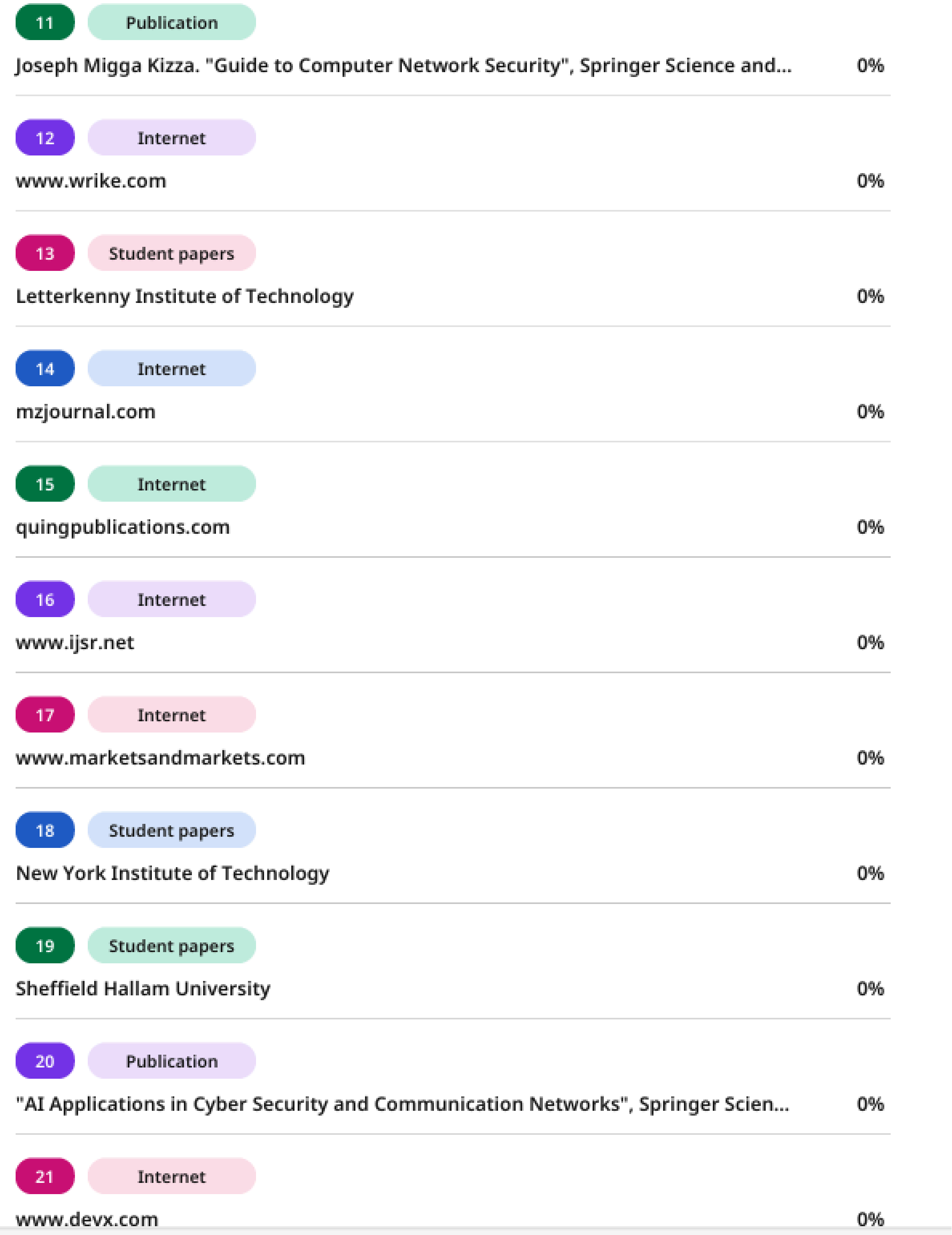
9%	Internet sources
8%	Publications
7%	Submitted works (Student Papers)



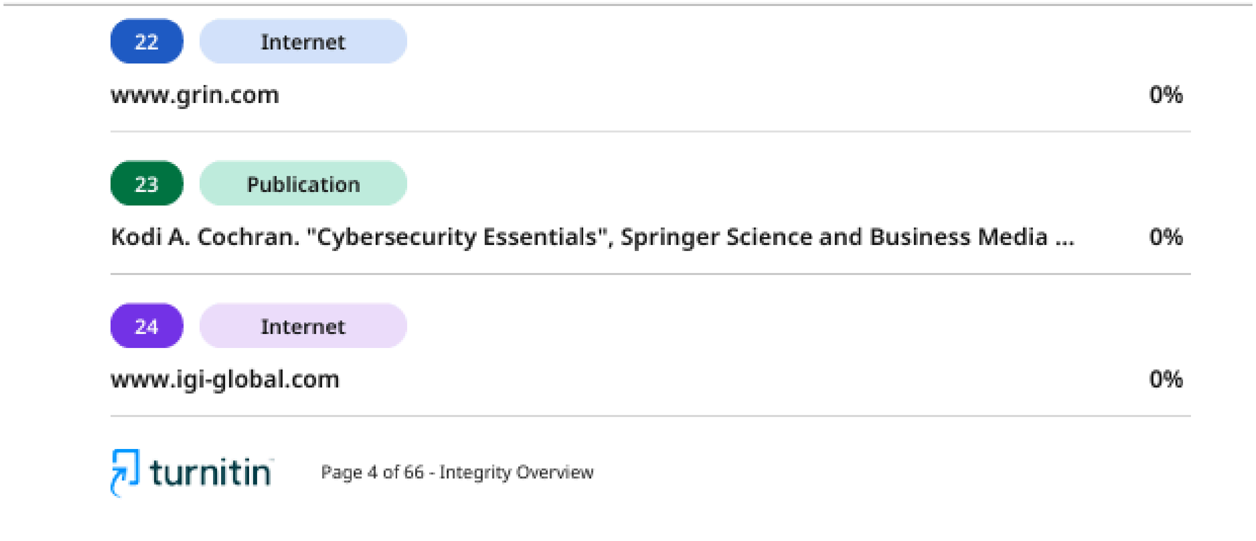
Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	University of California, Los Angeles	2%
2	Student papers	SRM University	1%
3	Publication	Dr. Jason Edwards. "Mastering Cybersecurity", Springer Science and Business Me...	1%
4	Publication	Puthiyavan Udayakumar, Dr. R Anandan. "Design and Deploy IoT Network & Secu...	1%
5	Publication	Dr. Jason Edwards. "Critical Security Controls for Effective Cyber Defense", Spring...	1%
6	Student papers	College of Banking and Financial Studies	1%
7	Internet	www.changinghands.com	1%
8	Internet	logz.io	0%
9	Publication	Al-Sakib Khan Pathan. "The State of the Art in Intrusion Prevention and Detection...	0%
10	Internet	www.coursehero.com	0%



11	Publication	Joseph Migga Kizza. "Guide to Computer Network Security", Springer Science and...	0%
12	Internet	www.wrike.com	0%
13	Student papers	Letterkenny Institute of Technology	0%
14	Internet	mzjournal.com	0%
15	Internet	quingpublications.com	0%
16	Internet	www.ijsr.net	0%
17	Internet	www.marketsandmarkets.com	0%
18	Student papers	New York Institute of Technology	0%
19	Student papers	Sheffield Hallam University	0%
20	Publication	"AI Applications in Cyber Security and Communication Networks", Springer Scien...	0%
21	Internet	www.devx.com	0%



22 Internet

www.grin.com 0%

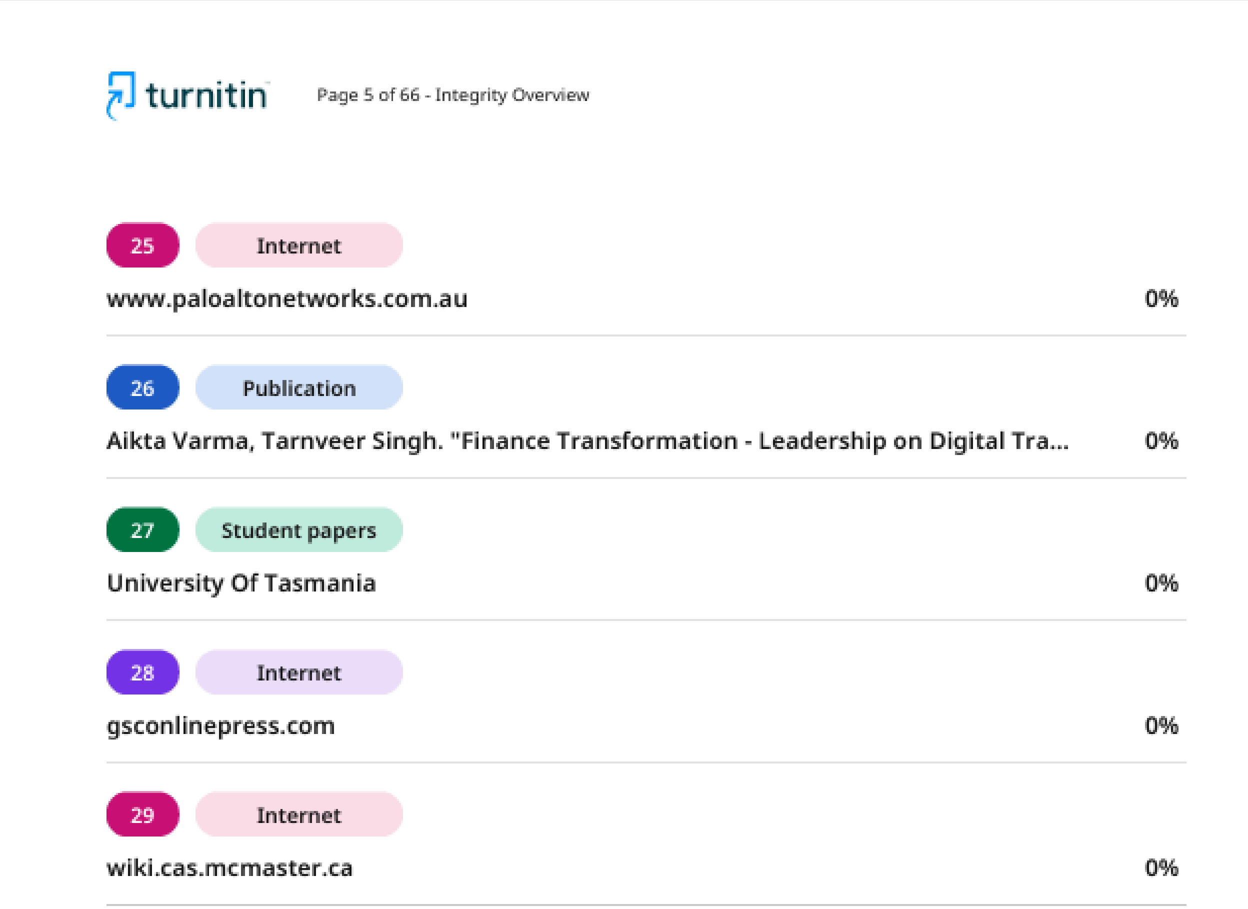
23 Publication

Kodi A. Cochran. "Cybersecurity Essentials", Springer Science and Business Media ... 0%

24 Internet

www.igi-global.com 0%

turnitin Page 4 of 66 - Integrity Overview



turnitin Page 5 of 66 - Integrity Overview

25 Internet

www.paloaltonetworks.com.au 0%

26 Publication

Aikta Varma, Tarnveer Singh. "Finance Transformation - Leadership on Digital Tra... 0%

27 Student papers

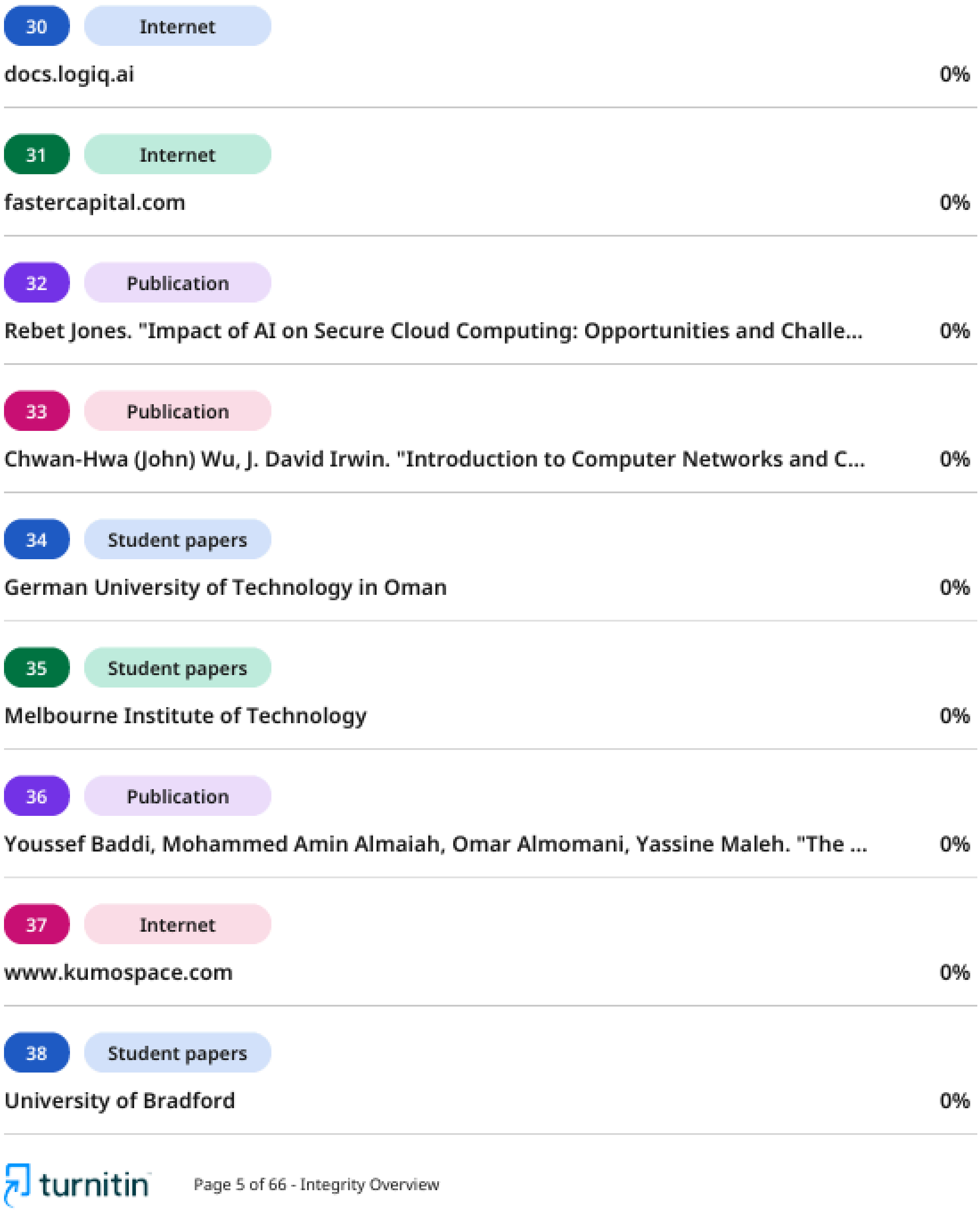
University Of Tasmania 0%

28 Internet

gsconlinepress.com 0%

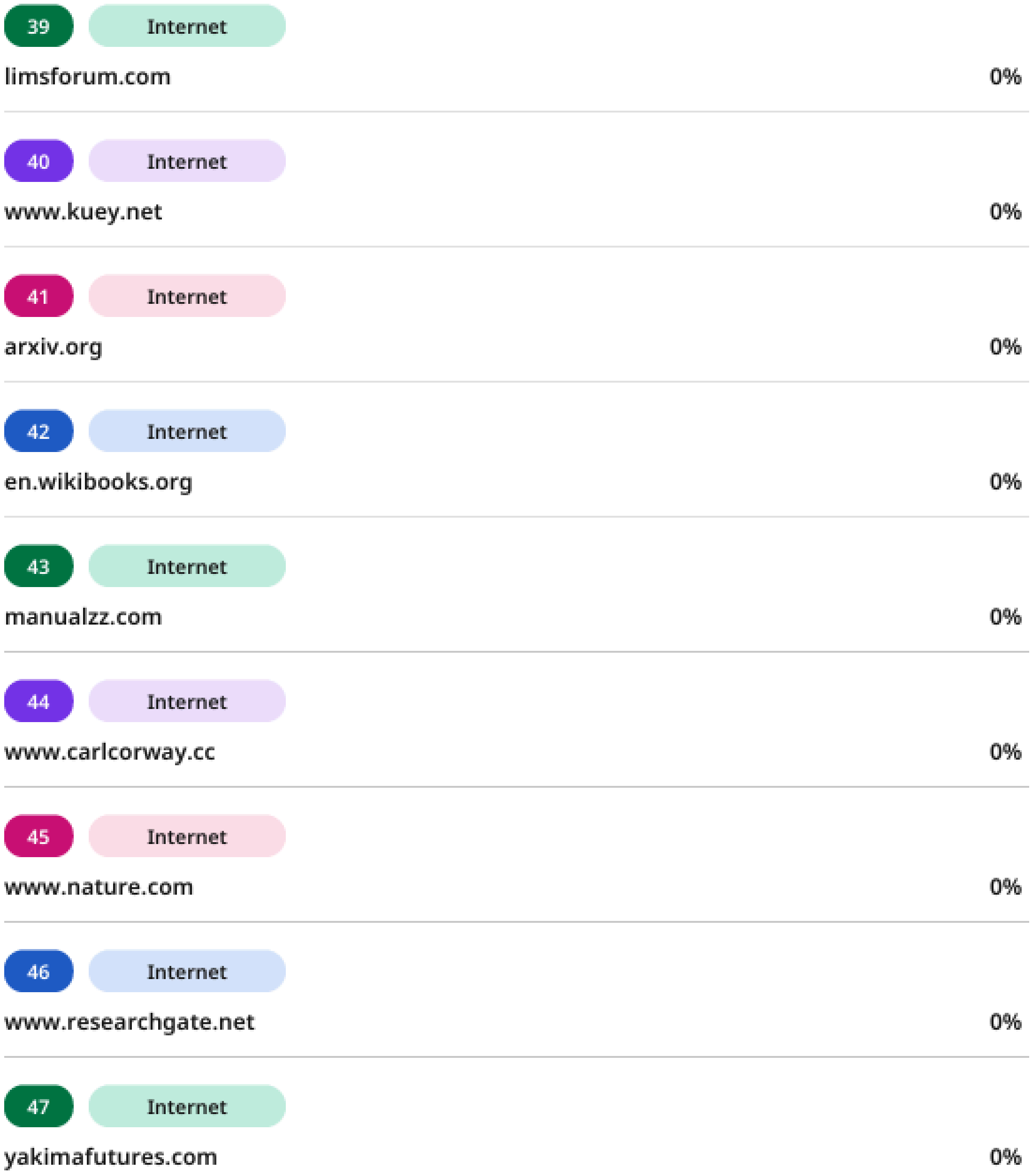
29 Internet

wiki.cas.mcmaster.ca 0%



30	Internet	docs.logiq.ai	0%
31	Internet	fastercapital.com	0%
32	Publication	Rebet Jones. "Impact of AI on Secure Cloud Computing: Opportunities and Challe...	0%
33	Publication	Chwan-Hwa (John) Wu, J. David Irwin. "Introduction to Computer Networks and C...	0%
34	Student papers	German University of Technology in Oman	0%
35	Student papers	Melbourne Institute of Technology	0%
36	Publication	Youssef Baddi, Mohammed Amin Almaiah, Omar Almomani, Yassine Maleh. "The ...	0%
37	Internet	www.kumospace.com	0%
38	Student papers	University of Bradford	0%

turnitin Page 5 of 66 - Integrity Overview



39	Internet	limsforum.com	0%
40	Internet	www.kuey.net	0%
41	Internet	arxiv.org	0%
42	Internet	en.wikibooks.org	0%
43	Internet	manualzz.com	0%
44	Internet	www.carlcorway.cc	0%
45	Internet	www.nature.com	0%
46	Internet	www.researchgate.net	0%
47	Internet	yakimafutures.com	0%

PLAGIARISM REPORT

Format - I

SRM INSITITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/ s 3 of UGC Act, 1956)

Office of Controller of Examinations

REPORT FOR PLAGIARISM CHECK ON THE DISSERTATION/PROJECT REPORTS FOR UG/PG PROGRAMMES

(To be attached in the dissertation/ project report)

1.	Name of the Candidate **(IN BLOCK LETTERS)**	LAKKAVARAM S M SHRIYA VARNITA PAVULURI LOLA YASWANTHI
2.	Address of the Candidate	SRMIST, KATTANKULATHUR
3.	Registration Number	RA2111030010201 RA2111030010256
4.	Date of Birth	17-08-2004 22-07-2003
5.	Department	Computer Science and Engineering
6.	Faculty	Engineering and Technology, School of Computing
7.	Title of the Dissertation/Project	Enhancing Remote Work Security: Integration IDS with SOAR for Improved Threat Detection and Response
8.	Whether the above project /dissertation is done by	Individual or group: Group a) If the project/ dissertation is done in group, then how many students together completed the project: 2 b) Mention the Name & Register number of other candidates: LAKKAVARAM S M SHRIYA VARNITA[RA2111030010201] PAVULURI LOLA YASWANTHI[RA2111030010256]
9.	Name and address of the Supervisor / Guide	**Dr. C. N. S. Vinoth Kumar** SRMIST, KATTANKULATHUR Mail ID: vinothks1@srmist.edu.in Phone Number: 9944599129
10.	Name and address of the Co- Supervisor / Co- Guide (if any)	N/A Mail ID: N/A Phone Number: N/A

11.	Software Used	Turnitin
12.	Date of Verification	11-11-2024
13.	Plagiarism Details: (to attach the final report from the software)	

Chapter	Title of the Chapter	Percentage of similarity index (Including self-citation)	Percentage of similarity index (Excluding self-citation)	% of plagiarism after excluding Quotes, Bibliography, etc.,
1.	INTRODUCTION	1	3	2
2.	SPRINT PLANNING AND EXECUTION	1	1	1
3.	LITERATURE SURVEY	2	5	4
4.	SYSTEM ARCHITECTURE AND DESIGN	1	1	1
5.	IMPACT OF IDS LIMITATIONS ON SECURITY INCIDENTS	4	3	3
6.	METHODOLOGY	2	4	2
7.	EXPERIMENTATION AND RESULT	1	1	1
8.	CONCLUSION AND FUTURE ENHANCEMENT	1	1	1
	Appendices	0	0	0

I / We declare that the above information has been verified and found true to the best of my / our knowledge.

Lola Yaswanthi Signature of the Candidate	14/11/24 Name & Signature of the Staff (Who uses the plagiarism check software)
14/11/24 Name & Signature of the Supervisor/ Guide	N/A Name & Signature of the Co-Supervisor/Co- Guide

M. Lakshmi

Name & Signature of the HOD