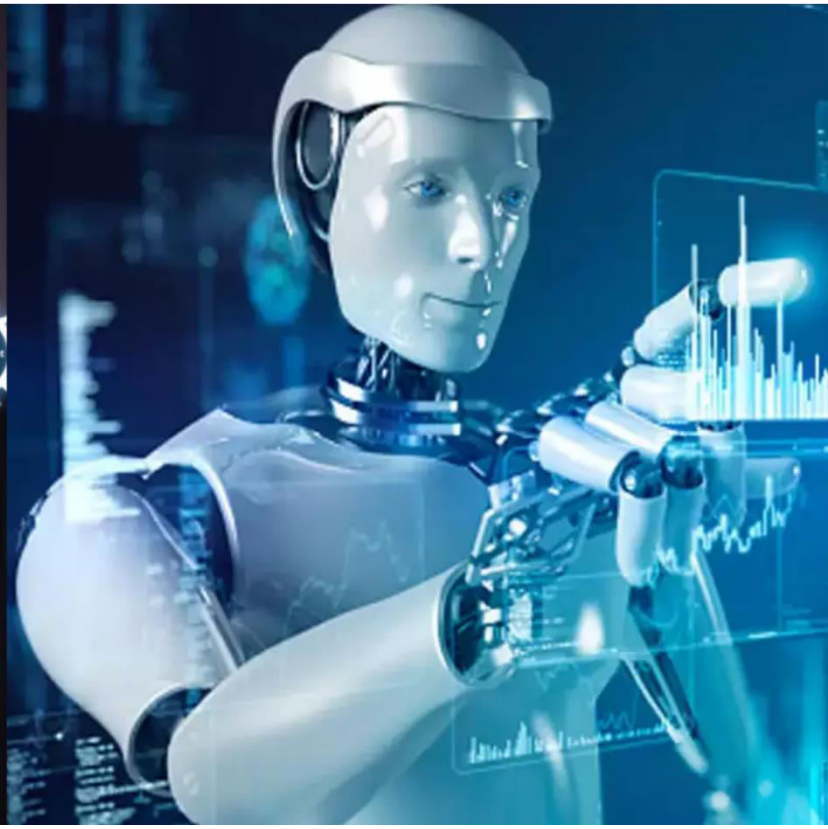
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

Next-Gen Intrusion Detection: Leveraging Suricata and Wazuh for Real- Time Network Threat Monitoring

Dr.Godlin Atlas[1], Puppala Arun Kumar [2], Annamalla Vijay[3], Godishala Sanjay Kumar[4]

Associate Professor, Department of CSE Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

B. Tech Students, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

ABSTRACT: Next-Generation Intrusion Detection: Suricata and Wazuh for Real-Time Monitoring of Network Threats As cyberattacks become more and more common, organizations need state-of-the-art intrusion detection and response to secure their networks. In this project, Suricata, which is a state-of-the-art high-performance NIDS, and Wazuh, an SIEM system, are combined in order to make a real-time network threat monitoring and response system. Suricata is used to scan network traffic, identify anomalies, and detect threats like DDoS attacks, brute-force login attempts, and malware activity, while Wazuh gathers and aggregates security logs, with centralized threat intelligence and forensic analysis. The system augments security with custom detection rules, automated incident response systems, and real-time visualization dashboards. Through extensive testing with simulated cyberattacks, the project measures detection precision, reaction time, and system performance. This cost- and scalable solution enhances network security, reduces false positives, and gives organizations proactive cybersecurity control.

KEYWORDS: Intrusion Detection System (IDS), Suricata, Wazuh, Network Security, SIEM (Security Information and Event Management), Real-time Monitoring, Threat Detection, Anomaly Detection, DDoS Attack Prevention, Brute-force Attack Detection, Malware Analysis, Security Logs Aggregation, Threat Intelligence, Forensic Analysis, Custom Detection Rules, Automated Incident Response, Visualization Dashboards, Cyberattack Simulation, False Positive Reduction, Scalable Security Solutions

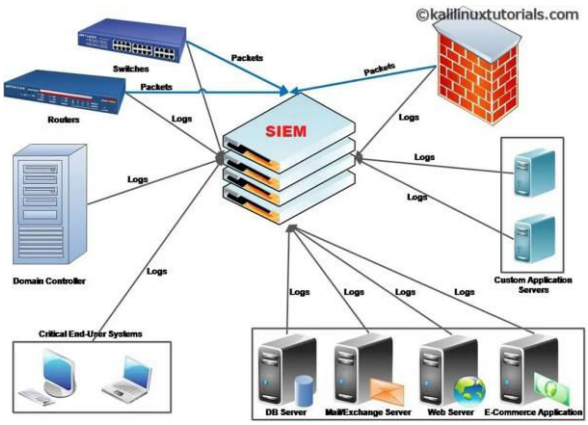


Fig 1:SIEM (Security Information and Event Management)

I. INTRODUCTION

Cyber attacks have been becoming increasingly sophisticated, leading security teams to implement Intrusion Detection and Prevention Systems (IDPS) to detect and respond to attacks in real time. Several Network Intrusion Detection

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

Systems (NIDS) have emerged, with Suricata leading the pack due to its high-speed packet inspection, anomaly detection, and multi-threading. Suricata trials against some other tools like Snort and Zeek accentuate the depth and scalability in protocol analysis that Suricata presents and has rendered it an exceptionally effective threat-detecting tool covering DDoS attacks, brute-force events, as well as malware traffic.Conversely, Security Information and Event Management (SIEM) products have gained popularity due to their ability to gather security logs, cross-correlate events, and offer real-time threat intelligence. Of numerous SIEM products, Wazuh is widely used as it's open-source by nature, can be combined with Elastic Stack (ELK), and possesses robust forensic capabilities.Comparative studies on Wazuh, Splunk, and AlienVault indicate that open-source tools offer economical monitoring without sacrificing enterprise-grade security functionalities.

Some investigations have investigated how combining NIDS and SIEM improves threat visibility and accelerates incident response. Experiments on Snort-Splunk and Zeek-ELK integrations show the advantages of correlating network-based detection with centralized log analysis to minimize false positives and enhance forensic analysis. Most of these solutions address passive monitoring instead of real-time automated response mechanisms.This project addresses this gap through the integration of Suricata and Wazuh to establish an active, real-time intrusion detection and response system. The solution differs from prior work as it focuses on bespoke rule engineering, automated mitigation of threats, and real-time visualization dashboards to enhance accuracy of detection as well as instantaneous response. It is tested for its performance with emulated cyberattacks to validate its performance, detection accuracy, and false positive levels, enabling a scalable as well as variable security framework to meet the standards of contemporary networks.

II. LITERATURE REVIEW

With the increasing sophistication of cyberattacks, security teams are adopting Intrusion Detection and Prevention Systems (IDPS) to detect and respond to threats in real-time. Various Network Intrusion Detection Systems (NIDS) have emerged, with Suricata standing out due to its high-speed packet inspection, anomaly detection, and multi-threading capabilities. Comparative analyses with other tools like Snort and Zeek highlight Suricata's superior scalability and deep protocol analysis, making it an effective tool for detecting threats such as DDoS attacks, brute-force attempts, and malware traffic.

On the other hand, Security Information and Event Management (SIEM) solutions have gained traction for their ability to aggregate security logs, correlate events, and provide real-time threat intelligence. Among the widely used SIEM tools, Wazuh stands out due to its open-source nature, seamless integration with the Elastic Stack (ELK), and advanced forensic capabilities. Comparative studies involving Wazuh, Splunk, and AlienVault indicate that open-source solutions offer cost-effective security monitoring without compromising enterprise-grade functionalities.

Several research studies have explored how combining NIDS with SIEM enhances security visibility and incident response. Experiments on Snort-Splunk and Zeek-ELK integrations demonstrate the advantages of correlating network-based threat detection with centralized log analysis, leading to a reduction in false positives and improved forensic capabilities. However, most of these solutions primarily focus on passive monitoring rather than real-time automated response mechanisms.

III. METHODOLOGY

Integrating Suricata with Wazuh for Enhanced Network Security
Integrating Suricata with Wazuh enhances network security by combining Suricata's intrusion detection capabilities with Wazuh's security information and event management features. This integration enables real-time monitoring, detection, and response to network threats. Below is a methodology to achieve this integration:

1. Infrastructure Setup
Wazuh Server: Deploy a Wazuh server to collect and analyze security data.
Endpoint Installation: Install the Wazuh agent on the endpoint where Suricata will be deployed

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

2. Suricata Installation and Configuration

Install Suricata:

On the chosen endpoint, install Suricata. For example, on Ubuntu:

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
```

Configure Suricata:

Download and extract the Emerging Threats ruleset:

```
cd /tmp/
curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz
sudo mkdir /etc/suricata/rules
sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```

Modify the Suricata configuration file (/etc/suricata/suricata.yaml):

Set HOME_NET to the IP address range of your internal network.

Identify the network interface to capture under the af-packet section.15

3. Wazuh Agent Configuration

Start Suricata:

Enable and start the Suricata service:

```
sudo systemctl enable suricata
sudo systemctl start suricata
```

Log Monitoring Setup:

Configure the Wazuh agent to monitor Suricata logs by adding the following to /var/ossec/etc/ossec.conf:

```
<localfile>
<log_format>json</log_format>
<location>/var/log/suricata/eve.json</location>
</localfile>
```

Restart Wazuh Agent:

Apply the changes by restarting the agent:

```
sudo systemctl restart wazuh-agent17
```

4. Active Response Configuration

Enable Active Response:

In the Wazuh manager's configuration (/var/ossec/etc/ossec.conf), define an active response for Suricata alerts:

```
<active-response>
<command>firewall-drop</command>
<location>agent</location>
<rules_id>201093,201094</rules_id>
<timeout>600</timeout>
</active-response>18
```

5. Testing and Validation

Simulate Attacks:

Use tools like nmap or hping3 to generate network traffic that triggers Suricata alerts.

Monitor Responses:

Verify that Wazuh receives Suricata alerts and executes the appropriate active responses, such as blocking offending IPs.

command: Specifies the action to execute (firewall-drop blocks the offending IP).

location: Determines where the action is executed (agent runs on the endpoint).

rules_id: Lists the Suricata rule IDs that trigger the response.

timeout: Duration (in seconds) the block remains active.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

Restart Wazuh Manager:
Apply the configuration changes:
sudo systemctl restart wazuh-manager

IV. RESULTS AND CONCLUSION

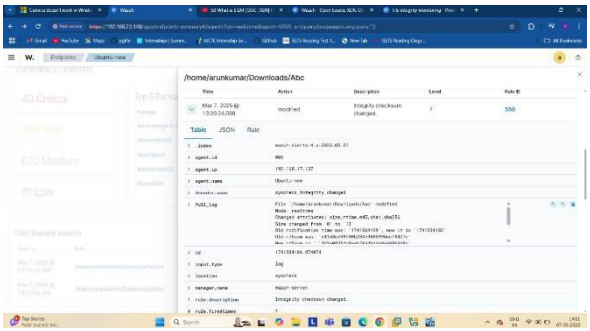


Fig 2:Network Threat Detection Dashboard

Network Threat Detection Dashboard – A real-time security dashboard showing detected threats, alerts, and logs.
Suricata Traffic Analysis – A graphical representation of Suricata analyzing network packets and identifying anomalies.
Wazuh SIEM Log Correlation – A log aggregation and correlation dashboard displaying security events and alerts.

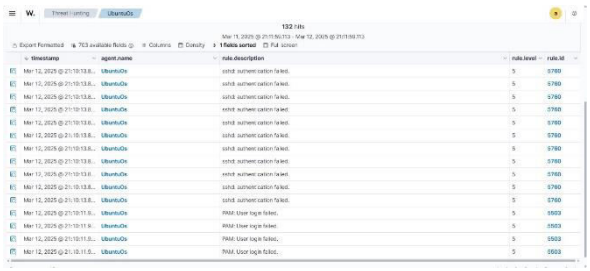


Fig 3. Brute Force Attack

Brute Force Attack on SSH Service – A server under attack, with Suricata detecting multiple failed SSH login attempts from various IPs and blocking suspicious sources to prevent unauthorized access.

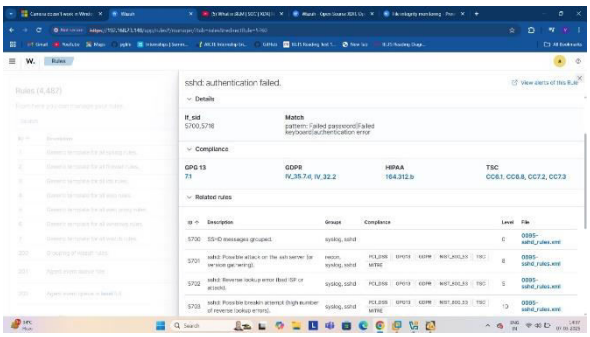


Fig 4: Log Analysis

Automated Incident Response Flow – A flowchart depicting how detected threats trigger automated security actions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

V. LIMITATIONS AND FUTURE WORK

5.1 Limitations

Despite the effectiveness of integrating Suricata with Wazuh for real-time intrusion detection and incident response, there are certain limitations to this approach

High False Positives:
Anomaly-based detection techniques can generate false positives, leading to unnecessary alerts and administrative overhead.
Fine-tuning of Suricata rules and Wazuh correlation logic is required to reduce false positives.

Performance Overhead:
Processing large volumes of network traffic in real time can impact system performance, especially in high-traffic environments.
Running Suricata alongside Wazuh and Elasticsearch may require significant computational resources.

Limited Automated Mitigation:
While Wazuh's active response can block malicious IPs and update firewall rules, it lacks advanced countermeasures such as automated rollback of system changes post-attack.
More complex threat response actions require external integrations with Security Orchestration, Automation, and Response (SOAR) platforms.

Dependency on Signature-Based Detection:
Suricata's core detection relies on predefined rule sets, making it less effective in identifying zero-day attacks and unknown malware.
Incorporating AI/ML-based behavioral analysis could enhance threat detection capabilities.

Scalability Challenges:
Deploying Suricata and Wazuh in large-scale networks with high-speed traffic requires optimized configurations and distributed architectures to prevent bottlenecks.
Horizontal scaling strategies must be implemented to handle growing data loads effectively.

5.2 Future Work

To address these limitations, future research and enhancements can focus on:

Integration with AI/ML for Advanced Threat Detection:
Implementing machine learning-based anomaly detection to complement signature-based IDS.
Training models on network behavior to detect emerging threats with minimal false positives.

Enhancing Automated Incident Response:
Expanding Wazuh's active response with automated playbooks for remediation actions (e.g., isolating compromised hosts, rolling back unauthorized changes).
Integrating with SOAR platforms for faster and more dynamic threat mitigation.

Optimizing Performance for High-Traffic Networks:
Implementing load balancing and distributed deployments for Suricata and Wazuh to support large-scale environments.
Exploring hardware acceleration techniques like FPGA and GPU-based packet processing to improve real-time analysis.

Threat Intelligence Integration:
Incorporating threat intelligence feeds (MITRE ATT&CK, STIX/TAXII) into Wazuh for proactive threat detection.
Automating threat hunting workflows to analyze emerging attack patterns and minimize risks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404070|

REFERENCES

[1] A. Santoyo-González, C. Cervelló-Pastor, D.P. Pezaros, “High-performance, platform-independent DDoS detection for IoT ecosystems,” 2019 IEEE 44th Conference on Local Computer Networks (LCN)

[2] Debnath, “LogLens: A Real-Time Log Analysis System”, 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)

[3] D. Panda, B.K. Mishra, K. Sharma, “A Taxonomy on Man_x0002_in-the-Middle Attack in IoT Network,” 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022

[4] G.R. Andreica, G.L. Tabacar, D. Zinca, I.A. Ivanciu, V. Dobrota, “Denial of Service Attack Prevention and Mitigation for Secure Access in IoT GPS-based Intelligent Transportation Systems”, Electronics 2024, 13(14), 2693.

[5] He, J. Zhu, S. He, J. Li, M.R. Lyu, "Towards Automated Log Parsing for Large Scale Log Data Analysis", IEEE Transactions on Dependable and Secure Computing, volume 15, p. 931–944, December 2018.

[6] M. Won, "Intelligent Traffic Monitoring Systems for Vehicle Classification: A Survey," in IEEE Access, vol. 8, pp. 73340-73358, 2020.

[7] R. K. Shrivastava, S. Mishra, V.E. Archana, C. Hota, “Preventing data tampering in IoT networks,” 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), December 19, 2019,

[8] Suricata IDS/IPS, Suricata, 2024, [Online]. Available: https://suricata.io/ [Accessed: March 10, 2024].

[9] S. Sudharsan, S.S. Sathya, “A Comparative Analysis of IoT Security Threats and Mitigation Techniques,” International Journal of Advanced Science and Technology, vol. 28, no. 10, pp. 224–231, 2019.

[10] Wazuh SIEM, Wazuh, 2024, [Online]. Available:https://wazuh.com/platform/siem/ [Accessed: February 22, 2024].

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details