Journal of
Open Source Developments

ISSN: 2395-6704
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoOSD

https://journals.stmjournals.com/joosd

Review JoOSD

AI-driven Cybersecurity: Enhancing System Resilience with Advance Security Automation Program (ASAP)

Garima Sharma[1,*], Ram Narayan[2]

Abstract

In the face of increasing cyber threats, this work presents advanced security automation program (ASAP) a revolutionary solution aimed at addressing modern cyber threats through the utilization of artificial intelligence (AI) and open-source technologies. Unlike conventional security systems like security information and event management (SIEM) and security operations center (SOC), ASAP provides automated defense mechanisms that surpass their limitations by significantly increasing both the speed and accuracy of incident detection by 50% to 90% and incident response efficiency by 30% to 70% holistically at no cost. By democratizing cybersecurity, ASAP enables organizations of all sizes and even individual systems to access robust protection without relying on expensive proprietary solutions. By integrating open-source tools and AI, ASAP enhances threat detection, simplifies incident response, and bolsters overall cybersecurity. The paper encourages collaboration by sharing not only ASAP's architecture but also development insights with the open-source community. By adopting ASAP, organizations can proactively strengthen their defenses, mitigate cyber risks and ensure operational continuity in the face of ever-evolving cyber threat. Our study not only contributes to the field by proposing ASAP but also identifies promising areas for future research such as integrating explainable AI techniques to increase user trust and understanding of ASAP's decision-making processes.

Keywords: Cyber-resilience, open-source technologies, advance security automation program (ASAP), security information and event management (SIEM), security operations center (SOC)

INTRODUCTION

In recent years, the world has witnessed a dramatic rise in cyber-attacks, presenting substantial challenges to individuals, businesses, governments, and critical infrastructure globally. Traditional cybersecurity measures like antivirus software and firewalls are struggling to keep pace with the increasingly sophisticated nature of these attacks. Furthermore, as organizations transition towards cloud-based services and integrate more devices into their operations, the need for robust defense mechanisms has become more urgent. However, this shift to cloud environments also widens the attack surface, leaving systems vulnerable to exploitation by cybercriminals. While there are options available, such as investing in powerful and expensive equipment or deploying real-time threat detection software, these solutions often come with their own set of limitations and resource requirements.

To address these pressing challenges, innovative approaches are emerging, among which is the advanced security automation program (ASAP). This groundbreaking solution leverages the capabilities of artificial intelligence (AI) and open-source technologies to deliver comprehensive, automated security measures. By democratizing cybersecurity, ASAP empowers organizations of all sizes with strong protection, eliminating the need for costly proprietary solutions.

***Author for Correspondence**
Garima Sharma
E-mail: garimasharma@ncuindia.edu

[1]Assistant Professor, Department of Computer Science and Engineering, The NorthCap University, Haryana, India
[2]Student, Department of Computer Science and Engineering, The NorthCap University, Haryana, India

Received Date: April 09, 2024
Accepted Date: April 26, 2024
Published Date: June 29, 2024

Citation: Garima Sharma, Ram Narayan. AI-driven Cybersecurity: Enhancing System Resilience with Advance Security Automation Program (ASAP). Journal of Open Source Developments. 2024; 11(2): 1–19p.

This study seeks to delve into the landscape of cybersecurity incident response and adaptation in light of evolving threats. Its primary goal is to develop a system capable of identifying critical assets, detecting potential cyber-attacks, assessing their impact, and formulating mitigation strategies to ensure uninterrupted business operations. Through a detailed methodology involving the analysis of existing security tools, the framework and implementation of a customized security system and an evaluation of its effectiveness, this paper aims to contribute to the advancement of cybersecurity practices. Moreover, this study will explore the emerging trend of security operations centers (SOCs), which offer an ideal approach to cybersecurity encompassing detection, investigation, response and prevention to threats.

While traditionally accessible only to large enterprises due to their high costs, ASAP presents a viable alternative for organizations with limited resources, promising enhanced security posture, greater control over attack surfaces, and expedited deployment times at a more affordable price point. By investigating these innovative cybersecurity approaches, this study seeks to provide valuable insights and practical recommendations for organizations aiming to strengthen their defenses and adapt to the ever-evolving threat landscape.

LITERATURE REVIEW

Present Intrusion Detection System Technologies

In the landscape of cybersecurity, intrusion detection systems (IDSs) play an important role in defending networks against evolving threats. These systems come in various forms: network intrusion detection systems (NIDSs) monitor network traffic across multiple locations, host intrusion detection systems (HIDSs) provide insight into system activity on personal computers or servers, and cloud intrusion detection systems (CIDSs) bolster network security within cloud environments. IDSs employ diverse detection techniques such as anomaly-based detection which analyses deviations from usual behavior, signature-based detection which compares network traffic against known attack patterns and stateful protocol analysis, which identifies potentially malicious command sequences. However, traditional IDS methods have limitations including false alarms, performance impacts, and the need for specialized expertise for configuration [1, 2].

In assessing IDS tools, several criteria are crucial. These include robust log gathering and management services, comprehensive log analysis systems equipped with pre-written tools for intruder detection, live network monitors capable of identifying anomalous activities, threat hunting capabilities for alerting on suspicious behavior, triage processes focusing on well-known intrusion actions, and offerings such as free trials or money-back guarantees for risk-free evaluations.

Present Incident Response System Technologies

Incident response systems (IRSs) are crucial components of cybersecurity infrastructure, offering a structured approach to identify, contain, eradicate, and recover from security incidents. These systems feature common functionalities such as continuous monitoring, alerting, investigation support, containment tools, remediation capabilities, and reporting functionalities. The IRS process encompasses several steps, including preparedness to establish response plans, detection to identify incidents, control to contain the situation, elimination to eradicate vulnerabilities, recovery to restore operations, investigation for root cause analysis, and continuous improvement for ongoing enhancement of security practices.

In evaluating IRS tools, key criteria include seamless integration from detection to resolution systems, integration with access rights managers and firewalls, customizable action rules, extensive action logging, provision of live status reports, availability of free trials or demo options for risk-free evaluation and value for money represented by automated systems at reasonable prices. Among the notable frameworks for incident response are System and Organization Controls, National Institute of Standards and Technology (NIST), and ISO 27001, each offering guidelines and best practices for effective incident management.

Challenges in Present IDS and IRS

On the basis of comparison made of various IDS and IRS technologies as shown in Table 1, there are significant challenges for IDS and IRS. These barriers include limited cost-effective outsourcing options, hindrances in log collection and analysis, reliance on signature-based detection leading to vulnerability against zero-day threats, lack of deployment flexibility, global skill shortage in cybersecurity, integration obstacles, regulatory compliance burdens, and the dynamic nature of the threat landscape [3].

Addressing these challenges is paramount to establishing a resilient security framework capable of effectively mitigating evolving cyber threats. Collaboration among stakeholders, continuous improvement of systems and processes, and a proactive approach to cybersecurity are essential for navigating the complexities of the current IDS and IRS landscape.

Optimal Improved Solution

Building an optimal integrated incident response (IR) model involves leveraging pervasive intelligence to navigate the complexities of the cybersecurity landscape. This analysis explores key features and their impact on cyber security, presenting the best solution for each aspect. Key functionalities of the proposed model should include hybrid security information and event management (SIEM)/security orchestration, automation, and response (SOAR) functionality that integrates log management and analysis with automated response capabilities. Real-time monitoring uses both SIEM and IDS software for immediate threat identification, promoting a proactive approach to reducing the impact of threats. Automated remediation and remediation mechanisms, along with comprehensive log collection and management, ensure rapid response and proactive risk mitigation. Advanced anomaly detection and tracking will further enhance threat identification capabilities. Integration and adaptability are critical to the model's effectiveness, with seamless integration ensuring compatibility with existing tools and scalability across different environments. Cost-effectiveness is achieved through outsourcing and open-source options, while cloud integration provides flexibility and resilience. Advanced capabilities

Table 1. Comparison among present intrusion detection system (IDS)/incident response system (IRS) technologies.

Feature	AlienVault	LogRhythm	Rapif 7 Insight IDR	Wazuh	Snort	Suricata	OpenVAS
Pros	- All-in-one solution	- Advanced analytics, AI-powered threat detection	- Real-time threat detection, endpoint visibility	- Open-source, customizable, advanced threat detection	- Open-source, fast installation	- High-speed network detection, open-source	- Open-source customizable
Cons	- Can be complex to set up and manage	- Can be expensive for large deployments	- Subscription model can be costly	- Resource intensive	- Limited visibility into encrypted traffic	- May require specific expertise to manage	- Requires manual effort for vulnerability assessment
Monitoring	- Real-time	- Comprehensive	- Security events and endpoints	- Real-time	- Network traffic	- Network traffic	- Vulnerability scanning
Type	Security information and event management (SIEM)	SIEM	SIEM	SIEM	Intrusion prevention system (IPS)	IPS	Vulnerability scanner
Deployment	On-device, cloud, hybrid	On-device, cloud	On-device, cloud	On-device, cloud	On-device	On-device, cloud	On-device, cloud
Focus	Threat detection and response	Threat detection and response	Threat detection and response	Security monitoring and analysis	Intrusion detection and prevention	Intrusion detection and prevention	Vulnerability assessment
Pricing	Free trial, paid plans	Free trial, paid plans	Free trial, paid plans	Free and commercial	Free, paid support	Free, paid support	Free, paid support

such as AI-powered threat detection and automated deployment increase response effectiveness, while adaptive response strategies ensure dynamic adjustments based on evolving attack patterns. System independence and security measures reduce the risks of breaches and maintain trust. Operational efficiency is prioritized through computational efficiency and user-friendly configuration, reducing complexity and optimizing resource allocation.

Finally, incorporating these features into a unified IR model empowers organizations to establish a robust incident response framework. This comprehensive approach effectively addresses evolving cybersecurity threats, optimizes resources and increases operational efficiency, enabling proactive defense against cyber adversaries in an increasingly complex threat landscape. So, the technologies selected to create the optimal framework is concluded on these results.

1. *Security information and event management (SIEM):* In 2022, Wazuh was chosen due to its open-source nature, affordability, centralized architecture, extensive rule sets, and cloud support, making it ideal for organizations seeking cost-effective SIEM solutions.
2. *Intrusion detection system/intrusion prevention system):* In previous years, Suricata was selected for its open-source nature, multi-threading capabilities, hardware acceleration, and extensive Wazuh integration documentation.
3. *Endpoint protection:* Wazuh's SIEM capabilities extend to extended detection and response (XDR), offering real-time correlation, threat detection, and on-device remediation, making it a cost-effective choice for comprehensive endpoint protection.

In summary, Wazuh and Suricata provide strong open-source security solutions for organizations seeking cost-effective SIEM, IDS/IPS, and endpoint protection capabilities [4–6].

STATE OF THE ART

ELK (Elasticsearch, Logstash, Kibana) Stack

1. *Elasticsearch*: It is a distributed, RESTful search and analytics engine constructed on Apache Lucene [7]. Renowned for its scalability, real-time processing, and ability to swiftly search and analyze extensive datasets, it offers potent full-text search functionalities, accommodates intricate queries, and facilitates aggregation for analytical purposes [4].
2. *Logstash:* An open-source data processing pipeline that concurrently collects, processes, and ingests data from multiple sources [8]. It parses and transforms data from various formats and sources, including logs, metrics, and other structured or unstructured data, before forwarding it to Elasticsearch or other designated destinations.
3. *Kibana*: A web-based data exploration and visualization tool seamlessly compatible with Elasticsearch [9]. It offers a user-friendly interface for crafting custom dashboards, visualizations, and reports to analyze and interact with data housed in Elasticsearch indexes. Supporting various visualization types, including charts, maps, and more, it enhances the capability to explore and understand data effectively.

Wazuh

It is an open-source security management platform designed to aid organizations in detecting and responding to security threats promptly. It comprises agents deployed on endpoints to gather security-related data and a central management server for processing and analyzing this information. Wazuh caters to a range of security use cases, such as file integrity monitoring, log analysis, intrusion detection, and compliance auditing.

Suricata

Open-source NIDS and IPS [10]. It performs on-time packet logging and traffic analysis on internet protocol (IP) networks. Suricata is capable of detecting and preventing a wide range of threats, including exploits, intrusion attempts, malware, and other suspicious activities, by inspecting network traffic against predefined rule sets.

Beats

Beats are lightweight data shippers or agents developed by Elastic [11, 12]. They are developed in a way to collect different types of data from servers, systems, and applications after that they send it to Elasticsearch or Logstash for analysis and visualization in Kibana. Beats come in different flavors tailored to specific data types, such as Filebeat for logs, Metricbeat for metrics, Packetbeat for network data, and Heartbeat for uptime monitoring.

Elastalert

Open-source framework using anomaly detection patterns for alerting of interest in data stored in Elasticsearch. It integrates seamlessly with Elastic-search and provides a flexible rule-based alerting mechanism. Users can define rules based (playbooks) on queries or metrics and specify alert actions, such as notifying via email or other channels, when matches occur.

Open Distro for Elasticsearch

It is a community-driven, open-source distribution of Elasticsearch enhanced with additional security features, alerting capabilities, and other enhancements. It includes plugins such as Open Distro Security, which provides authentication, authorization, encryption, and auditing features, and Open Distro Alerting, which enables users to create and manage alerts based on Elasticsearch data [13].

Praeco

An open-source alerting tool for Elasticsearch. Praeco offers a graphical user interface for managing and creating alerts utilizing Elastalert. It simplifies the alert configuration process by providing a query builder interface and supports multiple notification channels such as Slack, Email, Telegram, and HTTP endpoints.

Nessus Essentials

This is a very famous and free vulnerability scanner which enables organizations to identify and prioritize security vulnerabilities in the networks and systems. It facilitates comprehensive vulnerability assessments, including malware detection, configuration audits and web app scanning to help organizations remediate security risks and improve their overall security posture.

TheHive

It is an open-source Security Incident Response Platform (SIRP) designed to aid SOC teams in efficiently managing and responding to security incidents. It offers features for alert triage, case management, evidence gathering, collaboration, and reporting, enabling analysts to streamline and automate incident response processes.

Cortex

Open-source threat intelligence platform that integrates seamlessly with TheHive for data enrichment and analysis. It allows users to automate the enrichment of observables (e.g., IP addresses, domains, URLs) by querying external services and correlating indicators of compromise (IOCs) from various sources to enhance incident response capabilities.

Malware Information Sharing Platform (MISP)

It is an open-source threat intelligence platform specifically crafted for collaborating, correlating indicators of compromise (IOCs) [14], and managing relationships with malware and cyber threats. It serves as a centralized platform for cybersecurity professionals and organizations to share and analyze threat intelligence data, fostering collaboration and enhancing cybersecurity efforts.

VulnWhisperer

It is a vulnerability data aggregation and correlation tool that integrates with Elasticsearch and Wazuh. It helps organizations manage and prioritize vulnerabilities by collection and correlation of vulnerability data from multiple sources and points such as vulnerability scanners, threat intelligence feeds, and public databases.

Cloud-based Security Operation Center (SOC) as a Service

A cloud-based SOC as a service is a managed security service offering that provides organizations with comprehensive threat detection, incident response, security monitoring, and security analytics capabilities hosted in the cloud. It allows organizations to outsource their security operations to a third-party vendor or managed security service provider (MSSP) and leverage their expertise and infrastructure to enhance their security posture [7].

Virtual Private Network (VPN) Tunnel

A secure VPN tunnel established to transmit data securely from Wazuh agents and Beats to central processing components. It encrypts the data transmitted over the internet or untrusted networks, ensuring confidentiality and integrity.

PROPOSED SYSTEM

Figure 1 depicts the ASAP model, which appears to be a solution designed to handle various aspects of cyber security. It includes features like log retention, analysis, monitoring, alert generation, report generation, IOC enrichment and incident response management [3]. This model potentially serves as a comprehensive framework for managing cyber security incidents effectively and efficiently.

In the initial phase of building a robust security information foundation, the focus lies on collecting logs and security events from diverse sources across the network. This involves deploying agents such as Beats and Wazuh on hosts and network devices to gather critical data, which is securely transmitted to a central location, often through a VPN tunnel. Logstash serves as a central pipeline, receiving logs from various sources and performing essential tasks such as parsing them into a standardized format and enriching them with relevant metadata for better context. Once processed, the data is forwarded to Elasticsearch, which acts as an effective search and analytics engine. Elasticsearch efficiently indexes the security data received from Logstash, optimizing storage and enabling rapid retrieval. Security teams can leverage Elasticsearch's robust search capabilities to investigate potential security incidents and analyses historical data to identify trends and patterns.

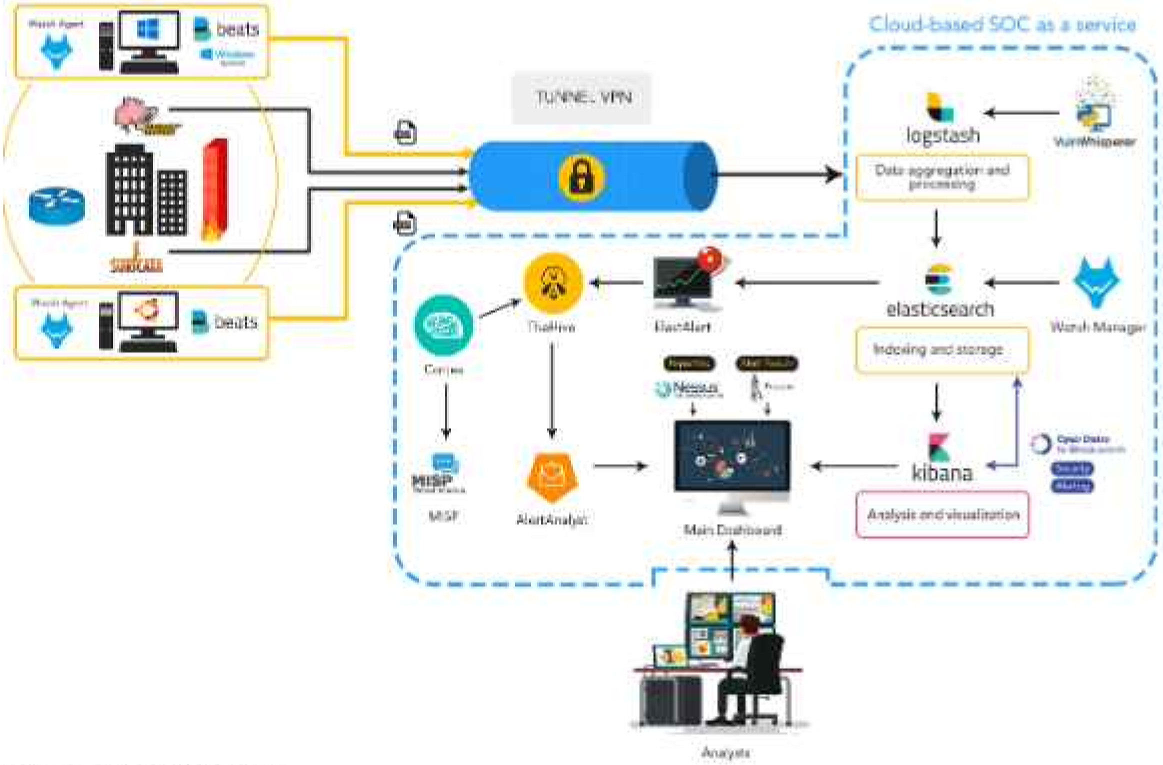


Figure 1. Model outline.

On top of Elasticsearch sits Kibana, a data visualization platform that provides user-friendly dashboards and visualizations transforming raw data into clear and actionable insights. Security analysts can utilize Kibana to identify anomalies, investigate suspicious activities, and monitor the overall security health of the system. Elastalert, a rule-based alerting engine, plays a crucial role in proactive threat detection by continuously monitoring the data within Elasticsearch for pre-defined IOCs or suspicious activity patterns. Upon detecting a potential threat, Elastalert generates security alerts within TheHive, a SIEM platform.

The ASAP model goes beyond traditional SIEM solutions by incorporating automation for faster and more efficient incident response. Within TheHive, workflows can be configured to automatically enrich cases with additional context, involving querying external threat intelligence platforms like cortex analyzers and MISP for relevant information. This can lead to either automated resolution of low-risk incidents or escalation to security analysts for further investigation. While technology plays a pivotal role in the ASAP model, human expertise remains the final line of defense. Security analysts claim and investigate escalated alerts within TheHive, leveraging enriched context from cortex analyzers and MISP to make knowledgeable decisions and take actions accordingly. The ASAP model fosters collaboration among analysts, enabling them to share knowledge and collaborate on incident response activities, ensuring a comprehensive and effective security posture. By collaborating use of open-source technologies ELK stack, cortex analyzers, TheHive, and MISP, the ASAP model offers a compelling alternative to expensive, traditional SIEM solutions, empowering organizations to automate essential security tasks, streamline incident response, and strengthen their overall cybersecurity posture.

Working

This hybrid security model ASAP leverages open-source tools to achieve comprehensive incident detection and response IDS and IRS across on-premises and cloud environments as shown in Figure 2.

On-premises Data Collection

1. *Wazuh Agent:* Installed on devices like servers and workstations, it actively collects logs and security data, including file integrity monitoring (FIM) data and system configuration information.
2. *Filebeat:* It captures logs from file systems, such as application logs, system logs, and other log files generated by various software applications.
3. *Winlogbeat:* Specifically designed for Windows systems, it captures Windows event logs, including security, application, and system logs.
4. *Auditbeat (optional component):* It collects supplementary audit logs to offer a broader perspective on system activities, covering areas like user authentication, file access, and system calls.
5. *Suricata:* It focuses on monitoring network traffic to detect potential malicious activities such as intrusion attempts, exploits, malware infections, and various other security threats.

Data Transfer (Secure)

All collected data is transmitted through a secure VPN tunnel to assure that sensitive information is safe during transfer over untrusted networks or the internet.

Cloud Data Collection (If Applicable)

Cloud agent: If deployed, collects logs and security data directly from cloud resources, such as virtual machines (VMs) and containers running in cloud environments like Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP).

Data Pre-processing and Enrichment

Logstash: Acts as a central processing hub, receiving data from all on-premises and cloud sources. It performs various tasks like parsing, filtering, and enriching the collected data to standardize formats and add additional context before storing it in Elasticsearch.

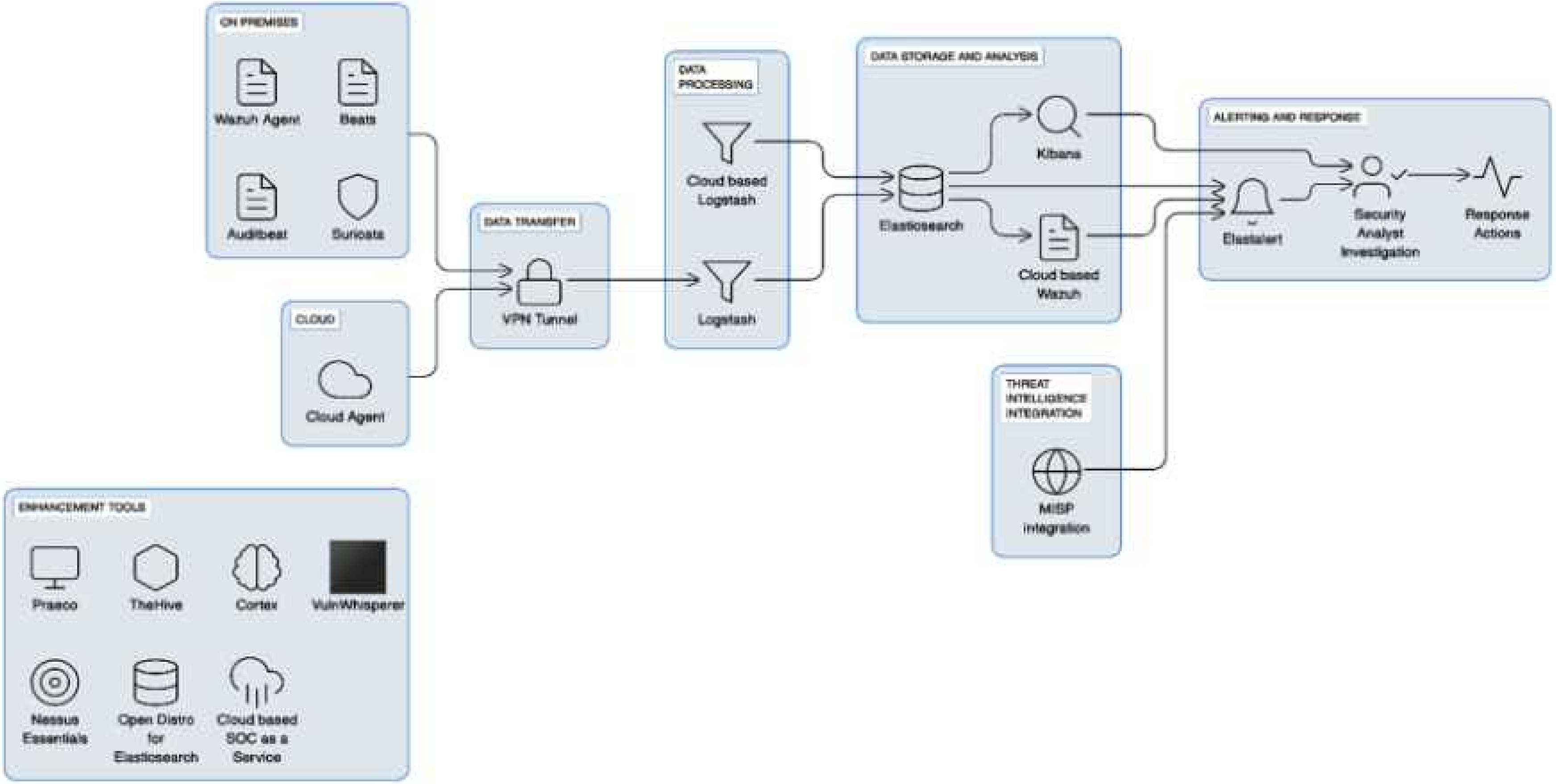


Figure 2. ASAP security management working stack.

Data Storage and Analysis

1. *Elasticsearch:* It serves as the central data store for indexing and storing all security-related data from both on-premises and cloud environments. It provides very efficient search and effective analytics capabilities, allowing security analysts to perform complex queries and analysis on the stored data.
2. *Kibana:* It facilitates user-friendly UI for visualizing, investigating, and analyzing the security data saved in Elasticsearch. It enables security analysts to create self-designed dashboards, visualizations, and reports generation to gain insights into security events and incidents.

Alerting and Response

1. *Elastalert:* It monitors the security data within Elasticsearch for anomalies, spikes, or other suspicious patterns that may indicate potential security incidents. It triggers alerts when such patterns are detected and sends them to security analysts for further investigation.
2. Upon receiving alerts, security analysts use Kibana to investigate potential security incidents, analyze the data, and take appropriate response actions, such as isolating compromised systems, remediating vulnerabilities, and implementing containment measures.

Threat Intelligence Integration (Optional)

MISP integration facilitates collaboration and sharing of threat intelligence data with trusted partners and sources. It enriches the analysis by providing additional context about known threats, IOCs, and attack patterns. This enhances the detection and response capabilities of the security system.

ASAP offers a robust and cost-effective approach to security management across your on-premises and cloud infrastructure. By leveraging open-source tools and employing a well-defined data flow with centralized security analysis and alerting, you can notably improve the incident detection and response capabilities.

IMPLEMENTATION

To implement this ASAP model, following steps must be followed.

On-premises Data Collection

- Deploy *Wazuh Agent* on endpoints for system monitoring and log collection.
- Deploy *Beats (Filebeat, Winlogbeat)* on key servers for centralized log collection.

Deploying Wazuh Agent

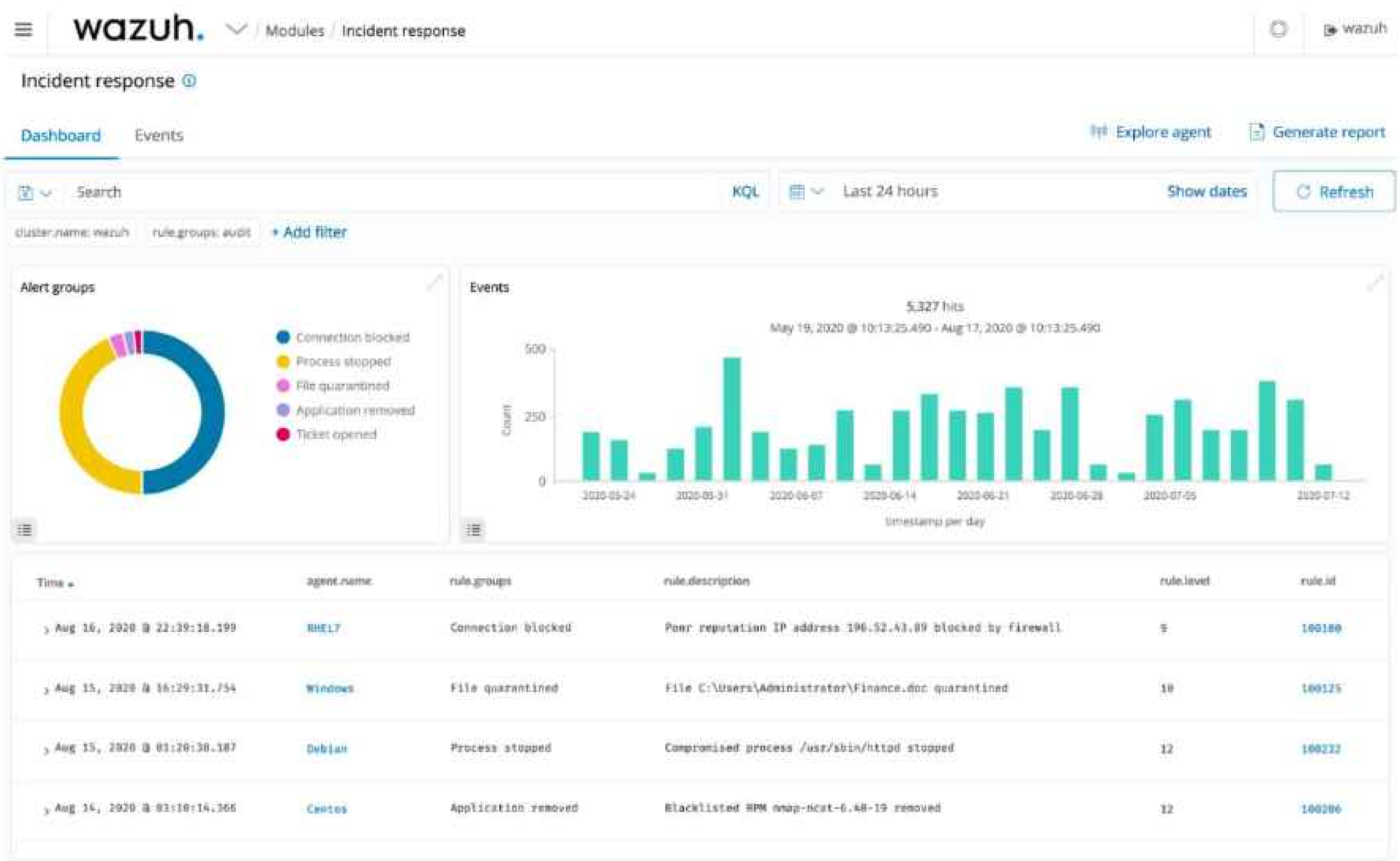
- Download the Wazuh Agent installer for your operating system from the official website or repository.
- Follow the installation instructions provided for your operating system (OS).
- Configure the Wazuh Agent to point to your Wazuh manager or manager IP address for centralized management and monitoring.
- Start the Wazuh Agent service.

Deploying Beats (Filebeat, Winlogbeat)

- Download the Filebeat and Winlogbeat installers for your operating system from the official Elastic website or repository.
- Follow the installation instructions provided for your OS.
- Configure *Suricata* for network traffic monitoring and security event generation.
- Set up an on-premises *Logstash* instance to receive and pre-process data from Wazuh Agent, Beats, and Suricata.
- (Optional) Consider adding Auditbeat for collecting additional audit logs from your systems.

Default Wazuh interface is shown in Figure 3.

- Configure Filebeat and Winlogbeat to point to your Logstash instance for centralized log collection.
- Start the Filebeat and Winlogbeat services.



Time	agent.name	rule.groups	rule.description	rule.level	rule.id
Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	5	100180
Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100232
Aug 14, 2020 @ 03:18:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100286

Figure 3. Wazuh interface.

Configuring Suricata

- Install Suricata on your server or network appliance. The installation process may vary depending on your OS.
- Configure Suricata to monitor network traffic on your network interfaces and generate security events.
- Customise Suricata rulesets according to your network security requirements.
- Start the Suricata service.

Setting up Logstash

- Download and install Logstash on a central server that has network connectivity to the endpoints, servers, and Suricata instance.
- Create Logstash configuration files (logstash.conf) for processing data from Wazuh Agent, Filebeat, Winlogbeat, and Suricata.
- Configure input plugins to listen for data from various sources (Beats, Wazuh, Suricata).
- Configure filter plugins to parse, enrich, and manipulate the incoming logs as needed.
- Configure output plugins to send the processed data to Elasticsearch for indexing.
- Start the Logstash service.

Optional: Adding Auditbeat

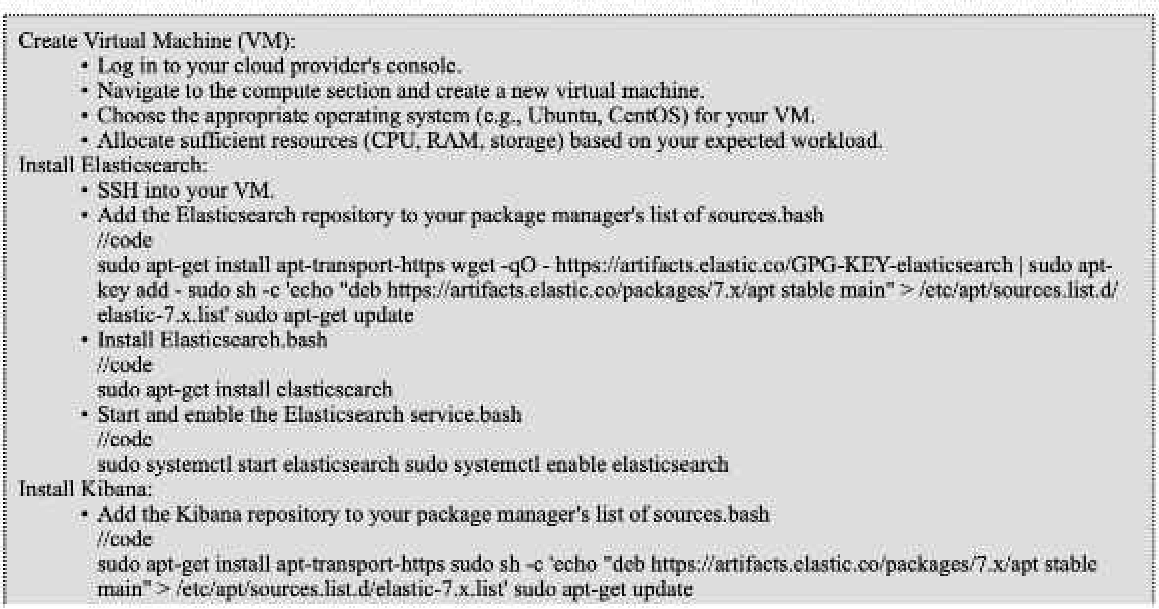
- Download the Auditbeat installer for your operating system from the official Elastic website or repository.
- Follow the installation instructions provided for your OS.
- Configure Auditbeat to collect additional audit logs from your systems.
- Configure Auditbeat to send the collected audit logs to Logstash or Elasticsearch.
- Start the Auditbeat service.

Cloud Data Collection (Optional)

1 Deploy *Wazuh Cloud Agent* on cloud resources to collect logs and security data.
2 Forward data from the Cloud Agent to a cloud-based SIEM platform.

ELK Stack Deployment

1. Install and configure the ELK (Elasticsearch, Logstash, Kibana) stack in your chosen cloud environment.



Create Virtual Machine (VM):

- Log in to your cloud provider's console.
- Navigate to the compute section and create a new virtual machine.
- Choose the appropriate operating system (e.g., Ubuntu, CentOS) for your VM.
- Allocate sufficient resources (CPU, RAM, storage) based on your expected workload.

Install Elasticsearch:

- SSH into your VM.
- Add the Elasticsearch repository to your package manager's list of sources.bash
  ```
  //code
  sudo apt-get install apt-transport-https wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add - sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list' sudo apt-get update
  ```
- Install Elasticsearch.bash
  ```
  //code
  sudo apt-get install elasticsearch
  ```
- Start and enable the Elasticsearch service.bash
  ```
  //code
  sudo systemctl start elasticsearch sudo systemctl enable elasticsearch
  ```

Install Kibana:

- Add the Kibana repository to your package manager's list of sources.bash
  ```
  //code
  sudo apt-get install apt-transport-https sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list' sudo apt-get update
  ```

```
        • Install Kibana.bash
          //code
          sudo apt-get install kibana
        • Configure Kibana to connect to Elasticsearch.bash
          //code
          sudo nano /etc/kibana/kibana.yml
          Set elasticsearch.hosts to point to your Elasticsearch instance.
        • Start and enable the Kibana service.bash
          //code
          sudo systemctl start kibana sudo systemctl enable kibana
Install Logstash:
        • Add the Logstash repository to your package manager's list of sources.bash
          //code
          sudo apt-get install apt-transport-https sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable
          main" > /etc/apt/sources.list.d/elastic-7.x.list' sudo apt-get update
        • Install Logstash.bash
          //code
          sudo apt-get install logstash
Configure Logstash:
        • Create Logstash configuration file(s) in /etc/logstash/conf.d/.
        • Configure inputs, filters, and outputs according to your requirements.
        • Start and enable the Logstash service.bash
          //code
          sudo systemctl start logstash sudo systemctl enable logstash
Accessing Kibana:
        •         By default, Kibana runs on port 5601.
        •         Open your web browser and navigate to http://<your-server-ip>:5601 to access the Kibana dashboard.
Security Considerations:
        •         Consider securing your ELK Stack components by configuring authentication, encryption, and access
          controls.
        •         Implement firewalls and network security groups to restrict access to the ELK Stack ports from external
          networks.
```

Default ELK dashboard interface is shown in Figure 4.

Secure Data Flow

- Establish a secure data flow between the on-premises and cloud-based Logstash instances (if using a Cloud Agent) using a *VPN tunnel* to encrypt data transfer.

Additional Security Layer (Optional)

- Deploy a cloud-based *Wazuh instance* for enhanced security analytics in the cloud environment.

Wazuh Integration

After setting up the ELK stack and data collection, integrate Wazuh to collect security-specific logs and send them to the ELK stack for analysis.

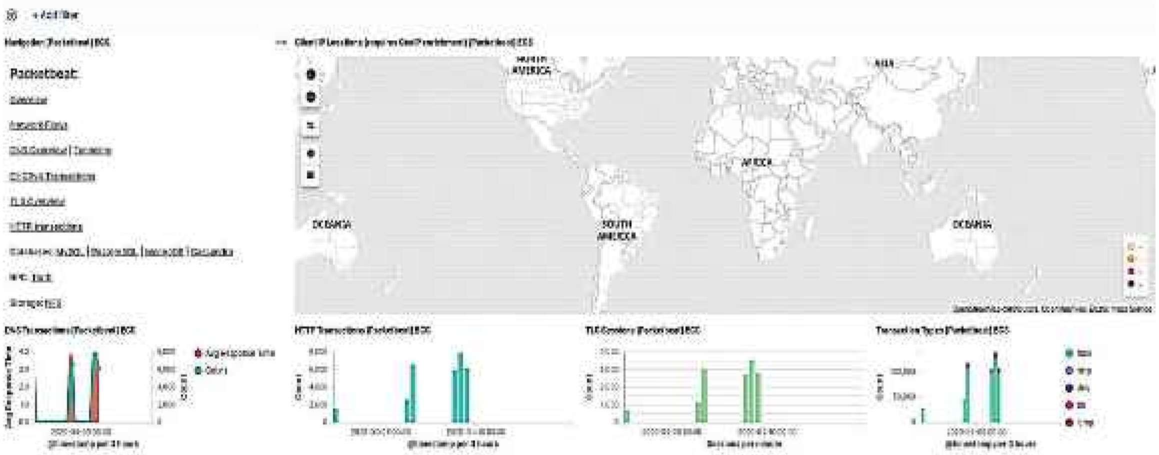


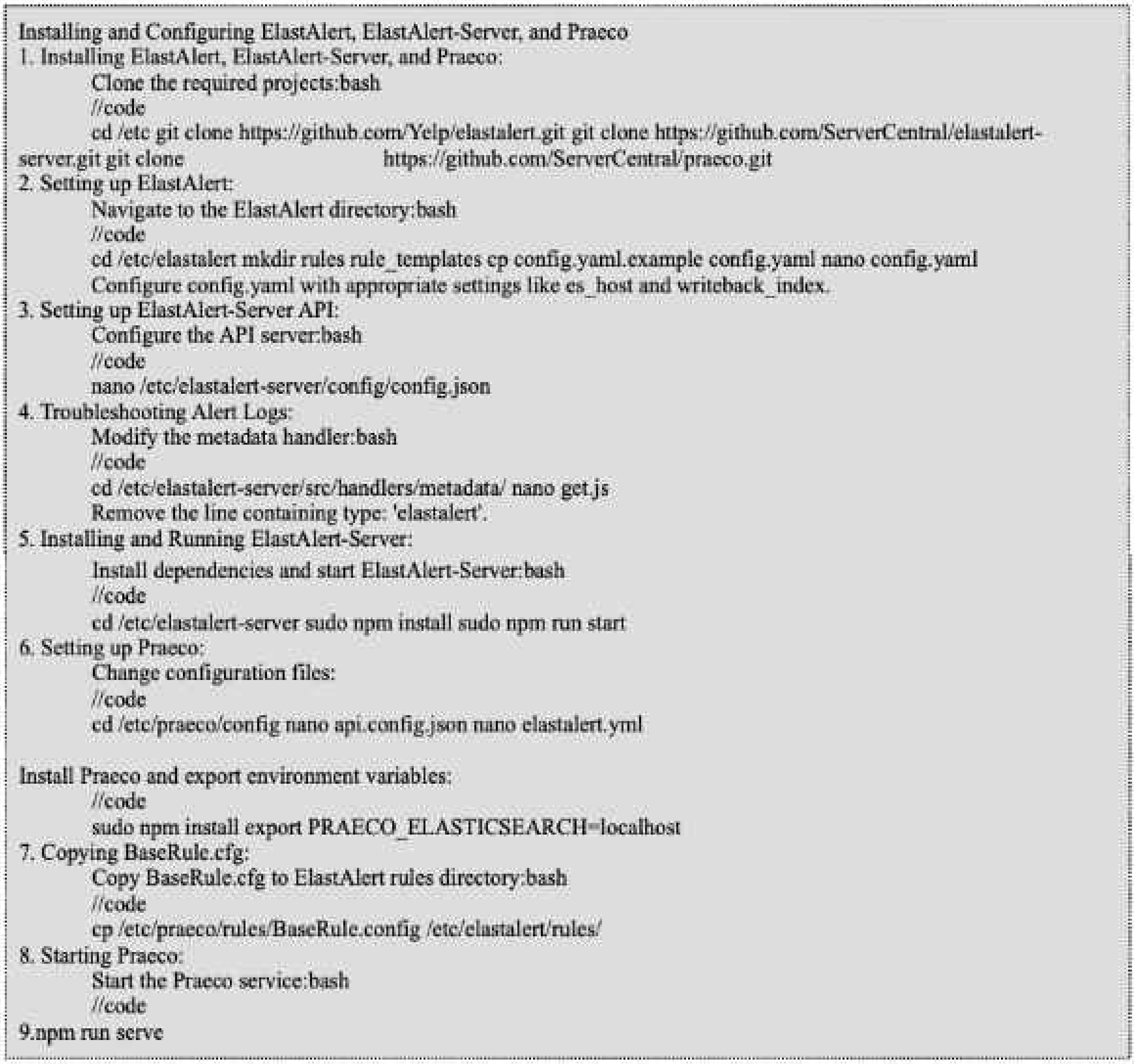
Figure 4. Default Elasticsearch, Logstash, Kibana (ELK) dashboard.

Visualizing Dashboards and ELK SIEM

Once Wazuh is integrated, create dashboards in Kibana to visualize security data from all sources (Wazuh, Beats, Suricata, etc.) and identify potential threats. This is where the SIEM functionality comes in.

Alerting

Configure alerts in Wazuh and the ELK stack to notify you when suspicious activity is detected.

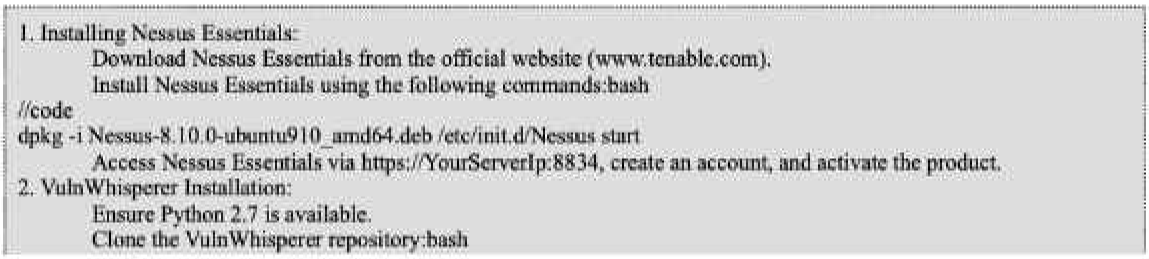


```
Installing and Configuring ElastAlert, ElastAlert-Server, and Praeco
1. Installing ElastAlert, ElastAlert-Server, and Praeco:
        Clone the required projects:bash
        //code
        cd /etc git clone https://github.com/Yelp/elastalert.git git clone https://github.com/ServerCentral/elastalert-
server.git git clone                    https://github.com/ServerCentral/praeco.git
2. Setting up ElastAlert:
        Navigate to the ElastAlert directory:bash
        //code
        cd /etc/elastalert mkdir rules rule_templates cp config.yaml.example config.yaml nano config.yaml
        Configure config.yaml with appropriate settings like es_host and writeback_index.
3. Setting up ElastAlert-Server API:
        Configure the API server:bash
        //code
        nano /etc/elastalert-server/config/config.json
4. Troubleshooting Alert Logs:
        Modify the metadata handler:bash
        //code
        cd /etc/elastalert-server/src/handlers/metadata/ nano get.js
        Remove the line containing type: 'elastalert'.
5. Installing and Running ElastAlert-Server:
        Install dependencies and start ElastAlert-Server:bash
        //code
        cd /etc/elastalert-server sudo npm install sudo npm run start
6. Setting up Praeco:
        Change configuration files:
        //code
        cd /etc/praeco/config nano api.config.json nano elastalert.yml

Install Praeco and export environment variables:
        //code
        sudo npm install export PRAECO_ELASTICSEARCH=localhost
7. Copying BaseRule.cfg:
        Copy BaseRule.cfg to ElastAlert rules directory:bash
        //code
        cp /etc/praeco/rules/BaseRule.config /etc/elastalert/rules/
8. Starting Praeco:
        Start the Praeco service:bash
        //code
9.npm run serve
```

Alerting rule creation and saving it shown in Figure 5.

Reporting

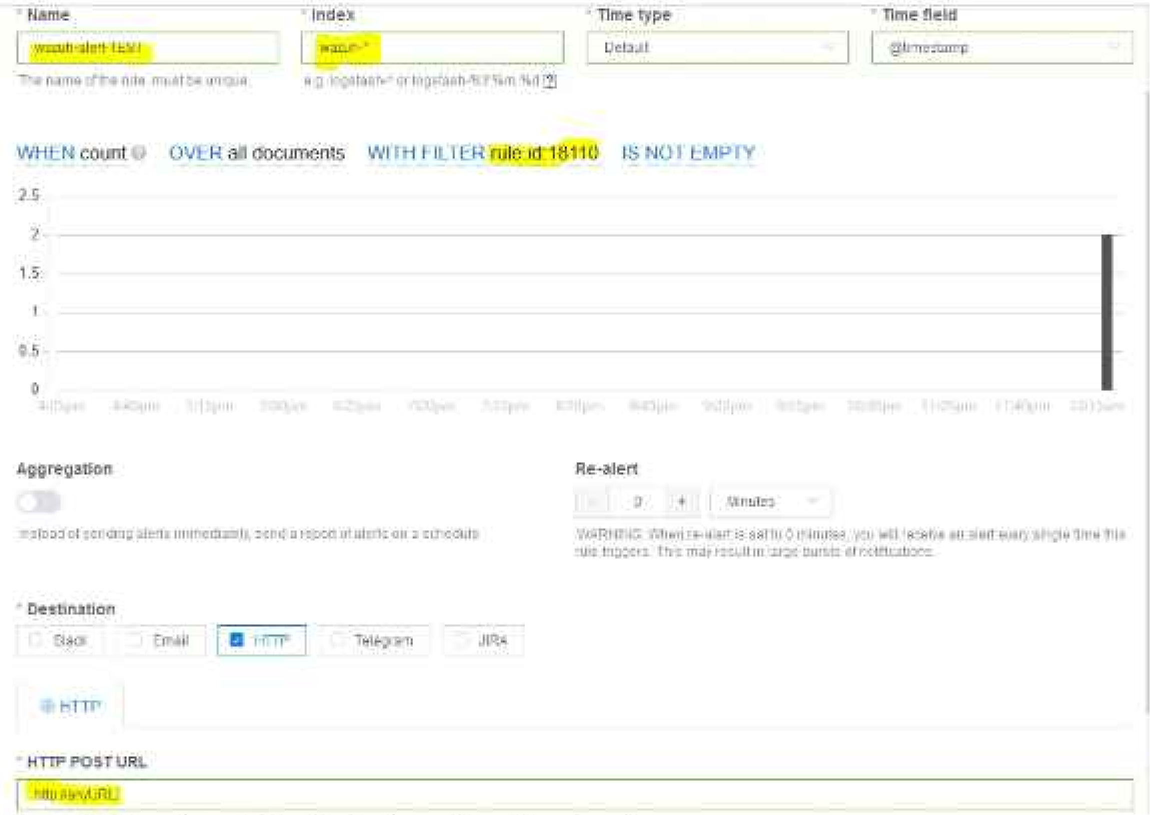
Generate reports from the ELK stack to analyze security trends and identify areas for improvement.



```
1. Installing Nessus Essentials:
        Download Nessus Essentials from the official website (www.tenable.com).
        Install Nessus Essentials using the following commands:bash
//code
dpkg -i Nessus-8.10.0-ubuntu910_amd64.deb /etc/init.d/Nessus start
        Access Nessus Essentials via https://YourServerIp:8834, create an account, and activate the product.
2. VulnWhisperer Installation:
        Ensure Python 2.7 is available.
        Clone the VulnWhisperer repository:bash
```

```
//code
cd /etc/ git clone https://github.com/HASecuritySolutions/VulnWhisperer cd VulnWhisperer/
        Install required dependencies and configure VulnWhisperer:bash
//code
sudo apt-get install zlib1g-dev libxml2-dev libxslt1-dev pip install -r requirements.txt python setup.py install nano
configs/frameworks_example.ini
        Configure the frameworks_example.ini file with Nessus credentials and select enabled modules.
        Check the Nessus connection and download reports:bash
//code
vuln_whisperer -F -c configs/frameworks_example.ini -s nessus
        Set up a cronjob to periodically check Nessus and download reports:bash
//code
crontab -e SHELL=/bin/bash * * * * * /usr/local/bin/vuln_whisperer -c /etc/VulnWhisperer/configs/
frameworks_example.ini >/dev/null 2>&1
        Import Elasticsearch templates and Kibana visualizations:
        Import Elasticsearch template from here.
        Import Kibana configuration from here.
3. Add Nessus Logstash Configuration:
        Copy the Nessus Logstash configuration file to /etc/logstash/conf.d/:bash
//code
cd /etc/VulnWhisperer/resources/elk6/pipeline/ cp 1000_nessus_process_file.conf /etc/logstash/conf.d/ cd /etc/logstash/
conf.d/ nano 1000_nessus_process_file.conf
        Modify the output configuration in the Logstash configuration file.
4. Restart Services and Check Reports:
        Restart Logstash and Elasticsearch services:bash
//code
systemctl restart logstash elasticsearch
        Verify that a new index is created for VulnWhisperer.
        Refresh the index pattern in Kibana to recognize all fields.
        Check the reports in Kibana Dashboards.
```

Cronjobs can be used to automate the process of report generation as shown in Figure 6 and after all virtualization using Kibana, the dashboard looks like in Figure 7.



* Name: wazuh-alert-test

The name of the rule, must be unique

* Index: wazuh-*

e.g. logstash-* or logstash-%Y.%m.%d

* Time type: Default

* Time field: @timestamp

WHEN count OVER all documents WITH FILTER rule.id: 18110 IS NOT EMPTY

Aggregation

Instead of sending alerts immediately, send a report of alerts on a schedule

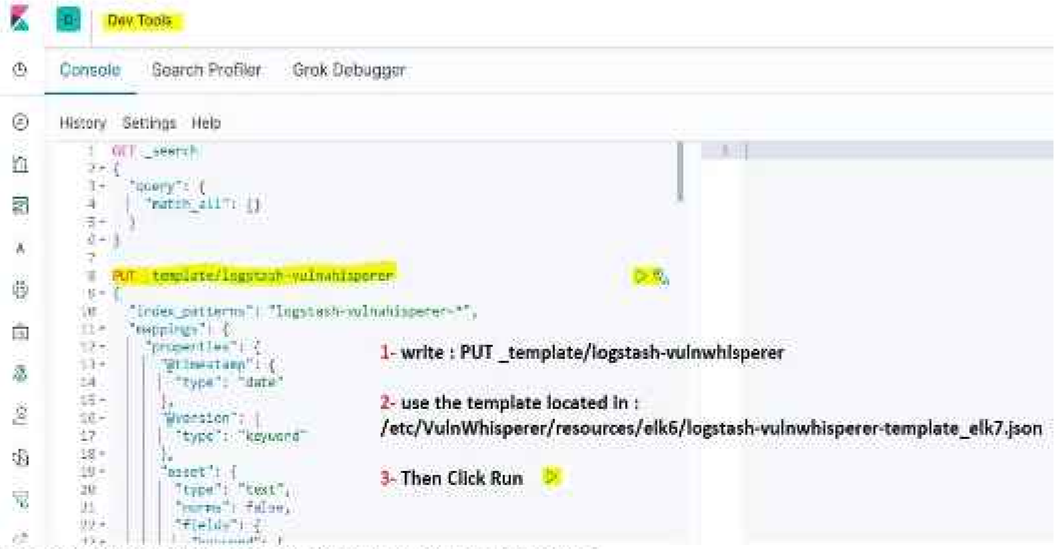
Re-alert: 0 Minutes

WARNING: When re-alert is set to 0 minutes, you will receive an alert every single time this rule triggers. This may result in large bursts of notifications.

* Destination: □ Slack □ Email ☑ HTTP □ Telegram □ JIRA

* HTTP POST URL: http://serverURL

Figure 5. Creating a Wazuh alerting rule and saving it.



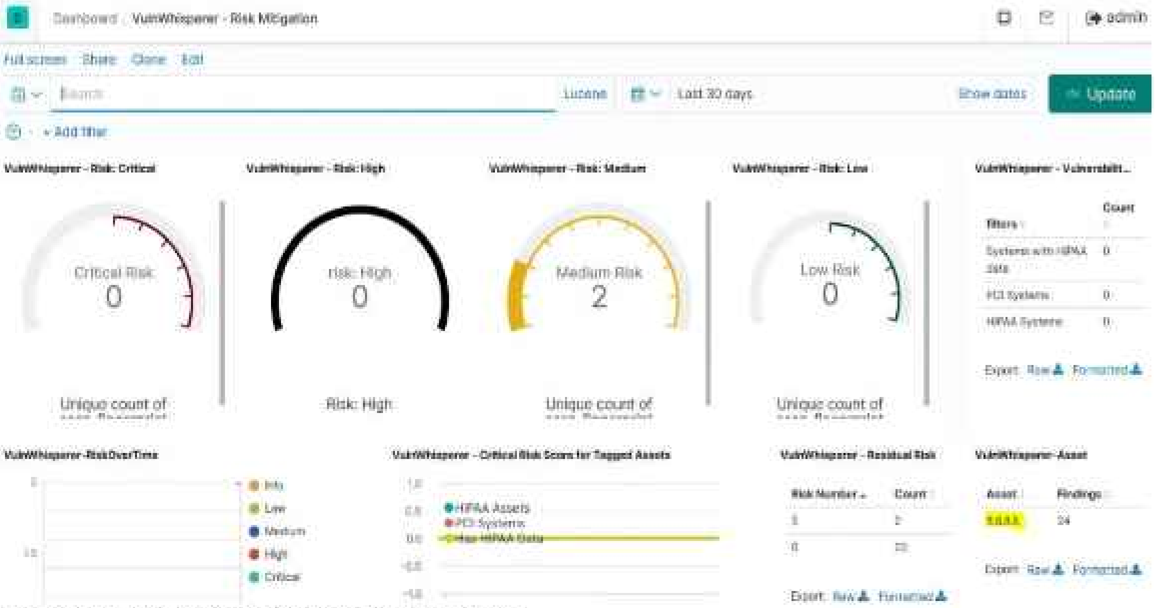
```
GET _search
{
  "query": {
    "match_all": {}
  }
}

PUT _template/logstash-vulnwhisperer
{
  "index_patterns": "logstash-vulnwhisperer-*",
  "mappings": {
    "properties": {
      "@timestamp": {
        "type": "date"
      },
      "@version": {
        "type": "keyword"
      },
      "asset": {
        "type": "text",
        "norms": false,
        "fields": {
          "keyword": {
```

1- write : PUT _template/logstash-vulnwhisperer

2- use the template located in : /etc/VulnWhisperer/resources/elk6/logstash-vulnwhisperer-template_elk7.json

3- Then Click Run

Figure 6. Creating a cronjob for report automation.



Filters	Count
Systems with HIPAA data	0
PCI Systems	0
HIPAA Systems	0

Risk Number	Count
1	2
0	22

Asset	Findings
8.8.8.8	24

Figure 7. The dashboard after virtualization.

Case Management (Optional)

Implement a case management system to track and manage security incidents identified through your SIEM solution.

1. Installation and Configuration of TheHive and Cortex:
- Deploy TheHive 3.4.0–1 and Cortex 3.0.1–1.
- Start Elasticsearch and TheHive/Cortex containers using Docker Compose.
- Ensure Elasticsearch is running and accessible.
- Access TheHive and Cortex dashboards on ports 9000 and 9001 respectively.
- Update databases, create admin users, and log in to both dashboards.

2. A Walk-through TheHive and Cortex Dashboards:
- Access TheHive and Cortex dashboards via web browsers.
- Create organizations and users in Cortex to manage Analyzers.
- Enable required Analysers in Cortex for data enrichment.
- Integrate Cortex with TheHive by creating a user for integration and generating an API key.
- Stop all containers, create an application configuration file for Cortex integration, and modify the docker-compose.yml file accordingly.
- Restart containers and verify Cortex integration in TheHive dashboard.

3. Installing MISP and Integrating it with TheHive:
3.1.MISP Installation:
- Update and upgrade system packages.
- Install MySQL client.
- Download MISP installation script and make it executable.
- Run the installation script, provide base URL and create a "misp" user when prompted.
- Access MISP web interface, authenticate, and change the initial password.
- Enable MISP integration in Cortex by configuring the MISP analyzer with appropriate settings.

3.2. MISP Integration with Cortex and TheHive:
- Create a user in MISP for Cortex integration and copy the AuthKey.
- Enable MISP_2_0 analyzer in Cortex with the MISP server URL and AuthKey.
- Configure Cortex to sync feeds from MISP and perform analysis on provided data.
- Test the integration by analyzing data from MISP feeds in Cortex and reviewing the results in TheHive.

4. Investigation: Case Management with TheHive:
- Utilize investigation cases in TheHive to manage security incidents from creation to closure.
- Add tags, rate severity, and track TLP levels for cases.
- Create tasks to track investigative actions and assign them to analysts.
- Use case templates to define common investigation workflows and pre-populate case metadata and tasks.
- Track observables within the context of a case, such as IP addresses, domain names, etc.
- Leverage Cortex integration to automatically submit observables to OSINT research sites for additional context and analysis.

Incident response approach from ELK to alert generation process is shown in Figure 8.

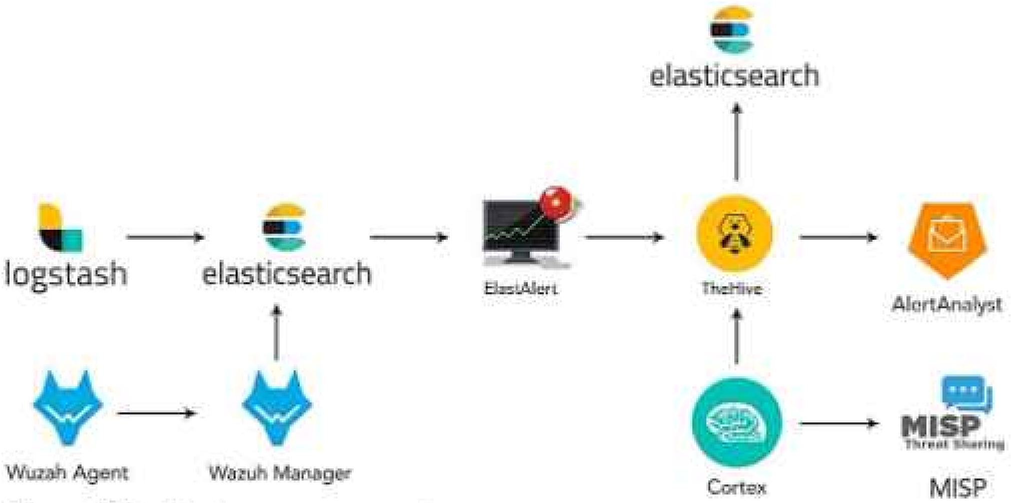


Figure 8. Incident response approach.

RESULTS

Evaluation and Testing

To evaluate the performance of the proof of concept for the proposed use case, multiple tests were conducted. These tests focused on assessing various aspects or components of the implemented architecture across the workflow, starting from alert reception to automated responses via the deployment of customized workflows.

1. Creating custom correlation rules from Suricata alerts
2. Creating Wazuh Active response configuration

```
        Open the /var/ossec/etc/rules/local_rules.xml file on your Wazuh server.
        Add the following rules inside the <group> tags named custom_active_response_rules:
<group name="custom_active_response_rules">
  <rule id="100200" level="12">
    <if_sid>86601</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET DOS Inbound GoldenEye DoS attack</match>
    <description>GoldenEye DoS attack has been detected.</description>
    <mitre>
      <id>T1498</id>
    </mitre>
  </rule>
```

```
    <rule id="100201" level="12">
      <if_sid>86601</if_sid>
      <field name="event_type">^alert$</field>
      <match>ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</match>
      <description>Nmap scripting engine detected.</description>
      <mitre>
        <id>T1595</id>
      </mitre>
    </rule>
</group>

//These rules will trigger the firewall-drop script
```

Open the Wazuh server configuration file /var/ossec/etc/ossec.conf and confirm the command section for firewall-drop exists. Add the configuration block below if it does not:

```
<ossec_config>
  <command>
    <name>firewall-drop</name>
    <executable>firewall-drop</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>
</ossec_config>
```

Edit the Wazuh server configuration file /var/ossec/etc/ossec.conf and add the following section:

```
<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100200, 100201</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```

Restart the Wazuh manager for the configuration changes to apply the configurations

These configurations will allow the firewall-drop script to include the malicious IP address in the firewall's block list on the monitored agent.

Observations

After setting the Wazuh with all the integrations properly a user can easily detect and response to the treat according to its own need providing the successful implementation of the ASAP model as shown in Figures 9 and 10, a simulated attack was held to check the proper functioning of the model. Low Orbit Ion Cannon (LOIC) software was used to execute a distributed denial of service (DDOS) attack

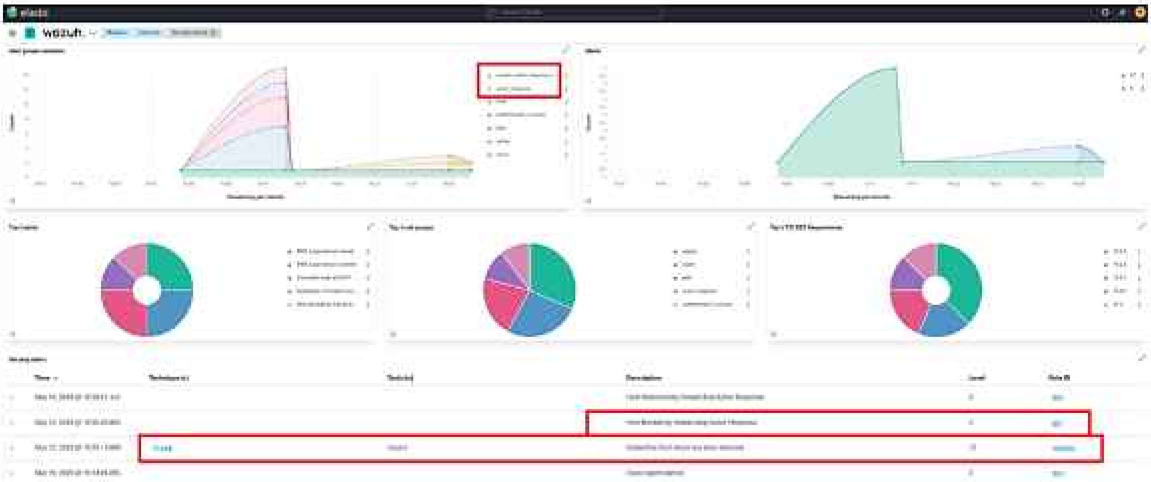
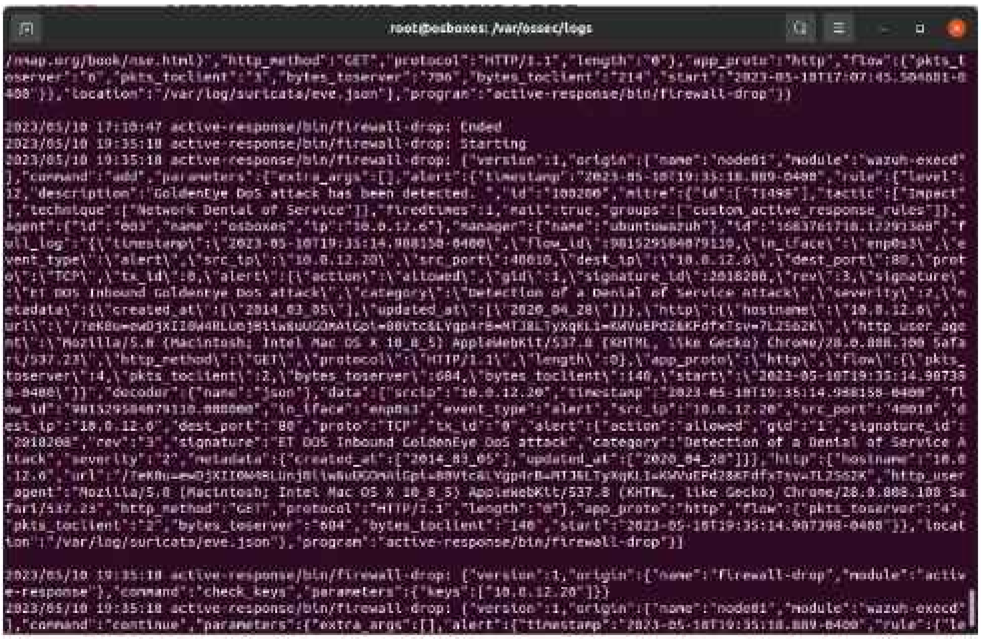


Figure 9. Wazuh distributed denial of service (DDoS)-active response alert that drop active response event log. The DDoS attack was blocked.



```
/nmap.org/book/nse.html)","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_t
oserver":"6","pkts_toclient":"3","bytes_toserver":"706","bytes_toclient":"214","start":"2023-05-10T17:07:45.504681-0
400"}},"location":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 17:10:47 active-response/bin/firewall-drop: Ended
2023/05/10 19:35:18 active-response/bin/firewall-drop: Starting
2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"add","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"level":
12,"description":"GoldenEye DoS attack has been detected. ","id":"100200","mitre":{"id":["T1498"],"tactic":["Impact"
],"technique":["Network Denial of Service"]},"firedtimes":1,"mail":true,"groups":["custom_active_response_rules"]},"
agent":{"id":"003","name":"osboxes","ip":"10.0.12.6"},"manager":{"name":"ubuntuwazuh"},"id":"1683761718.1229136θ","f
ull_log":"{\"timestamp\":\"2023-05-10T19:35:14.908158-0400\",\"flow_id\":981529584079110,\"in_iface\":\"enp0s3\",\"e
vent_type\":\"alert\",\"src_ip\":\"10.0.12.20\",\"src_port\":40010,\"dest_ip\":\"10.0.12.6\",\"dest_port\":80,\"prot
o\":\"TCP\",\"tx_id\":0,\"alert\":{\"action\":\"allowed\",\"gid\":1,\"signature_id\":2018208,\"rev\":3,\"signature\"
:\"ET DOS Inbound GoldenEye DoS attack\",\"category\":\"Detection of a Denial of Service Attack\",\"severity\":2,\"m
etadata\":{\"created_at\":[\"2014_03_05\"],\"updated_at\":[\"2020_04_28\"]}},\"http\":{\"hostname\":\"10.0.12.6\",\"
url\":\"/7eK8u=ewDjXIZ0W4RLUnjBliwBuUGOmAlGpt=80VtcǺLYgp4rB=MTJ8LTyXqKLi=KWVuEPd2&KFdfxTsv=7LZ562K\",\"http_user_age
nt\":\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Safa
ri/537.23\",\"http_method\":\"GET\",\"protocol\":\"HTTP/1.1\",\"length\":0},\"app_proto\":\"http\",\"flow\":{\"pkts_
toserver\":4,\"pkts_toclient\":2,\"bytes_toserver\":604,\"bytes_toclient\":140,\"start\":\"2023-05-10T19:35:14.90739
8-0400\"}}","decoder":{"name":"json"},"data":{"srcip":"10.0.12.20","timestamp":"2023-05-10T19:35:14.908158-0400","fl
ow_id":"981529584079110.000000","in_iface":"enp0s3","event_type":"alert","src_ip":"10.0.12.20","src_port":"40010","d
est_ip":"10.0.12.6","dest_port":"80","proto":"TCP","tx_id":"0","alert":{"action":"allowed","gid":"1","signature_id":
"2018208","rev":"3","signature":"ET DOS Inbound GoldenEye DoS attack","category":"Detection of a Denial of Service A
ttack","severity":"2","metadata":{"created_at":["2014_03_05"],"updated_at":["2020_04_28"]}},"http":{"hostname":"10.0
.12.6","url":"/7eK8u=ewDjXIIOW4RLUnjBliwBuUGOmAlGpt=80VtcǺLYgp4rB=MTJ8LTyXqKLi=KWVuEPd2&KFdfxTsv=7LZ562K","http_user
_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.8 (KHTML, like Gecko) Chrome/28.0.808.100 Sa
fari/537.23","http_method":"GET","protocol":"HTTP/1.1","length":"0"},"app_proto":"http","flow":{"pkts_toserver":"4",
"pkts_toclient":"2","bytes_toserver":"604","bytes_toclient":"140","start":"2023-05-10T19:35:14.907398-0400"}},"locat
ion":"/var/log/suricata/eve.json"},"program":"active-response/bin/firewall-drop"}}

2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"firewall-drop","module":"activ
e-response"},"command":"check_keys","parameters":{"keys":["10.0.12.20"]}}
2023/05/10 19:35:18 active-response/bin/firewall-drop: {"version":1,"origin":{"name":"node01","module":"wazuh-execd"
},"command":"continue","parameters":{"extra_args":[],"alert":{"timestamp":"2023-05-10T19:35:18.889-0400","rule":{"le
```

Figure 10. Wazuh distributed denial of service (DDoS) – host blocked by firewall (agent active-response.log).

on the machine IP and it was noticed that the ASAP model efficiently mitigates the incident and responds to it by turning on the firewall and blocking all the traffic packets as rules established during the model customization.

CONCLUSION

This implementation showcases the effectiveness of combining Suricata for network event detection and Wazuh for analysis and automated response to safeguard organizations against network-based attacks, offering a tangible example of Wazuh's active response module in action. Through thorough work and discussions with cybersecurity experts, valuable insights were gained from a recent cyber-attack incident. It became evident that having the appropriate security tooling, such as EDR/XDR/SIEM/Firewall, is pivotal for detecting and responding to cyber threats effectively. Moreover, maintaining a robust incident response plan and regularly reviewing and updating these processes are essential practices. Integration with external cybersecurity agencies or services can provide additional support for incident response planning, vulnerability assessments, and risk analysis. Equally important is ensuring that personnel possess the necessary skills and expertise to respond to cyber-attacks promptly. Regular training sessions on cybersecurity best practices can significantly enhance the organization's readiness to address security incidents. In conclusion, organizations across various sectors must establish a comprehensive cybersecurity framework encompassing incident response plans, regular assessments, automated response mechanisms, and effective communication strategies. By prioritizing these measures, organizations can bolster their resilience against cyber threats and safeguard their operations and data from potential breaches.

Future Work

Looking ahead, several avenues for future work can be explored to enhance the proposed cybersecurity system's effectiveness and resilience against emerging threats. One promising direction involves integrating additional Wazuh modules to augment the system's detection capabilities. For instance, incorporating the Wazuh malware detection module could provide a non-signature-based approach to identifying anomalies and rootkits, thereby strengthening the system's ability to detect sophisticated malware attacks. Moreover, integrating external features like VirusTotal offers the opportunity to leverage a vast repository of threat intelligence data. By automatically querying VirusTotal's application programming interface (API) with file hashes detected by the file integrity monitoring (FIM) module, the system can swiftly identify potentially malicious files and generate alerts for immediate investigation. This streamlined integration not only enhances threat detection but also accelerates response times, enabling organizations to proactively mitigate cybersecurity risks. Overall, these future enhancements underscore the system's commitment to staying ahead of evolving threats and ensuring robust protection for organizations' digital assets.

REFERENCES

1. ModSecurity: Open Source Web Application Firewall. [Online]. 2019. Available at https://www.modsecurity.org/about.html
2. Combs R. Snort 3.0 with Elasticsearch, Logstash, and Kibana (ELK). [Online]. 2019. Blog.snort.org. Available at https://blog.snort.org/2017/11/snort-30-with-elasticsearch-logstash.html
3. Bassett S, Paquette M. Improve security analytics with the Elastic Stack, Wazuh, and IDS. [Online]. Elastic Blog, April 1, 2019. Available at https://www.elastic.co/blog/improve-security-analytics-with-the-elastic-stack-wazuh-and-ids
4. Kuc R, Rogozinski M. Mastering Elasticsearch. 2nd edition. Birmingham, UK: Packt Publishing Ltd; 2015.
5. Taylor A. Detect Beaconing with Flare, Elastic Stack, and Intrusion Detection Systems. [Online]. Austin Taylor. Available at http://www.austintaylor.io/detect/beaconing/intrusion/detection/system/command/control/flare/elastic/stack/2017/06/10/detect-beaconing-with-flare-elasticsearch-and-intrusion-detection-systems
6. Paquette M. Using Machine Learning and Elasticsearch for Security Analytics: A Deep Dive. [Online]. Elastic Blog, May 2, 2019. Available at https://www.elastic.co/blog/using-machine-learning-and-elasticsearch-for-security-analytics-deep-dive
7. Elastic.co. Elasticsearch Documentation. [Online]. 2019. Available at https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
8. Elastic.co. Logstash Documentation. [Online]. 2019. Available at https://www.elastic.co/guide/en/logstash/current/index.html
9. Elastic.co. Kibana Guide. [Online]. 2019. Available at https://www.elastic.co/guide/en/kibana/current/index.html
10. Elastic.co. Suricata Module: Filebeat Reference [master]. [Online]. 2019. https://www.elastic.co/guide/en/beats/filebeat/master/filebeat-module-suricata.html
11. Elastic.co. Filebeat Documentation. [Online]. 2019. Available at https://www.elastic.co/guide/en/beats/filebeat/current/index.html
12. Elastic.co. Metricbeat Documentation. [Online]. 2019. Available at https://www.elastic.co/guide/en/beats/metricbeat/current/index.html
13. Secrepo.com: SecRepo – Security Data Samples Repository. [Online]. 2019. Available at https://www.secrepo.com
14. Moh M, Pininti S, Doddapaneni S, Moh T-S. Detecting web attacks using multi-stage log analysis. In: 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, February 27–28, 2016. pp. 733–738.