SUMMER INTERNSHIP REPORT

ON

SECURITY INFORMATION AND EVENT MANAGEMENT

(SIEM)

At

Defence Research & Development Organization(DRDO), RCI

Dr. APJ Abdul Kalam Missile Complex, Vignyana Kancha,
Hyderabad-500069

Submitted by- AVIV P JOJI

B.Tech, CSE with Cyber Security
Department of Networking and communication

SRM Institute Of Science And Technology, Kattankulathur

ACKNOWLEDGEMENT

Internship is an integral part of engineering curriculum providing engineers with first hand and practical aspects of their studies. It gives me great pleasure in completing my internship at Defence Laboratory (DRDO), RCI and submitting the internship report for the same.

I would like to thank Director **MR…...** for providing me a esteemed opportunity for internship

I take privilege to express my sincere thanks to **arjunsir** and **Praveen sir** for guiding and supporting me throughout the internship.

INDEX

SECURITY INFORMATION AND EVENT MANAGEMENT

(SIEM)

Introduction:

In the contemporary landscape of cybersecurity, organizations face an increasing array of sophisticated threats that challenge their ability to protect sensitive information and critical infrastructure. To address these challenges, Security Information and Event Management (SIEM) systems have emerged as a vital component of modern security strategies. SIEM provides a holistic approach to managing and enhancing an organization's security posture by integrating real-time monitoring, event correlation, and comprehensive log management.

SIEM systems operate by collecting and aggregating security data from a diverse array of sources, including network devices, servers, applications, and endpoint devices. This data is then analyzed to identify patterns, anomalies, and potential security incidents. By correlating events across different systems and environments, SIEM enables security teams to detect and respond to threats with greater speed and accuracy.

A key feature of SIEM is its ability to provide real-time monitoring and alerting. This ensures that security professionals are immediately notified of suspicious activities, allowing for swift investigation and mitigation. Additionally, SIEM systems offer advanced reporting capabilities, aiding organizations in meeting regulatory and compliance requirements by generating detailed reports on security events and incidents.

In essence, SIEM serves as the nerve center of an organization's security operations, providing a centralized platform for detecting, analyzing, and responding to security threats. By leveraging the capabilities of SIEM, organizations can enhance their ability to protect against cyber attacks, ensure compliance with regulatory standards, and maintain the integrity of their information systems.

ARCHITECTURE OF SIEM

Host System:

The host system in a virtualized environment provides the essential physical hardware and operating system that supports virtual machines (VMs). In a VMware setup, the host machine allocates resources such as CPU, memory, storage, and network connectivity to the VMs, ensuring they have the necessary capacity to operate. It runs the hypervisor software, like VMware ESXi, which creates and manages the VMs, ensuring each VM operates in an isolated and secure environment. The host machine also manages network connections, enabling VMs to communicate with each other and external networks, and handles storage resources and operations for the VMs.

Client System:

Clients initiate requests for data or services, such as accessing files, logs, or applications, from servers that host and provide these resources. Servers are specialized computers or software applications designed to respond to client requests, typically offering centralized resources and functionality that clients can access over a network, such as the internet or an intranet.

Log Shippers:

A log shipper is a critical component in modern IT environments responsible for collecting, processing, and forwarding log data from various sources to centralized storage or analysis systems. It plays a crucial role in monitoring and troubleshooting applications, systems, and networks by ensuring that log data is aggregated and accessible for analysis and compliance purposes.

A log shipper like filebeat, auditbeat ,winlogbeat operates as an agent or lightweight service installed on servers, applications, or devices generating log files. Its primary function is to gather log data in real-time or at scheduled intervals, parse and structure the logs into a standardized format, and transmit them securely to a designated destination.

Analytic tool:

Analytic tools like Elasticsearch plays a critical role in enhancing cybersecurity posture by leveraging advanced algorithms and machine learning techniques to detect, analyze, and respond to security threats. These tools utilize real-time data correlation, anomaly detection, and behavioral analysis to identify patterns indicative of potential security incidents or malicious activities across an organization's IT infrastructure. It also acts a database storing important information. By processing and contextualizing vast amounts of log data from various sources, analytic tools enable security teams to prioritize and investigate security events efficiently, minimizing response times and mitigating risks. They often integrate with incident response workflows, providing actionable insights through visual dashboards and reports that aid in decision-making and compliance auditing. Overall, analytic tools in SIEM systems empower organizations to proactively defend against cyber threats and maintain robust cybersecurity defenses.

Visualization tool:

Visualization tool like Kibana is a powerful data visualization and exploration tool that complements Elasticsearch within the Elastic Stack. It provides a user-friendly interface for visualizing and analyzing data stored in Elasticsearch, making it an essential component for gaining insights from large datasets. With Kibana, users can create customizable dashboards, charts, and graphs to monitor real-time metrics, detect trends, and investigate patterns within log data and other structured information. Its capabilities extend to data exploration through ad-hoc queries, filtering, and aggregation, enabling users to drill down into specific data subsets for detailed analysis. Kibana is widely used across industries for operational monitoring, business analytics, and security information and event management (SIEM), offering powerful visualization tools that enhance data-driven decision-making and operational intelligence.

REQUIREMENTS OF SIEM

The network requirements for a SIEM (Security Information and Event Management) system are crucial to ensure effective data collection, analysis, and response to security incidents across an organization's network infrastructure. Here are the key network-related requirements:

Network Visibility:

It should be comprehensive and visible into all network traffic, including internal and external communications, to monitor for suspicious activities and potential security threats.

Traffic Capture and Monitoring:

It should have the Ability to capture and analyze network traffic in real-time or near real-time from critical network segments, such as DMZs (Demilitarized Zones), LANs (Local Area Networks), and WANs (Wide Area Networks).

Packet Inspection and Deep Packet Analysis:

It should have the capability to perform deep packet inspection (DPI) and analysis to identify potential threats, anomalies, and suspicious behaviour within network traffic.

Protocol Support:

It should support for monitoring and analyzing a wide range of network protocols, including TCP/IP, UDP, DNS, HTTP/HTTPS, SMTP, FTP, and others commonly used in enterprise networks.

Network Device Integration:

It should Integration with network devices (e.g., routers, switches, firewalls, IDS/IPS) to collect logs, events, and flow data for correlation and analysis within the SIEM platform.

Bandwidth and Scalability:

Adequate bandwidth and network capacity is required to handle the volume of data generated by network monitoring tools and devices without impacting network performance or latency.

Secure Data Transmission:

Implementation of secure transmission protocols (e.g., TLS/SSL) to encrypt network traffic and ensure the confidentiality and integrity of data collected and transmitted to the SIEM platform.

Scalable Architecture:

Scalable architecture that supports distributed deployment models to accommodate growing network environments and increased data volumes over time.

Software Requirements:

VMware, Ubuntu, Elasticsearch, Auditbeat, Winlogbeat, Kibana, Bridged network between VMware Windows.

Hardware Requirements:

50GB disk space, 4GB RAM, 2 allocated processor in Vm Ware. At least 500GB disk space, 8GB RAM, 4 allocated processors in windows.

WORKING OF SIEM USING ELASTIC STACK

VMware:

Using Vm Ware host a virtual machine like Ubuntu in Windows. Here Ubuntu acts as as a host. VMware environments host critical applications and services, generating log and performance data that is essential for SIEM operations.

Elasticsearch:

Install Elasticsearch and configure host ports as the ip address of the host system in the YAML file and start the Elasticsearch services. Elastic search is an open source analytic tool and used by multiple MNC's to analyze raw data. Elasticsearch serves as the core data store and search engine within the Elastic Stack. It facilitates real-time indexing, storage, and retrieval of security-related data, including logs, events, and metrics.

Auditbeat for Linux:

Install auditbeat and configure the local host as the ip address of the host in the YAML file and start the auditbeat services. Auditbeat is a lightweight shipper for auditing and monitoring system-level activities and security-related events. It collects audit data from the Linux Audit Framework and other operating system audit logs, providing insights into system-level activities, file integrity monitoring, and user authentication events.

Winlogbeat for Windows:

Install Winlogbeat in windows and configure the local host as ip address of the software running in VMwear as the host(Ubuntu) and Winlogbeat services. Winlogbeat is a lightweight shipper for forwarding Windows event logs to Elasticsearch or Logstash for analysis. It collects event log data from Windows-based systems, including security events, system events, application events, and forwarded events.

Kibana:

Install Kibana and configure the local host as ip address of the software running in VMwear as the host and start Kibana services. All the logs from Auditbeat, Winlogbeat will be loaded into Kibana. Kibana is the visualization and user interface component of the Elastic Stack, providing tools for data exploration, dashboarding, and reporting. It allows security analysts to create custom dashboards, visualize security metrics, and conduct ad-hoc queries on data stored in Elasticsearch.

Benefits of Using Elastic Stack with Auditbeat, Winlogbeat, and VMware for SIEM

Comprehensive Visibility: Centralized logging and real-time monitoring of VMware environments, Windows-based systems, application logs, and security events provide comprehensive visibility into VM performance metrics, operational activities, and security incidents, enhancing threat detection and response capabilities.

Scalability and Performance: Elastic Stack's distributed architecture and lightweight data collection with Auditbeat, Winlogbeat, and ensure scalability and high-performance data ingestion and analysis, accommodating growing data volumes and operational demands within virtualized, Windows-based, and application environments.

Operational Efficiency: Automated data collection, processing, and alerting streamline security operations, improving incident detection, response, and resolution times effectively across VMware, Windows, and application environments.

Compliance and Reporting: Built-in audit trails, logging, and reporting capabilities facilitate compliance with regulatory standards (e.g., GDPR, PCI-DSS) within virtualized, Windows-based, and application IT infrastructures, supporting audit and governance requirements seamlessly.

SCOPE OF IMPROVEMENTS

Enhanced Data Sources and Coverage:

Additional Log Sources: Integrate more data sources such as network traffic logs, firewall logs, intrusion detection/prevention systems (IDS/IPS) logs, and cloud-based service logs to provide a more comprehensive view of the IT environment.

Endpoint Detection and Response (EDR): Implement EDR solutions to capture detailed endpoint activity and enhance threat detection capabilities.

Improved Threat Intelligence and Correlation:

Threat Intelligence Feeds: Integrate external threat intelligence feeds to enrich the collected data with known indicators of compromise (IOCs), threat signatures, and attack patterns.

Enhanced Correlation: Improve correlation rules to identify complex, multi-vector attacks by combining data from different sources and applying advanced analytics and machine learning techniques.

User Training and Awareness:

Comprehensive Training Programs: Develop and deliver comprehensive training programs for security analysts and IT staff to ensure they are proficient in using the SIEM system and responding to security incidents effectively.

Regular Workshops: Conduct regular workshops, drills, and tabletop exercises to keep the security team updated on the latest threats, SIEM capabilities, and incident response techniques.

Advanced Analytics and Machine Learning:

Anomaly Detection: Implement advanced anomaly detection algorithms and machine learning models to identify unusual patterns and behaviors that may indicate potential security threats.

Behavioral Analytics: Utilize behavioral analytics to understand normal user and system behavior and detect deviations that could signify malicious activities

AI Models for Threat Detection and Response:

Predictive Analytics: Develop AI models to predict potential security incidents based on historical data and trends, allowing proactive threat mitigation.

Natural Language Processing (NLP): Use NLP to analyze unstructured data, such as logs and incident reports, to identify patterns and extract relevant security insights.

Automated Incident Classification: Implement AI models to automatically classify and prioritize security incidents based on their severity and potential impact, enabling faster response.

Contextual Analysis: Use AI to provide contextual analysis of security alerts, correlating multiple data points to reduce false positives and highlight genuine threats.

Continuous Improvement and Feedback Loop:

Regular Reviews: Conduct regular reviews of the SIEM system's performance, capabilities, and effectiveness, and gather feedback from security analysts and stakeholders.

Iterative Enhancements: Use feedback to iteratively enhance the SIEM system, addressing any gaps, improving detection and response capabilities, and adapting to emerging threats.

CONCLUSION

The SIEM project utilizing Elastic Stack with VMware, Winlogbeat, and Auditbeat integration marks a transformative leap in cybersecurity by offering a comprehensive, scalable, and intelligent security solution. By incorporating robust data collection across diverse sources, real-time monitoring, advanced analytics, and AI-driven threat detection, the project provides a holistic view of the IT infrastructure, enhancing visibility and response capabilities. The integration with VMware ensures extensive coverage of virtualized environments, while AI models for predictive analytics and automated incident classification streamline threat mitigation. Continuous improvement, user training, and compliance enhancements further solidify the system's effectiveness in addressing evolving cybersecurity challenges, ultimately safeguarding critical assets in a dynamic and complex IT landscape.

This comprehensive approach not only improves the accuracy and efficiency of threat detection but also provides actionable insights and automated responses, thereby enhancing the overall security posture and resilience of the organization against emerging threats. The project's emphasis on scalability and performance optimization ensures it can handle increasing data volumes and operational demands, making it a future-proof solution that can adapt to the ever-changing threat landscape. Through strategic integration, user-friendly dashboards, and advanced AI capabilities, this SIEM system stands as a pivotal tool in modern cybersecurity defence, providing robust protection and peace of mind for the organization.

The utilization of AI and machine learning algorithms not only aids in real-time threat detection but also supports predictive analytics, enabling preemptive actions to mitigate potential risks. This holistic approach not only strengthens the organization's ability to detect and respond to cyber threats but also supports regulatory compliance efforts by providing robust auditing and reporting capabilities. As cyber threats continue to evolve in complexity and frequency, this SIEM initiative stands at the forefront of defense, safeguarding critical assets and maintaining the integrity of operations in an increasingly interconnected digital landscape.