An internship report submitted in partial fulfilment of the requirements for the

Award of Degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

By

ROSHNI VENKATESAN

Roll No: CB.EN.U4CYS21061

"A Lightweight ELK-Based Modular SIEM Pipeline For Real Time Threat Intelligence Using Distributed Log Correlation"

Under Supervision of

R. DEVENDAR NAIK

DEPUTY MANAGER, SCOF/RO

SDSC-SHAR, SRIHARIKOTA, ANDHRA PRADESH, 524124

(Duration: 24th April 2025 – 23rd May 2025)

AMRITA VISHWA VIDYAPEETHAM

DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956

TIFAC-CORE IN CYBERSECURITY

AMRITA VISHWA VIDYAPEETHAM COIMBATORE

AMRITA NAGAR P.O., ETTIMADAI,

TAMIL NADU - 641112

ACKNOWLEDGEMENT

I feel privileged and thankful to mention such esteemed dignitaries who aided me for successful completion of internship training. My best regards to **Shri G. GRAHADURAI, Deputy Director, RO**, for giving permission for doing internship at Range Operation. My best regards to **Srimathi. V. LATHA, General Manager, SCOF RO**, for her support throughout the Internship at Range Operations.

I express my sincere gratitude to **Shri. DEVENDAR NAIK,SCIENTIST/ENGINEER-SE, DEPUTY MANAGER, SCOF/RO** whose support and belief in me laid stepping stones in accomplishment of my project work. I would like to thank **Shri. NANDA SUVAN, SCIENTIST /ENGINEER - SC, SCOF/RO** for sharing guidance.

I express my sincere thanks and deep veneration to **Prof. M. SETHUMADHAVAN**, Centre Head at **AMRITA VISHWA VIDYAPEETHAM, COIMBATORE** for giving me this opportunity for successful completion of internship training. In conclusion, we shall remember our project training and put an oath of presenting the training experience to prove our ability and work for the pride of the organization in all respects wherever we work.

ROSHNI VENKATESAN

CB.EN.U4CYS21061

BONAFIDE CERTIFICATE

This is to certify that **ROSHNI VENKATESAN**, a student at **AMRITA VISHWA VIDYAPEETHAM, COIMBATORE ,** CB.EN.U4CYS21061 has completed her project training successfully at **SHAR COMPUTER FACILITIES** (SCOF)/RO, SATISH DHAWAN SPACE CENTRE, SRIHARIKOTA, ANDHRA PRADESH, 524124 from 24-04-2025 to 23-05-2025.

During the internship period his conduct was found to be_____.

V. LATHA
SCIENTIST/ENGINEER-SG,
GENERAL MANAGER
SCOF, RO

DEVENDAR NAIK
SCIENTIST/ENGINEER-SE,
PROJECT GUIDE
SCOF, RO

INDEX

ABSTRACT

"A Lightweight ELK-Based Modular SIEM Pipeline For Real Time Threat Intelligence Using Distributed Log Correlation"

This project presents a lightweight ELK-based modular SIEM pipeline aimed at delivering real-time threat intelligence through distributed log correlation and visualization. The primary goal is to unify and visualize massive log data from diverse sources such as Windows Event Viewer, Active Directory, and firewall logs. By leveraging Beats for endpoint data collection, Logstash for parsing and enrichment, Elasticsearch for structured storage, and Kibana for interactive dashboards, the system enables immediate insights into security-relevant activities.

Unlike traditional architectures that focus on post-incident log analysis, the proposed approach empowers users to write custom rules for monitoring parameters such as RDP request volumes, admin logins, privileged activities, blocked requests, suspicious event codes, and traffic spikes. This modular design supports real-time detection and visualization of anomalies, allowing for proactive security monitoring. Inputs are structured as key-value pairs, and the system supports flexible rule creation for event codes, protocols, IP tracking, and denied requests, all visualized through customizable Kibana dashboards.

Performance evaluation demonstrates that the pipeline delivers low-latency, real-time log visualization with secure, role-based access for multiple users. The results highlight a significant improvement in situational awareness and threat detection compared to conventional post-exploit log searches. Overall, this work underscores the value of modular, distributed log correlation in providing scalable, actionable security intelligence for modern enterprise environments.

CHAPTER-1

ABOUT THE ORGANIZATION

1.1 Introduction: -

The Satish Dhawan Space Centre SHAR (SDSC SHAR) in Sriharikota, known as the Spaceport of India, stands as a prominent hub within the Indian Space Research Organisation (ISRO), operating under the aegis of the Department of Space (DOS), Government of India. ISRO functions as an autonomous entity, playing a pivotal role in advancing India's space exploration endeavours.

Fig1.1 Satish Dhawan Space Centre SHAR, Sriharikota

Situated in Sriharikota, India, the SDSC SHAR is recognized globally as a leading rocket launch station. This state-of-the-art facility serves as a crucial nexus for launching a diverse array of space missions. These missions span a spectrum of objectives, including the deployment of satellites for remote sensing, communications, navigation, and scientific research.

The centre's commitment extends to ensuring reliable access to space for both indigenous and commercial satellites, contributing to its esteemed reputation on the global stage. The selection of Sriharikota Island in 1969 marked the genesis of this rocket launch station. Since its operational debut on October 9, 1971, with the launch of the Rohini sounding rocket, the center has continually expanded its facilities to meet the dynamic requirements of ISRO.

SDSC SHAR's operational activities are intricately categorized into various domains. These include Vehicle Assembly and Static Test Operations, Range Operations, Liquid Storage and Service Facilities, Solid Propellant, and the Space Booster Plant. These multifaceted operations are integral to supporting the launch of indigenously designed and developed vehicles, such as SLV, ASLV, PSLV, GSLV Mk-II, and GSLV Mk-III.

Fig:1.2 Chandrayaan-3 Launching

Fig:1.3 GSLV-MkII

Beyond its role in launching vehicles, the center takes charge of critical aspects such as program planning, human resources development, and the oversight of systems reliability groups. Administrative and auxiliary support for the center is seamlessly facilitated through the Sriharikota Common Facilities, completing the comprehensive infrastructure that underscores SDSC SHAR's pivotal role in advancing India's prowess in space exploration.

1.2 Range Operations: -

The Range Operations Entity serves as the central hub for overseeing launch operations across various missions conducted by the Indian Space Research Organisation (ISRO) at the Satish Dhawan Space Centre (SDSC) SHAR.

Fig1.4 Range Operations

This entity is entrusted with a diverse array of responsibilities, spanning tracking, tele-commanding, real-time systems for mission monitoring, and the deployment and maintenance of various networks, including the mission network, campus network, internet network, and surveillance network. It also manages networking services with secure features, computerization of administrative activities, web and mobile application development, as well as photography, including still and video coverage. Additionally, it provides meteorology services, ensuring constant weather monitoring to facilitate the clearance of various launch campaign activities.

Key operations of Range Operations at SDSC:-

1. **Launch Coordination:**

   Range Operations involve meticulous coordination of the launch activities, ensuring that all systems and components are functioning optimally before the launch sequence begins.

2. **Tracking and Telemetry:**

The range includes a network of tracking stations equipped with radar and telemetry systems to monitor the trajectory and performance of the launch vehicle throughout its journey. This real-time data is crucial for assessing the mission's success and making necessary adjustments.

3. **Safety Protocols:**

Range safety is paramount during launch operations. Rigorous safety protocols are established to protect personnel, the environment, and surrounding areas. These protocols include criteria for trajectory deviations, ensuring that the launch vehicle follows its planned path.

4. **Abort Criteria:**

Range Operations define criteria for mission abort or vehicle destruction in case of any anomalies that could jeopardize the mission or public safety. These criteria are established to minimize risks associated with launch failures.

5. **Communication Systems:**

The range is equipped with robust communication systems to maintain constant contact with the launch vehicle. This includes voice and data communication to provide real-time updates and receive commands.

6. **Flight Safety Analysis:**

Prior to each launch, extensive flight safety analysis is conducted to assess potential risks and determine the necessary precautions. This analysis considers various scenarios to ensure the safety of the mission.

7. **Post-Launch Analysis:**

After the launch, Range Operations continue with the analysis of post-flight data. This involves assessing the performance of the launch vehicle and its systems, identifying any anomalies, and applying lessons learned to enhance future missions.

8. **International Collaboration:**

ISRO's Range Operations may involve collaboration with international space agencies or organizations for tracking and telemetry support, enhancing the global network of space surveillance and monitoring.

The Range Operations Entity houses crucial facilities such as the Mission Control Centre, Computer and Communications Centre, Multi-Object Tracking Radar (MOTR), including mobile MOTR, and the SHAR Computer Facilities Operations (SCOF).

1.3 SHAR Computer Facility (SCOF) Operations: -

The SHAR Computer Facility meticulously addresses the computational requirements of the Center by unifying hardware, software, and networking necessities. Adhering to stringent security guidelines, the facility has implemented a segregation between the Internet and Intranet.

Noteworthy initiatives undertaken by SCOF include the establishment of a Network Operations Centre, which also serves the dual role of a Data Centre. State-of-the-art High-Performance Computing (HPC) servers have been strategically commissioned to cater to diverse needs, including meteorological and MOTR requirements within the Center.

Furthermore, the facility has successfully implemented three real-time systems as integral components of the mission network: the Range Safety (RS) real-time system, the Specialists' Display System (SDS) real-time system, and the Mission Control Centre (MCC) real-time system.

Fig:1.5 Mission control centre

These systems play a pivotal role in continuously monitoring the status of various ground stations leading up to launch. Additionally, they facilitate real time monitoring during the critical filling phase of the liquid and cryogenic stages of the launch vehicle in the countdown phase. Post-lift-off, these systems prove instrumental in monitoring the performance of vehicle subsystems.

CHAPTER-2

TECHNOLOGY USED

2.1 ELK Stack: -

The ELK Stack is a combination of three open-source tools—Elasticsearch, Logstash, and Kibana—designed to help users collect, search, analyze, and visualize large volumes of data from multiple sources. Logstash ingests and processes data, Elasticsearch stores and indexes it for fast search and analytics, and Kibana provides interactive dashboards and visualizations for real-time insights. This stack is widely used for centralized log management, security analytics, and infrastructure monitoring, making it easier to detect issues, monitor systems, and gain valuable operational intelligence.

2.1.1 Elasticsearch:

Elasticsearch is a powerful search and analytics engine that is used to store and manage very large amounts of data. It is designed to help people quickly find and analyze information from huge collections of records, such as logs or documents. When data is sent to Elasticsearch, it organizes the information so that you can search for specific details, filter results, and even run complex queries to spot patterns or trends. It is widely used because it can handle a lot of data at once and still provide answers in just a few seconds.

2.1.2 Logstash:

Logstash is a tool that helps collect, process, and prepare data before it is stored. It acts like a middleman that takes in raw data from many different sources, cleans it up, and changes it into a format that is easier to work with. Logstash can filter out unnecessary information, add extra details, and organize everything so that the data makes sense and is ready for searching or analysis. It is very flexible and can be set up to handle many types of data and different processing rules.

2.1.3 Kibana:

Kibana is a visualization tool that makes it easy to see and understand data stored in

Elasticsearch. It provides a web-based interface where users can create charts, graphs, and dashboards to display information visually. With Kibana, people can explore their data, spot trends, and monitor key activities using interactive visuals. It is especially helpful for turning complex sets of data into clear and understandable pictures that can be shared with others.

2.2 Data Collection Agents and Services: -

Data collection agents and services are lightweight programs or built-in features that gather and forward logs, metrics, or other machine data to centralized platforms for storage and analysis. Designed to operate efficiently, using minimal system resources, and play a crucial role in aggregating operational and security data from diverse sources such as servers, endpoints, and network devices.

Beats, a family of open-source, single-purpose data shippers developed by Elastic. Each Beat is tailored for a specific type of data—such as logs, metrics, or network traffic designed to be efficient to deploy, for large-scale data collection in distributed environments. Other services such as syslog servers are widely used for log collection and forwarding, especially from network appliances and security devices.

2.2.1 Winlogbeat:

Winlogbeat is a lightweight, open-source agent designed to collect and ship Windows event logs—including application, security, system, and hardware events—from Windows systems to destinations like Elasticsearch or Logstash for storage and analysis. It runs as a Windows service, continuously monitors specified event logs, and forwards new event data in near real time, making it easier to centralize and analyze Windows logs across multiple machines.

2.2.2 Syslog Server:

A syslog server built into FortiGate is a feature that allows the firewall to collect, store, and forward log messages about network activity, security events, and system operations. It uses the standard syslog protocol to send these logs to external servers for centralized monitoring and analysis. Administrators can configure which types of events and severity levels are logged, logs can be sent over different ports and protocols. Helping organizations track network behavior, detect threats, and maintain records for auditing and compliance.

2.3 Infrastructure: -

2.3.1 Ubuntu 24.04:

Ubuntu 24.04 is a modern version of the popular Linux operating system. It is known for being stable, secure, and user-friendly, making it a common choice for running servers and desktop computers. Ubuntu provides a flexible environment for installing software, managing files, and connecting to networks. It supports both graphical and command-line interfaces, allowing users to interact with the system in the way that suits them best. Regular updates and strong community support help keep Ubuntu systems reliable and up to date.

2.3.2 Active Directory:

Active Directory is a directory service developed by Microsoft that helps organizations manage users, computers, and other resources on a network. It acts as a central database where information about user accounts, permissions, and networked devices is stored. Active Directory makes it easier for administrators to control access, enforce security policies, and keep track of changes within the network. It is widely used in business and educational environments to organize and secure digital resources.

2.3.3 Event Viewer:

Event Viewer is a built-in tool in Microsoft Windows that records detailed information about system events, application errors, security incidents, and other important activities on a computer. It allows users and administrators to review logs, troubleshoot problems, and monitor the health and security of Windows systems. By examining events in the Event Viewer, it is possible to identify issues, track user actions, and ensure that the system is operating as expected.

2.3.4 Fortigate Firewall:

A FortiGate firewall is a security device that protects computer networks from unauthorized access and cyber threats. It monitors all incoming and outgoing network traffic, blocks harmful connections, and provides detailed logs about network activity. The firewall can enforce security rules, detect suspicious behavior, and help prevent attacks on the network. FortiGate firewalls are commonly used by organizations to maintain a safe and secure network environment.

CHAPTER-3

PROJECT DETAILS

3.1 Overview: -

The objective of this project was to design and implement a Security Information and Event Management (SIEM) solution using the ELK Stack (Elasticsearch, Logstash, Kibana) and Beats for data collection, with integration of additional log sources such as syslog servers. The project was driven by the need to meet regulatory standards and organizational security policies, while addressing critical use cases such as reducing incident response times, prioritizing compliance, and monitoring user behavior across the enterprise.

To achieve these goals, the SIEM architecture was planned to ingest logs from diverse data sources including firewalls, IDS, endpoint tools, authentication systems, and application logs, with a focus on sources identified as high-risk or critical. The implementation emphasized scalability, ease of use, and seamless integration capabilities, ensuring that the solution could be adapted to evolving business requirements. A proof-of-concept (POC) phase was conducted to validate integration with key data sources and to customize dashboards and correlation rules according to stakeholder roles.

Deployment involved setting up the ELK Stack on a cluster of Ubuntu virtual machines, configuring Beats agents (such as Winlogbeat) on endpoints, and integrating syslog feeds from network devices. Data normalization, correlation, and aggregation were implemented to standardize and enrich log data, enabling effective alerting and reporting. The solution was rigorously tested for accuracy and performance, with workflows established for alert handling and escalation. Post-implementation, continuous monitoring, performance optimization, and regular policy updates were instituted, alongside user training and periodic audits to ensure ongoing relevance and effectiveness.

3.2 Related Work: -

SIEM solutions have evolved significantly in recent years, driven by the increasing complexity of IT environments and the growing importance of regulatory compliance. Traditional SIEM platforms, such as Splunk and IBM QRadar, offer comprehensive log management and security analytics but often come with high licensing costs and complex deployment requirements. In contrast, open-source alternatives like the ELK Stack have gained traction due to their flexibility, scalability, and cost-effectiveness, especially when tailored to specific organizational needs.

Research and industry practice have highlighted the effectiveness of distributed log collection using lightweight agents (such as Beats) and syslog servers. Beats, developed by Elastic, are purpose-built data shippers designed to efficiently collect and forward logs, metrics, and network data from endpoints to central analysis platforms. This approach supports scalable, real-time monitoring and enables organizations to implement fine-grained data collection strategies based on risk and criticality.

Best practices, as outlined in NIST SP 800-92 and NIST SP 800-53, emphasize the importance of centralized log management, continuous monitoring, and proactive threat detection. These frameworks advocate for systematic event monitoring (AU-2), system monitoring (SI-4), and risk assessment (RA-10), aligning closely with the goals of this project. Recent case studies demonstrate the value of integrating SIEM with Active Directory, firewalls, and endpoint detection tools to enable comprehensive security monitoring and rapid incident response. The use of correlation rules—such as those for detecting brute force attacks, DDoS attempts, and anomalous user behavior—has been shown to significantly enhance the detection of sophisticated threats.

3.3 Flow Chart: -

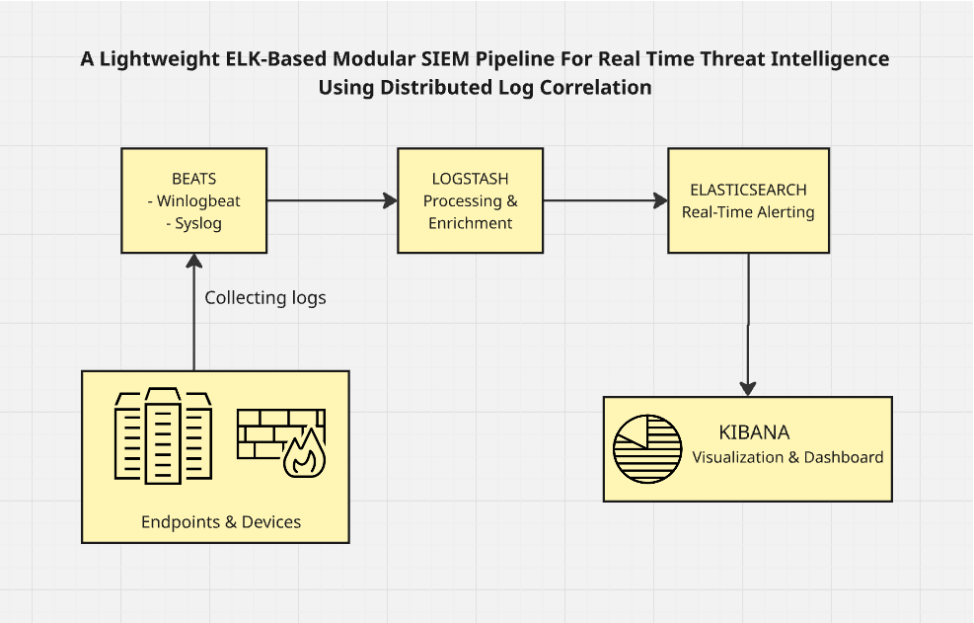

Fig. 3.1 Flowchart of the Project

3.4 Data Sources: -

A robust SIEM implementation relies on the integration of diverse data sources to provide comprehensive visibility across the IT environment. In this project, data sources were selected based on their criticality and risk profile, in accordance with regulatory standards and organizational policies. The primary sources included:

- **Firewalls:** Logs from FortiGate firewalls were collected via the built-in syslog server, providing insights into network traffic, denied actions, and potential intrusion attempts.
- **Intrusion Detection Systems (IDS):** IDS logs contributed to the detection of network-based threats and policy violations.
- **Endpoints:** Windows event logs from approximately 2,000 systems were collected using Winlogbeat, enabling detailed monitoring of user activity, system changes, and security events.
- **Authentication Systems:** Active Directory logs were ingested to track user logins, account modifications, group changes, and other critical security events. These logs were essential for monitoring user behavior and detecting unauthorized access attempts.

- **Application Logs:** Application-specific logs were included based on their relevance to business operations and risk level, ensuring that critical applications were adequately monitored.

Data collection was achieved through a combination of Beats agents (Winlogbeat for Windows events, Filebeat for application logs) and syslog feeds. The collected data was forwarded to a centralized Logstash server for parsing, normalization, and correlation, before being indexed in Elasticsearch for search, visualization, and alerting. This architecture enabled the aggregation of logs from multiple sources, standardization of log formats, and the establishment of relationships between log events for effective threat detection and compliance reporting.

3.5 Implementation and Results: -

3.5.1 Planning and Setup:

The implementation began with a detailed requirements analysis, focusing on regulatory standards (NIST SP 800-92, SP 800-53) and internal security policies. Data sources were prioritized based on criticality and risk, with an emphasis on firewalls, IDS, endpoints, and authentication systems. A proof-of-concept (POC) was conducted to validate the integration of these sources and to refine the scope and timeline.

3.5.2 Infrastructure Deployment:

Three Ubuntu virtual machines were provisioned to host Elasticsearch, Logstash, and Kibana. Java Development Kit (JDK) was installed as a prerequisite, with environment variables configured to ensure compatibility. Each component was installed and configured separately, with careful attention to cluster settings, network configuration, and security policies. System services were tested and debugged to ensure reliable operation.

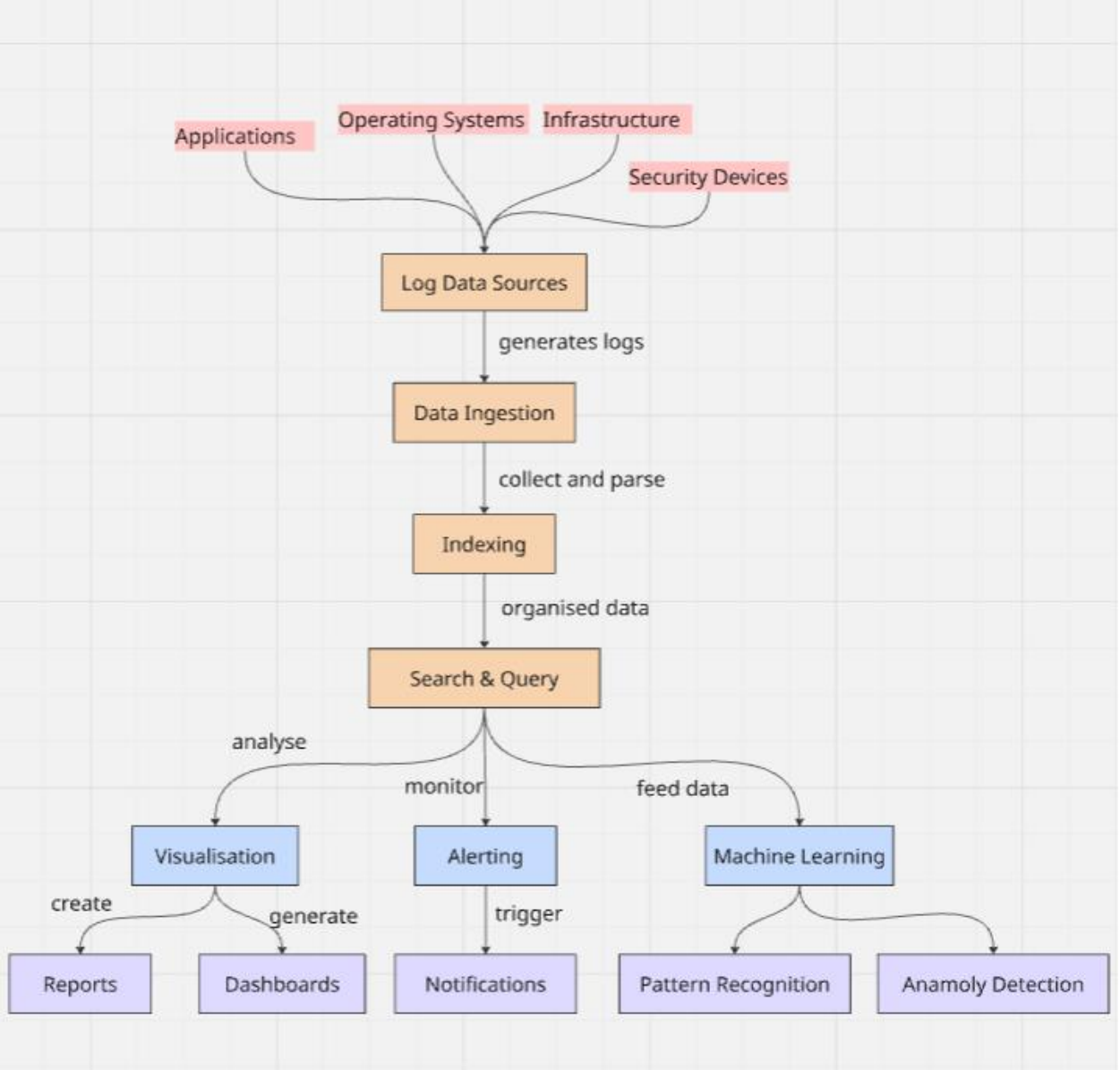

Fig. 3.2 Logical flow diagram of the project

3.5.3 Data Collection and Integration:

Beats agents were deployed to endpoints, with Winlogbeat configured to collect Windows event logs and forward them to Logstash. The Winlogbeat configuration specified the Logstash server IP and port, with certificates and direct Elasticsearch output disabled for initial testing. Syslog feeds from FortiGate firewalls were configured to send logs over UDP/TCP to the Logstash server.

3.5.4 Log Processing and Normalization:

Logstash was configured with custom pipelines to parse, normalize, and enrich

incoming logs. Grok filters were used to convert unstructured log data into structured, queryable fields. Data normalization ensured consistent formatting across diverse sources, while correlation rules were implemented to link related events (e.g., mapping user account creation events with Event ID 4720).

3.5.5 Indexing and Visualization:

Elasticsearch provided scalable, real-time indexing and search capabilities. Index management strategies were employed to optimize performance and storage. Kibana was used to create custom dashboards, visualizations, and alerts tailored to stakeholder requirements. Visualizations included unified multi-index charts, with index patterns created to enable flexible querying and analysis.

3.5.6 Correlation and Alerting:

Custom correlation rules were developed to detect security incidents such as brute force attacks, DDoS attempts, file integrity violations, and anomalous network activity. Alerts were configured to trigger on specific conditions, such as repeated failed login attempts or excessive data copying. Workflows for alert handling and escalation were established to ensure timely incident response.

3.5.7 Testing and Optimization:

The solution was tested for accuracy and performance, with simulated attack scenarios used to validate detection capabilities. Performance optimization included tuning Elasticsearch indices, refining Logstash pipelines, and adjusting Beats configurations. Continuous monitoring and regular audits were instituted to maintain relevance and effectiveness.

3.5.8 Results:

The implemented SIEM solution provided comprehensive visibility into security events across the organization. Incident response times were reduced through real-time alerting and

centralized log analysis. Compliance reporting was streamlined, with dashboards and reports aligned to regulatory requirements. User behavior monitoring enabled the detection of insider threats and policy violations. The open-source nature of the ELK Stack ensured flexibility and cost-effectiveness, while the modular architecture supported future scalability and integration with additional data sources.

3.6 Analysis: -

The ELK-based SIEM solution demonstrated significant advantages in terms of flexibility, scalability, and cost-effectiveness compared to traditional commercial SIEM platforms. The use of Beats agents enabled efficient, distributed data collection with minimal impact on endpoint performance. Integration with syslog servers and Active Directory provided comprehensive coverage of critical data sources.

Data normalization and correlation capabilities facilitated the identification of complex attack patterns and insider threats. Custom dashboards and visualizations in Kibana empowered stakeholders with actionable insights tailored to their roles. The open-source architecture allowed for rapid customization and adaptation to evolving security requirements.

However, the implementation also presented challenges, including the need for ongoing maintenance, tuning, and user training. Initial setup and configuration required significant technical expertise, particularly in parsing and normalizing diverse log formats. Performance optimization was essential to ensure scalability as log volumes increased. Despite these challenges, the solution met its objectives of reducing incident response times, supporting compliance, and enhancing security monitoring.

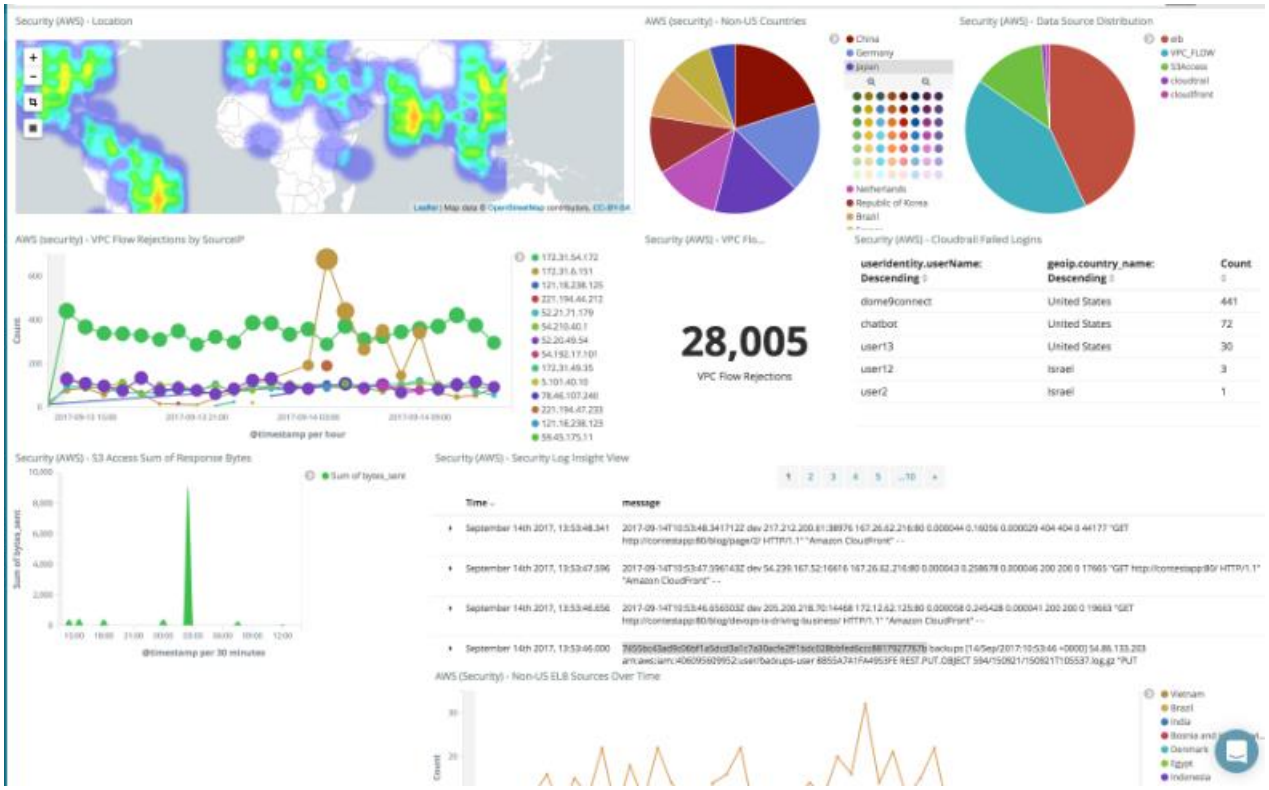

Fig. 3.3 Dashboard for the logs from the past 30 days

CHAPTER-4

CONCLUSION

Our project centered on designing, deploying, and evaluating an ELK-based SIEM solution, integrating Beats agents and syslog services to aggregate and analyze security data from a diverse set of sources—including firewalls, IDS, endpoints, and authentication systems. Through a systematic implementation process, we demonstrated how open-source tools like Elasticsearch, Logstash, and Kibana can be effectively combined with lightweight data collectors such as Winlogbeat to deliver real-time visibility and robust security monitoring across a large-scale enterprise environment.

By carefully planning the architecture, optimizing data normalization and correlation, and customizing dashboards and alerting workflows, we were able to build a flexible and scalable system that adapts to evolving security requirements. The successful integration of Active Directory logs and firewall events further strengthened the platform's ability to detect a wide range of threats, from brute force attacks to anomalous network activity.

One of the most significant takeaways from this project is the advantage of using modular, open-source solutions over proprietary SIEM platforms. While traditional SIEMs offer comprehensive features, the ELK Stack's flexibility, cost-effectiveness, and ease of customization make it particularly well-suited for organizations with unique or evolving needs. The experience also underscored the importance of continuous monitoring, regular policy updates, and ongoing training to maintain the effectiveness of any security solution.

On a personal level, working on this project my time at SHAR Computer Facilities (SCOF) has been a rewarding and transformative experience, providing invaluable hands-on experience with modern security architectures, Linux system administration, and the practical challenges of large-scale log management. The process of troubleshooting, optimizing performance, and collaborating with stakeholders deepened my technical and project management skills. Mentorship from experienced professionals and iterative problem-solving

were critical in overcoming obstacles and delivering a successful outcome.

Looking forward, this project lays a strong foundation for further enhancements—such as integrating advanced threat intelligence feeds, automating incident response, and expanding data source coverage. The insights gained here not only contribute to organizational security but also offer a practical blueprint for others seeking to implement open-source SIEM solutions in complex environments.

References

1. **Using the ELK Stack for SIEM,** logz.io
2. **Event Logging in Windows Events,** Microsoft
3. **SIEM Implementation in 4 Steps,** Exabeam
4. **Threat Hunting: Log Monitoring Lab Setup with ELK,** Hacking Articles
5. **Guide to Computer Security Log Management,** NIST SP 800-92
6. **Log analysis in ELK,** Netwerk Labs
7. **Security and Privacy Controls for Information Systems and Organizations,** NIST SP 800-53
8. **How we use Active Directory at work,** East Charmer
9. **Create a simple dashboard to monitor website logs,** Elastic
10. **The Complete Guide to the ELK Stack,** Logz.io
11. **SIEM Guide,** Elastic
12. **Getting started: Use Elastic Security for SIEM,** Elastic
13. **Complete Guide To ELK,** Logit.io
14. **Create a SIEM with the Open-Source ELK Stack,** Cybercademy
15. **Installing the ELK Stack SIEM,** LinkedIn Learning
16. **Using the ELK Stack for SIEM,** Logz.io
17. **What is ELK: Core Components, Ecosystem & Setup Guide,** Last9.io
18. **ELK Stack SIEM: Security Information and Event Management,** Elastic.co
19. **Getting Started with Beats,** Elastic.co