Industry Project

Report

On

SecureSys: Strengthening Infrastructure Security & Monitoring

Developed By: -	**Guided By:-**
ABEL_BENEDICT(20162171001)	Prof. Tejas Kadiya (Internal)
	Mr.Peter Raju (External)

Submitted to

Faculty of Engineering and Technology

Institute of Computer Technology

Ganpat University

Year - 2024

INDEX

LETTER OF INTERNSHIP

Dear Sir/Madam,

I am writing to formally acknowledge the successful completion of Abel Benedict's internship with IT HOST SOLUTION. Abel joined our team as a System Engineer – (Intern) under the IT Networking Department.

Here are the details of Abel's internship:

- Intern Name: Abel Benedict
- Internship Duration: From 1st December 2023 to 30th April 2024
- Department: IT Networking
- Role: System Engineer – (Intern)

During his internship, Abel demonstrated a strong commitment to learning and contributed significantly to various networking projects. His technical skills, problem-solving abilities, and teamwork were commendable. Abel actively participated in network configuration, troubleshooting, and system maintenance tasks.

We appreciate Abel's dedication and enthusiasm throughout his internship. His positive attitude and willingness to take on new challenges were valuable assets to our team.

We wish Abel all the best in his future endeavours and hope that the knowledge and experience gained during his internship will serve him well in his professional journey.

Thank you for providing Abel with this valuable opportunity, and we look forward to continued collaboration with IT HOST SOLUTION.

Sincerely,

Nilesh Upadhyay

Vice President – HR

BT-34, 3rd Floor, Radhe Business Park, Sardar Patel Ring Road, Aslali, Ahmedabad, Gujarat 382427
+91 88662 53295 / 88662 24586 peter@ithostsolution.com / dev@ithostsolution.com
GST No. : 24AITPY1643C1Z2

ACKNOWLEDGEMENT

Industry project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Rohit Patel, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Ravi Patel (Internal) for their guidance in Industry project work, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

ABEL BENEDICT (Enrollment No:20162171001)

ABSTRACT

This report documents the successful implementation of a centralized logging and monitoring system using the ELK stack (Elasticsearch, Logstash, Kibana). Over the course of four weeks, the project aimed to enhance security and visibility by aggregating, analyzing, and visualizing log data from diverse sources across the organization's infrastructure. Through meticulous planning and execution, each week focused on specific tasks, culminating in the establishment of a robust system for real-time log monitoring, analysis, and visualization.

WEEK-1

Installation and Setup of ELK Stack Components

Objective: Install Elasticsearch, Logstash, and Kibana to lay the foundation for the centralized logging and monitoring system.

Tasks

- Installed Elasticsearch on dedicated server for scalable storage and indexing of log data.
- Deployed Logstash to collect, parse, and forward logs from various sources to Elasticsearch.
- Configured Kibana for visualizing log data and creating custom dashboards.

Outcome: Completed installation and initial configuration of ELK stack components, setting the stage for further customization and optimization.

WEEK - 2

Log Collection and Parsing with Logstash

Objective: Configure Logstash to collect logs from diverse source and parse them for indexing in Elasticsearch.

Tasks

- Configured Logstash input plugins to collect logs from servers, applications, and network devices.
- Implemented parsing filters to extract relevant information from log entries and enrich log data.

Outcome: Successfully established a seamless flow of log data from various sources to Elasticsearch through Logstash, ensuring uniformity and consistency in log processing.

WEEK - 3

Indexing and Storage Optimization in Elasticsearch

Objective: Configure Elasticsearch for efficient storage and indexing of log data to ensure fast and reliable search and retrieval.

Tasks

- Defined Elasticsearch indices and mappings to optimize storage and indexing performance.
- Implemented index lifecycle management (ILM) policies for data retention and rollover.

Outcome: Improved storage efficiency and search performance in Elasticsearch, enabling faster access to log data and smoother operation of the centralized logging system.

WEEK - 4

Visualization and Monitoring Setup with Kibana

Objective: Integrate Kibana with Elasticsearch to visualize log data through interactive dashboards and monitor system health and security events.

Tasks

- Created custom visualizations and dashboards in Kibana to monitor key metrics and security incidents.
- Configured alerting and reporting features in Kibana for proactive monitoring and analysis.

Outcome: Established a comprehensive monitoring and visualization platform in Kibana, providing real-time insights into system activities and security events.

REFERENCES

- Elastic (2024). Elasticsearch Reference. Retrieved from https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

- Elastic (2024). Logstash Reference. Retrieved from https://www.elastic.co/guide/en/logstash/current/index.html

- Elastic (2024). Kibana User Guide. Retrieved from https://www.elastic.co/guide/en/kibana/current/index.html