# Basic Details of the Team and Problem Statement

**Ministry/Organization Name/Student Innovation:** Ministry of power

**PS Code:** SIH1389

**Problem Statement Title:** To develop centralized information security .Log-collection facility' or 'security operation centre (soc)' in the power sector, considering cEA cybersecurity (Power sector) Guidelines, 2021to keep lr and or networking System isolated and air-gapped.

**Team Name:** Opti-hack Engineers

**Team Leader Name:** Lokesh Manikanta

**Institute Code (AISHE):**

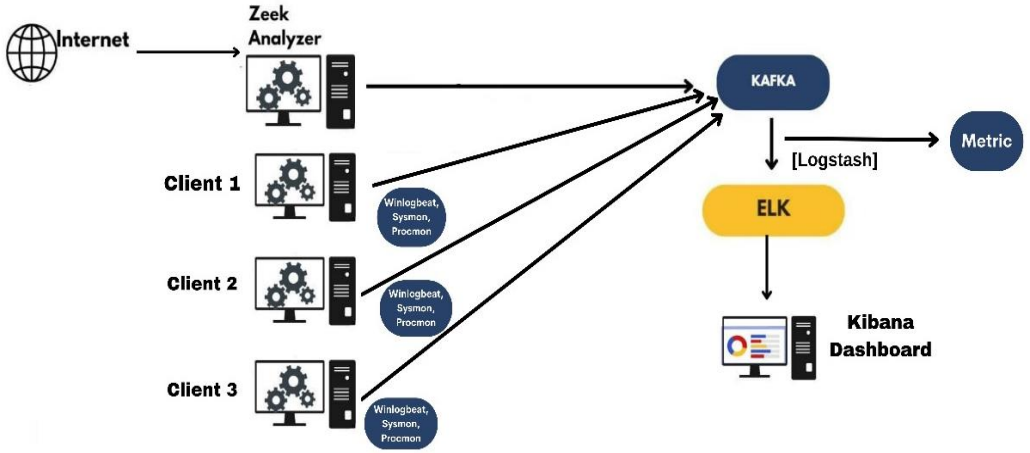
**Institute Name:** VIT-AP University

**Theme Name:**

# Idea/Approach Details

Our approach to enhancing network security combines Zeek, ELK stack and Fleet.

- Zeek monitors network traffic across individual systems and generates logs that securely flow to central server via Kafka.
- Fleet streamlines Elastic Agent management.
- On the central server the ELK Stack plays a pivotal role. Elasticsearch efficiently stores and organizes logs, while Logstash processes them for analysis. Kibana provides a user-friendly interface for exploration.
- Expanding our capabilities, we integrate additional log sources: Winlogbeat collects Windows system logs, Sysmon forwards system logs directly to ELK, and Procmon captures real-time system and process activity log
- Thus provides real-time monitoring, centralized log collection, scalability, and robust data correlation, fortifying network security with swift threat detection and comprehensive analysis across diverse log sources.




Add process flow chart or simulated image of prototype or any relevant image related to your idea

**Describe your Technology stack here**:

- Operating Systems ( Windows, Ubuntu, Kali )
- Log Collection Software
- Backup and Recovery Software
- Security and Monitoring Software

# Idea/Approach Details

## Describe your Use Cases here

- We can build a solid SIEM(Security Information and Event Management)
- We can build centralised log management, which would benefits  IT and DevOps
- Log management and Analysis
- It can be used for Network Security Monitoring(NSM)
- This setup can help organizations meet compliance requirements by securely storing and auditing log data.

## Describe your Dependencies / Show stopper here

- **Hardware and Infrastructure**: Ensure that the necessary hardware, virtual machines, or cloud resources are provisioned and configured correctly to support Zeek, ELK, and Fleet components.
- **Software Installation**: Installing and configuring Zeek, Kafka, Elasticsearch, Logstash, Kibana, and Fleet components correctly is a critical dependency. Any misconfiguration can lead to issues.
- **Critical Misconfiguration**: Any critical misconfiguration in Zeek, Kafka, or the ELK Stack can lead to data loss, performance issues, or security vulnerabilities, potentially becoming a showstopper.
- **Resource Exhaustion**: Inadequate hardware resources or improper resource allocation can cause system performance degradation or even crashes, acting as a showstopper.

# Team Member Details

**Team Leader Name:** **Lokesh Manikanta**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Member 1 Name:** **Jahin Justin**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Member 2 Name:** **Tejeswar Jangam**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Member 3 Name:** **Tarun**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Member 4 Name:** **Ranjith Ashok**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Member 5 Name:** **Sravya Sri**

Branch (Btech/Mtech/PhD etc): BTECH | Stream (ECE, CSE etc): CSE | Year (I,II,III,IV): III

**Team Mentor 1 Name:** **Sibi Chakkaravarthy**

Category (Academic/Industry): | Expertise (AI/ML/Blockchain etc): | Domain Experience (in years):