Banasthall Vidyapith

HACK CELESTIA

Where brainpower meet bold initiations

Team Name **VERTEX**

Track :

CYBER SECURITY

Ankit Satpute
Arshdeep Kaur
Reniyas Nadar
Rohan Benegal
Vashni Nadar

Fr. Conceição Rodrigues College of Engineering

Problem Statement

Cybersecurity Challenges

- Increasing sophistication and frequency of cyberattacks
- Manual detection and response methods are slow, inefficient, and reactive.
- High false positives from traditional systems reduce productivity and accuracy

Objective

To build an interactive platform integrating real-time pollution maps, educational resources, and eco-friendly initiatives to address water pollution and promote sustainable practices.

Solution/Approach Details

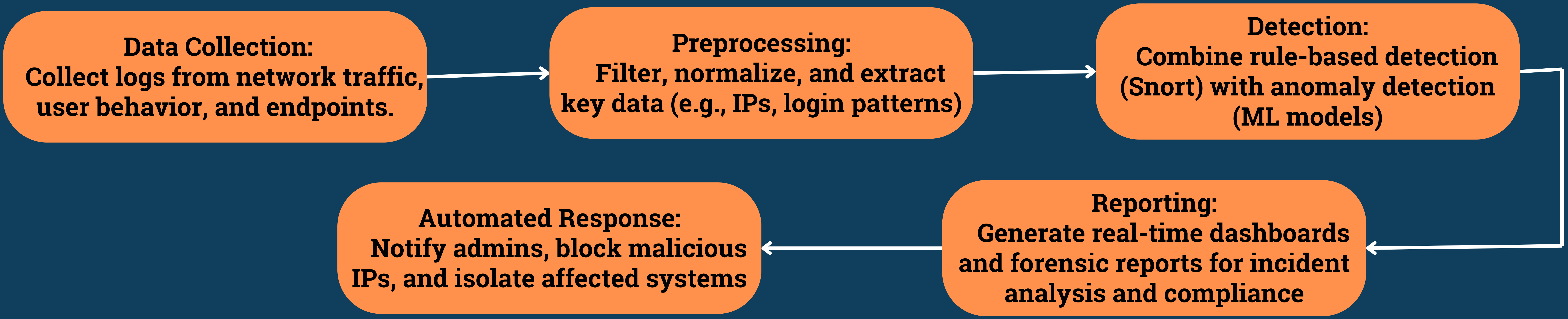
Key Features of the Solution

Honeypot Integration: Deploy fake systems to detect attacker behavior and prevent real asset compromise.

Threat Intelligence Integration*: Use real-time threat intelligence feeds (e.g., VirusTotal) to stay updated with emerging attack vectors

Behavioral Anomaly Detection: Detect insider threats and compromised accounts using ML-based user behavior analysis.

System Workflow



Data Collection: Collect logs from network traffic, user behavior, and endpoints.

Preprocessing: Filter, normalize, and extract key data (e.g., IPs, login patterns)

Detection: Combine rule-based detection (Snort) with anomaly detection (ML models)

Reporting: Generate real-time dashboards and forensic reports for incident analysis and compliance

Automated Response: Notify admins, block malicious IPs, and isolate affected systems

✸ USE CASE

Attack Type	A phishing email tricking a user into revealing credentials.
Detection	- Honeypot detects the attacker attempting to access decoy systems. - Behavioral anomaly detection flags unusual login locations and times.
Response	- System blocks attacker IP and alerts the admin in real time. - Automatically isolates the affected system to prevent lateral movement.
Industries Applicable	Banking, Healthcare, E-commerce, and IoT ecosystems.

Feasibility and Viability

Feasibility

Technology Used:
-Tools: Snort, Suricata, and ELK Stack.
-Programming: Python for automation, TensorFlow for ML models.
-Threat Intelligence: VirusTotal APIs for signature updates.

Deployment Options:
- Scalable for on-premise or cloud environments.
- Testable with simulated attacks (e.g., using Metasploit).

Viability

Cost Efficiency:
- Reduced need for manual intervention lowers operational costs.

Business Impact:
- Minimizes downtime and data loss during attacks.
- Ensures compliance with regulations like GDPR and ISO 27001.

Tech Stack

Programming Languages	Python (for automation), Java (backend development).
Detection Tools	Snort, Suricata.
Machine Learning Frameworks	TensorFlow, Scikit-learn.
Threat Intelligence	VirusTotal, AlienVault APIs.
Reporting	Kibana, Grafana dashboards.
Database	MongoDB or PostgreSQL for incident logging.

References

Public Datasets:
- NSL-KDD, CICIDS for ML model training.

Open-Source Tools:
- Snort, Wireshark, and the ELK Stack.

Documentation:
-Official resources for VirusTotal , TensorFlow, and Kibana.

Attack Simulation Tools:
- Metasploit Framework for controlled testing of the solution.