FUTURE FITS

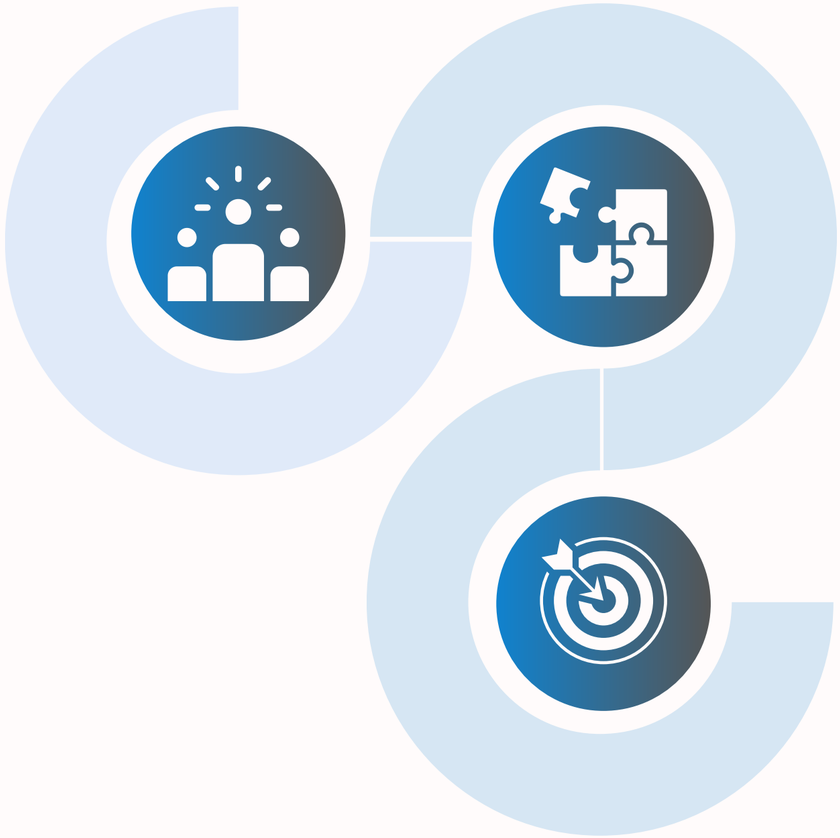
THREAT DETECTION SYSTEM

GOALS AND OBJECTIVES

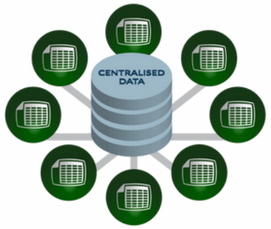
01 The framework employs advanced AI/ML models for innovative compromise detection, emphasizing anomaly detection and behavioral analysis.

02 Effortless deployment and integration are achieved, ensuring secure communication and integration strategies for various detection methods.

03 Evaluation criteria prioritize innovation, device versatility, deployment ease, and false alarm reduction for early compromise detection without relying solely on IoCs, advancing cybersecurity.



KEY FEATURES



Centralized Analysis

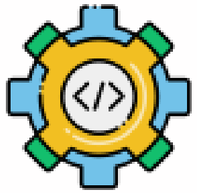
Delivering top-tier security with ease. Because your protection deserves the best.

Alarm System

Our alarm system ensures timely event reminders through instant, real-time notifications.

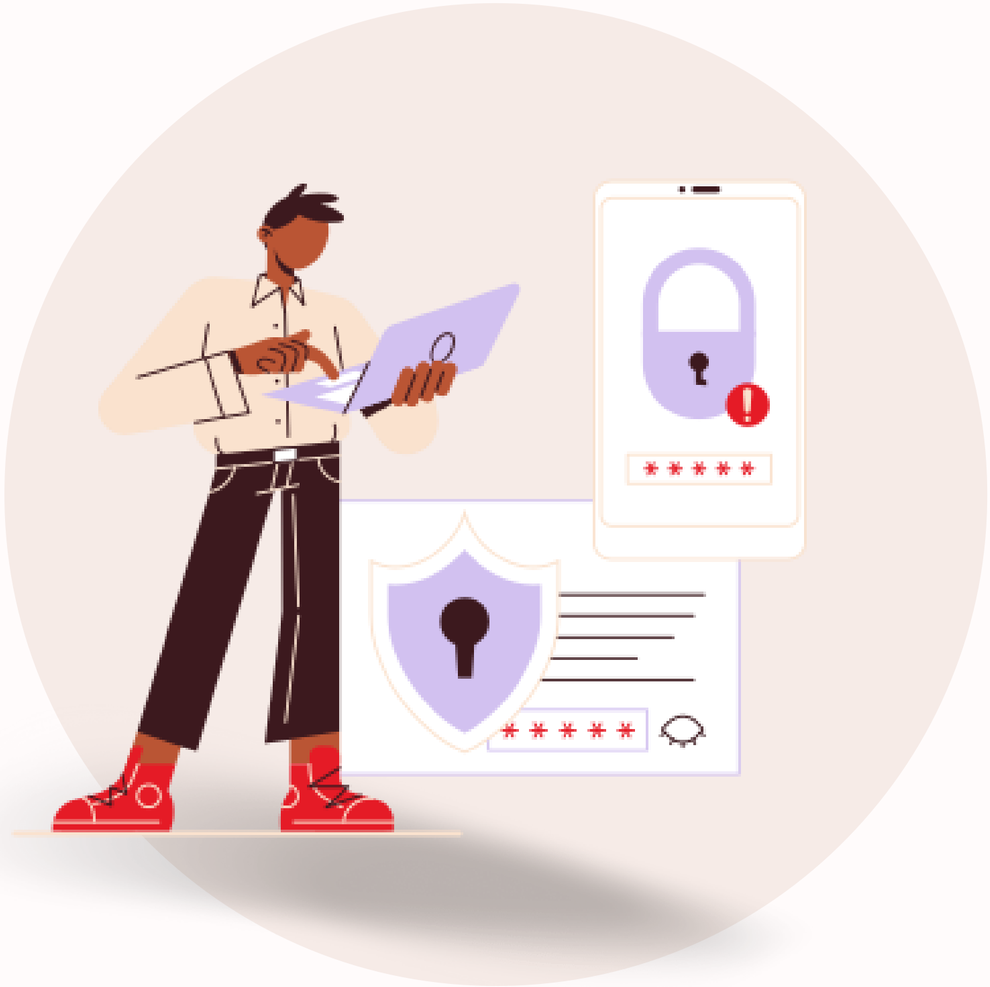
Stay Organised

Stay organized with our system, combining timely alerts and thorough analysis for ultimate vigilance in managing tasks or security measures efficiently.



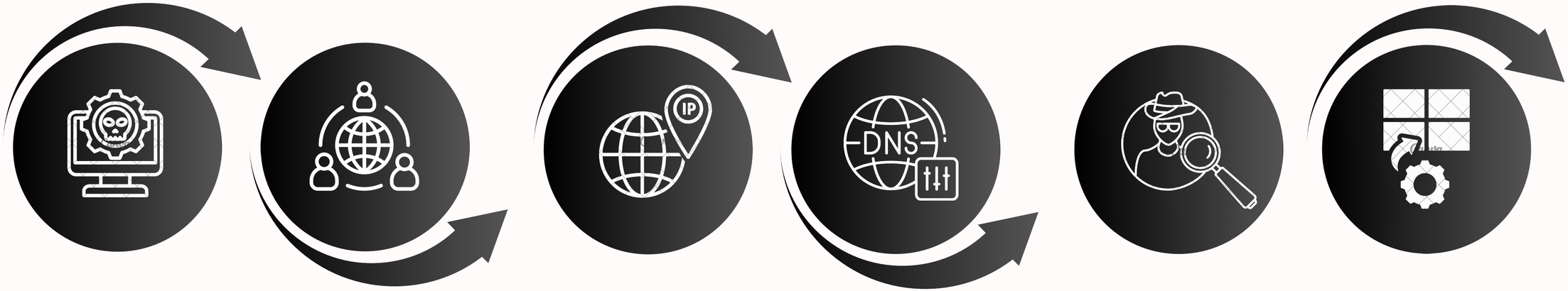
Integration Capabilities

Compatible with diverse platforms and systems, our solution ensures a unified experience for streamlined operations



How our cutting-edge cybersecurity solution will reshape industries

Our innovative system, powered by AI/ML, ensures robust threat detection. It monitors real-time malicious activities through system calls, detects network anomalies, filters IPs based on geolocation, and analyzes DNS activity. Adaptable to diverse devices, our secure reporting system and proactive measures minimize false alarms.



Malicious Activity Detection

Network Anomaly Detection

Geolocation-Based IP Filtering

DNS Activity Analysis

Ransomware Detection in Windows

Windows Event Logs and Registry Keys

How it used to work without AI

- Rule-Based Systems: detect threats by monitoring patterns, triggering alerts for manual response.
- Incident Response Plan: Establish a concise incident response plan for swift security incident handling.
- Firewall Logs Analysis: These logs expose unauthorized access and anomalies for swift analysis and detection.

How we tried integrating it with AI

- AI-Enhanced Threat Detection: focus on detecting anomalies and deviations for robust threat detection.
- Modular Flexibility: Independent components in Docker containers ensure flexible threat detection across diverse devices.
- Precision Reporting and Minimized False Alarms: Secure real-time reporting minimizes false alarms using whitelisting and continuous learning.

Our system uses process behavior analysis, tracking system calls to detect malicious activities through deviations from expected patterns.

MALICIOUS ACTIVITY DETECTION

Our system uses flow monitoring to group packets into flows, allowing efficient anomaly detection for enhanced network security.

NETWORK ANOMALY DETECTION

We boost network security with geolocation-based IP filtering, using statistics to identify anomalies precisely.

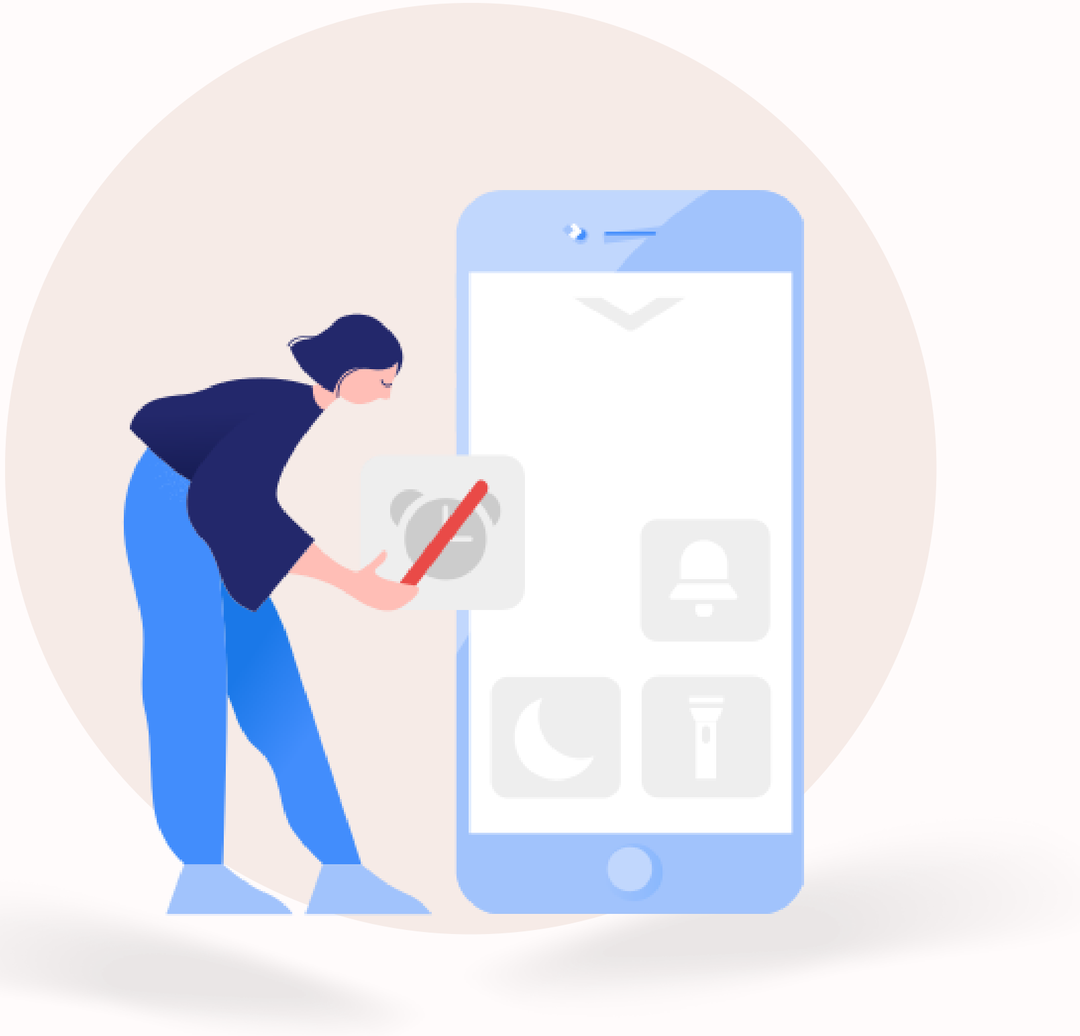
GEOLOCATION BASED IP FILTERING

Employs N-gram analysis and Deep Learning for Swift detection of changes in packets related to malicious DNS activities, enhancing security.

DNS ACTIVITY ANALYSIS

Utilizing whitelisting, continuous machine learning, and baseline profiling for enhanced threat detection accuracy using an alerting system.

MINIMIZING FALSE ALARMS



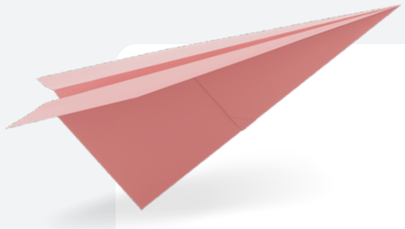
FUTURE WORK

OPTIMIZE LINUX SERVER DATA COLLECTION WITH SYSLOGS

PROTOCOL-AGNOSTIC ANOMALY DETECTION PROTOCOL

SILK FRAMEWORK AND PASSIVE DNS

DOCKERIZED PLATFORM INDEPENDENCE



THANK YOU

Please give us some suggestions.