AUSIEM

ALERTING TODAY FOR SECURE TOMORROW

FEATURES

Flexible Data Collection
Collection of events/logs from diverse data sources for threat detection.

Log Management
Efficient log management to achieve long-term data retention.

File Integrity Monitoring
Monitors file system, identifying changes in content, permission, ownership, and attributes of files.

Vulnerability Detection
Automated vulnerability assessment of critical systems through software audit.

User Behaviour Analytics
Detection of abnormal user activity and compromised user account.

IoT Devices Monitoring
Provides support for monitoring the IoT devices.

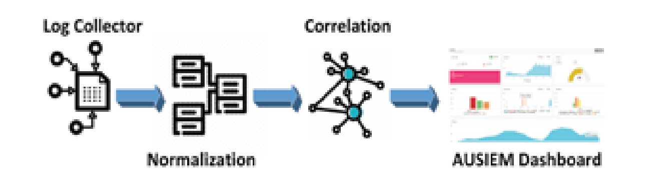
Threat Intelligence
Secure monitoring by unifying threat intelligence across enterprise network.

Real-time Alerting and Reporting
Provides real-time analysis to highlight issues for immediate attention by the network administrators.

Regulatory Compliance
Provides necessary controls to become compliant with industry standards and regulations.

KEY BENEFITS

- Real-time collection and analysis of logs and events
- Rapid Incident response, real-time analysis, and threat detection with live dashboard and alerting
- Active user behavior monitoring and analysis to mitigate insider threats
- Reduced operational risk and process automation following compliance standards
- Streamline analyst activities, end-to-end incident tracking with the active investigation, and alerting security operations



What is AUSIEM?

- Detects and prioritizes threats across the enterprise and also provides intelligent insights that enable security analysts to respond quickly
- Consolidates log events and network flow data from different devices and applications distributed throughout the network
- Designed to analyze high-volume streams of data in real-time to quickly and accurately detect non-compliant system activity, malicious behavior, security issues, and cyber threats

WHY AUSIEM?

- It provides centralized logging capabilities for enterprise sand security professionals can use it to analyze and report on the log entries that it receives
- It can detect various malicious activities and attacks across the enterprise network

AUSIEM DASHBOARD

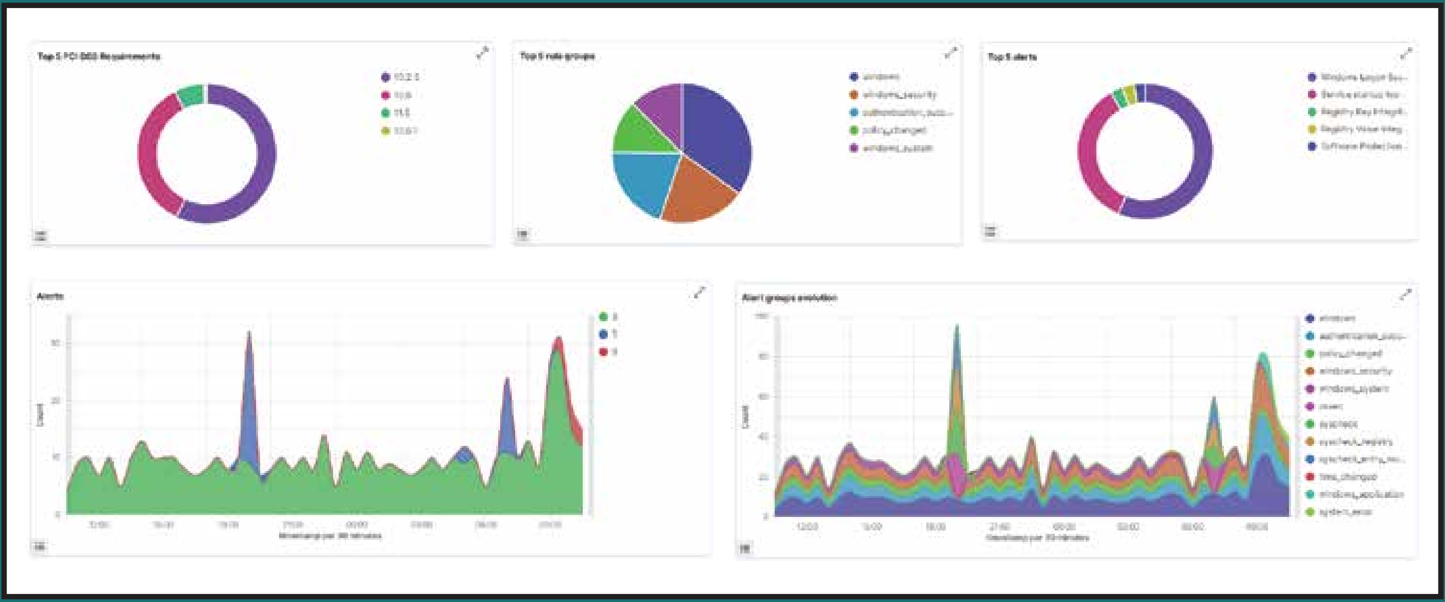
A smart and simple way to manage, visualize and prioritize network security alerts. Continuous real-time security that allows identification of activities, trends, and patterns easily. Dynamic real-time view of all network connections, system activities, and user interactions.

Devices & Network Security Lab

NETWORK CYBER DEFENCE GROUP

Securing network infrastructure against cyberattacks is among one of the top priorities in any private sector, government department, military or any other sensitive organization.

Our fundamental research is towards the development of an indigenous Security Information and Event Management (SIEM) solution, a system that provides real-time analysis of security alerts generated by applications and network devices.



WHO IS IT FOR?

- SOC Analyst
- Security Platform Operations Engineer
- Forensic Investigator
- Network Administrator

NCCS
NATIONAL CENTRE FOR CYBER SECURITY

DNS Lab, Air University, E9, Islamabad
+92-51-9153657 dnsl@nccs.pk