Tech4UK
SEERSIEM

Security Operation Center

About

SeerSIEM: Security Operation Center

Empower your organization to proactively defend against cyber threats with SeerSIEM. Our comprehensive Security Information and Event Management (SIEM) solution provides real-time visibility into your network, empowering you to detect, investigate, and respond to security incidents swiftly and effectively.

By centralizing log data from diverse sources, SeerSIEM enables you to analyze security events, identify anomalies, and detect advanced threats. With advanced analytics and machine learning capabilities, our solution automatically prioritizes critical alerts, reducing alert fatigue and enabling rapid response.

(ISAC) Information sharing and Analysis Center

(KB) Knowledge Base

(CRE) Correlation and Response Engine

(PD) Pattern Discovery

(LM) Log Management

(AD-VA) Asset Discovery and Vulnerability Assessment

(NDR) Network Detection and Response

(NIDS) Network based Intrusion Detection System

(LCA) Log Collector Agent

(LC) Log Collector

Product Architecture

Scalable and extensible architecture

- Distributed agent deployment
- Deployment of diverse analytical sensors in subsidiary organizations
- Hierarchical deployment architecture
- Scalable to handle hundreds of thousands of events per second

Data Collection

- Data Collection from Diverse Sources
- Contextual Data Normalization
- Customizable for a wide range of devices and systems
- Comprehensive coverage for hundreds of devices and services by default

Automated Response

- Automated command execution via API
- Supports Telnet and SSH protocols
- User-defined scripts for automation
- Full flexibility in defining command execution conditions
- Unified solution for multiple threat vectors

Intelligent threat detection

- Machine learning-based behavioral analytics
- Scenario-Based Attack Analysis
- Intelligent Event Classification
- Capability to Implement Custom Use Cases

Efficient data retention

- Powerful search capabilities
- Diverse data visualization options
- Fully customizable reports
- Minimal storage consumption with long-term data management

Knowledge base

- Continuous knowledge base updates
- Integrated Knowledge Management for All Modules
- Comprehensive coverage of diverse security scenarios and policies
- Full customization of data sources, rules, and policies

Security Operations Center (SOC) Services

- 24/7 Support
- Continuous updates and enhancements
- Managed security services
- Design and implementation of SOC solutions and processes
- Consultation for Evaluating and Improving SOC Metrics


Tech4UK
SEERSIEM