Cuttingej SIEM Appliance

Security Information and Event Management

Business Benefits

Enhanced Security Posture:

Improved threat detection capabilities and faster response.

Cost Efficiency:

Reduction in potential damage costs through early detection.

Compliance Readiness:

Supports adherence to multiple regulatory frameworks.

Customer Trust:

Increases security reliability for customers and stakeholders.

Differentiators:

Comprehensive security toolset

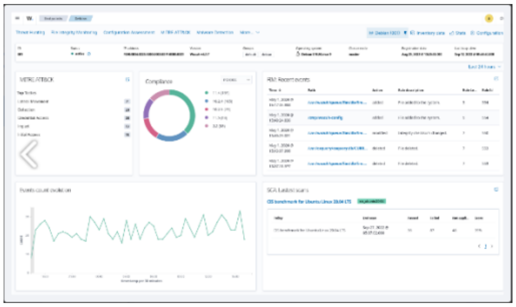
Seamless Zero Trust Integration

Integrated threat intelligence with OSINT

End-to-End Incident Management automation if required

Interoperability across environments

Enterprise support and Patch Management from Cuttingej



A **Security Information and Event Management (SIEM) appliance** is an essential tool for modern cybersecurity infrastructures, designed to provide real-time monitoring, detection, and response capabilities. A SIEM appliance aggregates, analyzes, and correlates data from a wide array of network sources, applications, and security devices, enabling organizations to detect security threats, manage compliance requirements, and respond to incidents in a timely manner.

Deployment Architecture:

- **Hybrid Infrastructure Support**: On-premises and cloud-based integration for log ingestion and monitoring.
- **Scalability**: Can be scaled to support growing log volumes and new data sources.
- **Interoperability**: Supports various data sources like firewalls, endpoints, and applications.

Use Cases:

- **Reconnaissance Detection:** Identifying and responding to attempts to gather unauthorized information.
- **Lateral Movement Monitoring:** Detection of threats moving within the network.
- **Ransomware and Malware Detection:** Identifying signs of malicious software activity.
- **Compliance Monitoring:** Ensuring that security controls align with industry standards.
- **Threat Intelligence Integration:** Automatic reputation checking of suspicious IPs, domains, and file hashes.

SIEM Solution Overview

- **Components and Tools:**
- **Wazuh**: Provides log analysis, threat detection, and vulnerability assessment.
- **Suricata**: Network threat detection engine with capabilities for intrusion detection (IDS) and prevention (IPS).
- **Spiderfoot**: OSINT tool for threat intelligence gathering.
- **OpenSearch**: Centralized search and analytics engine for log aggregation and analysis.

- **Solution Scope and Key Features:**
- **Log Analytics**: Aggregation and analysis of logs from various sources.
- **Threat Intelligence**: Integration of real-time threat intelligence feeds.
- **Anomaly Detection**: Detection of suspicious and malicious activities across network and endpoints.
- **Incident Response**: Workflow for handling security incidents.
- **Compliance**: Assists in meeting regulations like ISO, GDPR, HIPAA, and PCI.

Cuttingej Solutions India Pvt Ltd
www.cuttingej.com