Newsletter

Inside THE ISSUE

SIEM

A Security Information And Event Management (SIEM) solution supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.

SIEM Benefits

- Enhanced Security
- Early Threat Detection
- Compliance Management
- Improved Incident Response
- Centralized Visibility
- Data Analysis
- User and Entity Monitoring
- Historical Analysis
- Resource Optimization
- Integration Capabilities

SIEM Capabilities

- Log Management
- Real-time Monitoring
- Alerting and Notification
- Correlation Engine
- Compliance Management
- User and Entity Behavior Analytics (UEBA)
- Incident Response
- Threat Intelligence Integration
- Data Encryption and Security
- Integration Capabilities

Well Known SIEM Solutions

- Splunk Enterprise Security
- IBM QRadar
- LogRhythm
- ArcSight (Micro Focus Security ArcSight)
- AlienVault USM (now AT&T Cybersecurity)
- SolarWinds Security Event Manager
- McAfee Enterprise Security Manager (McAfee ESM)
- Elastic Security (formerly known as the ELK Stack: Elasticsearch, Logstash, Kibana)

SIEM Key Processes

- **Data Collection:** Gather data from various sources, such as logs and configurations.
- **Normalization:** Standardize data formats for consistent analysis.
- **Correlation:** Identify patterns by analyzing data from multiple sources in real-time.
- **Alert Generation:** Generate alerts for potential security incidents.
- **Incident Investigation:** Investigate alerts to understand the nature and impact of incidents.
- **Incident Response**: Develop and execute a response plan to contain and mitigate the incident.
- **Forensic Analysis:** Analyze incidents in-depth for understanding and evidence gathering.
- **Reporting:** Generate reports on incidents and security status for compliance and analysis.