SIEM Managed Security Service Solutions

SIEM Managed Services

Complete Integrated Managed Solutions:

- ☑ Security Monitoring
- ☑ Assess
  - Vulnerabilities
  - Threats
- ☑ Asset Management
- ☑ Alerting
- ☑ Forensics
- ☑ Compliance

PICK YOUR SIEM FEATURES

- Asset Management
- Log Monitoring, Correlating, Analysis
- Intrusion Detection
  - Host, Network, AP
- File Integrity Monitoring
- Vulnerability Assessment
- Behavioral Monitoring
- 24x7 or 8x5 Monitoring
- Alert Response
- Security Tuning
- Configuration Changes
- Maintenance & Updates
- Compliance Reports
- Forensic & Other Support

Demystifying Security

Compliance Level Managed Services for Security Monitoring

SIEM Solutions Regardless of Your Needs

eSecurity Solutions provides two solutions to satisfy compliance and enhanced security requirements in the area of Security Information and Event Management (SIEM).

1) We provide a completely Managed Unified Security (MUS) monitoring and security threat management solution for your business enabling compliance with all major security regulations. Our service goes beyond traditional SIEM solutions providing a customized managed solution that will a) detect security system vulnerabilities, b) alert you to security threats or intrusions, c) enable security systems optimization, and d) measure, manage and report on compliance 24x7.

2) We can also provide a more traditional log monitoring and event management solution that integrates monitoring of all of your log generating devices and systems into a single security solution.

Who Needs an SIEM?

Due to increasing regulations and pressure by business partners an increasing number of companies are needing to assess their security risks, plan and implement more comprehensive security for their businesses. Most companies are finding a void in their security around security monitoring, alerting, forensics and reporting.

Typical motivators for security monitoring are:

1) To be compliant with security regulations such as HIPAA, PCI, SOX, banking and financial etc.
1) Partners, suppliers or customers that require that they prove or attest to being security compliant
2) Protecting important digital assets like financial data, Intellectual property, customer private data (health, financial, SS#, etc)

Managed Unified Security (MUS)

MUS is unique because it provides five essential security compliance monitoring capabilities in a single solution, integrating security threat information from multiple data intelligence sources on your network. These capabilities include: asset discovery, SIEM, Threat detection (IDS), behavior monitoring, and vulnerability assessment. Unlike traditional SIEM only solutions, MUS provides a more complete security solution that extends beyond basic Log event and information monitoring. This makes your organization more secure and solves more pieces of the security solution puzzle.

Companies large and small are increasingly being asked to provide compliance level security for their companies. Using the MUS service solves 4 important security problems for companies:

1) Meet compliance requirements for HIPAA, PCI, SOX, Banking, ISO etc. Security monitoring is required by all major security standards
2) Satisfy 3rd party requirements for compliance such as business partners and customers.
3) Proactively monitor and alert for threats and intrusions in your security system and provide remediation alternatives. This is an essential part of any complete security infrastructure
4) Reduce the cost of managing and monitoring your security

Log Event Manager (LEM)

Log Event Manager provides a lower cost SIEM with the core capabilities that are required by security regulations and enhanced security. LEM provides log collection from security and network devices, servers, clients, cloud servers and apps and corporate applications. Once collected, they are analyzed, correlated and provide alerts and forensic capabilities. eSecurity Solutions wraps that up in a complete managed service so you don't have to become an expert in this advanced technology.

SIEM Managed Security Services

Managed Unified Security (MUS) Services vs Log Event Manager (LEM) SIEM

To satisfy the current requirements for thorough security, organizations are required to collect, analyze, report on and archive all logs to monitor activities inside their IT infrastructures. The intent is not only to detect external threats, but also to provide periodic reports of user activities and create forensics reports surrounding a given incident. Details of the two solutions provided by eSecurity Solutions are in the chart below.

SECURITY CAPABILITIES: MANAGED UNIFIED SECURITY (MUS) vs Log Event Mgr (LEM)

Security Control Capabilities	Managed Unified Security	Log Event Manger
Multi-Source Monitoring, Analysis, Correlation & Alerting	✓	**Logs**
Asset Management (Hosts, Services & Software Discovery)	✓	Opt
Vulnerability & Threat Assessment (Current & Historical)	✓	Opt
Threat Detection (NW, Host, File, Wireless IDS)	✓	**File**
User Management & Access Control	✓	**Logs**
Behavioral Monitoring & Anomaly Detection (OS Services, Net flow, NW Protocols & Packet Capture)	✓	
Forensics (Logs, Net flow, Packets, IDS, Vulnerability Scans, Assets)	✓	**Log & Event Data**
Reporting (Compliance & Custom)	✓	✓
Managed Services	**Yes - 8x5 or 24x7**	**Yes - 8x5**

Do-it-Your-Self Typically Does Not Work

Self-managed SIEM solutions typically have a shelf life of approximately 18-24 months before organizations give up and begin to look for another solution. Most organizations cannot support these deployments and many SIEM implementations fail.

Management Services Provided

We provide all the services needed to install, manage, maintain and support you with the Unified Security Service.

1) **Understand your security system architecture & Define the MUS Monitoring Policies**
2) **Install the necessary MUS agents and management support infrastructure**
3) **Configure and tune the MUS system**
4) **Provide these ongoing services:**
   a. Asset Inventory (MUS)
   b. Internal vulnerability scanning (MUS)
   c. Log collection
   d. Event correlation and analysis
   e. Host Intrusion Detection (MUS)
   f. File Integrity Monitoring
   g. 24x7 or 8x5 monitoring (depends on service)
   h. Daily review of prior day's activity as required by PCI and other regulations
   i. Setup customer reports
   j. System Maintenance, and software updates
   k. Email, ticket or phone Customer Support 24x7 or 8x5 (depends on service)

Providing your Company with Better Security, Visibility and Expert Partner Support

Visibility of your security infrastructure and correlated security intelligence is all available with eSecurity Solutions Managed SIEM. We monitor and analyze your security information and events and then work with you keep you secure and compliant.

You won't need to see all the data that we sort through on a daily basis so that you can focus on other key corporate objectives. We will customize reports to be sent to you to meet your needs and compliance requirements.

Call us today to discuss the right Managed SIEM solution for you.