

SIEM Managed Security Service Solutions

Managed SIEM 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 SIEM 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 proof of regulation compliance.
- 2) Protecting important digital assets like financial data, Intellectual property, customer private data (health, financial, SS#, etc)

Managed SIEM

Our Managed SIEM is unique because it uses the leading SIEM in the market **IBM QRadar**. It provides all 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, superior threat intelligence, Cloud or on-premise security monitoring, User Behavior Analytics (UBA), and vulnerability assessment. Unlike traditional SIEM only solutions, Managed SIEM 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 managed SIEM 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 SIEM 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 IBM QRadar SIEM vs Log Event Mgr (LEM)

Security Control Capabilities	Managed IBM QRadar SIEM Security	Log Event Manger
Multi-Source Monitoring, Analysis, Correlation & Alerting	✓	Logs
Integrates with >450 Security Products & Pre-Built Apps	✓	
Threat Intelligence Sources	IBM X-Force	Open Source
Correlates Events from On-Premise & Cloud Sources	✓	
User Behavior Analytics (UBA)	✓	
Vulnerability Management	Opt	
AI Incident Investigation	Opt	
Network Flow Inspection	Opt	
User Management & Access Control	✓	Logs
Asset Management	✓	Opt
Forensics (Logs, Net flow, IDS, Vulnerability Scans, Assets)	✓ (Varies by Options Selected)	Log & Event Data Only
Reporting (Compliance & Custom)	✓	✓
Managed Services & MDR Services	Yes - 8x5 or 24x7	Managed Only - 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 our SIEM or Log Management Services.

- 1) Understand your security system architecture & Define the managed SIEM Monitoring Policies
- 2) Install the necessary agents and management support infrastructure
- 3) Configure and tune the managed SIEM system
- 4) Provide the security management and monitoring services listed above for each managed product.
 - a. 24x7 or 8x5 monitoring (depends on service)
 - b. Daily review of prior day's activity as required by PCI and other regulations
 - c. Setup customer reports
 - d. System Maintenance, and software updates
 - e. Email, ticket or phone Customer Support 24x7 or 8x5 (depends on service)
- 5) Optional full MDR Managed Detection and Response service for IBM QRadar in an integrated security stack.

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.