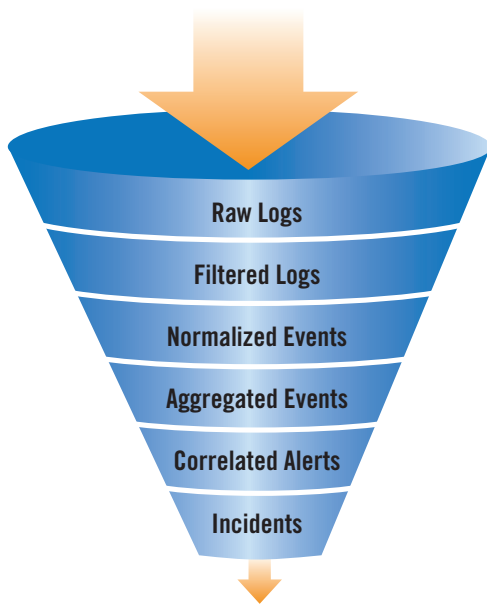


LogLogic® Security Event Manager

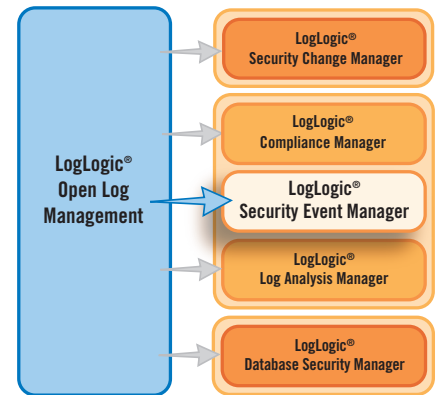
Simplify Security Event Management

Security and IT managers need a security incident response program that is highly effective, yet easy to implement and maintain. Whether the end-goal is to meet regulatory requirements, mitigate risk, or to achieve best practice objectives, the LogLogic Security Event Manager (SEM) provides organizations with the ideal solution to simplify their security management processes while improving overall security and forensics and reducing time to resolution.



By analyzing the thousands of complex events generated from firewalls, IDS/IPS, operating systems, databases and applications—in real time—LogLogic SEM reveals the most critical security incidents and provides deep insights into the security posture of the IT infrastructure. By correlating events with prioritized asset and vulnerability information, LogLogic SEM enables security analysts to quickly prioritize security incidents and mitigate threats.

LogLogic SEM's built-in incident workflow and service level agreement (SLA) management features provide security and operations personnel with the tools they need to be more efficient in responding to external and internal threats. The LogLogic SEM solution is a third generation security event management appliance, custom-built for security incident and threat management and powered by LogLogic's industry leading open log management platform.



Key Features and Benefits

Natural Language Policy Editor

LogLogic SEM employs a unique, top-down security event schema that enables human language communication. Rules are created and alerts are shown, using simple concepts such as “Accepted,” “Denied” and “Access Granted.” Generic rules are not only easier to use, but they also provide more accurate processing with fewer rules and increased performance.

Advanced Correlation and Analysis

LogLogic SEM's correlation engine distills millions of disparate log entries into logical categories and classifies them into related events. LogLogic SEM prioritizes security alerts based on event severity, asset criticality, system vulnerability and attack history.

Built-in Incident Workflow and SLA Management

LogLogic SEM maintains a built-in incident workflow and SLA management system tailored specifically to threat management and security professionals. LogLogic SEM also integrates with external incident management systems, such as BMC Remedy Action Request System.

LogLogic Security Event Manager

System Management

- AJAX-Powered GUI (Internet Explorer, Firefox)
- Command line interface

High Availability

- External backup capabilities
- Active/Standby high availability option
- Hot swappable redundant power supplies (SEM1060, SEM3060, SEM4060, SEM4070)
- RAID support (all models)

Operating Environment

- 64-bit RedHat Linux operating system

Virtual Appliances

- SEM4070 is designed especially for MSSPs and optimized for hosting multiple LogLogic SEM virtual appliances

Device Support

- Supports over 200 common devices and applications
- Wizard-based setup for custom log sources
- Any local log file collection through HTTP, HTTPS, SCP, SFTP, FTP, FTPS and SMB/CIFS
- Relational database collection through ODBC/JDBC
- Microsoft Windows event collection through Microsoft WMI or Lasso Enterprise
- All syslog and syslog-NG protocol compliant devices, including firewalls, VPNs, routers, switches, servers and other devices
- Check Point OPSEC devices including firewalls and VPN systems

Safety and Emissions Certification

- FCC (U.S. only) Class B
- ICES (Canada) Class B
- CE Mark (EN 55022 Class B, EN55024, EN61000-3-2, EN61000-3-3)
- VCCI (Japan) Class B
- BSMI (Taiwan) Class A
- C-Tick (Australia/New Zealand) Class B
- SABS (South Africa) Class B
- CCC (China) Class B
- MIC (Korea) Class B
- UL 60950
- CAN/CSA C22.2 No. 60950
- EN 6095

Appliance Specifications

	SEM1060	SEM3060	SEM4060	SEM4070
Events per second	1,500	3,000	5,000	10,000*
Storage capacity (Raw)	900GB (RAID 1)	1.8TB (RAID 10)	2.7TB (RAID 10)	1.8TB (RAID 10)
On-board Storage capacity (including compressed data)	600GB	1.2TB	1.9 TB	1.2TB
Power supply	2x670 watts	2x750 watts	2x750 watts	2x1050 watts
Chassis	1u	2u	2u	4u
Ethernet	2x10/100/1000	2x10/100/1000	2x10/100/1000	2x10/100/1000
Support external disk array	Yes, for ADA only	Yes	Yes	Yes
Support external SAN	No	No	Yes	Yes
High availability	No	Yes	Yes	Yes

*Based on an environment with multiple virtual appliances.

More information

Visit www.loglogic.com or contact a LogLogic representative by e-mail: info@loglogic.com, or phone: 1.888.347.3883.

LogLogic is a registered trademark in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. LogLogic reserves the right to alter product offerings and specifications at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document.

© 2009 LogLogic, Inc. All rights reserved.

