SOLARWINDS® LOG & EVENT MANAGER (LEM): USE CASES

SIEM is an integral piece of any effective security plan and goes well beyond compliance purposes. SIEM technology provides critical insight into network activity to detect threats, thwart attacks, and respond to breaches—external and internal. The goal of SIEM is to provide actionable intelligence to mitigate risks and remediate incidents as fast as possible, be it a security risk or IT operational issue.

The purpose of this document is to highlight the many use cases of SolarWinds Log & Event Manager (LEM)—a SIEM and log management solution that provides log collection, analysis, and true real-time, in memory event correlation to address an ever-increasing list of security threats, operational challenges, and compliance requirements faced by network and security admins.

Security Monitoring

SolarWinds LEM collects log and event data from security devices and applications and provides real-time analysis and correlation to deliver immediate awareness of security related issues like viruses, unauthorized access, denial of service, and a plethora of other security events. LEM has over 30 built-in automated responses, includingthe ability to disconnect an offending machine from the network at the NIC card level, start/stop services, kill applications, remove suspicious users from an administrative group, detect and prevent unapproved USB usage, and many more.

- Helpful resources to configure security devices and applications::
  - The complete list of Knowledge Base (KB) articles to configure connectors:
    - Log and Event Manager Connector List
  - Commonly used connectors:
    - Integrating Check Point with LEM
    - Integrating Juniper Firewalls with LEM
    - Configuring MSSQL Auditor on a LEM Agent
- How-to set up rules and take actions in real time:
  - LEM comes with a set of rules enabled by default. While none of these rules perform any action on the network, they do escalate events to security alerts, based upon inference
  - How-To KB: Creating Rules from LEM to take Automated Actions
  - How-To Video:
    - Creating Rules in your LEM Console
    - Actively Defending Your Network with LEM Custom Rules
  - List of KBs on how active responses work:
    - LEM Active Responses
  - Commonly used Active Responses:
    - How does the Disable Networking Active Response work?
    - How do the Kill Processes Active Responses work?
    - How does the Block IP Active Response work?

Compliance

LEM provides complete report packages for nearly all of the regulated industries to include PCI, GPG13, ISO, SOX, GLBA, NIST/FISMA, NCUA, FERPA, NERC/CIP and more.

LEM allows you to:

- Utilize over 300 built-in compliance report templates
- Filter information to customize reports for specific departments or recipients
- Produce graphical summaries to enhance your high-level reports
- Support forensic analysis findings with detailed reports
- Export reports to a variety of standard formats

Generating reports with LEM is simple and easy. You can utilize over 300 built-in report templates for internal and external regulatory compliance reports, such as: PCI DSS, GLBA, SOX, NERC CIP, or HIPAA, or create a custom report using LEM's intuitive reporting console.

Learn more about how to meet compliance requirements using LEM here:

- LEM PCI (Whitepaper)
- Compliance Security Simplified with LEM (Video)
- LEM Reports (Video)

Change Management

LEM can provide constant real-time awareness of change management activity across the enterprise. Customers can be alerted when changes occur on routers, switches, firewalls, user accounts, Active Directory®, and more. Active Responses can be attached to correlation rules to automatically mitigate change activity like privilege escalation or de-escalation.

Learn more about LEM's change management features here:

- Creating Rules from your LEM Console to Take Automated Action (KB article)
- Creating Rules in your LEM Console (Video)

Change-related rules that ship with LEM:

Name	Description
Auditable Events Change Policy Violation	Tracks group/account/machine changes by unauthorized users This rule uses the Change Management alert group, which is actually just a cor
Policy View/Change	Network Device Policy View/Change Events By checking for InsertionIP not equal to DetectionIP, we are looking for devices that are using a rer
Database User Change	Detects modifications to database users Note: You must be using a TriGeo database auditing utility (such as MSSQL Auditor) in order to captu
MSSQL Database Change Attempt	Monitors change attempts to an MSSQL Database Note: You must be using a TriGeo database auditing utility (such as MSSQL Auditor) in ord
MSSQL DB Object Change Attempt	Monitors change attempts to MSSQL DB Objects NOTE: You must have the MSSQL Auditor tool installed and monitoring the SQL database in

Built-in change management reports:

Change Management - General Authentication: Domain Events	Audit	Master	Authentication
Change Management - General Authentication: Domain Events - Change Domain Attribute	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - Change Domain Member	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - Delete Domain	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - Delete Domain Member	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - Domain Auth Audit	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - Domain Member Alias	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - New Domain	Audit	Detail	Authentication
Change Management - General Authentication: Domain Events - New Domain Member	Audit	Detail	Authentication
Change Management - General Authentication: Group Events	Audit	Master	Authentication
Change Management - General Authentication: Group Events - Change Group Attribute	Audit	Detail	Authentication
Change Management - General Authentication: Group Events - Delete Group	Audit	Detail	Authentication
Change Management - General Authentication: Group Events - Delete Group Member	Audit	Detail	Authentication
Change Management - General Authentication: Group Events - Group Audit	Audit	Detail	Authentication
Change Management - General Authentication: Group Events - New Group	Audit	Detail	Authentication
Change Management - General Authentication: Group Events - New Group Member	Audit	Detail	Authentication

Application and Server Monitoring

LEM provides the ability to monitor and control what applications can be utilized. It also provides visibility into critical service activity in the network to ensure everything remains operational. Additionally, correlation rules can be applied to automatically restart a critical service if it's stopped. This can be accomplished by defining a "Group" by specifying which processes should be running or which should not according to industry standards.

Learn more about application and server monitoring with LEM here:

- Getting Started with User Defined Groups (KB article)
- Creating Rules from your LEM Console to Take Automated Actions (KB article)
- Configuring MSSQL Auditor on a LEM Agent (KB article)
- Integrating your Oracle Database with SolarWinds LEM (KB article)

User Activity Monitoring

LEM provides real-time visibility into a user's behavior on the network, including Web usage, application usage, file access, and more.

Why Should I Monitor Successful Logon Attempts?

Although it may not seem intuitive to manage successful logon attempts, it's good practice to keep an eye out for successful logons that occur after multiple failed attempts. For example, if there are 50 failed attempts on a server or router followed by a successful logon, does it imply that the user simply remembered their credentials? Or does it mean that a hacker finally broke in and now has access? What about the case where a user logs on to the network at the headquarters and two hours later has a successful logon from the other side of the world? Monitoring successful logons can be very beneficial when correlated with other log activity.

User activity rules that ship with LEM:

Authentication - Unknown User	An authentication event for an account not in Domain Users
Unique User Logon Violation	Logs off a user that has simultaneously logged in from multiple source machines. This rule is related to HIPAA requirements of "unique u
User Logon After Hours	Monitors users logging in outside of business hours and logs them off
User Logon but no Agent	To be used in environments with Static IP addressing. Use this rule instead of the DHCP but no Agents rule, if you do not use DHCP.
Critical User Events	Looks for changes to Admin Accounts
User Account Events	Auditable User Events
New User Created/Enabled	Events that are created when a new user is added.
User Account Created	New user account created.
User Account Deleted	Account Administratively Deleted
User Account Disabled	Account Disabled by an Administrator Account actively disabled by administrator (not a self-lockout).
User Account Enabled	User Account Administratively Enabled
User Account Lockout (Updated)	Automatic Account Disable (Lockout) User disabled automatically by lockout mechanism.
User Account Properties Update	User account properties changed. If you are getting false positives from local PCs or events you can't make sense of, two suggestions are to
User Account Properties Update (2)	Account properties changed without a special detail event.
User Added to Group	Group member added
User Added to OU	User moved into an OU
User Removed from Group	Group member removed
User Removed from OU	User moved out of an OU
Database User Change	Detects modifications to database users Note: You must be using a TriGeo database auditing utility (such as MSSQL Auditor) in order to captu
MSSQL Unknown User Logon	Monitors authentication attempts from users not in the domain NOTE: You must have Directory Services integration configured and be using ar
VPN Unauthorized User Access Attempt	Attempted authentication to the VPN from an unauthorized user NOTE: You will need to populate the Authorized VPN Users User-Defined grou

Available User-based Active Responses within LEM:

User-based Active Responses:

- Add Domain User To Group
- Add Local User To Group
- Create User Account
- Create User Group
- Delete User Account
- Delete User Group
- Disable Domain User Account
- Disable Local User Account
- Enable Domain User Account
- Enable Local User Account
- Log Off User
- Remove Domain User From Group
- Remove Local User From Group
- Reset User Account Password

and more...

File Activity Monitoring

LEM provides real-time and historical visibility into file activity. Whether it's the notification of inappropriate file access or searching for that person who deleted an important document, LEM provides quick and easy access to the event data that reflects file behavior and is essential for protecting sensitive information.

Learn more about file activity monitoring with LEM here:

- Using the LEM Agent Installer for Windows® (KB article)
- How to Enable File Auditing in Windows (KB article)

Available reports on file auditing:

File Audit Events	Audit	Master	File Audit
File Audit Events - File Attribute Change	Audit	Detail	File Audit
File Audit Events - File Audit	Audit	Detail	File Audit
File Audit Events - File Audit Failure	Audit	Detail	File Audit
File Audit Events - File Create	Audit	Detail	File Audit
File Audit Events - File Data Read	Audit	Detail	File Audit
File Audit Events - File Data Write	Audit	Detail	File Audit
File Audit Events - File Delete	Audit	Detail	File Audit
File Audit Events - File Execute	Audit	Detail	File Audit
File Audit Events - File Handle Audit	Audit	Detail	File Audit
File Audit Events - File Handle Close	Audit	Detail	File Audit
File Audit Events - File Handle Copy	Audit	Detail	File Audit
File Audit Events - File Handle Open	Audit	Detail	File Audit
File Audit Events - File Link	Audit	Detail	File Audit
File Audit Events - File Move	Audit	Detail	File Audit
File Audit Events - File Read	Audit	Detail	File Audit
File Audit Events - File Write	Audit	Detail	File Audit
File Audit Events - Object Audit	Audit	Detail	File Audit
File Audit Events - Object Audit Failure	Audit	Detail	File Audit
File Audit Events - Object Delete	Audit	Detail	File Audit
File Audit Events - Object Link	Audit	Detail	File Audit

Endpoint Monitoring

As system and security admins, we tend to monitor server logs in order to understand various system activities so we can isolate faults, security breaches, and policy violations. However, it's also necessary to explore workstation logs for advanced system and user activity monitoring.

Workstations are arguably one of the most vulnerable entities on your network. They process content from the Internet and email, come in contact with infected files and external mass storage devices, and can connect to insecure networks over Wi-Fi.

Workstations generate a wealth of log data that provide detailed event information from the endpoint perspective. While server logs remain paramount to monitoring system and user activity, monitoring workstation logs in addition to server logs makes event analysis and user activity awareness even more comprehensive and actionable.

Learn more about endpoint monitoring with LEM here:

Why Workstation Log Management is Crucial for Network Security (Thwack article)

USB Detection and Prevention

Log & Event Manager includes built-in USB Defender technology that provides real-time notification when USB drives are detected. This notification can be further correlated with network logs to identify potential malicious attacks coming from USB drives. With LEM's USB Defender technology, you can take automated actions such as disabling user accounts, quarantining workstations, and automatically or manually ejecting USB devices. Additionally, LEM provides built-in reporting to audit USB usage over time.

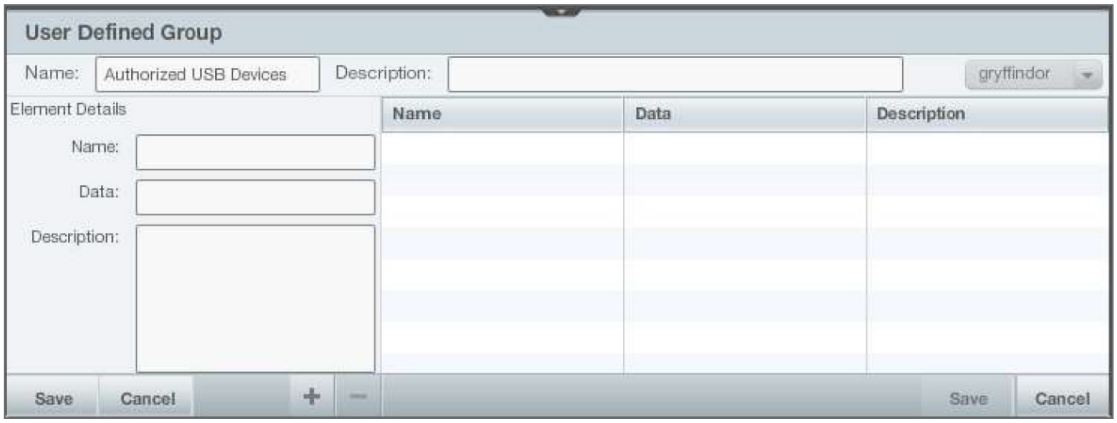
Learn more about USB detection and prevention with LEM here:

How does the Detach USB Active Response work? (KB article)

How to Allow USB Access for Select Devices on the Network

LEM addresses the complexity of providing USB access to select USB devices with a few simple steps.

- Build a group of "Authorized" USB devices
- Identify "Authorized" devices
- Add "Authorized" USB devices to a User Defined Group



Adding "Authorized" USB Devices to User Defined Group in SolarWinds LEM

Here's a view of adding the group of authorized USB devices to a rule using LEM's simple drag-and-drop interface:

Troubleshooting and Forensics

Log & Event Manager includes built-in USB Defender technology that provides real-time notification when USB drives are detected. Using real-time event monitoring, customers can gain visibility into issues that occur across the network. Events generated by operating systems and network and security equipment provide valuable information about overall network health. LEM's real-time correlation and notification can provide instant awareness and early indications of network issues.)

Automate IT issue resolution and decrease incident response times.

- Address critical issues immediately by taking automated actions like quarantining infected machines, blocking IP addresses, disabling user accounts, killing unauthorized processes, restarting services, and more
- Leverage a library of built-in Active Responses to respond to operational issues and to jumpstart proactive defense of your environment right out of the box

Log & Event Manager provides a single interface to troubleshoot, investigate, analyze and respond to IT issues. Use Active Reponses to automate actions that respond to events, avoid potential performance issues, and prevent problem recurrence. LEM includes an extensive library of built-in Active Responses that can be automatically executed, so you can start protecting your infrastructure right out of the box.

Built-in Active Responses include:

- Block an IP address
- Create, disable, or delete user accounts and user groups
- Kill processes by ID or name
- Log users off
- Remove user-defined group elements
- Reset user account passwords
- Restart or shutdown machines, send incident alerts, emails, popup messages, or SNMP traps

Learn more about troubleshooting and forensics features included in LEM here:

- Creating Rules for Real-Time Correlation and Response with LEM (Video)
- Defend your Network with LEM using Custom Rules (Video)

IT Management Inspired by You.

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with *unexpected simplicity* through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.solarwinds.com.

solarwinds

solarwinds.com

3711 S. MoPac Expressway, Building Two, Austin, Texas 78746
T: 866.530.8100 | F: 512.682.9301