GOOD PRACTICE GUIDE 13

LOG & EVENT MANAGER

AWARD-WINNING PROTECTIVE MONITORING SOLUTION FOR GPG13 COMPLIANCE REQUIREMENTS

INTRODUCTION

The Good Practice Guide 13 (GPG13) is a protective monitoring framework designed by the Communications-Electronics Security Group (CESG) for the departments and agencies of Her Majesty's Government (HMG), simply referred to as the British government. The aim is to establish security assurance guidelines that businesses can implement to safely and effectively handle confidential data, eventually reducing security risks.

GPG13 has 12 Protective Monitoring Controls (PMC) built around four recording profiles that map to the HMG Information Assurance Standard no: 1 Segmentation Model. There are four hierarchical segments within this Segmentation Model: **Aware**, **Deter**, **Detect & Resist**, and **Defend**.

Aware	Organisation has an obligation to be Aware of public domain threats, common attack vectors, and known vulnerabilities
Deter	Organisation has an obligation to Deter an attack from a skilled hacker. Appropriate controls should be in place to Deter such an attack
Detect & Resist	Organisation has an obligation to both Detect the attack and Resist the attack from a sophisticated attacker
Defend	Organisation has an obligation to Defend against an attack from a sophisticated attacker

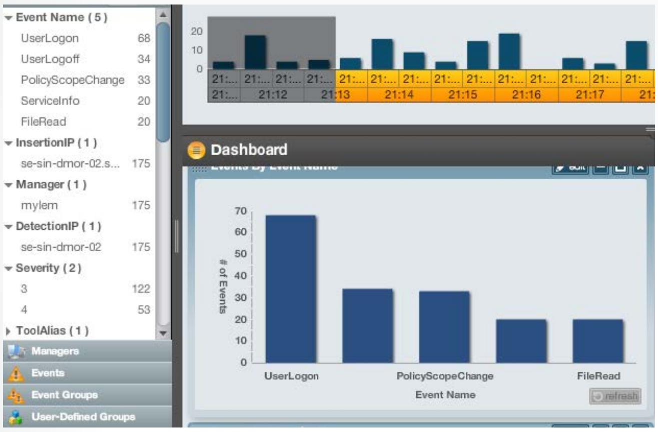
GPG 13 HIGHLIGHTS

12 Protective Monitoring Controls	UK Government (HMG) mandatory requirement
People and business processes and technology framework to improve company risk profiles	Security Policy Framework (SPF) published by the UK Cabinet Office
For organisations that process or store high-impact data	Ensure organisations get operational insight into IT systems use/abuse by internal/external agents

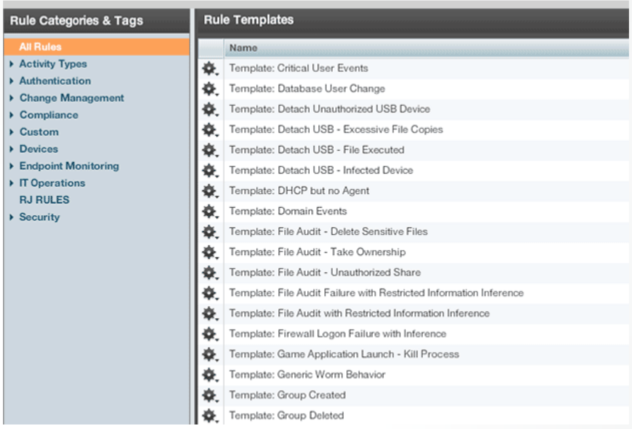
ACHIEVE GPG13 COMPLIANCE WITH LOG & EVENT MANAGER

Log & Event Manager (LEM) is an award-winning SIEM solution (Best SIEM Solution - SC Awards Europe 2015) that helps organisations become GPG13 compliant. LEM includes threat intelligence, real-time event correlation, active response and remediation, file integrity monitoring, privileged account abuse detection, and USB detection and abuse prevention. Deployed as a virtual appliance (VMware® or Hyper-V®), LEM provides a powerful, all-in-one SIEM solution to pinpoint potential security issues, simplify and automate incident response, and achieve GPG13 compliance.

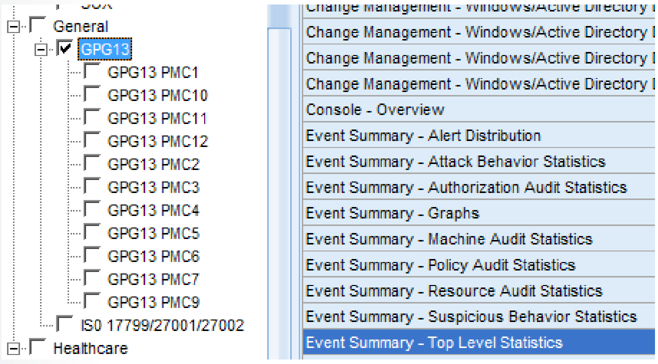
Most importantly, LEM provides built-in alerts and reports for GPG13, saving you weeks of manual effort in creating and implementing them.



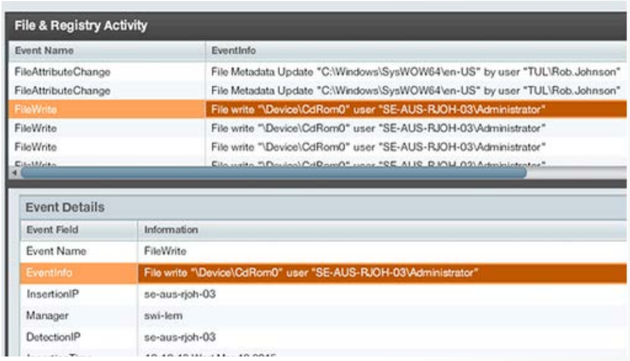
Event Name (5)	
UserLogon	68
UserLogoff	34
PolicyScopeChange	33
ServiceInfo	20
FileRead	20
InsertionIP (1)	
se-sin-dmor-02.s...	175
Manager (1)	
mylem	175
DetectionIP (1)	
se-sin-dmor-02	175
Severity (2)	
3	122
4	53
ToolAlias (1)	



Name
Template: Critical User Events
Template: Database User Change
Template: Detach Unauthorized USB Device
Template: Detach USB - Excessive File Copies
Template: Detach USB - File Executed
Template: Detach USB - Infected Device
Template: DHCP but no Agent
Template: Domain Events
Template: File Audit - Delete Sensitive Files
Template: File Audit - Take Ownership
Template: File Audit - Unauthorized Share
Template: File Audit Failure with Restricted Information Inference
Template: File Audit with Restricted Information Inference
Template: Firewall Logon Failure with Inference
Template: Game Application Launch - Kill Process
Template: Generic Worm Behavior
Template: Group Created
Template: Group Deleted



Change Management - Windows/Active Directory I
Change Management - Windows/Active Directory I
Change Management - Windows/Active Directory I
Console - Overview
Event Summary - Alert Distribution
Event Summary - Attack Behavior Statistics
Event Summary - Authorization Audit Statistics
Event Summary - Graphs
Event Summary - Machine Audit Statistics
Event Summary - Policy Audit Statistics
Event Summary - Resource Audit Statistics
Event Summary - Suspicious Behavior Statistics
Event Summary - Top Level Statistics



File & Registry Activity

Event Name	EventInfo
FileAttributeChange	File Metadata Update "C:\Windows\SysWOW64\en-US" by user "TUL\Rob.Johnson"
FileAttributeChange	File Metadata Update "C:\Windows\SysWOW64\en-US" by user "TUL\Rob.Johnson"
FileWrite	File write "\Device\CdRom0" user "SE-AUS-RJOH-03\Administrator"
FileWrite	File write "\Device\CdRom0" user "SE-AUS-RJOH-03\Administrator"
FileWrite	File write "\Device\CdRom0" user "SE-AUS-RJOH-03\Administrator"

Event Details

Event Field	Information
Event Name	FileWrite
EventInfo	File write "\Device\CdRom0" user "SE-AUS-RJOH-03\Administrator"
InsertionIP	se-aus-rjoh-03
Manager	swi-lem
DetectionIP	se-aus-rjoh-03

HOW LEM HELPS ORGANIZATIONS MEET GPG 13 - PROTECTIVE MONITORING CONTROLS

Protective Monitoring Control 1:

Accurate Time Stamps

To provide a means to ensure that accounting and auditing logs record accurate time stamps.

AWARE	DETER	DETECT & RESIST	DEFEND
• Ensure all accounting and audit logs include a time stamp • Any alerts generated should also be time stamped and should reference the original audit log	• Ensure you meet the requirements of lower recording profiles • Digitally sign the time stamp as a minimum. • Hash the log file that stores the collected audit log	• Ensure you meet the requirements of lower recording profiles • Hash the transaction and digitally sign, plus retain a copy of the audit log	• Ensure you meet the requirements of lower recording profiles
Operating systems have built-in time server capabilities. When these NTP servers are time-synced, LEM can accurately capture all insertion and detection time stamps	All logs are protected within the hardened virtual appliance, with detection and insertion times	Original logs are retained and protected within the hardened virtual appliance	Integrity of the original logs is retained within the hardened virtual appliance

Protective Monitoring Control 2:

Recording of Business Traffic Crossing a Boundary

To define a set of Alerts and Reports that will identify authorised vs non-authorised business traffic across the network boundary. This goal will be met if you can identify authorised vs non-authorised traffic, transportation of malicious code is prevented and alerted, and the identification of the manipulation of other business traffic.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report and Alert on Malware detected crossing the boundary	• Ensure you meet the requirements of lower recording profiles • Report and Alert on blocked web browsing activities • Report and Alert on failed file imports and exports across boundary	• Ensure you meet the requirements of lower recording profiles • Report on failed file imports and exports across boundary and keep a copy of file content for auditing purposes • Report on failed file imports and exports across boundary and keep a copy of file content, Security Label and File Signature, for auditing purposes • Report on accepted web traffic across boundary • Report on accepted incoming and outgoing file transfers across boundary	• Ensure you meet the requirements of lower recording profiles • Report on accepted incoming and outgoing file transfers across boundary, including a copy of the file content • Report on accepted file imports and exports across boundary and keep a copy of file content, Security Label and File Signature, for auditing purposes • Report on files that have been placed in a file cache, including its URL, content, Security Label, Signature and time to live
Based on the configuration of the malware/anti-virus module on the firewall and LEM's built-in threat intelligence and malicious activity rules, malware trying to enter via boundary devices is alerted and reported	Based on firewall/Web proxy configurations, alerting, reporting, and correlation is enabled for authorised and unauthorised/ malicious traffic and blocked/ accepted Web browsing traffic crossing the boundary devices	Based on the configuration of the firewall/Web proxy, LEM reports and alerts on blocked/accepted Web browsing activities and failed file imports and exports across the boundary	Based on the configuration of the firewall/Web proxy, LEM, with real-time correlation and notifications, reports and alerts on blocked/accepted Web browsing activities and failed/accepted file imports and exports across the boundary. The data can be viewed on an intuitive dashboard, and drilled down for further investigation

Protective Monitoring Control 3:

Recording Relating to Suspicious Activity at The Boundary

To define a set of alerts and reports that will identify suspicious network traffic crossing the network boundary.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report denied or dropped packets on the firewall	• Ensure you meet the requirements of lower recording profiles • Report and alert on critical console messages from boundary devices • Report and alert on authentication failures on boundary devices and systems • Report and alert on suspected attacks at the boundary • Report on error console messages from boundary devices • Report on user sessions on the boundary devices and consoles • Report on changes to firewall and boundary device rule base • Report on changes to firewall and boundary device rule base in response to a detected attack • Report on status changes to security software monitoring tools, such as your Security Incident and Event Management, Intrusion Detection software, Intrusion Prevention software, etc	• Ensure you meet the requirements of lower recording profiles • Report on warning console messages from boundary devices • Report on all commands issued to boundary devices or boundary consoles • Report on packets traversing the boundary device, including packet header, size, and firewall interface • Report on packets traversing the boundary device, including full packet capture, size, and firewall interface	• Ensure you meet the requirements of lower recording profiles • Report and alert on all automated responses at the boundary
Based on the configuration of the firewall, LEM can report denied or dropped packets from the firewall	LEM supports continuous monitoring and provides correlation rules to monitor user activity and privileged account abuse. Any sudden or suspicious increase in network activity at a specific boundary device is detected and reported in real-time. Based on built-in and customisable event correlation rules, LEM can detect and alert on warning console messages, commands to boundary devices, and packets traversing the boundary devices for in-depth log analysis and security incident identification	Based on the configuration of the boundary devices, LEM detects and reports any sudden or suspicious increase in network activity at a specific boundary device in real-time. Based on built-in and customisable event correlation rules, LEM can detect and alert on warning console messages, commands to boundary devices, and packets traversing the boundary devices for in-depth log analysis and security incident identification	LEM can be customised to create alerts and reports on all automated responses at the boundary

Protective Monitoring Control 4:

Recording on Internal Workstation, Server, or Device Status

To define a set of alerts and reports that will identify configuration and status changes on internal workstations, servers, and network devices.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report and Alert on all Critical and above messages from hosts in scope • Report and Alert on all detected Malware on hosts in scope • Report on all Error messages from hosts in scope • Report on changes in status to Malware signature base	• Ensure you meet the requirements of lower recording profiles • Report on Failed access attempts to files • Report on changes to File or directory access rights of system folders • Report on changes to the status of networked hosts. • Report on changes in the status of attached devices connected to controlled hosts • Report on the status of storage volumes of monitored hosts • Report on changes to software configuration of monitored hosts	• Ensure you meet the requirements of lower recording profiles • Report and Alert on changes to system files or folders • Report on all critical messages below Warning level from hosts in scope • Report on changes to system configurations on monitored hosts • Report on changes to system processes on monitored hosts	• Ensure you meet the requirements of lower recording profiles • Report on changes to software configuration of monitored hosts, including software inventory • Report on changes to system files, including before and after content • Report on changes to system configurations on monitored hosts, including before and after content
LEM helps detect malware activity, and alerts and reports on critical/error messages from hosts in scope with its threat intelligence, event correlation, analysis, and reporting features	With file integrity monitoring, and user, group, and policy audits, LEM can alert and report on failed attempts to access files, changes to files/registry settings, or directory access and changes to software configurations on monitored workstations, servers, and network devices. LEM continuously monitors and detects changes to files and registries, and correlates logs from anti-virus/IDS/IPS systems to help prevent zero-day malware threats on the network	With file integrity monitoring and built-in alerting, LEM can report on changes to files or folders and changes to software configurations and processes on monitored hosts	Built-in file integrity monitoring can alert on changes to files/folders, system files and system configurations on monitored hosts

Protective Monitoring Control 5:

Recording Relating to Suspicious Internal Network Activity

To define a set of alerts and reports that will identify suspicious activity across internal network boundaries from either internal or external agents.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report on all denied or dropped packets on the firewall	• Ensure you meet the requirements of lower recording profiles • Alert and report on all critical and above console messages from internal firewalls • Alert and report on all authentication failures from internal network devices and monitoring consoles • Report on all error status messages from the console or internal firewalls • Report on user sessions on the console or internal firewalls • Report on changes in the status of rules based on internal firewalls and network devices	• Ensure you meet the requirements of lower recording profiles • Alert and report on suspected internal attacks • Report on all warning messages from internal network devices • Report on all commands sent to network devices or firewalls • Report on accepted packets being transferred by internal firewalls • Report on all denied or dropped packets on internal firewall, including full packet capture • Report on responses to internal attacks and actions undertaken • Report on status changes to internal security software monitoring tools, such as your Security Incident and Event Management, Intrusion Detection software, Intrusion Prevention software, etc	• Ensure you meet the requirements of lower recording profiles • Alert and report on all automated responses by internal IPS • Report on accepted packets being transferred by internal firewalls, including full packet capture
Based on the configuration of the firewall, LEM can report denied or dropped packets from the firewall	Based on the configuration of firewalls and network devices, LEM continuously monitors and alerts on all activity/error logs from these devices. When a privileged user group is modified on a core-router by an admin or external agent, LEM reports and alerts this activity based on the preconfigured correlation rules. Remote connections, failed login attempts, suspicious user sessions, and changes to server configurations are alerted and reported	With built-in threat intelligence and real-time correlations, LEM alerts and reports on all warning messages and denied/dropped packets based on the configuration of internal network devices and firewalls	Not Applicable

Protective Monitoring Control 6:

Recording Relating to Network Connections
To define a set of alerts and reports that will identify temporary connections to the network, such as those made via a VPN or wireless connection.

AWARE	DETER	DETECT & RESIST	DEFEND
• Alert and report on all remote authentication failures • Alert and report on failed attempts to connect to the VPN • Report on DHCP-assigned IP registrations • Report on remote access user sessions • Report on changes to VPN node registrations	• Ensure you meet the requirements of lower recording profiles • Alert and report on failed equipment connection attempts to protected network attachment points • Alert and report on critical and above messages • Alert and report on authentication failures on network consoles • Report on error messages from network consoles • Report on all connection attempts to wireless access points • Report on user sessions to network connection consoles	• Ensure you meet the requirements of lower recording profiles • Alert and report on all suspected wireless attacks • Report on commands issued on network connection consoles • Report on remediation steps taken in response to internal attack notifications • Report on status changes to IPS and IDS signatures	• Ensure you meet the requirements of lower recording profiles • Alert and report on non-approved wireless interfaces and wireless access points
LEM's in-depth log analysis and event correlation rules alert and report on suspected user activity, remote access user sessions, and failed VPN connection attempts	LEM alerts on and logs failed connection attempts to protected network attachment points and wireless access points, authentication failures and user sessions on network connection consoles	Based on the configuration of IPS/IDS devices, LEM can report on IPS/IDS signature status changes, which are securely logged	Based on switch/AP device configurations, LEM alerts and reports on all non-approved wireless interfaces and access points on the network

Protective Monitoring Control 7:

Recording on Session Activity by User and Workstation

To define a set of alerts and reports that will identify suspicious user activities or allow forensic analysis of user activities within the network.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report on user network sessions • Report on user account changes • Report on user privilege or group changes • Report on administrator or super user application management	• Ensure you meet the requirements of lower recording profiles • Alert on user account lockouts.Report on user privilege escalation on critical workstations and all servers • Report on the execution of accountable user transactions	• Ensure you meet the requirements of lower recording profiles • Report on user sessions on critical workstations • Report on local user account changes on critical workstations • Report on changes to local user accounts or group memberships on critical workstations • Report on the execution of all network commands and executables	• Ensure you meet the requirements of lower recording profiles • Report on the execution of accountable user transactions, including the content of the transaction • Report on the execution of all workstation-critical commands and executables
LEM reports on all user activities, and privileged account user/group changes with its comprehensive log management and event correlation features	LEM alerts and reports on user account lockouts, user privilege escalation on critical workstations/servers, and logs all user transactions	LEM alerts and reports on user sessions and account changes, and group membership changes on critical workstations. All network commands are logged and presented on the dashboard	Based on activity alerts, and even correlation, LEM alerts and reports on critical user activities on the network

Protective Monitoring Control 8:

Recording on Data Backup Status

To ensure that a backup and recovery process is defined and adhered to, such that the business can be confident of the integrity and availability of the network resources.

AWARE	DETER	DETECT & RESIST	DEFEND
• Report on backup, test and recovery operations • Alert on backup, test and recovery operation failures	• Ensure you meet the requirements of lower recording profiles	• Ensure you meet the requirements of lower recording profiles • Report on backup, test and recovery operations, including catalog details	• Ensure you meet the requirements of lower recording profiles • Report on backup, test and recovery operations, including catalog details, site information and version information
Based on the configuration of the backup software logs, LEM alerts and reports on backup activity. For example, it will detect and report on a failed router configuration backup from the network change and configuration management system	Not Applicable	Based on data backup log settings, LEM reports on backup, test, and recovery operations	Based on data backup log settings, if backup, test, and recovery operations are logged, LEM detects these events and triggers alerts based on correlation rules

Protective Monitoring Control 9:

Alerting on Critical Events
To define a set of real-time alerts and reports that will identify events classified as "critical" by the organisation.

AWARE	DETER	DETECT & RESIST	DEFEND
• Alert and report on all alert messages generated by the SIEM solution	• Ensure you meet the requirements of lower recording profiles • Alerts and reports to be delivered by secondary delivery mechanisms, such as email, SMS, etc • Report on changes to alert rule base	• Ensure you meet the requirements of lower recording profiles • Ensure alerts are visible on consoles and/or wall displays	• Ensure you meet the requirements of lower recording profiles • SIEM solution should allow multi-casting of alerts to several locations
LEM enables severity specification in alerts and reports. When hundreds of alerts are generated and classified, the most critical alerts can be addressed without being drowned out or buried by other less-critical alerts. All alerts are visible on LEM's intuitive dashboard console, and can be further customised based on the business/network requirements	You can create alerts and report on changes to the alert rule base, and set up alerts to be triggered via secondary delivery mechanisms such as email	All reports are visible on LEM's intuitive dashboard console, and can be further customised based on the business/network requirements	LEM supports sending alert messages to specific or multiple destinations. For example, if a group of users are trying to plug in a USB device, LEM can send warning messages to their consoles, and eject the devices

Protective Monitoring Control 10:

Reporting on the Status of the Audit System
To define a set of alerts and reports that will generate confidence in the integrity of the auditing system, such that the output of this system will be valid in a court of law.

AWARE	DETER	DETECT & RESIST	DEFEND
• Alert and report on logs cleared or reset, log collection errors, and threshold exceptions • Report on the status of active log storage, space allocated, space used, space remaining, and total record count	• Ensure you meet the requirements of lower recording profiles • Report on the status of active log storage, space allocated, space used, space remaining, and total record count trended in a graph over time • Report on the status of active log storage, space allocated, space used, space remaining, and total record count, plus log rotation information • Your SIEM solution should be able to prove chain of custody, including that each part of the chain adds source and origin information. Original timestamps should not be modified • Report on log sources.Your SIEM solution should be able to prove chain of custody, including that each part of the chain adds source and origin information, trended in a graphical format over time	• Ensure you meet the requirements of lower recording profiles • Alert and report on integrity, checking failures anywhere within the chain of custody • Report on log access requests via queries or reports • The SIEM should have the capability to search online and archived log data	• Ensure you meet the requirements of lower recording profiles
LEM alerts and reports on logs cleared or reset, log errors and thresholds, space usage, and log record counts	LEM protects original timestamps, source and origin information, log space used, remaining, etc., via a graphical user dashboard that's intuitive and customisable	Original logs are retained and encrypted, and alerts are triggered in case of failures. LEM provides the capability to search raw, archived log data	Not Applicable

Protective Monitoring Control 11:

Production of Sanitised and Statistical Management Reports
To define a set of reports that will provide feedback to management on the performance and effectiveness of the protective monitoring system.

AWARE	DETER	DETECT & RESIST	DEFEND
• Reports must be sanitised and omit identifying and sensitive information such as usernames, IP addresses, workstation names, and server names • If Web reports are produced, they must also be sanitised	• Ensure you meet the requirements of lower recording profiles • If external managed security service providers are used, they might include custom reports that can be used specifically for management	• Ensure you meet the requirements of lower recording profiles • It is expected that an enterprise solution is deployed to meet your GPG13 requirements, most likely a SIEM working with a number of other technologies, such as IPS, IDS, anti-virus, etc • A complete protective monitoring solution is likely to include an audit or compliance check software such as Trend Micro®	• Ensure you meet the requirements of lower recording profiles • It is required to use defense-in-depth at this segment level, meaning different vendors for the different technologies required for a complete protective monitoring solution such as a different SIEM vendor from anti-virus, IPS, IDS, and audit or compliance check software
LEM prevents the inclusion of sensitive information in the alerts/reports, and can easily be customised to maintain anonymity	Not Applicable	LEM provides comprehensive protective monitoring, complying with GPG13 requirements, and also connects with other security technologies like IPS, IDS, and anti-virus software	Not Applicable

Protective Monitoring Control 12:

Providing a Legal Framework for Protective Monitoring Activities
To define a requirement that will ensure all monitoring is conducted in a lawful manner, and that the collected data is, in itself, protected and treated as sensitive data.

AWARE	DETER	DETECT & RESIST	DEFEND
• No recording profile required at this segment level	• Report on user sign-up activity to defined terms and conditions of network usage	• Report on user sign-up activity to defined terms and conditions of network usage, to include digital user signatures • Any re-affirmation should also be logged and reported	• Report on user sign-up activity to defined terms and conditions of network usage, to include digital user signatures and hardware tokens or smart card reference • Any re-affirmation should also be logged and reported
Not applicable	LEM can report on user sign-up activity that complies with the network usage terms and conditions	LEM can report on user sign-up activity that complies with the network usage terms and conditions. Re-affirmations are also logged and reported	LEM can report on user sign-up activity that complies with the network usage terms and conditions. Re-affirmations are also logged and reported

ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT operations management software to more than 150,000 customers worldwide—from small business to more than 450 of the Fortune 500 companies. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scalability, and flexibility needed to manage today's IT environments.

SolarWinds' growing online community, thwack®, offers users problem-solving and technology-sharing for all of SolarWinds' products, including SolarWinds® LEM. This active user-community input is combined with decades of IT management experience to deliver a wide range of solutions and tools to address the real-world needs of IT professionals.

Additional LEM Resources:

Log & Event Manager-related videos: LEM playlist on YouTube

Log & Event Manager Datasheet and Product Page

SolarWinds thwack® Community: SolarWinds thwack online community adds value to IT pros

Log & Event Manager on thwack.

Follow us on Twitter: @solarwinds.

Email us: nationalgovtsales@solarwinds.com ; Phone: +353 21 233 0440