LEM and NIST

ADDRESSING NIST REQUIREMENTS FROM SPECIAL PUBLICATION 800-171

Ingram, Curtis

Disclaimer

Content posted herein is provided as a suggestion or recommendation to you for your internal use. This is not part of the SolarWinds software that you have purchased from SolarWinds, and the information set forth herein may come from third party customers. Your organization should internally review and assess to what extent, if any, recommendations will be incorporated into your environment. Content obtained herein is provided to you “AS IS” without indemnification, support, or warranty of any kind, express or implied.

Table of Contents

3.1 Access Control

3.1.1

LEM does not manage user permissions, but you can create (and templates exist) for alerts and correlations such that “If FILE is modified by USER, and USER is not in AUTHORIZED GROUP” then take an action and send an alert. This can also be used to alert on activity like user logons and remote sessions.

3.1.2

Likewise, LEM can alert on activity in applications and systems (assuming the appropriate logging is available, connectors exist, and the logs are gathered to LEM for correlation and analysis)

3.1.3

LEM can monitor file activity and activity like USB use, as well as integrating with a variety of DLP solutions for alerting and correlations

3.1.4

This is outside LEM and more of a business practice issue, but we could be alerting and correlating as described above to help keep admins aware of violations

3.1.5

Like 3.1.4

3.1.6

Like 3.1.4

3.1.7

Like 3.1.4, LEM does not manage the permissions but can provide auditing of these executions on many systems

3.1.8

LEM would not enforce this (that’s a GPO, typically) but it would provide audit trails of unsuccessful logons and account lockouts

3.1.9

Not a LEM function

3.1.10

Like 3.1.8, provide audits of things like workstation lock and unlock events with options for correlation and alerting based on said events

3.1.11

LEM rules can terminate a user session or shut down a machine based on event patterns and correlations

3.1.12

Like 3.1.10

3.1.13
This is outside LEM for other systems, but LEM is secure (described in our KB)

3.1.14
LEM can audit changes on firewalls and routers and alert off config changes. Additional information would be gathered by applications like the Network Configuration Manager, Network Performance Monitor and (if you're a Cisco shop) IPSLAs managed by VNQM.

3.1.15
Like 3.1.10

3.1.16
LEM could be auditing logs from wireless controllers and APs, device tracking would be enhanced by User Device Tracker, otherwise like 3.1.8.

3.1.17
Like 3.1.14 and 3.1.16

3.1.18
Like 3.1.16

3.1.19
Solarwinds does not have a MDM solution at this time

3.1.20
LEM can help with some DLP natively (see: USB Defender) as well as integrating with other systems for alerting and correlation

3.1.21
As 3.1.20

3.1.22
LEM can collect and audit logs from devices like firewalls, proxies and web filters and use that information to alert to activity that may suggest violations

3.2 Awareness and Training
Training on security principles is outside the purview of LEM and SolarWinds

Training on the LEM product is available to LEM customers

3.3 Audit and Accountability
3.3.1
LEM is engineered to protect data at rest and in storage, as described in our KB.

3.3.2
Confirmed functionality

3.3.3
This is a feature of LEM, specifically the Reports console and nDepth

3.3.4
This is a feature of LEM, specifically Rules and Alerts. Many template rules and alerts are available with LEM, as well as the ability to create custom alerts.

3.3.5
Confirmed feature of LEM

3.3.6
As 3.3.4

3.3.7
Confirmed feature of LEM, audit logs are stamped with universal time (in the format of Unix Epoch) derived from LEM's local time settings

3.3.8
As 3.3.1

3.3.9
LEM includes RBAC for users interfacing with LEM

3.4 Configuration Management
LEM is not a CMDB solution, for the SolarWinds offering in this space see Network Configuration Manager. However, LEM can collect and audit logs regarding changes on systems. LEM can also (for certain firewall vendors) take actions based on audit logs like shunning or blocking IPs on a firewall or router automatically.

3.5 Identification and Authentication
LEM is not an Identity Management solution, but can provide auditing and alerting off key identity events like password resets, workstations locking and unlocking, logons and logoffs (including failures) and other key events. LEM also supports the use of CAC/SSO for authentication to the LEM itself.

3.6 Incident Response
SolarWinds does not provide Red Team exercises

3.7 Maintenance
As described above, LEM can help with auditing users and devices as well as integrating with other systems for DLP

3.8 Media Protection

3.8.1

LEM can help with monitoring and auditing digital information, but doesn't do anything to track paper records

3.8.2

LEM can provide audit records to show which users accessed information as well as alerting and correlating off those audit trails

3.8.3

LEM does not provide this functionality

3.8.4

LEM does not provide this functionality

3.8.5

LEM does not provide this functionality

3.8.6

LEM does not provide this functionality

3.8.7

LEM can assist with this requirement via USB Defender

3.8.8

As 3.8.7

3.8.9

LEM does not provide this functionality

3.9 Personnel Security

3.9.1

LEM does not provide this functionality

3.9.2

LEM can audit user events, and correlate/alert if activity like a disabled account attempting to logon to a system is detected

3.10 Physical Protection

LEM does not currently integrate with any physical access systems, but this could be a feature request if your system makes audit logs available to a third party

3.11 Risk Assessment

LEM does not perform vulnerability scans or assessments, but can integrate with a number of other system scanners to collect data for alerting and correlation

3.12 Security Assessment

LEM can help with the monitoring requirements, but does not perform evaluations or assessments. Audit trails stored by LEM can be used to assist with design and optimization of security controls

3.13 System and Communications Protection

As described above, LEM can collect, store, correlate and alert off of logs from devices and systems to keep admins aware of potential problems and violations. This includes data from border and internal firewalls and systems

3.14 System and Information Integrity

LEM does not perform assessments or have an awareness of CVEs (although the Network Configuration Manager can perform this function for some devices). LEM is not a malware or antivirus platform, but it can integrate with many third party solutions to provide auditing and alerting of malware and antivirus systems

LEM does have a Threat Intelligence function natively to identify known malicious IPs in logs that are analyzed.

Reference

LEM Connector List on THWACK (a list of currently supported product integrations and log parsers for LEM)

NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," pulled June 29, 2017; dated June 2015