Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Champagne SIEM on a Beer Budget

Copyright SANS Institute
Author Retains Full Rights
Champagne SIEM on a Beer Budget

March 2014
A SANS Analyst Product Review

Written by Jerry Shenk

Installation and Configuration PAGE 2

Ops Center Overview PAGE 3

SIEM in Action PAGE 9

Reports for Detection, Remediation and Audit PAGE 13

©2014 SANS™ Institute
Organizations of all sizes have difficulty finding the time, personnel or cash to install a security monitoring solution, so they make do with periodically checking logs—except the logs often don’t get checked, and many times, the personnel doesn’t even know how to look for security issues.

The updated SolarWinds Log & Event Manager (LEM) is targeted at organizations without vast IT resources—the classic small-to-medium-size business (SMB)—and we took the opportunity to take it for a spin. We reviewed the base version that supports 30 networked nodes (such as servers, routers, firewalls or other security devices) and sells for $4,495. LEM ships as a virtual appliance for Microsoft or VMware virtual environments; we performed our tests using the latter.

LEM was easy and quick to set up, and it included visualization and reporting tools that will be helpful for IT staff to use when reporting to nontechnical staff. It also has search capabilities and the capability to look at event details for more technical staff. If LEM detects suspicious events, it can take action—such as interrupting network communications, disabling USB devices or killing processes—while sending reports to the compliance and security team (often the same person in a small organization).

Combined, the features and functions we reviewed provide organizations that have limited resources with the forensic intelligence and the compliance and security information they need to manage their operations themselves.
LEM’s installation went quickly, in part because it is a virtual appliance. The OS and applications are preinstalled on a system image, and the deployment consists mostly of entering site-specific settings (e.g., IP address or network time server).

LEM can be installed on an existing virtual server installation, but if an acceptable environment does not already exist, the free version of VMware can be installed. (LEM requires, as a minimum, either VMware VSphere 4.0 or Microsoft Hyper-V Server 2008 R2.) Installing the software starts with downloading it from the company’s website.¹

We copied the package—an Open Virtualization Appliance (OVA) file containing the virtual appliance’s files in the form of a tar archive—onto our VMware host using the vSphere Client and then installed Log & Event Manager Reports (LEM Reports), a standalone report generator.² Once the appliance was installed and running, we were able to connect to it using IE or Chrome on Windows (and Safari on OS X) and access the LEM console.

¹ www.solarwinds.com/log-event-manager.aspx
² We use host to refer to the combination of hardware and virtualization software; when a distinction between these components is necessary, we use physical host and hypervisor.
The LEM Ops Center has a number of configurable widgets that can give a quick indicator of network health. Figure 1 shows a typical Ops Center dashboard.

![Figure 1. Typical Ops Center Dashboard](image)

In this example, the upper-left widget provides a quick check of node health. Green is good, yellow warns that a node has not reported in for an hour, and red indicates that a node has not reported in for more than 24 hours.

Using all the panes together, we can see Events per Minute, Top 10 Rules by # of Rules Fired, Top 10 Nodes by # of Events, Change Management Events by Type and PCI Events by Type. This pane view is completely configurable.

These six panes represent serious issues that are critical overall indicators. It’s important to know that your security solutions are collecting data and to have a quick, visual way to spot anomalies. If there are an abnormal number of events or multiple rules firing, that’s something we want to know about; if a node hasn’t reported in within the expected period of time, we want to know that also.

The default console view immediately following installation has a Getting Started widget with an informative five-minute video that provides a quick tour of LEM’s approach to security information management, intelligence gathering and reporting.
Immediate Detection

When we initially started LEM, we had numerous “No UDP server to service request” events, as shown in Figure 2.

The majority of those events were broadcast attempts to connect to UDP port 17500—that’s Dropbox, a known application on our network, so we know that’s OK. Dropbox constantly tries to find other nodes on the local network, so it sends out broadcasts on that port. We disabled this feature of Dropbox, leaving us with a fair amount of traffic to UDP port 137 (NetBIOS), which is quite normal for Windows machines.
Syslog Configuration

The next task was to get the various devices in the lab to send their data to LEM. In theory, it’s simple—point the device at a syslog server—but devices typically differ in how this is done. Devices with a GUI management screen may have an Enable Syslog option requiring the syslog server IP address. In this case, that would be the address of the LEM appliance.

The first device we set up was a Cisco ASA firewall, which we configured to send syslog data to LEM with the following commands:

```
logging enable
logging timestamp
logging buffered debugging
logging trap debugging
logging history debugging
logging asdm informational
logging facility 23
logging queue 4096
logging host outside 10.1.1.116
```

Typically, the log server or security information and event management (SIEM) system will be on the same side of the firewall as the LEM appliance, and that last line would reference the “inside” interface. However, in this case the appliance is between our edge firewall and the ASA firewall that sits in front of the lab network.

After we entered these commands into the ASA and the appliance had a few seconds to collect the events, a message popped up indicating that a new connector—which parses incoming data—had been “found”; this indicates that LEM recognized the syslog data’s format and enabled the respective connector. Figure 3 shows this, in the yellow banner.

![Figure 3. Detail of Ops Center Dashboard Showing New Node Connection](image)

Once we completed the connector setup, LEM was able to receive log and security events from the ASA, including management events (e.g., login attempts and configuration changes) and events related to network traffic, such as allowed and blocked packets. Once a connector has been enabled, it should recognize log data from similar devices without further intervention.
Windows Agent Configuration

LEM uses an agent to pull log data including application, OS and USB activity from Windows systems; Linux and OS X systems have their own versions of the LEM Agent. Installing the LEM Agent is a simple matter of clicking Add Node in the Getting Started widget, which prompted us for details including the IP address of the LEM appliance, the local admin credentials and specific features to enable. After we clicked Done, Ops Center displayed the “New Connector(s) Found” message, as shown in Figure 4.

![Figure 4. Ops Center Dashboard with Newly Discovered Windows Workstation](image-url)

We just followed the prompts to finish configuring the connector, and new events from the Windows client appeared on the monitor page of the console.
Email Notification

One key feature of any SIEM system is notification, which can be a double-edged sword if it is set up for too many rules. Nevertheless, for the most serious events, we’d like to know what’s happening as quickly as possible. To set up notification from the Appliances screen (under the management interface’s Manage tab), we clicked on the gear icon on the left side of the entry for the appliance and clicked on Connectors. In the Connectors screen, we typed “email” in the search window to limit the number of displayed connectors and chose Email Active Response, shown in Figure 5.

![Figure 5. Configuring Email Notification](image-url)
We selected the gear icon next to the “Email Active Response” connector and clicked New to enable email to be sent from the appliance. We filled in the form with the IP address of a mail server that would forward messages from LEM to the incident response team, as shown in Figure 6.

We then created a user who would be notified, through the Users screen (under the management interface’s Build tab); including an email address in the user information made it possible for LEM to send alerts to this user. LEM allows the use of multiple email addresses per user; in effect, this creates a group notification list.

Although it’s possible to add an email notification to any event LEM detects, we limited ourselves to setting up notification for three events:

- A log clearing event
- Firewall login failures
- Copying too many files to a USB drive

Each of these events is described in detail in the following section.
LEM is a good security solution, especially for overstretched IT shops with limited resources. We reviewed the main features under the following scenarios:

- Catching attacks aimed at hiding their tracks (through log clearing)
- Detecting and acting upon insider attacks using a USB drive to steal files
- Providing forensic or historic views of activity related to specific events

Under these scenarios, we found LEM to be quite adept at using the combination of SIEM, endpoint monitoring and real-time, in-memory event correlation that much larger organizations often demand from their SIEM and analytics platforms.

### Catching Concealed Activity

Because hiding one's presence by turning off security and logging is a common tactic of attackers, we mimicked an unauthorized clearing of our logs on a Windows Server 2008 R2 machine running the LEM agent for Windows systems. Initially, the rule did not fire, but we were able to determine (with assistance from SolarWinds' tech support) that our time settings were out of sync: Our VMware host's time was six minutes ahead of the LEM-monitored Windows server. Once that was resolved, an alert was sent to the user we'd set up previously.

The rules are easily understandable—although someone whose main role isn't IT might feel lost at first, the user interface is straightforward enough to keep the learning curve from turning into a Matterhorn. Figure 7 shows a built-in rule to monitor for the event log being cleared.

![Figure 7. Event Log Monitoring Rule](image-url)
Blocking Suspicious USB Events

One feature that SolarWinds emphasizes is LEM’s active policies and active response. For example, LEM can monitor for inappropriate USB use and deactivate the device based on the rules.

In our case, we chose one of the built-in rules—“Detach USB – Excessive File Copies”—to dismount a USB device if 10 or more files are copied to it. It’s probably a little simplistic to think this would have caught Edward Snowden downloading NSA files, but the concept certainly addresses a range of similar “hostile insider” scenarios.

To start, we copied 10 files to the USB drive, and it was immediately dismounted. That’s a good start, but how would an administrator know if this happens? To address this, we set notification to send administrators an email whenever this rule disabled a USB drive.

We also wanted to see how the correlation capabilities worked, so we added a timeframe to the rule, after which LEM would only alert to USB file copies if more than 10 files were copied within 30 seconds, and then, only after 6:15 PM on January 10, 2014. The rule configuration screen appears in Figure 8.

![Figure 8. Monitoring USB Device Activity](image-url)
We then verified that the updated rule would not fire before 6:15 PM by first running our batch copy of 10 files, then copying three files every 10 seconds. These scenarios did not trigger the alert, which is what we expected and wanted. Then, when we ran the same tests after 6:15 PM, alerts were triggered as they should have been, and the USB drive was dismounted. Monitored system functions can include processes, specific files, worm-like behavior or numerous other aspects.

In addition to sending email and disabling a USB drive, LEM can take other actions, such as blocking an IP address, creating and disabling Active Directory users and groups, disabling networking altogether, killing processes or even shutting down the computer. Rules can include lists of allowable USB devices, times and other information and exclude or include a wide range of specific details; they can be as simple or complex as needed.

**Collecting Data for Follow-Up**

The Monitor view of the LEM user interface displays collected log events in a scrolling format. One can filter the event list using a number of built-in security and operation-based filters or, for ad hoc or custom reports, with user-defined filters. These filters can have actions assigned to them in much the same fashion as the rule-based notification and can be used to generate reports through LEM’s nDepth screen for remediation and compliance purposes.

For example, we selected the built-in filter Top PCI Events. This makes quick work of identifying recent events that match a predetermined set of PCI-related criteria. In Figure 9, we can see that the ASA is being modified as a user executes the “enable” command—an interesting event because it can demonstrate change controls, or the lack thereof.

![Figure 9. Monitoring a Network Device](image)
Here we see the highlighted event and several attempts to log into the ASA firewall as the user admin; firewall changes are also listed. From a PCI standpoint, this type of activity needs to be logged and, ideally, it should show up in a report documenting that changes are monitored. This is a good tool for any organization that needs to monitor changes across multiple devices.

**Providing Historical Data**

Reports such as the network device monitoring report shown in Figure 9 can be run on a regular basis by clicking the Explore tab, choosing nDepth and then selecting a range of dates for the report. Clicking on the gear-shaped icon in the upper-right corner allowed us to edit the schedule so that this report can be emailed as a PDF from this screen or as a CSV file on daily, weekly or monthly schedules.
Reports for Detection, Remediation and Audit

Reports are generated by two different means: a report writer in the standalone LEM Reports application that we installed on a desktop machine during our deployment of LEM and a report export function in the Explore tab’s nDepth screen.

Standalone Report Writer

LEM Reports includes a number of prebuilt reports designed for specific scenarios including PCI, HIPAA, SOX and other compliance regimes. However, they are a little awkward to work through because each report runs separately with no coordination or grouping among them. Even in our lab network, reports run against only a week of data include a few hundred pages of detail, so most reports will require some filtering. Typical examples of such reports would be a login report limited to show only administrative accounts or limiting network reports to focus on internal or external IP address ranges.

One very handy feature is that the reports can be exported in many formats, depending on one’s needs. PDF reports are handy for storage and sharing, while the HTML and RTF versions are good for use in presentations and documents. The Excel, text and CSV formats are excellent for data aggregation and correlation with custom spreadsheets and when used by other security and compliance reporting programs.

In Figure 10, we show an image from the “Network Traffic Audit – Web URL Requests by Source Machine” report.

![Figure 10. Graph Showing Events by Host IP Address](image)

This type of graph would work well in a report to management about user abuse of the corporate network for personal use.
Figure 11 shows a visualization of events by host name, as generated by LEM Reports.

These reports can also be scheduled, customized and saved. By default, the generated reports are left in the C:\Program Files (x86)\SolarWinds Log and Event Manager Reports directory.

**Ad Hoc nDepth Reports**

LEM also offers ad hoc reports, which can be accessed from the web interface by clicking on the gear icon in the upper-right corner of the nDepth screen and using the Export option. The only option for saving these reports is PDF; they nevertheless include some interesting visualization templates, including a bubble chart, tree map or word cloud, as well as bar, line and pie graphs, and a text report format. These reports can be saved and scheduled, with the results delivered via email.
Figure 12 shows a typical view of nDepth, which is providing us with the events for a week, listed by criteria including name, IP address and device type.

![Figure 12. View of nDepth Screen](image)

To get this level of visibility, we double-clicked on `UDPTrafficAudit` and `InternalNewToolData` and put them in the search bar. The red Xs are indicators of what we want to exclude from the search; to the right of the blue arrow (in the upper right of the screen) is a drop-down box to pick a timeframe for the search—we have it set to “Last week.”

Overall, the reports were satisfactory. Those we created with LEM Reports took advantage of the many prebuilt reports and a variety of export options, while the reports we built through the nDepth interface were functional, intuitive and easier to work with than the ones from LEM Reports. This is critical for organizations needing to make sense of their log and security data and is an issue that even large organizations—with all their IT resources—still struggle with, as shown in the SANS 2012 Log and Event Management Survey.\(^3\)

\(^3\) [www.sans.org/reading-room/analysts-program/SortingThruNoise.pdf](http://www.sans.org/reading-room/analysts-program/SortingThruNoise.pdf)
The SolarWinds Log & Event Manager is an excellent option for all sizes of organizations wanting to increase the security of their networks by keeping an eye on their security-related log data without breaking the bank.

SolarWinds monitored the security data in our 30-node sample network, providing a usable interface that enabled us to view security events and to take proactive action to stop suspicious activities.

LEM does not require a degree in packet-level diagnostics to be useful; it maintains the log data and has the necessary tools that enable an IT person to capitalize on the advanced features without being encumbered by a GUI that gets in the way of serious investigative work.

SolarWinds has long been known for its network management expertise; Log & Event Manager will solidify its place as a security company.
Jerry Shenk currently serves as a senior analyst for the SANS Institute and is senior security analyst for Windstream Communications, working out of the company’s Ephrata, Pennsylvania location. Since 1984, he has consulted with companies and financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans networks of all sizes, from small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds six Global Information Assurance Certifications (GIACs), all completed with honors: GIAC-Certified Intrusion Analyst (GCIA), GIAC-Certified Incident Handler (GCIH), GIAC-Certified Firewall Analyst (GCFW), GIAC Systems and Network Auditor (GSNA), GIAC Penetration Tester (GPEN) and GIAC-Certified Forensic Analyst (GCFA). Five of his certifications are Gold certifications. He also holds the CISSP certification.

SANS would like to thank its sponsor:

solarwinds
## Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

Last Updated: March 21st, 2015