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.

Sentinel Log Manager Review

Copyright SANS Institute
Author Retains Full Rights
Sentinel Log Manager Review

A SANS Whitepaper – January 2010

Written by Jerry Shenk

Sentinel Log Manager Setup
Collection
Storage
Reporting and Search
Nearly 90 percent of organizations are collecting log data, according to the 2009 SANS Log Management Survey. They are using log data for a number of reasons, primarily to respond to events and achieve compliance, and they are beginning to use their data to achieve operational efficiencies. In addition, they want to use their logs for many other purposes that have value to business departments. SANS has predicted that logs will ultimately be used to help improve the bottom line as well as provide security enhancements.¹

Respondents to the SANS survey also reported having problems getting their log management systems to deliver on what they require from their logs. The biggest problem reported by these organizations was “using log data to enhance IT operations.”

In order to get more value from their logs, many companies are beginning to implement log management in conjunction with their security information event management (SIEM) systems. There are differences between log management and SIEM that make them complementary. The most basic log management systems collect the logs and allow them to be searched, while a SIEM system has the ability to parse the log data coming from many different sources and combine the data through meaningful analysis.

In July 2009, Novell introduced a new stand-alone log management system that will provide an upgrade path into Novell’s Sentinel full-featured SIEM. Sentinel Log Manager also integrates with Novell’s compliance, identity and data protection tools.

This paper is a review of the stand-alone Sentinel Log Manager and how it stands up to key concerns that survey respondents raised about log managers, including collection, storage and searching/reporting capabilities. Even though the Novell Sentinel Log Management system is a relative newcomer to the log management field, the tool performed well in the critical areas of searching, collection and storage. Reports and reporting features also show good promise but lack some detail. Upgrades to Sentinel’s reports and feature sets are scheduled for Novell’s next Hot Fix at the end of January, 2010. Sentinel Log Manager’s search capability was straightforward and quick, and the system collects from a number of common network, security and systems in use today. Storage management was feature rich, and reporting capabilities are in line with other leading log management products.

A more detailed review of the Sentinel Log Manager follows.

¹ [www.sans.org/reading_room/analysts_program/logMgtSurvey_Apr09.pdf](www.sans.org/reading_room/analysts_program/logMgtSurvey_Apr09.pdf)
The Novell Sentinel Log Manager is currently available for installation on a customer’s hardware, with an appliance-based version available soon. Self-installation provides for more flexibility in hardware and allows the installer to gain some insight into how the program works. It also makes the installation process take much longer than setting up an appliance. Once installed, setup was straightforward and the Sentinel Log Manager immediately began accepting log data from devices in the lab.

Events per Second (EPS) is a popular method for rating the speed of a log server. Often log servers only hit their rated EPS with certain types of data, and the Novell Sentinel Log server is no exception. With appropriate tuning and enough CPU power and RAM, Novell licenses the software for up to 7,500 EPS, with a sustained capability of 80 percent of that rate, or 6,000 EPS. I was able to collect at a sustained 6,000 EPS in the lab using a dual quad-core Xeon server (8 cores total) and 32 GB of RAM. A more moderately-powered dual dual-core XEON server (4 cores total) with 6 GB of RAM and no tuning was able to maintain an average of 800 EPS with a variety of data types.

One of the biggest problems with collecting logs is log format. Different devices log similar events in completely different formats. Log management systems attempt to normalize data so that an operator can request a report for all similar events. For example, if an administrator wants a report of all failed and successful login activity to identify password cracking attempts or configuration errors, the log management server will attempt to pull the appropriate data from the logs that have been collected from different devices throughout the enterprise. The Sentinel Log Management server did well with most events, and Novell engineers are continuing to improve coverage of additional log types. In fact, the event coverage increased during the testing. Novell plans for additional collection from more than 200 new log-generating devices during 2010.
In regards to reporting, many of the stock reports that come with the system include a graphic of events, which can help spot problem trends quickly. Some reports include a timeline that will help identify security events and system issues. Most reports show every event that matches the query, leaving pages and pages of events to sort through. It would be nice to see subtotals of the detail, such as a summary of all failed logins or perhaps a summary of all logins by usernames. Sentinel’s reporting features are being enhanced, and an upgrade is expected in a hot fix being released by Novell the end of January, 2010. In addition to prepackaged reports, Novell uses the JasperForge iReport software, which enables users to customize reports to meet additional needs.

Searching for raw data was straightforward and quick. I had no difficulty searching through 30 days of data for an IP address that attempted to attack the lab’s network, and the results were delivered in a few seconds. This search speed can make a big difference, especially when the IT department is dealing with a problem. One nice search feature is the ability to drill-down into events to narrow the search criteria using either AND or AND NOT searches.

A discussion of storage could fill an entire book. Sentinel Log Manager has a number of storage choices and options, including the ability to automatically delete different types of data at different schedules, to archive data to a variety of online (but separate storage) platforms, as well as the availability of near-online and tape storage.
Based on the results of the 2009 SANS Log Management Survey, it’s clear that the amount of data companies store in the future will be more than they’re collecting today. So it’s best to build a log server that will allow you to grow into it.

Novell’s Sentinel Log Manager is currently a software application that runs on the 64-bit version of Novell’s SUSE Linux Enterprise Server 11. The log manager has heavy processing requirements that must be met in order for the product to be effective. In particular, load up on RAM. Memory is cheap, and your investment will be worthwhile. Below are the current hardware requirements for Sentinel Log Manager to achieve peak EPS rates of 2,500 and 7,500. Novell recommends a sustained EPS rate of 80 percent of the licensed rate.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Sentinel Log Manager (2,500 EPS)</th>
<th>Sentinel Log Manager (7,500 EPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compression</td>
<td>Up to 10:1</td>
<td>Up to 10:1</td>
</tr>
<tr>
<td>Devices</td>
<td>250</td>
<td>750</td>
</tr>
<tr>
<td>Max EPS</td>
<td>2,500</td>
<td>7,500</td>
</tr>
<tr>
<td>CPU</td>
<td>One Intel® Xeon® E5450@3 GHz (4 core) CPU or Two Intel® Xeon® L5240@3 GHz (2 core) CPU (4 cores total)</td>
<td>Two Intel® Xeon® X5470@3.33 GHz (4 core) CPUs (8 cores total)</td>
</tr>
<tr>
<td>Random Access Memory (RAM)</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>2 x 1 TB, 7.2k RPM drives (Hardware RAID with 256 MB cache, RAID 1)</td>
<td>6 x 450 GB, 15k RPM drives, (Hardware RAID with 512 MB cache, RAID 5)</td>
</tr>
</tbody>
</table>

*Table 1. Sentinel Log Manager Hardware Requirements*
The log manager setup is fairly straightforward. However, the documentation doesn’t include a step-by-step installation guide, so installation involved a lot of reading and rereading of the manual\(^2\) to get started (see setup guide in the Appendix). In the long run, all the reading provided good familiarization with the product, but it added a lot of time to setup. If you are using the setup guide in the Appendix, allow a few hours to get the operating system installed and another hour to get Sentinel loaded. A familiarity with any Linux operating system is helpful in working with SUSE server. Note that a lot of this installation process will not be required if customers choose to purchase the software version scheduled for a new release in March 2010, which will install from a disk image (ISO) on bare metal. The hardware version, available soon, will require no installation.

Basic setup steps include installing the 64-bit SUSE Linux Enterprise Server 11,\(^3\) Sentinel Log Manager 1.0\(^4\) and Hot Fix 3.\(^5\) I setup a log server in the lab using a server with two dual-core XEON 3 GHz processors, 6 gigs of RAM and 1.5 TB of drive space. The operating system installation took about two hours, and the installation of Sentinel Log Manager and the Hot Fix took about an hour. The initial installation was a bit difficult due to the different software and documentation issues mentioned above. A fresh installation, after understanding the process, took just over three hours from booting the SUSE DVD to accepting the first log data.

Once the initial setup is complete, the log manager is accessible using a web browser, and the device is ready to start accepting log data. The main additional setup procedure was to configure SMTP alerts. To configure the SMTP server that would accept outbound alerts, I went to the Rules tab from the upper left corner of the screen and then used the configuration link within the Rules tab. From there, I was able to set up the IP address of the internal SMTP server that will relay mail for the log manager. I also set up a From: address. After this is set up, the log manager can send any report on a daily, weekly or monthly schedule.

The hardware in the lab has 1.5 TB of drive space, so external storage wouldn’t be a requirement for quite some time under the lab’s normal load. However, in most cases external storage is eventually needed. The Sentinel Log Manager supports three types of archival storage: CIFS, NFS and SAN storage. The setup for all three options is essentially the same. An NFS server was already set up in the lab so that’s what was used in testing.

\(^3\) [http://download.novell.com/Download?buildid=hwRS9NNA004%7E](http://download.novell.com/Download?buildid=hwRS9NNA004%7E)
\(^4\) [http://download.novell.com/Download?buildid=woGGwp3Mab4%7E](http://download.novell.com/Download?buildid=woGGwp3Mab4%7E)
\(^5\) [http://download.novell.com/Download?buildid=R0FWDqe_xDA~](http://download.novell.com/Download?buildid=R0FWDqe_xDA~)
Chapter 5 in the documentation gives step-by-step details on setting up the data archiving. The Log Manager’s main screen has an option for storage. I clicked on that and then on the Configuration tab, where I was able to choose the storage type and configure how full the local storage should be before archiving starts. The documentation suggests starting archiving when the disk reaches 90 percent of capacity and continuing to archive until the disk is 75 percent full. My disk was about 60 percent full, so I set archiving to start at 55 percent and continue archiving until the disk capacity dropped to 50 percent, as illustrated in Figure 1.

![Image of Sentinel Log Manager](image)

Figure 1. Storage Configuration Options

Overall, the initial setup was a little complicated, but that was primarily due to the lack of an initial setup guide. Once I understood the setup process, setup was fairly straightforward for specified applications and uses, including the e-mail alerts and archiving setup. Don’t skimp on the hardware if you have an environment in which you anticipate a high rate of log events per second.
Collection

The Novell Sentinel web site\(^6\) contains a number of collectors that are designed for specific devices, including many types of Cisco devices; other switches and routers; Novell, Unix and Linux systems; Windows systems (using Snare); as well as web security devices and other critical log-generating devices commonly used in today’s enterprises. You can download additional collectors to support additional types of log data, but most of the available collectors are already packaged with Sentinel Log Manager.

New collectors continue to be added and updated, so it is a good idea to keep an eye on the collector section of Novell’s web site, where new types of log messages and reports are made available. The site offers important PDF files that give detailed information about how to set up logging for specific devices. Because configuring logging on different devices within an enterprise can be a research-intensive task, this site is a valuable resource for anybody setting up a log server.

When it comes to collection, there are two primary performance issues with log servers. One issue is Events per Second—specifically what rate of EPS can the log server collect. Another issue is the user interface—particularly how responsive the interface is while under load and how quickly searches and reports come back with useful information.

In this review, I tested performance using two different log servers both running the 64-bit version of SUSE Enterprise Linux 11 and the Sentinel Log Manager 1.0.0.2 (version 1.0 with Hot Fix 2 applied). The A test server was patterned after an enterprise deployment supporting 7,500 EPS of log data and had two quad-core XEON 3.33 GHz processors, 32 gigs of RAM and 1.8TB of RAID drive space. The B server met the recommendation for a maximum EPS of 2,500 and was sized to relate to smaller organizations and had two dual-core XEON 3 GHz processors, 6 gigs of ram and 1.5 TB of drive space.

\(^6\) http://support.novell.com/products/sentinel/secure/sentinel61.html
To test EPS, log data was generated using a variety of Cisco, Windows, Checkpoint, Nortel and Linux data. The log data was sent using both TCP and UDP protocols. Data was sent to the servers for a period of about four weeks so there would be some history to search through during testing. This data was sent from devices on the local subnet as well as devices connected across relatively low speed T1 links. Traffic to the log servers was measured during testing to verify that the interfaces were able to support the traffic and that the expected amount of traffic was being generated. Log events vary quite a bit in size, but on average, 800 EPS equals 1Megabit per second of network traffic.

The A server was able to maintain a sustained 6,000 EPS and the B server was able to maintain a sustained 800 EPS. Those speeds are consistent with the EPS ratings for the hardware on which I was running the tests. It is possible that additional tuning would increase the throughput. At this time, if you are in an environment with an extremely high number of events per second, carefully plan your capacity requirements and take advantage of the 90-day trial period that Novell offers.

Overall, the collection rates were within the range that Novell claims when using the appropriate hardware and proper tuning. You can also do additional tuning and load balancing to optimize the data collection per CPU.
Storage

Reviewing the storage options in this product was almost as extensive as reviewing the whole product. It offers several methods of offline storage and flexible data retention options. The main storage is in the form of database storage, but some flat file storage that is physically connected to the log manager is also included.

One excellent feature is that the Sentinel Log Manager stores both raw log and event data. Raw log data is just that—the raw events that come into the log server. From a forensic standpoint, there are advantages to having the actual, unprocessed data available. If there is any question about how the log management system, SIEM or other system interpreted the data, the original data is still available for review. Novell’s documentation includes the layout of the raw files so that this data can be parsed by other methods, if necessary.

It is often difficult for companies to determine just how much storage capacity they need when starting out with log management. This is partly due to the fact that they don’t have a good way to estimate how much log data they will have before they start collecting it. Another factor that makes estimating storage needs complicated is the fact that a log management system that works well will grow—meaning new devices and software will be configured to use the log management system as the business requires. The Sentinel Log Manager storage options include graphs on how much data is currently in use, both on the local system and in the archive, and how much space is available. It also charts the rate of use, which will help with capacity planning and keep the IT department from being surprised when the system runs out of disk space.

In the lab tests, after throwing log data at the system at a rate of thousands of EPS for weeks, Sentinel’s Online Capacity Forecasting estimated that this server would need 1.9 TB of data for the next 90 days. After moving some data to archive, online storage will need 1.35 TB of data as shown in Figure 2. The system then continued archiving data as needed to maintain the configured amount of free space.
The options for storage and archiving are impressive, and everything I tested worked flawlessly. The documentation gives details about how storage is handled, where the storage is, and even the format of key files in storage.
Reporting and Search

After setup, the log manager can be set to send reports on a daily, weekly or monthly schedule. To e-mail an ad-hoc search, it must be saved as a report and then run from the report viewer pane. It is also possible to export the ad-hoc search results as a CSV (comma separated values) file so that it can be loaded into a spreadsheet or otherwise processed locally.

Figure 3 is a report that graphically charts a spike in failed login activity on the evening of December 20. Such a report would be something an administrator would want to research immediately to determine whether the network was under attack.

![Figure 3: Spike in Failed Login Attempts Could Mean Attack in Progress](image)

The Figure 3 screenshot displays the results of a test that I ran to detect failed logins. In this test, I logged in correctly to a variety of device types using a number of different user accounts. Then I attempted to login to those same devices with the same usernames and enter incorrect passwords. In the “All Vendors All Products Authentication by User” report, I found accurate data from all successful and failed logins. The report also included a graph that visually represented the time of all successful and failed logins, making it easy to see the spike in failed attempts.
The Sentinel Log Manager comes with a number of reports. In the version I tested, the reports are fairly basic and don’t lend themselves to recognizing and analyzing issues quickly. I was able to find all the events I was looking for, but they weren’t organized in a way to make it apparent that access to the same accounts was being attempted across multiple devices. The report for the prior day was 29 pages long and included 844 different login events. Instead of having to go over the whole list, it would have been helpful to have a list of successful and failed logins per user and per server. Such breakdowns are expected to be included in Novell’s next Hot Fix at the end of January, 2010. These breakdowns will be helpful in determining if all the failed logins were a single user on a single system—possibly a software misconfiguration or a password brute force attack.

Another key element of reporting is search capabilities. An operator needs to be able to enter search data in a meaningful way and get back relevant results. For example, while testing the Sentinel Log Manager, the lab firewall came under an attempted SSH brute force attack and an e-mail alert was sent out by using an existing alerting process I’d setup in the lab. In this brute force attack instance, the firewall’s logs were being sent to the Sentinel Log Manager, so I was able to search for the offending IP address in current events and find it in a few seconds. I then searched through the last 30 days worth of events to see if this IP address had done any reconnaissance or been seen before. It took about 15 seconds to search through 289 GB of data to determine that the IP address had not been seen before. If the IP address had been seen and logged by any of the devices in the lab, the search window would have shown the related log events.

I also did a related search for other similar events and found that 110 systems had attempted a similar brute force attack over the past 10 days. In both of these searches and in the other searches conducted, the responsiveness of the system was good.

Overall, the log manager has the capability of generating reports on a schedule. Those reports can be e-mailed to people who can use the data, or they can be reviewed from the graphical screen. The current reports have a graphic that gives a useful quick overview of information being requested, but they lack the organization needed to enable a user to drill-down quickly and find the necessary details. Search is fast and accurate. Ad-hoc searches are quick to return search results even on a heavily loaded system.
Summary

For the past five years, professionals taking the SANS Annual Log Management Survey have voiced a variety of problems with log management, starting simply with collecting data. As data collection became easier, users moved on to more sophisticated problems to be solved with log data being collected. In particular, this past year survey takers voiced concern with generating useful reports to support the business. In 2009, using log data to enhance IT operations was identified as the biggest problem IT departments were having.

The Novell Sentinel Log Manager is a high-end log manager that aims to meet growing security and management requirements involving log usage. Novell’s Sentinel Log Manager can also integrate into Novell’s Sentinel Security Information and Event Management (SIEM), as well as Novell’s access management and data protection systems.

As a stand-alone log management server, Sentinel Log Manager is able to collect log data at high enough rates to satisfy the needs of many organizations—specifically, sustained 6,000 EPS on a high-end server, which is consistent with Novell’s advertised rates. The search functions are quick, even when performing searches through hundreds of millions of events while the system is under a heavy load of incoming log data. The Sentinel Log Manager comes with a number of pre-built reports and the ability to create additional reports using Jasper. The current built-in reports are lacking in drill down, but new reporting features are on the way in the next Hot Fix, scheduled for the end of January, 2010. Reports can be viewed on the device, and they can also be generated on a schedule and e-mailed to the appropriate personnel on a periodic basis.

In the future, expect demands on log managers to push for coverage of more types of devices that come online and are deemed critical to the business and to regulators. Look for log management systems to provide a solid upgrade path and integration with SIEM systems, as Novell has done. This integration can provide the real-time correlation that will have both security and operational advantages that enterprises need to derive from their log management systems.
Appendix A: Installation Quick-Start

Derived from Chapter 3 and other sections of the “Novell Sentinel Log Manager Guide,” and the Hot Fix installation instructions on the Hot Fix 3 download page.

1. Install the 64-bit version of SUSE Enterprise Linux, version 11. Download the operating system from Novell’s site and burn it to two DVDs. You must have a registered account to download the software, but that is available at no cost. In most cases, you can select the default options for the installation. Give the server a static IP address.

2. Login to the server as root.

3. From the graphical desktop on the newly set up server, start the browser by clicking on Computer in the lower left corner and then clicking on Mozilla Firefox.

4. Browse to download.novell.com and login. If you don’t have a Novell account, you can create one here.

5. After you’ve logged in and are at the download page, make sure you are on the Basic Search tab and use the dropdown menus to select Sentinel Log Manager as the product and Sentinel Log Manager 1.0 as the version. Then click the SEARCH button.

6. Make sure the Products tab is highlighted and click on Sentinel Log Manager 1.0 and then click on the Proceed to Download button in the upper right corner. This will take you to a page with details on the file. Click on the download button in the upper right corner of the screen to start the download of sentinel_log_mgr_1.0_x86-64.tar.gz.

7. This will launch Firefox’s download dialog box. Select Save File and click OK to start the transfer. This will store the file on the desktop. If you are familiar with Linux and want to put this file someplace else, that’s not a problem. I have used desktop here in the example for simplicity.

8. Once the file has been downloaded, open a terminal window by clicking on the GNOME Terminal icon under Computer and then More Applications. This will open a command-line terminal with the user’s default directory. If you are logged in as root, that should be /root.

9. Change to the Download directory with the command cd Download and press Enter. Note, case in important in Linux.
10. Extract the setup directory with the command `tar -xzvf sentinel_log_mgr_1.0_x86-64.tar.gz sentinel_log_mgr_1.0_x86-64/setup`. This command will use the tar program to extract the setup directory from the archive. The tar utility is the tape archive program for most Linux and Unix operating systems, but it is not limited to using tapes. The `x` switch tells tar to extract. The `z` switch tells tar that the archive is compressed. The `v` switch stands for verbose mode—so tar shows files as they are extracted. The `f` switch followed by the filename tells tar what file to extract and the directory (`sentinel_log_mgr_1.0_x86-64/setup`) tells tar to only extract the setup directory.

11. Once the setup directory has been extracted, run the `root_install.sh` script by using the command `./sentinel_log_mgr_1.0_x86-64/setup/root_install_all.sh sentinel_log_msg_1.0_x86-64.tar.gz` and press Enter.

12. The installation script will ask you to pick a language, verify the license agreement and then pick a license option. Use option 1 for the 90-day trial license if you are just trying the Sentinel Log Manager out. You will be asked for passwords for the database administrator and the administrator user—that’s the administrator user within the Sentinel application.

13. Once the application has been installed, you’ll want to install Hot Fix 3. Redo steps 3 through 5 above. This time click on the Patches tab and select Sentinel Log Manager 1.0.0.3. Click on Proceed to download and then select the Download button beside `SENTINEL_LOG_MANAGER_1.0.0.3_04.zip`.

14. This will launch Firefox’s download dialog box, select Save File and click OK to start the transfer. This will store the file in the file in the `/root/Desktop` directory.

15. Once this file has been downloaded, it should be in the `/root/Download` directory, where the Sentinel install file was saved. If you still have the terminal window open, go back to that window. If you closed that, get back to that directory (see steps 8 and 9 above).

16. At this point, you should be in the `/root/Desktop` directory. Type `mv SENTINEL_LOG_MANAGER_1.0.0.3_04.zip /home/novell` and press Enter to move the newly downloaded file to the Novell user’s directory. This step is needed because the Novell user will not have appropriate permissions in root’s Desktop directory.

17. You will not be able to install the Hot Fix as root, so you’ll need to switch users to the Novell user. Type `sudo –u novell sh` and press Enter to switch to the Novell user while staying in the same directory.
18. Type `cd /home/novell` and press Enter to change directories.

19. Type `unzip SENTINEL_LOG_MANAGER_1.0.0.3_04.zip` to extract the Hot Fix.

20. Type `cd SENTINEL_LOG_MANAGER_1.0.0.3_04/` to change into the newly created directory.

21. Type `./service_pack.sh` to install the Hot Fix. Accept the default options.

22. The firewall needs to be configured to allow incoming traffic to the GUI, so click on Computer, YAST, Firewall, and then click on Allowed Services and use the advanced button to enter the ports that need to be allowed. On the TCP line, enter 8443 1443 1468 and on the UDP line enter 514. Then press the OK button, then Next and Finish to apply the new firewall rules.

23. Type `exit` and press Enter to switch back to the root user.

24. Type `shutdown –r now` to reboot the server.

25. When the system comes back up, it should be ready to accept log events. You can access the GUI interface by browsing to `https://[ip address of server]:8443`.

26. There is a script that needs to be entered after you have started the log manager. Open a command prompt (step 8 above) and type `/opt/novell/sentinel_log_mgr_1.0_x86-64/bin/config_firewall.sh` and press Enter. This command can be added to the `/etc/rc.d/after.local` script to automate the startup process.

Congratulations! You've successfully installed the Novell Log Manager and should be ready to go.
Jerry Shenk currently serves as Senior Analyst for the SANS Institute and is the Senior Security Analyst for Windstream Communications in Ephrata, PA. 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 from small home office systems to global networks. Along with some vendor-specific certifications, Jerry holds six GIAC certifications (5 gold), including GCIA, GCIH, GPEN, GCFW, GSNA, and GCFA, all completed with honors.
SANS would like to thank this paper's sponsor:

Novell®
<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Format</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>