Managing User Risk: A Review of LogRhythm CloudAI for User and Entity Behavior Analytics

In this product review, we explored the recently released LogRhythm CloudAI, which applies user and entity behavior analytics (UEBA) capabilities to enhance traditional event management and security analytics toolsets to monitor behaviors tracked over time, alerting analysts to unusual events or patterns of events.
A SANS Product Review

Written by Dave Shackleford

April 2017 (Revised February 2018)

Sponsored by
LogRhythm
In today’s fast-paced threat environment, speed to detect and respond is critical. Yet, according to multiple SANS surveys, analysts are finding it difficult to keep up with the speed in which hackers attack their systems.

While attackers run automated scripts and programs, our security and logging systems must intake and interpret this data down to actionable information in as near real time as possible—without bogging down defenders and responders with too much unnecessary information.

Unfortunately, for many defenders and responders, this level of actionable defense is not achievable. In addition to lack of visibility, the vast majority of organizations in SANS surveys cite a lack of personnel and dedicated resources as their key impediments to rapid and accurate detection and remediation of real threats that apply to their enterprises.

Security information and event management (SIEM) platforms and similar tools are meant to consume log and event information from a variety of endpoints, security devices and network flows, while providing a dashboard for analysts to drill down into events and use the information to accurately respond and remediate. Over time, SIEM tools have evolved to ingest more forms of log, threat, event and intelligence data, integrate and correlate it against threat intelligence and other contextual information, and advance their analytics techniques to include artificial intelligence and machine learning.

Just how scalable, fast and accurate are these tools when under load? We decided to put the LogRhythm 7.2 Threat Lifecycle Management Platform to the test. We found that its clustered Elasticsearch indexing layer supported large log volumes of security and event data during simulated events that would require investigation and remediation.

Some of the core strengths of LogRhythm's system include its data processing, machine analytics, rapid search, and drilldown—all of which speak specifically to the need for speed and accuracy. Other strong features include LogRhythm's security automation and orchestration through case management and SmartResponse™. We also found the Metrics tab for a case to be a helpful tool in benchmarking mean time to detect and other useful metrics, including time and completeness of remediation, and utilizing any new-found intelligence for trending and reuse.
LogRhythm’s latest Threat Lifecycle Management Platform includes many new and enhanced features and behind-the-scenes improvements, primarily focused on reducing detection and response time for security operations and investigations. LogRhythm’s data aggregation and query engine now uses Elasticsearch, which is a highly scalable indexing and querying layer. Native language search and contextual searching are available from most locations in the interface as well. We focused on scalability and performance in this review, as well as host-based policies and configuration capabilities that are new in the platform.

In this review, SANS focused specifically on:

- Ease of use
- Scalability and performance across large, distributed data sets
- Host-based policies and configuration capabilities
- Rapid searching, analysis and incident correlation
- Case management tools that can help security operations teams operate more effectively

Components

The following components were included in the LogRhythm deployment (numbers in parentheses indicate quantity configured within the review environment):

- **Platform Manager (1)**—Centrally manages alarms, notifications, and case and security incident management. Enables real-time dashboards, SmartResponse actions and reporting.
- **Data Collector**—Provides local and remote agentless collection of machine data.
- **System Monitor Agent**—Monitors endpoints for file integrity, user activity, network communications, and applications and processes. Our testbed used the agents for Linux systems; AIX, HP-UX, Solaris and Windows are also supported.
- **Network Monitor**—Performs deep packet inspection of network traffic for application identification, extraction of searchable metadata, full packet capture and deep packet analytics.
- **Data Processor (5 sets of 4)**—Processes data from Data Collectors, System Monitors and Network Monitors. Extracts and enriches metadata, enabling machine- and search-based analytics. Data Processors scale vertically and horizontally.4

---

4 LogRhythm introduced an updated data processor in the Fall of 2017, DP 7470. While SANS has not tested this, LogRhythm reports that this new processor reduces the data processor components by 25% to five sets of three components.
Review Environment

- **AI Engine (5)**—Performs real-time, stream-based analysis of contextualized machine and forensic data, and generates risk-prioritized alarms using a broad set of algorithmic techniques. AI Engine nodes scale vertically and horizontally with a unique scaling model to preserve centralized analysis.

- **Data Indexer (5 sets of 10)**—Uses an Elasticsearch back end to store copies of both original unstructured machine data and contextualized, structured metadata to enable search-based analytics. Data Indexers support clustering for greater scalability, performance and availability.

The environment was configured with the following parameters and capacity considerations:

- 300,000 MPS aggregate collection load (25.8 billion messages per day)
- 130,000 unique log sources
- 100 percent of data processed within the distributed architecture
- 100 percent of data analyzed in real time by analytics layer, with no data queued
- 100 percent of data rapidly searchable
- 100 percent of data available, persistent and archived

These were the objectives and environment for our review. However, substantially higher scalability is available with further hardware investment. A diagram of the environment is shown in Figure 1.

---

LogRhythm introduced an updated data indexer in the Fall of 2017, DX7500. While SANS has not reviewed the updated data indexer, LogRhythm reports that this new configuration reduces the data indexer components by 50% to five sets of five.

---

Figure 1. LogRhythm Test Environment Architecture

---

5 LogRhythm introduced an updated data indexer in the Fall of 2017, DX7500. While SANS has not reviewed the updated data indexer, LogRhythm reports that this new configuration reduces the data indexer components by 50% to five sets of five.
The evaluation environment included content from two LogRhythm Knowledge Base modules, which are bundles of analytics, reports, rules and other analytics tools. LogRhythm Labs creates and maintains these packages. Some areas these modules cover include:

- Core Threat Detection Module, which includes foundational tools for threat detection and response. It uses preconfigured rules and leverages common sources of log data and security events, helping customers realize value quickly.
- Top 20 CIS Critical Security Controls Module, which delivers analytics to ensure organizations are aligned to the CIS Controls.

We applied this content to several specific use cases, which are covered in detail in the final section of this paper.
Scaling to Today’s Threat Landscape

LogRhythm’s Threat Lifecycle Management Platform is designed to reduce detection and response time for security operations and investigations. As such, this section of our review focuses on its scalability and performance at several tiers:

- Collection
- Processing
- Machine analytics
- Persistence
- Search analytics

This section then explores aspects of LogRhythm that streamline administration and configuration.

Data Collection and Generation

Scalable and resilient collection of event data is key to business and security teams alike, as poor performance of aggregation and central collection functions can degrade systems, applications and even network links.

The following attributes are important to consider when evaluating event collection:

- **Volume and velocity of data.** LogRhythm provides a horizontal distribution of data collected and so supports tens of thousands of data sources remotely or with agents. To validate this during the performance review, we observed LogRhythm collecting over 300,000 MPS. This was done with just 60 System Monitor agents collecting 5,000 MPS apiece, demonstrating the agent’s ability to forward a significant amount of data. LogRhythm reports supporting deployments with significantly more agents (10,000 or more), a capability we verified in an earlier review of LogRhythm.

- **Distributed architecture.** LogRhythm’s distributed collection architecture can collect data close to the source, ensuring efficient and secure forwarding to a central location. (This function was not specifically examined.)

- **Variety of sources and data types.** LogRhythm can collect any message-based data from any source, through a variety of remote or agent-based collection techniques. We saw that 130,000 unique log sources were generating events. Figure 2 depicts the distribution of these log sources across a small, distributed collection footprint.
Data Processing

The processing and enrichment of disparate types of log and event data into a consistent format is an extremely resource-intensive process. It must be executed nearly instantly so as to enable downstream machine analytics and search analytics. LogRhythm's data processing tier uses load balancing to provide scalability at this layer.

LogRhythm's patented Machine Data Intelligence (MDI) Fabric provides automatic processing and enrichment for over 750 data sources out of the box. This entails the extraction of metadata, the normalization of key fields (e.g., time of collection) and use of enrichment to ascertain other data (e.g., directionality). In the testing environment we reviewed, these techniques were applied to every collected log, preparing them for immediate analysis.

To evaluate the total processing capability of the review architecture, we measured events being processed at 302,000 MPS in the LogRhythm test environment, with 20 data processors handling an average of 15,000 MPS, as shown in Figure 3.
To see how rapidly LogRhythm could process data and make it available for searching and analysis, we reviewed activity monitors to see when specific events were first seen by the system and then verified when they were processed. We observed the system collecting an event, and then processing and indexing it within seconds.

**Machine Analytics**

The heart of any analytics platform is the automated analysis of data that has previously been collected and processed. LogRhythm’s analytics tier is comprised of its patented AI Engine nodes, which perform stream-based analytics using a blend of scenario-based and behavioral anomaly detection-based techniques. Any event-management platform that performs complex analytics should exhibit or possess the following capabilities:

- **Perform real-time analysis.** To meet the need for real-time throughput, AI Engine leverages stream-based, in-memory analysis to recognize activity within seconds of collection and processing. We verified that alarms raised by AI Engine were visible within seconds of the associated data being collected.

- **Perform multiple analytics techniques.** We noted that AI Engine supports a variety of analytic techniques, such as advanced correlation and behavioral analysis, including automated behavioral, histogram, statistical and whitelist profiling. The deployment was set up with 16 real-time rules. Several real-world use cases that demonstrate these analytics capabilities are detailed in the Use Cases section of this paper.
• **Analyze data from across the environment.** Monitoring for sophisticated threats and modeling complex behaviors also require a holistic view of the environment. AI Engine’s analytics rules accepted the spectrum of collected data across all device types we used in the mock environment.

• **Scale vertically and horizontally.** Each AI Engine analyzed data at a very high velocity (up to 75,000 MPS), and analysis was distributed across multiple AI Engine nodes in support of horizontal scaling or distributed analysis. We observed that 100 percent of collected data was analyzed using the five AI Engine servers in the review deployment.

### Data Persistence

Storing larger amounts of event data for longer periods of time allows security and forensics teams to perform deeper queries over longer periods, effectively building better and more accurate behavioral trending and alerting models. This idea of data persistence is a critical one for security analysis, especially in large, busy environments.

LogRhythm’s data persistence tier uses Elasticsearch, a high-performance indexing back end suited to very large environments. The technology sustains heavy concurrent read/write operations, so heavy write activity doesn’t degrade the ability to search through large volumes of data. LogRhythm provides the scalability of Elasticsearch without the attendant complexities and costs of a build-your-own open source deployment.

To verify the volume and velocity of event data persisting on the system, we reviewed the various Data Processor metrics, including data indexing, data archiving and logs being “flushed” through the system. Metrics for a handful of the 50 DX appliances are shown in Figure 4.

![Figure 4. Graphs Showing 26.1 Billion Logs Being Processed and Indexed in a 24-hour Period](image-url)
Search Analytics

LogRhythm’s analyst UI is streamlined, with easy-to-read dashboards and a simple configuration utility for creating new dashboards and quickly adding “widgets” that display the data we need for security operations. Figure 5 shows a dashboard that includes a number of common security operations events and metrics analysts need to gain insight into trends or utilize for intelligence and follow-up.

This dashboard provides widgets enabled for log processing rate, top alarms in the past 30 days, top common events and classifications, top impacted hosts and applications, event direction and others. Dashboard widgets can be added, deleted or customized through the UI. These widgets give analysts at-a-glance visibility into the deployment’s operational health and a security-oriented view of the environment’s activity.

We were also able to centrally search across all data sources using the Precision Search interface, which is located in the upper-right section of the analyst UI. Users can perform unstructured searches, contextualized searches and “precision searches” that combine these types of queries. These options narrow results down to a more relevant set of results for faster investigation. Precision Search capabilities are made possible by LogRhythm’s Elasticsearch back end, which provides a massively scalable central indexing layer.

Figure 5. Security Analyst Dashboard
Search is precise and fast, even when under a 300K MPS workload. As a demonstration, we searched for all log activity with the classification of “Access Success,” an Origin User on a list of terminated users, and containing either the term confidential or forecast in the log message. This query is shown in Figure 6.

![Figure 6](image)

**Figure 6. Precision Search with Both Contextualized and Unstructured Elements**

**Exploring Host Agents and Policies**

This version of LogRhythm has streamlined administration of host agents with powerful configuration management and monitoring capabilities. These changes provide consistency of administration across hosts, ensuring standardized monitoring of file integrity, process activity, network communications and user activity. There are multiple policy types available out of the box, and policies can also be created and modified easily. For example, in our review, we tested a standard policy for file server.

LogRhythm provides pre-canned agent settings for several operating systems. After we selected the file server policy, we customized how the agent would behave and what actions it would take, including the data processors it communicates with, the types of logging and events it collects, SNMP settings, file integrity monitoring rules and more (see Figure 7).
We also tested agent fault tolerance by disabling the primary data processors selected in the policy configuration, and observed failover to the next available processor.

Overall, we found policies to be intuitive to today’s risks and helpful to administrators. It was easy to create our own policies on the fly.

As we reviewed LogRhythm’s ability to scale, we found it scales and performs well under a load of 300K MPS. In our review environment, LogRhythm was capable of consistent log collection, processing, analysis, indexing and search performance. Further, we found that LogRhythm’s embedded security automation and orchestration tools continue to perform well under these production-like circumstances.
Our use cases were designed to show the speed and responsiveness of LogRhythm’s security automation and orchestration, while also demonstrating functionality, including alarming, case management, SmartResponse automation and more. Throughout the review, and under the heavy load of our 300,000 MPS testing conditions, LogRhythm returned queries in seconds and triggered actionable alarms quickly.

Next we review LogRhythm under two monitoring and response use cases involving different forms of user-based threat.

**Case I: Identifying Privileged Account Creation**

Insiders represent the top threat to systems and data, according to multiple SANS surveys. For example, in the SANS 2016 survey on healthcare cybersecurity risks and practices, 39 percent see insider threats as the main cause of threats affecting their networks.6

Monitoring privileged IT groups for new and unusual activity is a common event monitoring strategy because privilege escalation and abuses of privilege are hallmarks of an attack already in progress. So, in our first scenario, we used LogRhythm to monitor an emulated environment where an insider with administrative privileges first creates a domain administrator account and then attempts to delete sensitive data files. This case allowed us to explore the LogRhythm UI and SmartResponse features to not only detect but also respond to these events in near real time.

**Triggering Alarms**

In this case, when the emulated insider created a new domain administrator account, it triggered a high-priority alarm in the LogRhythm console, as seen in Figure 8.

---

The alarm was triggered through LogRhythm’s real-time analytics engine and an algorithm from the Core Threat Detection Module. LogRhythm’s SmartResponse (part of LogRhythm’s security automation and orchestration capabilities) triggered automatic additional monitoring of this account (curly.howard) so that all additional activity related to the account was monitored more closely for things such as lateral movement to other systems.
Taking Automated Actions

Drilling into the event was easy through the console, allowing us to see affected groups, systems, execution time and more. For example, when the hypothetical user we were monitoring attempted to delete important files, SmartResponse performed several actions automatically and in near real time: first disabling the user and then logging off the user per our preconfigured policy of what to do when these actions are detected by LogRhythm (see Figure 9).

![Figure 9. SmartResponse Disabling and Logging Off the User](image-url)
We then drilled down into the event to see more details and used the pivot functionality to monitor the other activities of the user, our protagonist, curly.howard. That’s when we caught curly.howard accessing other systems and interacting with additional accounts he shouldn’t be accessing, as shown in Figure 10.

While we explored this as an insider abuse case, these lateral moves are also typical of an external attacker who has credentials and is trying to pass himself off as a privileged insider who is accessing the systems in a perfectly legitimate manner. This is why so many of these activities go undetected without tools such as LogRhythm to detect the patterns, sound alarms and connect the illicit activities into a threat snapshot.
Managing and Provisioning

We also had easy visibility into and control over our own roles ranging from system management to SOC analysts to auditors needing access with different privileges. LogRhythm made this simple to provision and manage, with the capability to connect Active Directory and assign roles to users and groups, as shown in Figure 11.

Throughout the case study, we found the interface to be intuitive and simple to navigate, whether viewing dashboards (where many SOC analysts will spend a good deal of time), monitoring alarms (a dynamic dashboard of risk-rated events), creating and editing incident cases, or querying for events and correlation relationships.

Case II: Spearphishing

The second incident monitoring and response use case we pursued was that of a user being phished, which, according to the SANS 2016 survey on endpoint security, is the most critical vector attackers use to compromise endpoints. It found 75 percent of impactful threats infiltrated organizations through an email attachment, and of those, 46 percent were executed by users clicking links in emails.7

For our review, we executed a typical phishing attack path starting at the endpoint to give us more exposure to the LogRhythm UI, alarms, and pivoting and case management tools. The attack pattern went as follows:

1. A user clicked a link in email.
2. Once clicked, the link opened the door to a local exploit.
3. That exploit then communicated with an external site on a known threat list.
4. The attacker performed lateral movement by brute forcing admin accounts on neighbor systems using PsExec.
5. The attacker then set up an SSH tunnel for data exfiltration.

**Sounding Alarms**

As soon as we started the above scenario, a “severe priority” alarm for a phishing attempt was sounded by LogRhythm AI Engine, which was automatically analyzing data to generate risk-prioritized alarms, as seen in Figure 12.

![Figure 12. A High-Severity Phishing Alarm](image)

We investigated our phishing incident by drilling down into this suspicious activity and created a new case from the initial analysis.
Managing Cases

One of the great features in LogRhythm 7 is the enhanced case management capability, which comprises part of its security automation and orchestration function. With Case Manager, we could open a new case with any detected events or incidents, add status information, rank by priority (1 is the highest), indicate whether we believed this was an incident or merely event data, and add a due date and description.

Creating a case in the LogRhythm interface is simple—you can click the New Case button in the alarms console (shown in the lower left of the screen in Figure 12). We then drilled into the phishing alarm and added it to the new case, as seen in Figure 13.

![Figure 13. Adding a Phishing Alarm to the Case](image-url)
Integrating Threat Intelligence

We then pivoted in the console to the affected system compromised during the attack. By monitoring this system and its associated behavior, LogRhythm (through integration with one of its third-party intelligence feed partners) alerted us that the compromised system accessed a network that had previously been spotted on a known botnet threat list.

We also noted that the attacker used PsExec from the impacted host to perform brute force password guessing against neighboring hosts, with a new alarm (raised by AI Engine) indicating brute force activity, represented in Figure 14.

![Figure 14. Lateral Movement and Brute Force Attacks](image)

In this alarm, we see the PsExec file detected, authentication failures, the administrator account as a target and other impacted hosts.
Monitoring Network Flows

Network monitoring capabilities within LogRhythm capture the flows in a session, identify the application through deep packet inspection, and extract the metadata necessary to detect and respond to events.

In our review environment, LogRhythm Network Monitor captured abnormal traffic flows to neighboring systems, followed by outbound data exfiltration, which generated new alarms. By drilling into these new alarms, we leveraged Network Monitor to obtain a packet capture (PCAP) file of SSH exfiltration tunneling, which we added to the case, as shown in Figure 15.

The PCAP we added can be sent to network forensics team members easily, and any of the noted events within the LogRhythm dashboard can be added as logs to the case. When time to respond is of the essence, having all the event data associated in a single case file helps investigators respond to events as they are happening.

Figure 15. Downloading Suspicious Traffic as a PCAP File
Quarantining Impacted Systems

To wrap up this case, we needed to quarantine the initial system affected by the phishing attack, as well as others involved in the brute force attack. To implement the quarantine, all network access to and from these systems was automatically blocked using LogRhythm SmartResponse actions, and with the PCAP files, additional forensic analysis can be performed.

Ranking and Sharing

This use case illustrates a number of capabilities in the new version of LogRhythm:

- Immediately surface alarms that are ranked and prioritized based on risk.
- Perform rapid drill-down into events to get more details about users, systems, applications, traffic and other associated elements.
- Add all data, events and evidence to cases, which can then be shared with other team members as needed.

Improving Efficiency

The two use cases depicted above show how LogRhythm can help an organization detect and respond to a cyberthreat. Data can be used to monitor time from case creation and status elevation to mitigation and completion, as depicted in Figure 16.

![Figure 16: Case Metrics Data, Showing Detection and Response Times for a Specific Case](image)

Organizational mean time to detect and mean time to respond can be tracked over time and displayed via a dashboard widget, enabling continual process improvement.

We were able to drill into events as they occurred in near real time, as well as get fast access to historic data and comparison reports. We were able to correlate data centralized by LogRhythm with additional intelligence from third-party vendors, create cases, add evidence and assign team members to cases. All of these capabilities save time and resources—which, according to many SANS surveys, organizations simply don’t have.
Conclusion

Security professionals are facing more challenges than ever before. We have more data, more adversaries, less time and nowhere near enough skilled professionals to help defend our network environments. LogRhythm 7 is a platform that can help analysts, providing ease of use and broad and powerful functionality that streamlines the process of detecting and responding to cyber security incidents.

As with a previous review we conducted in 2015,8 LogRhythm 7.2 scales and performs to meet the critical needs of security operations teams. It offers significant benefits to security operations teams and analysts who need a unified platform for threat detection, with behind-the-scenes data processing, machine analytics, response and orchestration.

In this version, we also took note of the scalability and performance of the platform, with a test bed that mimicked a large real-world deployment. The testing environment operated at 300K MPS (26 billion logs per day). Collection was drawn from over 130K log sources, and processing and analytics were performed on all data. In addition, we noted some of the newer host-based policies and configuration capabilities added into the system, with flexible and easily managed agents that are resilient, easily modified and upgraded, and simple to deploy.

Defenders and responders need tools that are easier to use, with deep and robust capabilities to search intuitively for malicious behavior and respond quickly. In our review, the tools we explored—including a number of automated SmartResponse actions—helped prevent data loss by detecting malicious activities as soon as we initiated them. As important, the LogRhythm platform is self-learning and provides a full-circle feedback loop that risk managers can use to improve security.

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

SANS would like to thank this review’s sponsor:

LogRhythm
The Security Intelligence Company
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS San Francisco Spring 2018</td>
<td>San Francisco, CAUS</td>
<td>Mar 12, 2018 - Mar 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Spring - Tysons 2018</td>
<td>McLean, VAUS</td>
<td>Mar 17, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>ICS Security Summit &amp; Training 2018</td>
<td>Orlando, FLUS</td>
<td>Mar 18, 2018 - Mar 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich March 2018</td>
<td>Munich, DE</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Canberra 2018</td>
<td>Canberra, AU</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2018</td>
<td>Austin, TXUS</td>
<td>Mar 19, 2018 - Mar 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Spring 2018</td>
<td>Boston, MAUS</td>
<td>Mar 25, 2018 - Mar 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2018</td>
<td>Orlando, FLUS</td>
<td>Apr 03, 2018 - Apr 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Abu Dhabi 2018</td>
<td>Abu Dhabi, AE</td>
<td>Apr 07, 2018 - Apr 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Pre-RSA® Conference Training</td>
<td>San Francisco, CAUS</td>
<td>Apr 11, 2018 - Apr 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich 2018</td>
<td>Zurich, CH</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2018</td>
<td>London, GB</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2018</td>
<td>Baltimore, MDUS</td>
<td>Apr 21, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training 2018</td>
<td>Louisville, KYUS</td>
<td>Apr 23, 2018 - Apr 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Seattle Spring 2018</td>
<td>Seattle, WAUS</td>
<td>Apr 23, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha 2018</td>
<td>Doha, QA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2018</td>
<td>Riyadh, SA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta Two</td>
<td>Crystal City, VAUS</td>
<td>Apr 30, 2018 - May 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Automotive Cybersecurity Summit &amp; Training 2018</td>
<td>Chicago, ILUS</td>
<td>May 01, 2018 - May 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 in Thai 2018</td>
<td>Bangkok, TH</td>
<td>May 07, 2018 - May 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2018</td>
<td>San Diego, CAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2018</td>
<td>Melbourne, AU</td>
<td>May 14, 2018 - May 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Reston Spring 2018</td>
<td>Reston, VAUS</td>
<td>May 20, 2018 - May 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2018</td>
<td>Amsterdam, NL</td>
<td>May 28, 2018 - Jun 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta 2018</td>
<td>Atlanta, GAUS</td>
<td>May 29, 2018 - Jun 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Singapore 2018</td>
<td>OnlineSG</td>
<td>Mar 12, 2018 - Mar 24, 2018</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>