The Expanding Role of Data Analytics in Threat Detection
Time-honored threat detection methods and perimeter-based security defenses add valuable layers of protection around information system assets, but neither is sufficient to defend completely against modern threats. Organizations now depend on 24/7 connectivity to support access to myriad web, mobile and social applications both inside and outside their network boundaries. As such, attackers have stepped up their game with new threats, using highly sophisticated and automated techniques that allow them to infiltrate corporate networks undetected, enabling unfettered access to valuable resources and sensitive data.

In this new age of security, information security professionals must deliver effective, real-time defenses, defenses that can predict inherent threats to critical assets. Often, however, they are charged with defending data across networks over which they have little control. The evolution and diversity of the threat environment, the uncontrolled nature of the infrastructure that needs to be protected, and the increasing volume and intensity of recent attacks like those at Sony and Target—unthinkable a decade ago—give the security community no other choice than to look at adopting new methods and tools.

To this end, tools based on data science and machine learning can help organizations quickly detect malicious activity and act according to the inherent risk presented by potential rogue elements. Analytical methods can be used to monitor critical performance characteristics, such as network traffic, CPU usage and port activity, and identify unique events or trends that exhibit the behaviors of malicious activities. Analytics can also be used to flag abnormal behavior of end users, applications and other elements inside the organization by identifying activities that depart from a normal baseline established over a period of time.

This paper will examine the properties of a modern attack and techniques of detection methods that have been in use since the 1980s. It will then explore ways that automated threat detection may be able to complement or improve upon traditional methods in order to fulfill goals defined within the Critical Security Controls (CSCs).
The evolution of the threat environment has already changed the dynamics of attack and defense enough to turn a litany of once radically negative assumptions into routine advice: Consider a breach as inevitable—perimeter protections will fail, and attackers will get in and stay in until their mission is accomplished, which could take months. The anatomy of a modern attack is shown in Figure 1, a model similar to the classic Cyber Kill Chain model originally proposed by Lockheed.¹

1. **Getting In (Penetrate and Establish a Foothold):** Attackers commonly use a combination of social engineering and malware—for example, an email phishing attack. Specifically, they target an organization using information harvested via social engineering, social media and open source data, and then lure unsuspecting users into downloading malware onto their computers.

2. **Staying In (Escalate Privileges and Move Laterally):** With an initial foothold established, attackers obtain legitimate credentials—especially those with privileged access—or create new credentials so that they can move laterally to perform reconnaissance and gain higher levels of access. Attackers can remain present in a targeted organization for long periods of time undetected, blending in with the environment.

3. **Acting (Complete the Mission/Cause Damage):** Attackers stage the data they are after—such as intellectual property, identity information or financial data—and complete the process of stealing data through (often long-term) exfiltration. The process often causes other damage inadvertently through purposeful vandalism.


3 “Detecting cyber attackers—how long does it take?” IT Governance blog, March 12, 2015, www.itgovernance.co.uk/blog/detecting-cyber-attackers-how-long-does-it-take/
Threat detection can focus on individual platforms, networks, systems, endpoints or almost any other IT resource. It can also cover a range of functions, including intrusion detection, remediation of viruses, malware or spyware, or simply observing the unauthenticated and unauthorized use of programs or networks. Since SRI International and Dorothy Denning developed the Intrusion-Detection Expert System in the 1980s, advancements in threat detection seem to be correlated with advances in intrusion detection systems (IDS). The concepts behind IDS apply to a whole range of security tools that defend information systems and networks from dangerous threats like malware, spyware, spam and much more.

Although IDS/IPS, antivirus and similar signature-based products are successful against single-vector attacks, the fact is, more and more major security breaches are occurring where these traditional approaches to security no longer work. While the shortcomings of signatures used by IDS and other perimeter security systems are well known, much of the industry effort has been focused on delivering signatures faster. This tactic has simply led to faster attackers or the use of vectors with no known signature.

Today, signature-based detection is still the predominant method of finding and eliminating security threats in the enterprise, but new trends are on the rise. Specifically, methods from data science and machine learning coupled with increased computational power (at lower cost) and the availability of relevant data are making inroads into automated threat detection that identifies new patterns, detects events that may not match a specific signature, determines behavioral abnormalities, and subsequently acts on the possibility of compromise.
Detection Methodologies

Most systems depend on one or more of these threat detection methodologies:

- **Signature-Based (or Misuse) Detection** uses a set of rules to identify threats such as intrusions and viruses by watching for patterns of events specific to known and documented attacks. The basic architecture is shown in Figure 2. Preprocessing methods, such as deep packet inspection for network traffic, find possible signatures in captured network traffic. The resulting signatures from the monitored environment are matched to known signatures in a signature database. If a match is found, an alert is issued, and if there is no match, the detector does nothing.

  ![Figure 2. Signature-Based Detection (Simplified)](image)

  This method typically produces fewer false positives than traditional methods, with relatively low processing demands. The main disadvantage is that it only detects attacks for which a defined signature is known and available. New attacks must be identified, modeled and added to signature databases, which must be updated regularly to keep innovative exploits, or those based on previously unknown flaws, from evading defenses.

- **Anomaly-Based (or Behavior-Based) Threat Detection** depends on the assumption that attack behaviors differ enough from normal activity that malicious actions can be detected and identified. Tools using this method begin by creating models of behavior patterns that represent “normal” behavior for the networks, systems, applications, end users and devices that make up the environment in which they’re installed. They then look for deviations from that pattern. The basic architecture is shown in Figure 3.

  ![Figure 3. Anomaly-Based Detection (Simplified)](image)

  The advantage of this method is the ability to spot a threat without first knowing its signature. Historically, this advantage has been offset by high false positive rates, the difficulty of training a system in a highly dynamic environment, and computational expense.
Continuous System Health Monitoring detects intrusions by active monitoring of key system “health” or performance factors to identify suspicious changes or trends in activity and resource usage. On the network, this may mean monitoring network protocol usage over time, looking for ports experiencing unexpected traffic increases.

This method involves efforts to develop and tune systemwide measures and understand the significance of identified variations and trends, ultimately mapping both to unique behaviors that malicious activities may have in common.

Teaching Machines to Identify Threats

Modern machine learning (ML) techniques are more highly evolved descendants of the post-Turing artificial intelligence movement in the 1950s and ‘60s, which evolved partly from advances in statistical inference and probability made in the early 20th century. ML has been used in the financial industry since the 1970s to detect fraudulent behavior but is just now beginning to show up as a potentially useful option for information security. The factors moving ML tools and techniques from the research lab to the operational domain include both the phenomenal growth in inexpensive compute power and bandwidth and the overwhelming amount of data generated and dumped into security information and event management (SIEM) tools daily. These tools can now be used to develop the mature algorithms and modeling techniques for real-time automated threat detection.

Although ML tools can be very effective, they produce very different results depending on the source and quality of data being analyzed. Specific domain knowledge related to security—as opposed to clinical research or finance, for example—is needed to design a threat detection system using appropriate ML mathematical and statistical algorithms. A data scientist must apply security domain knowledge to identify primary and secondary sources of data, determine how to clean and transform acquired data and select the best ML analytical method or algorithm for the problem at hand. Primary sources for the security domain include network packets, ML-based analysis of which reveals otherwise invisible communication patterns from an attacker inside the network. Secondary sources are logs routinely collected from other devices, which may provide additional depth to the analysis but not direct evidence of activity because of the nature of their role in providing security defenses.

https://en.wikipedia.org/wiki/Artificial_intelligence

Machine learning describes a collection of algorithms and techniques used to design systems capable of acquiring and integrating knowledge automatically. Machine learning can be supervised, inferring a function from labeled training data, or unsupervised, developing and modifying the behavior model without owning a previous model, through constantly analyzing available data. Supervised ML can identify a threat almost immediately without knowing anything about the threat or environment; unsupervised ML needs to learn the local context of what is “normal.”

Data science is the ability to take data and understand it, process it, extract value from it, visualize it and communicate insights derived from it. More formally, it is the extraction of knowledge from large volumes of data that are structured or unstructured, which is a continuation of data mining and predictive analytics, also known as knowledge discovery.

Systems that Learn

A system capable of learning results in an automated threat detection and management tool that is both efficient and effective and that continuously self-improves. There are three main layers:

1. **Data acquisition and feature extraction.** To be useful in threat identification, data—network traffic or process execution events from various endpoints and host systems—must be sensed and captured in ways that allow it to be analyzed consistently over time and despite changes in the components producing the data being gathered. A feature extraction module is used to convert the raw data into feature vectors or datasets. This is a key step. If features are improperly selected, the performance of detection models will be negatively affected. Classifier construction also presents a challenge because it is very difficult to detect new attacks by only training on limited audit data.

2. **Real-time detection.** This determines whether an observed pattern or a sequence of patterns is normal or abnormal, as it happens, based on the detection model and how the system has been trained.

3. **Machine learning.** This is the heart of the system, containing the various algorithms for anomaly detection, audit or training data (dynamically updated either by human analysts or the ML algorithms), and the actual behavior-based detection model. Selection of an appropriate algorithm includes several considerations, all of which can affect performance and the validity of the outcomes: accuracy, training time, use of linearity, number of parameters, and number of features.

---


7 https://en.wikipedia.org/wiki/Data_science
Figure 4 presents a basic reference architecture using both data science and ML.

**Figure 4. Threat Detection Reference Architecture Based on Machine Learning**
So where does all this innovation leave security practitioners trying desperately to protect their data and systems from threats that easily bypass perimeter defenses? How does intelligence-based threat analysis work in tandem with or change existing information security management?

The Critical Security Controls (CSCs), developed through federal and community efforts, coordinated by the SANS Institute and currently maintained by the Center for Internet Security, are designed to mitigate modern attack profiles. Figure 5 shows the three interlocking segments with the types of security defenses needed for each segment and the relevant CSC families for each.

The following sections explore some of these challenges for the given stages of an attack, illustrating how CSC families can help.

---

*Figure 5. Attack Segments and Security Defenses Based on CSC Objectives*09

---


---
Getting In but Not Staying In: Complementing Sandboxes and Malware Detection

Network-behavior analytics complements signature-based perimeter security defenses (firewalls and IDS/IPS), sandboxes and SIEM systems to achieve the objective of CSC 5: Malware Defenses, which states, “Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action,” as well as its sub-controls 5–8 and 5–9.

CSC 5–8: Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection.
CSC 5–9: Use network-based anti-malware tools to identify executables in all network traffic, and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

Sandboxes serve a valid purpose, but as Table 1 outlines, attackers use many techniques to create malware equipped to evade sandbox detection. Network-behavior analytics can come to the rescue, identifying traffic that indicates active malware in the network, such as communications with command-and-control (C&C) communication servers that may have been initially missed by the sandbox.

File-based sandboxes, designed to detect and stop an attack before it can expand inside an enterprise, have become a critical component of modern perimeter security. They analyze potentially malicious behaviors, including changes to registry keys, creation of new processes, installation of new services, modification or deletion of host files and initiation of C&C communications. The sandbox provides signatures that identify malicious files and blacklists that contain C&C servers contacted by the malware. Perimeter security defenses, in turn, use these signatures and blacklists to block known malicious files and C&C connections.

A sandbox cannot detect exploits it cannot see. Table 1 enumerates some common evasion techniques. Malware can still slip through perimeter defenses, even after having been caught by sandboxes that execute code but don’t recognize it as malicious.

---

### Table 1. Sandbox Evasion Techniques¹¹

<table>
<thead>
<tr>
<th>Evasion Category</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human Interaction</strong></td>
<td>Malware determines if an actual human is interacting with the target before executing its malicious code. Techniques include looking for mouse activity or injecting malicious code deep in a document so that merely opening the document will not launch the malicious code and the malware passes automated detection.</td>
</tr>
<tr>
<td><strong>Virtualization Specific</strong></td>
<td>Sandbox is built on known virtualization/emulation environments (e.g., VMware). Malware detects specific characteristics of the environments, such as specific services or unique files, and hides its malicious payload until it is running in the target environment.</td>
</tr>
<tr>
<td><strong>Environment Specific</strong></td>
<td>Malware looks for system artifacts specific to its target. If these artifacts—such as a certain software package or browser, company-specific domain names, login banners or user-specific files—are not found, the malware does not execute its malicious payload.</td>
</tr>
<tr>
<td><strong>Configuration Specific</strong></td>
<td>Malware uses known default configurations of the analysis sandboxes such as the following to avoid detection:</td>
</tr>
<tr>
<td></td>
<td>• Default file size for analysis. Malicious files larger than this default limit avoid detection.</td>
</tr>
<tr>
<td></td>
<td>• Delaying execution of malicious code until after reboot. This tactic takes advantage of the fact that file-based sandboxes do not normally reboot during analysis.</td>
</tr>
<tr>
<td></td>
<td>• Sleep calls. Sandboxes are typically configured to analyze a sample for a defined period of time. By configuring the malware to wait for execution long enough to time-out the sandbox, the malware can avoid detection.</td>
</tr>
</tbody>
</table>

Even malware caught in sandboxes may continue to operate by communicating with C&C servers in ways that a sandbox would not normally identify and interdict. What happens if the sandbox analysis has captured only a portion of the malware behavior—such as the initial communications to a C&C server, or just one method of communication to a C&C server—but misses the same application’s switch to HTTPS, Tor, P2P or other alternative ways to phone home? Network-based behavioral analysis looks for all phases of an extended attack, over both short and long time frames in the actual network environment. Complementing the initial detection of anomalous behavior by a sandbox with network-based tools that use data science and ML gives security staff more in-depth visibility and, hence, intelligence to more quickly respond to and stifle cyber threats.

Staying In: Compromise of the Privileged User

The Duqu 2.0 attack against Kaspersky Labs, reported in June 2015, demonstrated the level of complexity possible using advanced attack methods. Duqu 2.0 made heavy use of zero-day vulnerabilities to compromise the first systems it infected.\footnote{Kaspersky Finds New Nation-State Attack—In Its Own Network, “Kim Zetter, Wired, June 10, 2015, www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/} Attacking apparently targeted a vulnerability (CVE-2014-6324) in the Kerberos protocol that allows remote elevation of privilege in domains running Windows domain controllers. Attackers with the credentials of any domain user can then elevate their privileges to that of any other account on the domain, including domain administrator accounts.\footnote{Microsoft patched this vulnerability in November 2014 with update MS14-068. More information about this vulnerability can be found at http://blogs.technet.com/b/srd/archive/2014/11/18/additional-information-about-cve-2014-6324.aspx} The attackers used these elevated privileges to move laterally and deliver MSI packages, infecting additional hosts.\footnote{For a detailed analysis of the Duqu 2.0 attack, refer to the technical report by Kaspersky Lab at https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf}

Analysis of anomalous behavior that encompasses activities tied to user identity, privileged accounts, network traffic and endpoint events, both internal and external to the network perimeter, provides the fabric for discovering the presence of an attacker. Both supervised and unsupervised ML are critically important for addressing the various elements of the “staying in” phase:

- Attackers use both automated and manual control channels for managing their attacks. They have become adept at maintaining their presence, hiding from signature-based detection by leveraging commonly used applications such as Gmail for C&C and common RDP tools for Remote Access Tunnel (RAT). Supervised ML models can quickly identify the unique patterns of C&C or external remote access with no on-site learning.

- Attackers are almost always after privileged access. An attacker with Active Directory domain admin access can create a golden ticket—a Kerberos-generating ticket that is good for 10 years (the default lifetime on a golden ticket) or, in reality, however long the attacker chooses—that allows an attacker to do anything within Kerberos’ authentication capabilities, including creating usable Kerberos tickets for user, computer or service accounts that do not even exist in Active Directory.\footnote{“Fear the golden ticket attack!” Roger A. Grimes, InfoWorld, August 19, 2014, www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html} If a security admin is responding to a potential domain compromise and sees unusual network activity/Kerberos traffic, perhaps even from nonexistent users, then a golden ticket attack could possibly be underway.\footnote{“Kerberos in the Crosshairs: Golden Tickets, Silver Tickets, MITM, and More,” Mike Pilkington, SANS Digital Forensics & Incident Response, November 24, 2014, http://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more} User behavior analysis based on unsupervised ML can find these often very subtle malicious activities masquerading as approved users, but that requires some time for learning.

Relevant CSCs include:

- **CSC 12: Controlled Use of Administrative Privileges**
  - CSC 12-1: Implement focused auditing on the use of administrative privileges and monitor for anomalous behavior.
- **CSC 14: Maintenance, Monitoring and Analysis of Audit Logs**
  - CSC 14-9: Creation of a service is an unusual event and should be monitored closely.
- **CSC 16: Account Monitoring and Control**
  - CSC 16-13: Profile each user’s typical account usage.
Identity and access management (IAM) systems supply attributes such as role, entitlements and organizational structure that can support user behavior analytics. This data is often correlated with other sources collected from logs or a SIEM, but the resulting granularity or timeliness of the information may not be adequate. Detection tools based on unsupervised ML can complement the IAM system by automatically learning what is normal in the environment and alert on what is anomalous—down to the level of a specific identity. The behavior of that identity can be mapped across physical locations, endpoints, and mobile and wearable devices, allowing quick containment. This approach supports dynamic risk-based authentication that calculates an aggregated risk score to determine how an authentication request should be handled—low-risk logon attempts proceed normally, suspicious attempts are denied, and legitimate users traveling abroad must use two-factor authentication.

Figure 6 shows the elements required for intelligent user activity monitoring.

Information Sources for User Activity Analysis

- IP reputation data (blacklist)
- Device fingerprint
- Geographical information (geo-location, geo-fencing, geo-velocity)
- Expected behavior(s) associated with the identity profile(s) (login, keystroke and touch dynamics, apps used)
- Group membership and credentials

17 IdM = identity management, AD = Active Directory
**Avoiding the Morbid Post-mortem**

Attackers exploit a window of opportunity inherent between the design of good defenses and their implementation, between the announcement of a vulnerability and the availability of a vendor patch, and between the time of infection and the time of detection. Many time-honored methods, including analysis of alerts with SIEM and log management systems, can effectively diagnose attacks after the fact. These methods are time-intensive and designed to confirm a suspected breach as opposed to proactively detecting it. This post-mortem approach is increasingly insufficient, and not all organizations have access to the skilled professionals who perform the analysis. This is evident from the giant scope and months of free access attackers achieved in the months-long, multimillion-dollar “Carbanak” bank attacks discovered in February 2015, the J.P. Morgan attack discovered in August 2014, and the theft of more than 11 million records from Premera Blue Cross in March of 2015. In each case, attackers were able to penetrate and remain present in the victim’s network for months without detection.

Techniques such as penetration testing and red teaming provide significant value only when basic defensive measures are in place and performed as part of an ongoing program. Automated threat detection using network behavioral analytics can help reshape traditional approaches.

CSC 20-1, a sub-control in CSC 20: Penetration and Red Team Exercises, states penetration testing should be conducted from both outside the network perimeter as well as from inside its boundaries to simulate both outside and insider attacks. Without a well-defined perimeter, today's attacks are often successful because the myriad indicators of compromise (IOCs) are disjoint.

Regin, for example, is a multipurpose, sophisticated strain of malware designed to quietly infect, spread and persist within a target network for long periods of time. Signs of infection can be missed by time-honored, signature-based detection methods. The malware uses a RAT to administer an attack downloading customized payloads for which there are no existing signatures to extend the functionality of the malware. It employs various methods to hide its communications, embedding commands within HTTP cookies and proxying traffic through multiple infected hosts to exfiltrate data. It spreads through a network by compromising system administrators, using their credentials to move laterally across Windows administrative shares.

Network behavioral analysis can consume these various IOCs, correlate them to the hosts under attack and then help visualize what the attacker is doing even if the specific tools being used by the malware have not been seen before. Defensive tools based on data science and ML can detect telltale patterns and behavior of RAT tools, identifying and helping kill the RAT in the network even if the specific tool has not previously been seen. Using a trained defensive system to replay old attacks or possibly simulate new ones is another approach to help security teams learn how to take real-time action confidently in a dynamic threat environment.
Looking holistically across all activities and events of an organization, independent of the network perimeter, automated threat management can build the baselines that define normal business behavior and provide true visibility into operational risk by:

- Expanding the defensible perimeter for an enterprise in light of the modern threat model, and increasing user demand and usage of mobile and cloud services
- Identifying and stopping malicious behavior before damage or loss happens
- Protecting against insider threats by detecting and managing anomalous user behavior through risk-based authentication procedures that target and contain a bad actor without impacting normal users

Data science and ML applications in the security industry are still emerging, but they bring true promise for holistic, intelligence-driven security, regardless of context. Current advances in the tools supported by these technologies point the way to a hopeful future in which security goes from a reactive, forensic operation to an adaptive—and predictive—discipline, greatly reducing the risks of advanced threats.
Barbara Filkins, a senior SANS analyst who holds CISSP and SANS GSEC (Gold), GCH (Gold), GLSC (Gold), and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. She focuses on issues related to automation, including privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today’s mobile and cloud environments.
## 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 Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2018</td>
<td>New York, NYUS</td>
<td>Feb 26, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>CyberThreat Summit 2018</td>
<td>London, GB</td>
<td>Feb 27, 2018 - Feb 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>OnlineSA</td>
<td>Dec 02, 2017 - Dec 07, 2017</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>