Combatting Cyber Risks in the Supply Chain

By some estimates, up to 80% of breaches may originate in the supply chain. Read this paper to get some guidance on best practices to protect your organization from vulnerabilities introduced by your vendors and suppliers.
Combatting Cyber Risks in the Supply Chain

A SANS Whitepaper
Written by Dave Shackleford
September 2015

Sponsored by
Raytheon|Websense
The latest and greatest advances in technology have created greater efficiency and effectiveness for organizations and their supply chains. However, with the pace of data breaches and intrusions into computer systems accelerating at an alarming rate, this increased level of access and integration within host organization environments can present risks and potential new avenues of compromise. We are seeing unprecedented advancements in the sophistication of perpetrators, making supply chain vendors equally vulnerable to advanced attacks.

To manage these risks, host organizations must adapt their security procedures to include vendors, partners and even customers. In addition, they must closely evaluate their own people, processes and technology. This paper will look at the potential weaknesses in the supply chain, attack vectors those vulnerabilities could introduce and ways to secure the supply chain.
Introduction to Supply Chain Security

So what exactly is supply chain security? In short, supply chain security is a program that focuses on the potential risks associated with an organization’s suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organization’s customer environments, some of which may be sensitive in nature. Sophisticated attackers are willing to use any means necessary to gain access to sensitive data, and third-party suppliers and vendors may have fewer security controls in place than host organizations, making them easier targets of an initial attack. Once breached, attackers can leverage these vendors’ access as an ingress point into their ultimate target.

There are many ways a supply chain breach could occur. For example, a software manufacturer could be breached via malware that modifies source code that is then distributed to enterprises that use the software. Another common compromise vector might be the theft of a vendor’s credentials that grant remote access to an enterprise the vendor works with, leading to infiltration of the enterprise network from an already trusted source (the vendor network). Figure 1 illustrates a typical supply chain breach.
In the past several years, there have been a number of high-profile breaches with supply chain involvement. In late 2013, retailer Target experienced a significant breach involving the theft of roughly 110 million customers’ data and at least 40 million payment cards. During the course of the investigation, it was found that Target was initially breached through a connection established by one of its vendors, HVAC vendor Fazio Mechanical Services. The attackers stole network credentials from Fazio and then used them to successfully access the Target network and ultimately steal staggering quantities of data over several months.¹

Home Depot, another large retailer, also claims that a credit card breach it experienced in 2014 was initially due to stolen credentials from a third-party vendor.² In many of the most public cases we have seen, the attackers have targeted personal, health care and financial information, including debit and credit card details.

In many sophisticated attacks, however, the data breached includes intellectual property and sensitive government information. In 2015, the U.S. Office of Personnel Management (OPM) revealed a massive breach of 22 million records, including sensitive data tied to numerous federal employees, contractors and military personnel.³ This breach, like many others, seems to have originated with stolen credentials from a background-check provider that worked with OPM, KeyPoint Government Solutions.⁴ Another significant supply chain breach involved security vendor RSA, whose breached multifactor token data led to later compromise attempts and successful attacks on customer networks.⁵

When sensitive data is breached and exposed, the impact to organizations and consumers is far-reaching. Business may experience financial penalties, legal costs, loss of consumer confidence, drops in stock price and overall hits to their reputation. Consumers find themselves as targets for phishing attacks and identity theft, as well as potentially experiencing financial issues and inconveniences from having to replace payment cards and bank accounts. The average cost to an organization of a data breach, as reported in 2015, was $6.5 million U.S.⁶

¹ http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
Despite the growing threat and evidence surrounding the supply chain attack vector, there are few specific compliance mandates addressing third parties, although third-party risk is usually implicated in a number of other areas—for example, vendor due diligence, risk management and contract requirements. However, some compliance and regulatory bodies have issued guidance explicitly dealing with vendor management and third-party risk management. The Federal Deposit Insurance Corporation (FDIC) has published guidance for all covered entities that specifies how to assess and manage third-party risk.7 This guidance describes how to evaluate contracts with vendors and other organizations, as well as which types of controls and best practices to look for when evaluating the use of third-party services (due diligence).

The Payment Card Industry Data Security Standard (PCI DSS) Version 3.1 is another compliance framework that directly addresses the issue of third parties and the supply chain.8 In the January 2015 version of the standard, there are two updated vendor management guidelines (in addition to 12.8.3 and 12.8.4, which require exercising due diligence in assessing service providers and monitoring annually for PCI compliance at selected service providers):

- Requirement 12.8.5 requires merchants to identify which PCI requirement is handled by the merchant and which is enforced by the service provider for each vendor.
- Requirement 12.9 now requires service providers to provide PCI compliance agreements to merchants, similar to Requirement 12.8.5.

As vendor management and supply chain security are increasingly linked to data breaches and security incidents, it is likely that more explicit requirements will become commonplace in most major compliance mandates. Organizations should stay aware of all mandates and standards and make necessary revisions in policy or procedure to accommodate those changes.

---

8  www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
Organizations should evaluate their vendor management programs as the first step in addressing supply chain security. Vendor management involves a number of different roles and responsibilities within an organization that must be defined and managed. An effective and secure vendor management program should define a risk-based approach—complete with periodic reviews, assigned owners and the acceptable balance of risk and reward for high-value relationships—to assess existing vendors and any potential new vendors. In addition, vendor management policies should encompass the types of controls documentation and contract assertions (SSAE 16, ISO standards, financial documentation, SLAs, etc.) used for evaluating vendors and their controls. Figure 2 illustrates the steps in building a program to manage vendors.
Define Important Vendors

To get started, first define the most critical vendors you work with. For example, mission-critical vendors may be those where performance failure or a breach may have a significant impact on operations, strongly affect revenue generation, or adversely impact clients or the organization as a whole (through direct contact or loss of sensitive data), or where it may be difficult to find an appropriate and timely replacement. Examples of such vendors might include important partners, financial or legal services, hard-to-replace software vendors and more. Different tiers of vendor criticality will likely call for separate approaches to policy enforcement as well.

Specify Primary Contacts

Next, organizations should define the primary contact for each vendor. This person, often called the vendor owner, serves as a liaison between an organization’s security, risk and compliance teams and the vendor. This is rarely a dedicated role, as the person usually fulfills other duties within the organization alongside this one. The vendor owner should be responsible for the following duties:

- Coordinate due diligence on vendors and report to senior leadership using a risk-based approach, relying on judgment and expertise as well as standard processes and categorization.
- Maintain knowledge of, and compliance with, policies and reporting requirements.
- File documentation and paperwork with the legal and contracting teams to ensure there is a central repository and audit trail.
- Coordinate broad communication with those who can add value in vendor oversight. This may include conducting on-site and/or remote audits, reviewing vendor policies and procedures, providing training to all responsible parties related to vendor management within the organization, monitoring vendor-related litigation or regulatory issues, and monitoring contract terms and service level agreements.

Once the role of a vendor owner has been defined, the organization should strive to ensure a comprehensive vendor management policy is in place. This vendor management policy should establish guidelines and controls to ensure that the organization has consistent processes and sufficient oversight to manage the monitoring of key vendors and outsourced service providers.
Establish Guidelines and Controls

The policy, which should be reviewed biennially (at a minimum), should classify vendors and identify appropriate controls for service providers based on access granted to sensitive organization data. It should reference controls frameworks and requirements in separate documents and be amended whenever necessary to document regulatory changes. It is important to include a service level agreement to remediate any major issues discovered. Other issues the policy should cover include the following:

- Requiring the right to audit and test the security controls of vendors and service providers annually, upon significant changes to the relationship and in response to audit requests or events.
- Requiring vendors to adhere to security monitoring requirements.
- Requiring periodic reports from the vendors and service providers demonstrating service level attainment and performance management.
- Requiring vendors and service providers to provide timely notification pursuant to any security breaches or incidents that may cause impact to the organization. This is usually specified in a contract and may conform to data breach notification laws that affect either or both parties. A good example of guidance for businesses related to data breach notification is that offered by the Massachusetts attorney general.9

Integrate with the Organization’s Practices

With the pieces in place, a vendor management program can now start to integrate with the organization’s assessment and audit practices, which should outline both internal best practices and those required of vendors with which the organization associates. With the increased use of cloud computing services, many organizations have had to revamp their external audit and due diligence processes—so much so that the Cloud Security Alliance (CSA) has published an extensive list of best practices and questions to ask cloud service providers, many of which can easily be extrapolated to general supply chain due diligence processes. The questionnaire, dubbed the Consensus Assessments Initiative Questionnaire (CSA CAIQ) is available at the CSA site.10 More detail on this type of checklist and due diligence process is provided in the “Process” section of this paper.

---

10 https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1
The next several sections outline some of the best practices and changes organizations need to make internally to ensure that they are not exposing themselves to risks from vendors and partners that comprise their supply chains. Best practices typically involve the triad of security operations: people, process and technology, as illustrated in Figure 3.

Figure 3. The Triad of Security Operations

11 Based on “Building a World-Class Security Operations Center: A Roadmap,”
www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907,
p. 3, Figure 1
People

The first area of focus for organizations assessing their internal security programs should be people. In most organizations, human resources teams routinely perform background checks when employees join the organization. This can help to ensure that employees and contractors are legitimate, law-abiding citizens with no prior history of criminal activities or actions that may indicate potential risks to the organization.

Most HR teams, however, only perform background checks when employees first join the organization, often by outsourcing the job to third parties such as HireRight, Intelius, US Search and LexisNexis. Background checks should be performed on a regular basis for both new and existing employees and contractors. An ideal time frame for checks would be every six to 12 months, and possibly more often for sensitive positions, although few organizations meet that standard. Organizations should require that vendors and partners take this same approach, and there should be some sort of audit check performed regularly to ensure that any supply chain staff who work with the organization’s data or systems comply with required background check criteria.

Monitor all staff that work with your organization’s data and systems for changes to job status and requirements. For example, if a partner’s database administrator changes positions, he or she may no longer require access to the organization’s internal database systems. Through ongoing communication between the vendor owner and the partner, you should know about such a change prior to its occurrence and be able to plan for it accordingly. Job changes at supply chain vendors may go undetected for longer periods of time than they would for internal team members, which can lead to significant risk if an account is compromised. Access to critical systems should be monitored, and all third-party access should be revoked after a defined period of inactivity (which could indicate a job or personnel change).

Finally, HR and security teams should verify that security requirements are clearly spelled out in contracts for external staff and that acceptable use provisions are in place for internal employees through their employment agreements. All personnel that interact with sensitive systems and data, whether employees or contractors, should understand their responsibilities and obligations related to security controls and awareness of potential attack vectors.

TAKEAWAY:
Performing background checks, verifying supply chain partner background checks, and monitoring for job or role changes within organizations are critical steps to improving supply chain security.
Best Practices (CONTINUED)

Process

In line with the vendor management discussion earlier, organizations should first look at process changes related to evaluating vendor security. The most fundamental supply chain security processes focus on risk assessment and pre-engagement controls analysis, typically completed by using checklists. Most organizations will need to develop or revise security controls checklists, such as the aforementioned CSA CAIQ, for evaluating vendor and partner security programs. The checklists should include such topics as breach notification, legal jurisdiction, sensitive data handling, data confidentiality, data life cycle and product integrity.

An effective security controls checklist should include a requirement to implement tools to monitor and block malicious actions and behaviors **within** the environment, including proxies, data loss prevention (DLP) and even cloud-focused tools such as cloud access security brokers.

Teams will also want to ensure that supply chain participants have a defined incident response process that can be shared and articulated as needed. Other areas often included in vendor/supply chain security assessment questionnaires are illustrated in Figure 4.

Along with putting together more stringent and detailed lists of security questions, organizations need to develop a process for in-depth security reviews that align with these areas. The best way to get started with this is by leveraging the same review processes employed internally by audit teams examining your organization’s own security controls and applying them to supply chain organizations. When assessing a third-party organization’s controls, on-site audits are ideal, but most audit areas will likely be covered remotely with a series of questionnaires and interviews with personnel. This type of review needs to be performed on a regular basis, usually every six to 12 months.
Organizations that are adapting their security review processes to better encompass the supply chain should follow these guidelines:

- **Decide on a list of controls with which supply chain organizations need to demonstrate compliance.** This list may vary for each organization, depending on the type of business performed, data and asset sensitivity involved, and other factors. Classifying organizations into categories based on these factors, and then defining specific lists of security requirements per category, is a manageable way to handle reviews.

- **Determine the frequency of security reviews for internal and regulatory compliance needs.** Reviews should be completed at least annually, but twice per year (or even more frequently in some types of organizations) is preferred.

- **Define a remediation and arbitration process for handling supply chain organizations that are not currently meeting security requirements.** This process should include specific timelines for remediation, as well as termination of the relationship if security requirements cannot be met.

For software vendors in the supply chain, organizations need to take a more proactive stance regarding the security and robustness of the code running in their environments. There are quite a few code/binary analysis tools available on-premises or in a hosted environment that organizations should use to analyze software products before they are installed internally, as well as prior to any updates or installation of new version releases. Code reviews should ideally be the responsibility of the vendors, and they should attest to software security via a report issued prior to installation or updates (or on a regularly scheduled basis). Contracts with these vendors should include a requirement to perform the code reviews/analysis.

There are other significant security implications within the supply chain related to process issues. Many vendor products cannot be patched or updated without direct input or code from the vendors themselves, leaving organizations potentially vulnerable to numerous risks when vulnerabilities that affect these products are disclosed. In 2014 alone, the Heartbleed and Shellshock flaws\(^\text{12}\) affected an enormous number of systems running particular versions of Linux Bash shells and OpenSSL libraries. Some of these flaws were present in vendor products long after initial disclosure.

Organizations should require supply chain vendors to notify them of data or security breaches in a defined amount of time after breach identification. This may be contingent on the affected parties’ data being included in the breach investigation, or it can be a blanket requirement to notify solely based on potential concern for risks related to continued hacking or collateral damage.

Best Practices (CONTINUED)

Technology

In addition to the people and process changes needed, organizations will want to look at a number of technology changes to adequately mitigate risks. The first, and perhaps simplest, change is to begin using technology services that offer supplier risk ratings or rankings compared to other industry organizations. Monitoring the overall risk ratings of supply chain participants from other organizations working with them provides information on industry perceptions of security posture. Multiple and consistent expressions of concern about the security posture of a supply chain partner warrant closer examination.

For years, the information security community has debated whether the threat of internal attack or external attack is of the greatest concern for organizations. Security practitioners have generally concluded that the volume of external attacks is far greater than internally based attacks, simply due to the number of probes and attacks pounding their networks every day.

On the other hand, despite their smaller volume, inside attacks generally cause significantly more damage because the attackers already have access. Nowhere is this more applicable than with privileged users. A privileged user, by definition, is a “user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users.”\(^{13}\) Monitoring the actions of these users is paramount for security and compliance reporting. However, monitoring at this level has been a challenge for many organizations.

Privilege Management

Technology solutions for mitigating supply chain risk should include privilege management. Privileged user monitoring is a large part of Carnegie Mellon University’s Computer Emergency Response Team’s (CERT)\(^{14}\) recommendations for prevention of insider threats and for compliance reporting of administrator actions.

---

\(^{13}\) [www.yourwindow.to/information-security/gl_privilegeduser.htm](http://www.yourwindow.to/information-security/gl_privilegeduser.htm)

\(^{14}\) [www.cert.org](http://www.cert.org)
Some of the mechanisms to prevent privileged insider abuse highlighted by CERT include the following:15

- **Enforce separation of duties and least privilege.** *Separation of duties* implies that no one employee can perform all privileged actions for a system or application. *Least privilege* implies that employees are granted only the bare minimum privileges needed to perform their jobs. By using these controls, an organization limits the damage a privileged user could inflict.

- **Implement strict password and account management policies and practices.** This should be enforced for all users, including administrators and other privileged users. This practice makes it harder for attackers to guess or crack credentials.

- **Log, monitor and audit employee online actions.** Organizations need to be vigilant about what actions privileged users are taking, and should use a variety of logging and monitoring techniques to detect malicious or suspicious actions quickly and initiate response actions if needed.

- **Use extra caution with system administrators and privileged users.** Because these users are often granted the “keys to the kingdom” in terms of access and capabilities, additional safeguards often need to be implemented to adequately monitor and manage their behavior.

Most important, all organizations need a policy and approach to managing and monitoring privileged users. By examining the levels of access needed to perform most daily activities and crafting policy that supports these job functions while still maintaining separation of duties and the principle of least privilege, organizations are off to a good start. Processes for granting access should be in place and in line with the privileged user policies. Periodic audits should also be a part of the program.

---

The next step is to implement traditional security controls, such as firewalls and network access controls (limiting access to systems), intrusion detection systems, identity and access management solutions, and so on. All systems should have logging enabled, and system logging for all user activity should be in place, especially for privileged actions and logon/logoff events. Managing privileged users is usually accomplished by the following:

- **Creating and enforcing policies that forbid the use of single, “all powerful” accounts.** This is the first step to managing the actions privileged users can take. In order to define more granular roles and privileges for privileged users, each user must have a unique user account or user ID that can be tied to him or her.

- **Leveraging privilege control tools.** Tools such as sudo can have policies defined for various users and groups that control what actions can be taken and what permissions are available to specific resources. For example, user accounts associated with managing particular applications or services can be granted explicit privileges to only those resources—and no others. In addition to controlling privileges, more detailed audit trails can be associated with more specific actions taken on systems. There are many commercial privileged user management tools that organizations can use to help them manage such.

### Network Isolation and Segmentation

Network isolation and segmentation changes can help with improving supply chain security as well. Using both Layer 2 (VLAN) and Layer 3 (IP addresses and subnets) segmentation to isolate traffic into “zones” can be effective for keeping traffic related to supply chain organizations separate from other internal traffic and result in better malware detection and control (in the case that a breach does occur within or transiting the supply chain network). Most sophisticated malware and attacks rely on lateral movement in networks. Careful zoning and network isolation with strategic access controls can help prevent this. More rapid detection of lateral movement attempts can also be accomplished by carefully monitoring logs and events from switches, looking for events such as duplicate MAC addresses seen on a switch or unusual access attempts from switch ports.

In addition, requiring supply chain clients connecting into the network to use virtual desktops or “thin clients” can help keep assets centrally located, while simultaneously preventing data exposure or exfiltration at the endpoint. This can also play a role internally, requiring less traditional network segmentation and access control to implement because the core systems and assets are always in the central data center.

16 [www.sudo.ws/sudo/](http://www.sudo.ws/sudo/)
Analytics and Threat Intelligence

Many organizations use or plan to use security analytics tools and threat intelligence to help identify and combat advanced attacks. Highly customized analytics platforms, while expensive and complex, can provide enormous value in the form of more predictive trends, granular patterns of internal and external-facing network and application behavior, and even user and group profiling for target analysis. In fact, monitoring specific users that are known to be high-value targets is a viable technique that could help to detect targeted attacks quickly, although privacy concerns are important to take into account.

Many organizations are also incorporating threat intelligence data feeds and services into their supply chain security strategies. Threat intelligence can help to correlate information gleaned from internal sources with indicators of compromise spotted by other organizations.

Another source of threat intelligence commonly leveraged today is the “community of trust,” which includes various information sharing and analysis centers (ISACs) and, in particular, Financial Services and Critical Infrastructure ISACs. Other groups that share information include Georgia Tech’s Apiary (formally known as Titan) and the SANS Internet Storm Center (ISC).

Exfiltration Monitoring

Monitoring egress points from the internal network is another way to improve security within the supply chain. Sometimes referred to as egress monitoring or exfiltration monitoring, intercepting user traffic bound for the Internet before it hits the perimeter allows security teams to see what data is being sent to the Internet over internal network channels. This is likely where security personnel will detect infected end-user systems transmitting bot command and control information. Some of the most common protocols and standards used for data exfiltration or command and control include HTTP/HTTPS, FTP/FTPS/SFTP, SSH, IRC, email, P2P, and DNS or ICMP for covert channels.

The most common locations to perform exfiltration monitoring include border gateways, at-edge IDS/IPS platforms, in the DMZ/DMZ firewall zones and within internal IDS/IPS that are in-line. DLP platforms can also do network exfiltration monitoring for data types, keywords and other more advanced pattern matches. This is becoming a common strategy in conjunction with some of the others mentioned.

17 http://apiary.gtri.gatech.edu
18 https://isc.sans.edu
As more organizations look to improve their supply chain monitoring and security controls strategy, they quickly realize that supply chain security (much like most security initiatives) is comprised of people, processes and technology adaptations. Organizations may need to make quite a few changes to ensure the security of their supply chain, but the following can begin immediately:

- Define a vendor management policy that includes vendor classifications, vendor owners within the organization and security controls for each tier of vendor listed.
- Ensure a sound vendor management program is in place within the organization and that the proper organizational roles have been defined to manage the various aspects of coordinating supply chain contracts, risk assessments and other major tasks involved in a supply chain management program.
- Ensure a list of security questions and risk assessment controls are defined that can be used to properly evaluate supply chain partners.

In the longer term, organizations should look to implement more stringent people and technology controls that include employee and partner background checks, privileged user monitoring and management, analytics and threat intelligence, and exfiltration monitoring. When connecting supply chain partners to the network, ensuring they are properly segmented from the main production environment via VLANs and Layer 3–7 firewall rules is integral to your supply chain security strategy. However, this may take some time to plan and implement.

Table 1 summarizes basic and more comprehensive supply chain security elements.

<table>
<thead>
<tr>
<th>Table 1. Elements of Supply Chain Security Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic</strong></td>
</tr>
<tr>
<td><strong>People</strong></td>
</tr>
<tr>
<td>Background checks</td>
</tr>
<tr>
<td><strong>Process</strong></td>
</tr>
<tr>
<td>Contract review</td>
</tr>
<tr>
<td>Vendor security control and risk review</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
</tr>
<tr>
<td>Network segmentation</td>
</tr>
<tr>
<td>Privilege management and monitoring</td>
</tr>
<tr>
<td><strong>More Comprehensive</strong></td>
</tr>
<tr>
<td>Security requirements spelled out in contracts</td>
</tr>
<tr>
<td>Implementation of a complete vendor management program</td>
</tr>
<tr>
<td>Third-party code review and vulnerability management</td>
</tr>
<tr>
<td>Exfiltration monitoring</td>
</tr>
<tr>
<td>Security analytics and threat intelligence</td>
</tr>
</tbody>
</table>

Supply chain partners are just as likely to be attacked today as any organization, and if not managed properly, they may afford attackers a back door into the networks of host organizations. At the very least, those responsible for supply chain security need to be more vigilant and aware of what is happening at supply chain organizations and keep up with the state of their security controls in much the same manner as they monitor controls internally.
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 its sponsor:

Raytheon  websense
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Date Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<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 London April 2018</td>
<td>London, GB</td>
<td>Apr 16, 2018 - Apr 21, 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 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 Riyadh April 2018</td>
<td>Riyadh, SA</td>
<td>Apr 28, 2018 - May 03, 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 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 Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Crystal City 2018</td>
<td>Arlington, VAUS</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit and Training 2018</td>
<td>Munich, DE</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo June 2018</td>
<td>Oslo, NO</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2018</td>
<td>Manila, PH</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vancouver 2018</td>
<td>Vancouver, BCCA</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2018</td>
<td>Minneapolis, MNUS</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2018</td>
<td>Canberra, AU</td>
<td>Jun 25, 2018 - Jul 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2018</td>
<td>OnlineFLUS</td>
<td>Apr 03, 2018 - Apr 10, 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>