The SANS 2013 Help Desk Security and Privacy Survey

May 2013

A SANS Whitepaper

Written by Barbara Filkins

Help Desk: A Snapshot  PAGE 2

Help Desks Are Meant to Help: That’s the Problem  PAGE 5

Protection: Technology, Training and Tools  PAGE 10

Countermeasures  PAGE 15
Introduction

The enterprise help desk is most often where a user turns to resolve a problem with all matters IT—access, endpoints and service. It is often a hub of activity with the primary goal of solving user issues as quickly and effectively as practical.

As help desks are ordered to help, they are ripe for others who wish to take advantage of their mission. For decades, the help desk has been a back door to enterprise network resources through social engineering—the art of trickery to get others to give up information they shouldn’t. Imposters are increasingly using social engineering techniques to obtain credentials and unauthorized access to other confidential data, according to the 2013 Verizon Data Breach Investigations Report. The survey also reports that social engineering is the most successful tactic used against service desks.

Are organizations aware of the risk their help desks represent for their enterprises? If so, what measures are they taking to protect their enterprises? To find out, the SANS Analyst Program conducted an online survey of more than 900 people between January and March 2013. Respondents reported handling several call types in their work, foremost among them escalating and checking on status of incidents, followed by password-reset requests. Any of these activities can provide a back door into an organization, with the right amount of social engineering.

The good news is, there is awareness and training around social-engineering-based attacks. In this SANS survey on help desk security, more than 70% of respondents reported that they are aware of social engineering, and some are even training their help desk staff to be suspicious. The bad news is that organizations are not factoring security into the overall help desk budget; security technologies are underutilized, and nearly 40% have weak or no security policy around their help desks.

This survey and resulting report are designed to serve as a starting point to promote awareness and help bridge the educational gap between what a help desk is and what a secure help desk should be.

---

1 www.verizonenterprise.com/DBIR/2013/?gclid=CP66mNTehbcCFelxQgodqHYAoA, p. 6
Help Desk: A Snapshot

Today, the corporate user considers the help desk as the resource to contact when having problems with technical or communication issues, whether related to applications, devices or service(s). Help desks generally follow a tiered support structure, with problems escalated as needed to higher tiers staffed with increasingly knowledgeable (and often, empowered) personnel. This structure can vary widely across organizations, ranging from one person in a small shop who is “good with computers” to teams of dozens or more who perform all levels of support for a global enterprise.

Nearly all organizations have a help desk regardless of industry type and size. In the survey, respondents cut across various industries, including government (18%), finance (15%) and education (13%); health care, high tech and telecommunications were also well represented. Survey takers also represented a balance in terms of size of organization, with the largest individual survey group having more than 25,000 users to support, as shown in Figure 1.

![Figure 1. Help Desk Support by Organizational Size](image)

The majority (38%) were local organizations or were limited to a specific geographic area within a country, followed by 23% that provided global support (24/7 or offering “follow the sun” support). The next largest group had national (including overseas territories) and international responsibilities (e.g., U.S. and Europe) at 20% and 19% of respondents, respectively.
Help desks handle the common, low-level requests that plague enterprises, such as resetting passwords, restoring email and troubleshooting connectivity. Survey respondents reported that password resets and troubleshooting basic productivity applications, such as email, account for the majority of requests to the help desk for service, followed in descending order by support for line of business applications, initial password generation, checking on the status of incident report/service requests and escalation of problems to additional support tiers.

Many of these services could offer basic, but critical, information to an attacker if the requester is not properly verified. The majority of respondents identified social engineering as a chief concern for compromise of the help desk, yet organizations still prefer to rely on a human help desk agent over automated tools, as shown in Figure 2, even for services that could easily be automated, such as password resets and status checks.

In today’s mobile environment, automation of these services could help reduce the potential for compromise due to social engineering, better validate the location of a mobile user, and improve first call resolution through online access to user-oriented tools for troubleshooting and correction. One respondent explained that his organization is piloting a self-service solution that uses text messaging to employee cell phones for validation. “More and more of our workforce is mobile. They don’t call from one of our sites with a fixed caller ID; they use a personal cell phone, which makes verification of user identification much harder than in the past.”
Let’s take, for example, password resets. Most of us are comfortable with the self-service password reset processes for our online services. Automation of password resets potentially lowers the opportunity for user impersonation by obsolescing complicated (and risk-prone) phone-based processes that are vulnerable to social engineering:

- The help desk resets the password, but does not share the password with the user.
- The help desk calls the internal desk phone of the user and leaves the password in voicemail.
- The user retrieves the password from voicemail and must change the password at the next login.
- The help desk emails the user’s manager, who is responsible for calling the employee before close of business, to verbally confirm the password reset.
- The help desk emails the user’s manager to confirm the password reset request is legitimate.²

Despite the time, costs and vulnerabilities such processes present, most survey respondents still rely on live help desk agents to complete password resets, even when self-service provisioning services are offered. One respondent stated, “Most of our users still call the help desk to be led through the self-service protocols.” Another called this issue the “chicken and egg” problem of self-service: The functionality is complex enough that users still require assistance with the process. In any event, self-service protocols won’t remove the need for proper authentication of all callers to prevent a clever or well-informed social engineer from impersonating legitimate users.

Taking a proactive approach to help desk security requires attention be paid to the design and implementation of related processes, tools and technology. For example, flaws in an automated password reset scheme may allow an unauthorized individual access to information before normal auditing or monitoring would catch the problem. Such “gaps in the wire” must be identified and eliminated to the greatest degree possible.

Help desks are vulnerable because they are in place specifically to help.

Generally, help desk planning and management enlists key performance indicators (KPIs) to establish and measure acceptable service and performance levels. KPIs are often driven by the size of the user base—employees, contractors, and in some cases, customers; they usually include one or more of the following types of measures:

- Quantity (daily counts of calls answered, incidents resolved or incidents assigned)
- Quality (correctness and accuracy of notes in logs)
- Timeliness (how quickly incidents are responded to and resolved)
- Compliance (execution and logging of authentication procedures for every password, without exception).

Unfortunately, the measurement of help desk performance is too often based on two factors: quantity and timeliness, which effectively sets up the human agent to be the weakest link in the security of the help desk. Agents, especially those working Tier 1 support, are trained to be friendly and get as many calls completed, resolved or transferred as quickly as possible, according to the established KPIs. As a result, an agent may ignore or work around compliance or quality requirements by trying too hard to meet the goals for quantity and timeliness.

Respondents ranked the top privacy and security threats to the security of the help desk to be in four general areas: social engineering, disclosure of protected or sensitive information, user identity verification and access to corporate resources, as shown in more detail in Figure 3.

---


Figure 3. Top Privacy and Security Risks by Survey Respondents
Social Engineering

Respondents perceive social engineering as the greatest threat to help desk security. Such attacks are nothing new; primordial hackers such as Kevin Mitnick were using basic social-engineering techniques long before there was a Web. The fundamentals have not changed much since then, as demonstrated at the 2012 Defcon, where a social engineer hacked Wal-Mart. Consider another example of the simple, yet effective, power of social engineering:

The facilitator of a live Computer Security Institute demonstration neatly illustrated the vulnerability of help desks when he “dialed up a phone company, got transferred around, and reached the help desk. ‘Who’s the supervisor on duty tonight?’ ‘Oh, it’s Betty.’ ‘Let me talk to Betty.’ [He’s transferred.] ‘Hi Betty, having a bad day?’ ‘No, why?’ [He replied:] ‘Your systems are down.’ She said, ‘my systems aren’t down, we’re running fine.’ He said, ‘you better sign off.’ She signed off. He said, ‘now sign on again.’ She signed on again. He said, ‘we didn’t even show a blip, we show no change.’ He said, ‘sign off again.’ She did. ‘Betty, I’m going to have to sign on as you here to figure out what’s happening with your ID. Let me have your user ID and password.’ So this senior supervisor at the Help Desk tells him her user ID and password.” Brilliant.

This account of an attack dates from 2001, but it might as well have happened last week.

Password compromises can also come from within. One respondent’s organization does not see impersonation attacks from the outside; instead, his challenge is the person inside “innocently” trying to bypass normal procedures “in the interest of time” to gain access to information in another user’s account while that person is absent or unavailable.

These examples highlight the need for more automation of processes and continued training of help desk and end user staff.

---

5 www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
Disclosure of Protected or Sensitive Information

This threat can be the wrongful disclosure of personally identifiable information (PII), intellectual property (IP) or other data; disclosure of any of these types of data can have devastating effects on an enterprise, although the “hammer” may differ.

Although this threat is often associated with credit card theft or a WikiLeaks-style compilation of documents and data, the greatest risk may not be the release of sensitive information to an outside entity—it may be the inadvertent capture of sensitive information by the help desk itself.

“We had lots of PII and PHI (protected health information) problems,” reports a manager of a global help desk who was interviewed for this report.

For example, an agent talking to a client on the phone would keep notes on the contact, notes that often included information like an SSN. There was also a persistent problem with e-mail communication between users and the help desk—the user would type sensitive information, either PII or PHI, into the e-mail being sent to the help desk. The major problem is that all this information would be translated into our help desk database and bang! All of the sudden the help desk system would contain PHI and PII.

The manager added that solutions to these problems involve continuous training of help desk agents and users, as well as continuous monitoring. In addition, the manager’s team members are now using technologies that filter PII or HIPAA-protected information from data entered into the help desk management system.

Another respondent echoed the need for continuous training and awareness:

While we are audited quarterly, [inadvertent, but prohibited activity such as jotting down sensitive information about a caller] DOES still occur—less on the help desk side of things and more on the member service departments. I’ve trained our help desk staff on how to manage sensitive information, and we provide tools to make it easier (shredders, shred bins, erasable pads, encrypted removable storage, password management tools and process changes) to avoid those issues. But, if we drop the level of diligence, the poor habits return quickly.

Some have responded to the concern over PHI exposure in this scenario, attempting to avoid that situation by not using any type of personal or sensitive information in a help desk situation. A third respondent stated:

We use other auditable indicators for identification. One is the user’s long distance [access] PIN. Because we cannot [place a long distance call from one of our sites] without this PIN [which is unique to the employee], the LD PIN is a number that can be looked up by help desk staff [and] used for verification, but if this information is misused by anyone but the assigned user, that action is traceable.

This particular approach is problematic in bring your own device (BYOD) environments, where an employee may rely on his or her personal phone to place long distance calls, thereby dodging this control. However, this example illustrates how a help desk may use other indicators for verification of user identity.
Inadequate Verification of User Identity

User identification and verification is another area of great concern to help desk experts, largely because the methods used remain relatively primitive. When it comes to authenticating users, respondents ranked the following methods in the order shown in Figure 4.

![Figure 4. Methods Used to Verify User Identity](image)

Obviously, a dedicated attacker could spoof or bluff past most of these methods, even when they are used together. Respondents ranked the verification of call-in users (44%) as a much greater concern for manual verification processes than for self-service ones (11%), indicating a possible preference for, and gradual growth in, self-service capabilities.

---

Even so, implementers appear to recognize the limitations of self-service capabilities. A survey respondent who attended a recent Information Systems Security Association conference in Houston told of an informal discussion that included participants from medium-size businesses, global enterprises (chiefly energy and aviation) and state agencies. Their expressed concerns, including accurate verification of user identity, still hold back many large organizations, including his, from fully automating help desk processes. Even when self-service is an option and the resulting account creation or password reset is automated, actually granting access requires secondary verification by an authorized and trusted person.

**Risks of Self-Service**

Increased self-service capabilities can go hand in hand with improved verification as necessary safeguards for critical assets, potentially reducing the likelihood of a human help desk agent being socially engineered into lowering his or her defenses.

However, self-service technology (such as for password resets) has its own set of risks that makes some respondents shudder. For example, a respondent reports how social engineers use public information to target their victims and their self-help accounts:

> One of the problems I see is that, as the volume of information individuals make public through social media, [such as] Instagram, Flickr, [and others] continues to grow, the harvesting of target information is becoming dramatically easier, which makes identity verification processes all that much easier to spoof. All self-service technology has that same weak link inherently, that somewhere, some piece of information must be stored that “proves” the user is who they say they are.

Another “chicken and egg” problem is that automation can improve the process, but automation can also be the Achilles heel by opening new doors for determined attackers.

Identity “proofing” policies and procedures are fundamental to both user verification and the prevention of social engineering attacks against automated and non-automated provisioning processes. One can argue that this requires better tools, but it also requires better training and financial resources, and it must reflect a process that incorporates security into the workflow, with technical tools assisting where they are most effective.
The need for robust help desk security is even more important when a help desk could potentially access and expose enterprise resources, even without being tricked into giving away access, PII or security information. This is why integrating security processes and technologies into the help desk infrastructure was specified in the 2007 release of Information Technology International Library (ITIL) Version 3. The enterprise “service desk” of today—with its exposure into the management of an organization’s network, systems, databases and security operations—offers attackers a target-rich environment, and new developments in IT have only complicated the picture.

Good security design for the help desk infrastructure is imperative and should not be overlooked. Pay attention to keeping solutions current, enforcing performance parameters that address security and ensuring robust auditing.

An example of practical training from the author’s recent experience came during a session on privacy and security awareness in which a hacker called the help desk on the corporate telephone system, spoofing his location by routing the call through the PBX. It was a prime example of social engineering assisted by technology, demonstrated live.

Help desk activities and tools should be integrated into the normal support patterns of a company and, if possible, with the technical infrastructure that can be compromised. This includes (but is not limited to) interactive voice recognition (IVR) and phone systems, email and text messaging platforms, and asset-management tools.

**Help Desks in the Cloud**

Technology research giant Gartner predicts that, by 2015, 50% of all new IT service desk purchases will be a SaaS model versus about 10% today. Traditional on-premise help desk platforms are being ditched for numerous reasons, including cost, a need for scalable service and flexibility (to meet rapidly changing operational and customer demands in an increasingly mobile world), and avoidance of technology obsolescence.

Such convenience comes, admittedly, with the inherent risk of a SaaS solution presenting a new attack surface, because help desk databases usually include some personally identifiable information and access credentials that an attacker could exploit. As the SaaS model for help desk technology gains traction, companies need to consider their security requirements and make sure that the traditional controls follow the solution into the cloud.

---

7 [http://blog.gotoassist.com/2013/01/16/top-predictions-for-it-trends-for-2013](http://blog.gotoassist.com/2013/01/16/top-predictions-for-it-trends-for-2013)
Help Desk Security Policies Still Evolving

The good news is: Respondents are aware of the need for help desk security. More than 50% have moderate approaches to help desk security, which essentially involve reviewing risks and incidents as part of their overall corporate security plan, but not necessarily focusing on how help desk staff can be trained to incorporate security controls in their daily routine. Only 10% feel they have robust plans for risk management and security awareness training of their staff. Unfortunately, almost one-third of respondents have weak controls, if any, as depicted in Figure 5.

Figure 5. Ranking of Help Desk Security Approaches
Training Versus Tools

When it comes to protections, 45% of survey respondents favored personal training by managers and supervisors to improve help desk security, and nearly an equal share (44%) favored technical tools for tracking help desk activities and end user activity. Authorization tools were nearly as important, and 30% of respondents are automating training where they can do so with internal resources, as shown in Figure 6.

![Figure 6. Methods Deployed to Improve Help Desk Security](image)

As we’ve said earlier, automation can be the key to reducing errors and vulnerabilities that lead to successful breaches and theft of PII; training and technology appear nearly equally important to respondents.
Justification for Funding and Resources

Survey respondents are also considering technical tools to track and report on activities (44%), to identify end users (41%) and to authorize users (36%). In addition, respondents are considering automated training for help desk staff, either through the provision of internal tools (30%) or from service providers or the cloud (13%).

These tools and services require funding, but typically, the help desk is far from being the most critical line item on the corporate budget. As with any technology expense, help desk security proponents must present a business case to secure funding.

Survey responses indicate several weaknesses that could reduce the likelihood of corporate dollars and resources being committed to improving help desk security.

To begin with, respondents are unaware of what a breach would cost them and do not budget with risk in mind. The majority of respondents replied that they did not take the cost of a security incident (such as the compromise of a user password) into account when they established their help desk budget (43%) or that they were unaware of whether that cost was considered when the budget was developed (33%), as shown in Figure 7.

![Figure 7. Consideration of Security Incident Cost](image)

In addition, 31% of respondents do not have a specific budget for help desk activities. Of those who do, 54% establish the budget and sizing for their help desk on simple metrics related to the number of users, and 27% simply guess. Many responses to this question were open ended, indicating that, again, no specific budget exists or the respondents are not involved in setting their budgets. In another question, 40% of the respondents do not track the cost of a help desk call, and 37% indicate that the cost is unknown.

Without even an estimate of a budget, or knowledge of the cost per call or the cost of an incident, it is extremely difficult to establish a cost justification (ROI or TCO) for new processes, additional staff or training, or new technology that could mitigate security risks.
Staffing

When comparing responses to the size of organization represented in the response, the number of help desk managers or supervisors remains relatively small. This is consistent across every size of the user base being served by the help desk. When looking at responses as a whole, the majority indicated that they employ no more than five help desk managers as distinguished from the agents that directly handle calls or requests. However, when analyzed against the size of the organization, the number of agents appears to scale with the number of users being served, as shown in Figure 8.

![Figure 8. Size of Organization Versus Number of Agents](image)

Help desks are notorious for high rates of staff “churn”—annual turnover rates of 30 to 40% are common. The 2012 Technology Industry Survey by UK recruiter Mortimer Spinks and Computer Weekly reported that more than 55% of an organization’s service desk staff would be leaving in the next 12 months.® Most help desk agents hold an entry-level position with low pay and high turnover, making them minimally invested in the organization’s security posture, even though they are often the first line of support a user encounters.

Relying mostly on training of personnel by managers and supervisors may appear to be a cost-effective solution at first, but as we have seen, managers and supervisors are a limited resource even in the largest organizations, and depending on those bosses to train their staff—a workforce that traditionally has a high turnover rate—carries with it a host of problems. Even the largest help desks risk being understaffed, and depending on a top-down approach to training a help desk team in security skills and awareness is not operationally effective.

Effective help desk operations are as much a security problem as they are anything else, but it’s a problem that falls through many cracks because the risks are hard to quantify and resolve. The following strategies can address the points raised in this report.

**Regroup and Retool Human Processes**

Centralized security operations and their top-down structures are challenged today by employees who have ubiquitous access to information and are encouraged by the so-called BYOD phenomenon. Corporate policies and procedures can no longer be written in a vacuum, ignoring the mindset of the workforce; centralized systems still depend on people adhering to processes.

A help desk is in a unique position to help educate, confirm and enforce correct user behavior, thanks to its existing capabilities and commitments. Even the best of centralized systems depend on humans’ adherence to process. If good security practices can be simplified and structured to the point where they become as much a habit as breathing or coffee breaks, the result will be a more effective help desk and a more secure organization.

Kevin Johnson, SANS Analyst and Senior Security Consultant at Secure Ideas, has implemented this approach both at his company and with his clients with great success. As Johnson explained in an email to the author, “We call it Tactical Sec Ops and have found that it can be VERY successful.”

**Return to Metrics**

Help desks are often measured and motivated by metrics that emphasize quantity and speed; to meet service levels, agents are tempted to use whatever procedures and tools will get the job done quickly, even if they cut corners. Basing performance solely on such metrics, and ignoring factors such as security, means that the help desk may be approaching problems in ways that don’t meet the organization’s security standards.

To address this, IT leaders need to equip help desks with tools that will allow efficient problem resolution while adhering to security and privacy requirements. These tools should also be able to measure attempts to exploit the help desk and how well they were blocked; unfortunately, this is easier said than done. With the rapidly expanding universe of applications, devices and platforms in use, IT security issues are much more complex than ever before and may require a more collaborative approach to problem solving than those found in policies and processes that have their roots in batch processing and punch cards.

**Make Your Case**

Quantify your help desk risk and justify the needed changes in your business and your technology. You need to be able to present the business case for the technology you select and integrate with your help desk processes. Perform a risk assessment on your help desk operations, involving your security practitioners, “red-team” social engineering and technical means to discover weaknesses. Understand the outcomes of this assessment and establish a basis to justify any changes and/or improvement to your operational security. Do this by tallying the cost of a help desk incident, the cost of proposed changes, operational improvements and cost reductions brought about by streamlined security; finally, include the impact on both the budget and the actual services provided to end users.
Conclusion

When it comes to areas of risk, most organizations consider their endpoints, servers and critical applications. What they don’t consider enough, according to the results of this survey, is the help desk. Help desk services are a rich entry point for social engineers and technical attackers. Help desks—and their applications—hold the “keys to the kingdom” to better serve user requests.

Resetting passwords, providing remote access capabilities for troubleshooting or linking to key assets within the enterprise all create risks for attackers and social engineers to exploit. Survey respondents show that they are aware of the social engineering issues, and although most have a healthy concern in this area, they look for more automation of processes, leaving them vulnerable to exploitation.

As to their security practices and technologies, organizations are currently over-relying on education and training, particularly given the high turnover of help desk staff. However, they still need to integrate security into their development, and overhaul and update processes. They need to harden their practices and technologies against attacks and should educate human help desk operators to avoid falling victim to social engineers while identifying and validating users.

Watch the technology event horizon for those tools and services that will meet your business needs and your budget. At the same time, address the challenges of emerging technologies such as cloud and mobile computing. Finally, stay informed by sharing information with peers, following breach and security reports, and asking more of your tools.
Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls “policy, process, platforms, pipes and people.” She has focused most recently on HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by modern society that is dependent on automation—privacy, identity theft, exposure to fraud and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold) and GCIH (Gold), and the GHSC.
## 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 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 Secure Singapore 2018</td>
<td>Singapore, SG</td>
<td>Mar 12, 2018 - Mar 24, 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 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 Secure Canberra 2018</td>
<td>Canberra, AU</td>
<td>Mar 19, 2018 - Mar 24, 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 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®reg; 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>SANS Seattle Spring 2018</td>
<td>Seattle, WAUS</td>
<td>Apr 23, 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 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 London March 2018</td>
<td>OnlineGB</td>
<td>Mar 05, 2018 - Mar 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>