Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprises

What the boss doesn't understand is how much that costs, in terms of software, hardware and, most importantly, the specialized talent required to operate it. Sticker shock is a reality when SMEs talk security, and often, the dedicated staff to support security products is forgotten.
Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprise

A SANS Whitepaper
Written by Jacob Williams
June 2014

Sponsored by
AlienVault

©2014 SANS™ Institute
If you work in a small- to medium-sized enterprise (SME), you know how challenging securing your technology assets can be. The boss (who is often the owner) wants the same level of security that Fortune 500 companies enjoy. What the boss doesn’t understand is how much that costs, in terms of software, hardware and, most importantly, the specialized talent required to operate it. Sticker shock is a reality when SMEs talk security, and often, the dedicated staff to support security products is forgotten.

Attackers understand the challenges SMEs face, too. And although there are bigger paydays out there, they typically have better security, meaning the SME is an easy target. Some SMEs erroneously believe that they have nothing to lose, no intellectual property (IP) to protect. But that isn’t true. Look carefully at the data on your network. If you wouldn’t publicly post this data on pastebin or email it to a competitor, then it clearly has value—and you should be protecting it. Consider the case of a North Carolina SME fuel distributor that lost $800 million in 2013 to unauthorized Automated Clearinghouse (ACH) transfers after its systems were hacked. They weren’t the biggest target out there, but they still had valuable data that, when compromised, provided a significant payday.

With that said, there are solutions. In this paper, we walk through a typical compromise at an SME, consider security controls that can be used by SMEs and investigate how these might change the outcome of an attack. Then we offer some advice (tailored to the SME, but universally applicable) on evaluating security controls for deployment.

---

1 For the purposes of this paper, we have defined an SME as a company with 100–999 employees (www.gartner.com/it-glossary/sombs-small-and-midsize-businesses).

2 http://krebsonsecurity.com/2013/05/nc-fuel-distributor-hit-by-800000-cyberheist
Business leaders might believe that, because there are larger organizations in their industry, they will not be targeted for compromise. Nothing could be further from the truth. The reality is that many attackers looking to compromise a company within a specific vertical market will target the weakest link, which often can be an SME.

Many SMEs have deployed a very flat network structure, offering little segmentation. This approach is actually ideal for minimizing overhead in network administration. It also allows the organization to purchase cheaper networking equipment that typically uses unmanaged—instead of fully managed—switches. Unfortunately, this convenience comes at the cost of security. Once an attacker compromises the first endpoint (and they will compromise an endpoint), the lack of segmentation in the network infrastructure means that the attacker has no roadblocks and can pivot mercilessly through the network. And, despite growing security issues, VLAN adoption that would layer additional security has been very slow among SMEs. Regarding VLAN use, an information security consultancy recently noted that only 8 of 47 customers (17%) they worked with over the last year were using VLANs.3 When companies don’t use VLANs, other security controls are all the more important to compensate.

Accurate hardware and software inventories have been well established as critical to effective security as well as meeting regulatory requirements, such as PCI. However, these inventories require significant resources to construct and keep updated and are not widely deployed in smaller organizations. These inventories give organizations a clear window into their systems, software and network so they can identify potential vulnerabilities and protect their assets.

Lack of accurate inventories impacts the development of an appropriate patch management strategy, which is also a perpetual challenge for SMEs. Keeping Windows patched is usually fairly straightforward—although many enterprises often fail to apply regularly published patches. Third-party apps and non-Windows OSes, on the other hand, are an even bigger patching challenge, especially for those with the most limited resources.


Key Problem Areas
The following characteristics of SMEs make them vulnerable to attack:
- Lack of realization that they are targets
- Flat networks offering little segmentation
- Poor inventories of IT resources and critical data
- Missing patches and poor patch management in general
- Inadequate funding and/or competition for budget dollars
- IT security (and IT in general) understaffed
- Lack of specialized staff or security training to operate complex tools
Upgrading the OS is another challenge not unique to, but particularly challenging for, most SMEs. Expensive custom code developed for business purposes may use features unique to a particular version of an OS. Even more problematic, many custom applications exploit undocumented features of the OS. Unfortunately, SMEs are particularly impacted by OS upgrades because they frequently cannot afford the costly endeavor of porting code to the new OS.

A shortage of qualified IT and security staff remains an issue. In today’s employment market, where there is a wealth of opportunities for information security professionals, many employers are competing for the same limited resource pool. Due to limited budgets and less enticing benefits, SMEs struggle to attract and retain talent.

Funding may also contribute to understaffing in the SME information security departments (if they have dedicated information security staff at all). They lack the budget to acquire more complex tools or the staff to deploy and manage them. And many enterprises find that even if they purchase complex security tools, their less experienced staff lacks the technical training or time to use them effectively.
In this section, we introduce a case study showing how a fictitious company, Southern Circus Performers Federal Credit Union (SCPCU), was breached. Like many regional credit unions, SCPCU is an SME with limited information security resources. In 2012, SCPCU’s management directed that an executive blog be created “right now.” To save on hosting provider costs, SCPCU decided to host their WordPress (WP) blog on an existing server in the DMZ. Of course, all sorts of “bells and whistles” were enabled on the blog by adding several WP plug-ins. Figure 1 illustrates the network SCPCU created.

As the all-too-familiar story plays out, the executives posted a few entries on the blog and then largely forgot it existed. Because the blog was installed outside of any normal change control process, IT lost visibility on the blog as well. However, attackers were able to locate the blog in early 2014 by following all the links on SCPCU’s website.

When they found the blog, the attackers knew they had struck gold! Why? Because in the two years since the blog had been deployed, multiple vulnerabilities had been discovered in WP and many of the enabled plug-ins. Exploiting the unpatched vulnerabilities in WP and the plug-ins to upload a web shell to the server was a trivial matter for the attackers.

The web shell gave the attackers access to the command line on the web server, albeit as an unprivileged user. However, SCPCU also lacked a good vulnerability management program and did not realize that the Linux kernel running on the web server was vulnerable to multiple privilege escalation vulnerabilities. This allowed the attackers to escalate to “super user” status on a critical server in SCPCU’s DMZ. Fortunately for SCPCU, the informational website is hosted on a different server from the core online banking functions. The attackers cannot (yet) control financial account data.
Using their control of the web server, the attackers can infect website visitors using malicious links and drive-by downloads. Although the attackers might wish to infect customers visiting the website, their best chance for controlling financial data in bulk is pivoting to employee machines inside the network. Many of the machines inside SCPCU’s network are still running Windows XP (an operating system for which patches are no longer available)⁴ and have outdated versions of Java installed. From their privileged position, attackers could potentially compromise machines running newer operating systems, but compromising Windows XP machines (especially those with outdated patches) is like shooting fish in a barrel.

The attackers use publicly available browser exploits to compromise a dozen internal machines, but none of them offers access to the coveted financial transaction (ACH) systems.

However, the attackers are able to leverage their position in the DMZ to compromise an internal database server. The attackers use the logs on this server to determine the location of the system administrator. This is important because the system administrator is likely able to access the jump server that separates administrative systems from the financial processing systems.

Financial and other high-security networks often segregate sensitive data on a particular portion of the network. Frequently, these networks are referred to as “red” (low security) and “black” (high security). Segmentation, however, impacts system administration. To reach black networks from a red workstation, administrators often deploy a so-called “jump server.” Because this server is attached to both networks, the administrator can use a remote desktop protocol (RDP) to connect to the jump server and then from there to any machine in the black network. Although jump servers simplify administration, they are prime targets for attackers and should be subjected to additional monitoring and security controls.

The attackers compromise several internal users before finally gaining access to a system admin’s machine. From there, attackers leverage their position to identify the location of the admin’s jump server to the financial processing network.⁵ Soon, the attackers have deployed key logging malware on the administrator’s workstation and have captured credentials to the jump server and servers in the black network. The compromise is complete, and the attackers begin performing ACH transfers to offshore accounts.

---

⁴ Although Microsoft no longer supports Windows XP, as of this writing, the OS is still used on 25.27% of desktop computers (www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0).

⁵ http://blog.industrialdefender.com/blog/security-basics-jump-boxes
In this section we examine the compromise described in the case study with an emphasis on identifying what steps an SME with a small security budget can take to mitigate it. Examining the compromise through the lens of the SME is important because recommended security controls must be within financial reach (measured both in capital and human costs).

In general, the recommendations revolve around the following compensating controls (see Figure 2):

- Device inventory
- Software inventory and vulnerability assessment
- Log aggregation and review and event correlation, possibly using a security information and event management (SIEM) system
- Host-based intrusion detection systems (HIDS)
- Threat intelligence

One excellent place to start improving the SME’s security posture is implementing a few of the easily deployed Critical Security Controls (CSCs).
Inventoring Devices

Before an organization can architect a secure network, it must understand what devices are present on the network. The first CSC, “Inventory of Authorized and Unauthorized Devices,” focuses on this first step in enhancing security.6

An accurate device inventory should include both the physical hardware and the operating system running on the device. Accurate inventories are essential pieces in the daunting task of change control and make possible the detection of rogue devices. Device inventories would help SCPCU’s staff locate Windows XP machines (and other devices running unsupported OSes) and target them for additional security controls and/or remediation.

The Windows XP machines obviously should be removed from SCPCU’s network. However, newer operating systems often do not support custom software found in many businesses. SMEs, in particular, may lack the resources to have custom business applications updated. In other cases, companies may simply have begun the migration away from Windows XP too late and found their limited IT resources dedicated to other projects. In either case, the inability to completely abandon Windows XP makes the enhanced host-based protections provided by HIDS (such as real-time monitoring for malware creating new services) more important. In the absence of updates, enhanced logging in XP is critically important. But logging by itself isn’t enough. Reporting the logs to a centralized source and correlating the logs to spot intrusions is critical.

Software Inventory and Vulnerability Scanning

The compromise began when the attackers located and compromised the abandoned WordPress blog buried on the website. Two specific security controls would help prevent this critical portion of the attack.

First, any vulnerability assessment would have located the out-of-date WordPress blog before the attackers did. The vulnerability assessment could be completed by remote scanning or by checking software inventories on the server, looking for known vulnerable software.

6 www.sans.org/critical-security-controls/control/1
Continuous vulnerability assessment, also significant, is the fourth CSC, “Continuous Vulnerability Assessment and Remediation.” Unfortunately, many SMEs lack the capability to build and maintain software inventories or perform vulnerability assessments. While vulnerability scanners are often considered just a software purchase, correlating the (often voluminous) reports with software inventories and logging data is a daunting task. Because manually correlating vulnerability assessment data requires more time than most SMEs can afford to assign to the task, they should seek to deploy solutions that automate some (or all) of the correlation.

Second, accurate software inventories offer indisputable value in securing networks, so much so that the second CSC is “Inventory of Authorized and Unauthorized Software.” Even if vulnerability scanning somehow missed the out-of-date WordPress software, an accurate software inventory would have highlighted the presence of the blog (and the need to patch or remove it). These complementary controls are what defense in depth is all about.

Aggregating and Correlating Logs

When attackers probe a website for vulnerable applications in general (and WordPress plug-ins specifically), their actions generate a significant number of logs. Analysis of audit logs is CSC 14, “Maintenance, Monitoring, and Analysis of Audit Logs.” Additionally, the Verizon Data Breach Report indicates that correlating threat intelligence with log data is useful in accelerating detection and containment of threats. However, web servers are constantly being scanned by would-be attackers. How can SCPCU determine which scans detected vulnerable software and which didn’t? The answer lies in the purchase of a SIEM system.

The primary purpose of a SIEM is to aggregate logs in a central location where correlation of event data is performed. Event correlation with a SIEM helps security professionals discover previously unknown attacks and act to prevent data loss. However, SIEMs are usually costly to deploy and often require significant training to use effectively. Cost and ease of use may be obstacles to adoption for an SME. Enterprises with fewer resources should evaluate SIEM products that are intuitive and have minimal deployment timelines (hours to days rather than weeks to months) and can be more easily used and maintained.

---

**Four Valuable Questions for Potential SIEM Vendors**

Learn about each vendor’s capabilities by asking these questions:

- **How quickly can you get meaningful insights from the SIEM?**
- **How much training is required for staff to use the SIEM?**
- **How easily does the SIEM scale as the business grows?**
- **Does the SIEM integrate host-based agents, or is it limited to receiving logs from syslog or other forwarders?**

---

7 [www.sans.org/critical-security-controls/control/4](http://www.sans.org/critical-security-controls/control/4)
8 [www.sans.org/critical-security-controls/control/2](http://www.sans.org/critical-security-controls/control/2)
9 [www.sans.org/critical-security-controls/control/14](http://www.sans.org/critical-security-controls/control/14)
Implementing Host-Based Intrusion Detection Systems

HIDS, in particular, are critical software for Windows XP machines and greatly enhance security by detecting (and blocking) threats that traditional antivirus software might miss. Traditional antivirus software and network IDS systems are most often signature based and, as such, can only detect known attacks. However, someone has to be the first to be hit with a new attack. When you’re the first, signature detection won’t protect you (there’s no signature yet). HIDS monitors the OS for actions that are often performed by malware, such as creating new administrator accounts or configuring programs to start at boot.

Skilled attackers blocked by a HIDS system will eventually figure out how to compromise a system by observing what is blocked. Therefore, it is critical that system administrators monitor their HIDS logs to discover attempted compromises before attackers adapt their tactics. This operational need drives a real requirement for centralized logging and correlation of HIDS data. Of course, all systems will benefit from the added protection offered by HIDS, but it is particularly critical for high-risk systems.

In our case study, once the web server was compromised, the subsequent compromise of its back-end database server was virtually guaranteed. Attackers simply used the plaintext database credentials stored in various web application configuration files to log into the database management system (DBMS). However, a HIDS system on the database server could definitely identify the use of commands that would allow the attackers to gain a standard shell on the system. Further, credentialed vulnerability scanning would identify configuration issues that allow attackers to pivot from a database login to a shell on the database server.

Regarding the compromise of the system admin’s machine, HIDS is again likely to help detect initial attempts by attackers to install malicious software (such as a keylogger). However, the larger issue is what the attackers do from the system admin’s machine. Remember, it is only a means to an end. SCPCU’s jump server needs maximum logging configured because it serves as the bridge between networks of different security postures. Staff must review logs, looking for anomalous logins to the jump server and connections from the jump server to high-security destinations (financial servers). Staff must promptly act on any detected anomalies because the attackers are not going to wait long to transfer funds after they have access to the ACH system. Any automated detection of anomalies and alerting that can be configured will help dramatically, because the number of log entries generated in a SME such as SCPCU could be upwards of 5,000 events per second.
Using Threat Intelligence

Threat intelligence, which provides data on malicious IP addresses and domains as well as other indicators of compromise associated with the threat groups (for example, protocols in use), can help SCPCU detect and repel (or even prevent) the attack. The attackers must exploit systems and control their malware from somewhere. The nebulous “somewhere” from which attackers launch their attacks and exfiltrate (steal) data takes the form of domain names and IP addresses. Attackers often use the same IP addresses and domain names when attacking multiple targets. As a result, threat intelligence may provide early warning when prioritizing alerts. For instance, scans directed at the web server that originate from an IP address known to be a malicious actor take on special significance and should be a priority. If the attacker has already succeeded in compromising the network, command and control communications or data exfiltration to a known malicious IP address may facilitate detection of the initial compromise.

Given multiple active events under investigation, those communicating to known malicious domains and IP addresses should receive priority attention because they are least likely to be false positives and most likely to result in data theft. Without threat intelligence, prioritizing which event to investigate first is left largely to chance.

Finally, malicious IP addresses and domain names should not be analyzed on a purely individual basis. Attribution of these IP addresses to known threat actors may help the SME understand the motivation of those attacking them and how to protect themselves. For example, attackers from a particular threat group may lease servers from the same datacenter for each of their campaigns. Knowing this, defenders can identify traffic from this datacenter, immediately know to expect the attackers’ techniques in use in the attack and be prepared to protect their systems.
The following sections describe techniques that can help keep your organization out of the headlines. Review your infrastructure and processes to incorporate these ideas.

**Integration**

When evaluating controls for deployment, SMEs must be cognizant of TCO, particularly as it relates to personnel staffing, and balance effectiveness against resources. A security control logging alerts that nobody ever reviews provides little value to the organization. In fact, it may actually weaken security by creating a false sense of security.

Integrating security functionality can decrease ongoing manpower costs for security controls. When security controls are integrated, the administrator monitors one console for evidence of a compromise (rather than many). Deployment and configuration should also be centralized, further reducing TCO. Correlation of event data, essential for spotlighting the events that need to be examined first, is obviously easier when events are reported to a single, central location where they can be reviewed and classified. With more intelligent tools, remediation steps are more easily decided upon, allowing operations to return to normal as quickly as possible.

However, there’s also another benefit. Whether we realize it or not, the cognitive load of our workflow actually influences how long we can work on a complicated problem—and classifying security alerts certainly qualifies as a complicated problem. Researchers have found that the correlation between the cognitive load experienced while working a problem and how long we work on it before giving up is actually hardwired into our brains. Cognitive load in classifying alerts is dramatically reduced by integrating multiple capabilities into a single console used by the analyst. By extrapolating on these results, it’s not hard to see that integrating security alerting capabilities will increase accuracy in correctly classifying security alerts.

But in the real world, integration of multiple products is difficult. Equally difficult is taking time away from regular staffing operations to deploy new security controls. Redirecting IT staff away from their regular day jobs to deploy new controls is difficult even in the largest of organizations. But in the SME, where most IT functions are staffed “one deep,” spending weeks to build a project plan, deploy a solution and integrate the solution into the existing workflow is simply unacceptable. Put bluntly, SMEs need a solution that is up and running in hours, not weeks or months.

---

**Recommendations**

Take the following actions to avoid being in the headlines:
- Integrate tools into a single operating console or dashboard.
- Maintain a continually updated software inventory.
- Use continuous vulnerability monitoring.
- Complete a hardware inventory.
- Use network mapping.
- Incorporate log aggregation and correlation.
- Take threat intelligence feeds for threat identification and prioritization.

11 [http://seriouspony.com/blog/2013/7/24/your-app-makes-me-fat](http://seriouspony.com/blog/2013/7/24/your-app-makes-me-fat)
Updating the Asset Inventory

When Microsoft announced that April 2014 was finally the end of patches and updates for Windows XP (no more extensions), large companies deployed task forces to eradicate it from their environments. However, smaller companies don’t usually have IT task forces, and the end of support for Windows XP has hit them considerably harder.

Now more than ever, they need HIDS on their endpoints (especially those still running XP). But just running HIDS isn’t enough; analysts need to see the alerts from HIDS in a central location to correlate with alerts. Ideally, HIDS alerts should also be correlated with network intrusion detection systems (NIDS) and other security data (such as vulnerability assessment data) across the enterprise. As an enterprise moves away from Windows XP, updating the asset inventory will likely be an issue. Knowing you have an up-to-date asset inventory (and the ability to correlate this data) is a huge benefit, especially when operating on a skeleton staff.

Device Inventory and Network Mapping

SMEs dealing with credit card data are subject to the requirements of PCI DSS. One requirement of the PCI DSS is the availability of network maps detailing the network components that store, process or transmit credit card data (PCI/DSS 1.1.2). Even if the SME doesn’t deal with PCI data, these maps are still important for architecting security and incident response. Network maps are really just an expansion of the device inventory concept (CSC 1) discussed earlier.

SMEs should deploy security solutions that (at least partially) automate the device inventory process to support the creation of the PCI-required network map. If the security control can create the map and assess vulnerabilities in the mapped devices, all the better. While many products can generate a network map, often these solutions are one-trick ponies. SMEs need solutions that accomplish more than one objective. Again, when budget and staffing are tight, integration is key.

12 [www.pcisecuritystandards.org/documents/pci_dss_v2.pdf](http://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)
Threat Intelligence

*Threat intelligence* is the new buzzword in security. It seems that everyone wants it, but few (including larger enterprises) have the skill to effectively use it. SMEs can truly benefit from threat intelligence, including proactive monitoring of IP addresses and domain names for compromise.

Third-party threat intelligence services are a force multiplier: They make existing IT security resources more effective by saving staff time and allowing that time to be spent on other key security tasks. When selecting a threat intelligence service, carefully evaluate whether the service provides actionable data in a form that is immediately usable via detailed response/remediation guidelines. Here again, integration is key to success. Look for a threat intelligence feed that integrates with SIEM and HIDS software to obtain maximum value.
While SMEs are by definition smaller and have fewer resources than their larger enterprise brethren, they face the same threats from cyber attackers. Unfortunately, they often lack the resources, staffing and expertise to adopt the same controls to combat these threats, which puts them at an unfair disadvantage against attackers.

In the current cybersecurity landscape, SMEs must assume that they are under active attack—they are either currently under active attack or their systems have already been compromised. A threat this serious can’t be ignored. Every dollar an organization spends on security must maximize ROI. When investing in security controls, SMEs must also carefully consider TCO. Buying a security control that the SME lacks the expert skills or staffing to properly employ is wasting money.

Effective security controls include HIDS, SIEM and log aggregation, asset inventory and vulnerability assessment tools, and threat intelligence. However, as the organization deploys each of these items, the manpower load increases. After all, a security control that isn’t monitored leaves the organization open to further compromise. To maximize ROI, SMEs should look to products that fuse security data from multiple sources into a single, easy-to-navigate console.
About the Author

Jake Williams is the chief scientist at CSRgroup computer security consultants and a certified SANS instructor and course author. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics and malware reverse engineering. Before joining CSRgroup, he worked with various government agencies in information security roles. Jake is a two-time victor at the annual DC3 Digital Forensics Challenge.

Sponsor

SANS would like to thank this paper’s sponsor:
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>OnlineTXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>