Be Ready for a Breach with Intelligent Response

By preparing a careful plan and resilient response infrastructure before an attack, organizations can limit both data loss and the reactive, post-incident expenses. The result: greatly reduced impact and costs associated with events.
Be Ready for a Breach with Intelligent Response

A SANS Analyst Program Whitepaper

Written by James Tarala

November 2014

Sponsored by

McAfee/Intel Security

©2014 SANS™ Institute
We live in a new age of risk-driven cybersecurity where the bad actors are gaining the advantage and victimized companies are lacking the visibility and focus they need to properly respond to attacks.

According to several recent SANS surveys, organizations of all types and sizes are experiencing multiple advanced, hard-to-detect attacks. And once they do, they’re taking from days to weeks (and, in some cases, months) to find them. In all these surveys, respondents repeat that they lack the visibility and clarity they need to properly detect and respond to threats occurring on their networks.

Traditionally, organizations solved the security-incident dilemma by hiring talented people who did whatever was necessary to protect the company and solve cyberchallenges. That solution simply does not scale well today, with the volume of malware and threats combined with complexity in networked information systems. Modern incident response now consists of workstation, application and network analysis. Investigators can no longer be experts at one or another and expect to be able to understand the breadth of the attacks they’re seeing. These professionals need deep skill sets for analyzing multiple endpoint technologies (such as point-of-sale, workstations, mobile devices and servers), as well as for performing network analysis (such as intrusion detection and network forensics).

Given such scarcity (and the high cost) of these skills, how do we get more visibility into attacks across our environments, improve our response and reduce time to respond? The solution is automating functions that should be automated and connecting the dots between detection systems and response. Connecting these dots and applying intelligence provides responders rich context into the observed behaviors for taking action. Integrating these processes improves accuracy, while reducing time, manpower and costs involved in detecting and managing events. This paper explores how to achieve this.

---

1 "Incident Response: How to Fight Back,”
www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342;
“Critical Security Controls: From Adoption to Implementation,”
www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-adoption-implementation-35437;
“Analytics and Intelligence Survey 2014,”
Let’s begin by taking a look at the traditional, mostly manual, incident handling process used in many organizations. This will demonstrate the steps that are performed manually today that would greatly benefit from automation.

Imagine, it is a normal Friday morning at ACME Corporation. As an ACME executive, you have heard rumors of network problems. ACME’s IT staff assures everyone that it is temporary and part of normal operations, but there have been unexplained outages and slowdowns on the network for months. But today is different: Law enforcement is on site and wants to talk about your security breach.

Due to resource constraints, the officers cannot investigate the case for you. It is up to you and your team to scope the breadth of the breach, determine what data was lost and stop the bleeding—all while trying to determine what sensitive data laws were violated and who to report those violations to. As a part of this process, your team must do their best to perform a forensics investigation in order to reconstruct the technical details of how the data breach occurred. Then, you need to interact with the vulnerability management team to patch and repair the vulnerabilities. And, should the same attack methodology happen again, you hope that your ace team can now recognize it and block it next time around.

In the old, mostly manual model, the first step is to start collecting the data trail left by the attack, but from where? IT security staff will likely begin their investigation by looking at system and network logs, thumbing through the data collected in their security information and event management (SIEM), pulling alerts from their IDS/IPS and checking for access anomalies. If the case involved sensitive data or potential litigation, they’d also need to perform manual and time-intensive activities, such as creating forensic images of suspect computers—a skill in itself that requires specially trained and certified forensics specialists. All of these functions can now be mostly automated, which we’ll discuss in the following sections.
Think Like an Analyst

While most of these steps can be automated today, the trick is connecting the actions of the attack, the processes invoked and the paths traveled to track and trace the activity across the enterprise. The other trick is applying that “gut instinct” or knowledge of attack chain across their systems. And organizations will still need other specialty skill sets available for use in other cases, such as those involving litigation.

This level of skills is hard to come by, according to the 2014 SANS Incident Response survey and the 2014 SANS Analytics and Intelligence survey, and is one of the biggest barriers to effective response. See Table 1.

<table>
<thead>
<tr>
<th>Impediment</th>
<th>Overall</th>
<th>First</th>
<th>Second</th>
<th>Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of visibility into applications, underlying systems and vulnerabilities</td>
<td>39.1%</td>
<td>19.8%</td>
<td>9.5%</td>
<td>9.9%</td>
</tr>
<tr>
<td>Inability to understand and baseline “normal behavior” (in order to detect abnormal behavior)</td>
<td>36.2%</td>
<td>12.3%</td>
<td>13.6%</td>
<td>10.3%</td>
</tr>
<tr>
<td>Lack of people and skills/dedicated resources</td>
<td>30.0%</td>
<td>11.1%</td>
<td>9.5%</td>
<td>9.5%</td>
</tr>
<tr>
<td>Not collecting the appropriate operational and security-related data to make associations with</td>
<td>26.3%</td>
<td>6.2%</td>
<td>9.1%</td>
<td>11.1%</td>
</tr>
<tr>
<td>Lack of visibility into the network</td>
<td>24.7%</td>
<td>11.9%</td>
<td>7.8%</td>
<td>4.9%</td>
</tr>
<tr>
<td>Lack of visibility into the endpoints and specific users</td>
<td>22.2%</td>
<td>9.1%</td>
<td>9.1%</td>
<td>4.1%</td>
</tr>
<tr>
<td>Lack of visibility into mobile devices</td>
<td>19.3%</td>
<td>4.5%</td>
<td>8.2%</td>
<td>6.6%</td>
</tr>
<tr>
<td>Lack of context to know what threats are important based on criticality of assets</td>
<td>18.5%</td>
<td>4.9%</td>
<td>9.1%</td>
<td>4.5%</td>
</tr>
<tr>
<td>Lack of external perspective/intelligence on new threats/indicators of compromise</td>
<td>15.6%</td>
<td>3.7%</td>
<td>3.3%</td>
<td>8.6%</td>
</tr>
<tr>
<td>Lack of visibility into the cloud-based applications and processes</td>
<td>14.4%</td>
<td>3.3%</td>
<td>4.9%</td>
<td>6.2%</td>
</tr>
<tr>
<td>Lack of central reporting and remediation controls</td>
<td>13.6%</td>
<td>2.1%</td>
<td>2.5%</td>
<td>9.1%</td>
</tr>
</tbody>
</table>

The skills needed to conduct these investigations are either hired or pulled from other departments, increasing disruption. According to the Incidence Response survey, 61% used this method of staffing to respond to events, while 23% drew from outside resources.

Because of this lack of expertise needed to respond, organizations need to automate as many controls as possible for incident data collection and response.

---


Plan for Barriers

By preparing for cyberthreats before an attack, organizations can potentially limit both data loss and the reactive, post-incident expenses. In fact, making proper preparations to protect against cybercrime can positively impact a company’s bottom line. The longer a breach stays undetected, the further it spreads and the more it costs organizations in terms of data lost and response actions.

Unfortunately, as shown in Table 1, barriers to achieving this level of automation and visibility are many. As a result, response is lacking. According to 20% of respondents to the Incident Response survey, 2–7 days was the most common time to containment and remediation, while another 17% took 1–2 days.

In that same survey, respondents identified a lack of time to review and practice incident response procedures and a lack of budget resources for tools and technology as their key impediments. There are other reasons why organizations are not always properly prepared, but the themes of resources and tools are ones that regularly surface across multiple SANS surveys. They are also asking for more automated, integrated product sets that may or may not have competing interests, as shown in Figure 1.


It is also clear from these results how automation and visibility tie together and should lead to overall improvements in accuracy and response time. IT managers must continually ask their teams what the processes are that they do repeatedly that can be automated and how the processes in place today can be connected (usually through APIs) for more holistic viewing and response. For example, could they consider automating network traffic analysis and alerting, system log analysis and alerting, or the process for identifying deviations from the organization's approved system baselines to assist with incident management?
We can see from multiple surveys that organizations are struggling to see into events and respond appropriately. There are multiple steps organizations should take to improve their automation and their visibility together. In accordance with the Critical Security Controls, these steps essentially include:

- Baselining systems and assigning responsibility
- Planning for anomalies
- Centralizing response

**The Role of Baselining**

Before businesses can begin automating their incident response processes, they need to understand specifically what they are protecting. This process itself can be automated through a variety of tools including endpoint discovery, access control management, asset management tools and vulnerability managers.

Typically, baseline inventories are needed of:

- All devices on a network subnet
- All software installed on a system
- The configuration of system and security settings on a system
- Wireless access points allowed on a network
- Listening network services on a system
- All network protocols used on a network subnet
- User accounts on a system

Despite the availability of tools that can automate baselining, inability to understand and baseline “normal behavior” (in order to detect abnormal behavior) was the second largest problem, cited by 36% of the respondents to the Analytics and Intelligence survey. The first two controls of the CSCs call for inventorying of software and hardware; however, only 27% of organizations to take the 2014 SANS Critical Security Controls survey have fully implemented Control 1 (hardware inventory) and 22% have fully implemented Control 2 (software inventory). In contrast, 50% are fully automated in their malware defenses, 49% in boundary defenses and 43% in wireless access control.

---

Without knowing what’s normal in the network, systems and usage patterns, detecting what’s abnormal is infinitely more difficult for malware and boundary devices. If, for example, there is an unknown system with an unknown application that happens to be malicious in nature, how can the organization detect the malware if it doesn’t even know what applications are approved and accepted?

This latter process, application whitelisting, results from knowing your system’s approved applications and denying those that are unapproved. Whitelisting is one of the more common forms of automation available today.

**Detection and Response**

Once a baseline is known, it becomes easier to apply application whitelisting and behavioral analysis to weed out false positives and detect anomalous behavior that is not known or documented in the baseline. For example, if an unapproved and unknown software application attempts to install on a system, if a new device appears on the network or if traffic starts communicating across a port and protocol combination that no one has ever seen before, these could all be situations worth investigating as a possible system compromise.

Often, incident handlers refer to such anomalies as *Indicators of Compromise (IoCs)*. IoCs are the artifacts that incident handlers look for to identify malicious activity. The better an organization understands its information systems, the better it will be at identifying these signatures and the better it will eventually become at automating the detection of such security threats.

Automating the incident response process relies on comparing the knowledge obtained during baselining to new knowledge of new behaviors that are IoCs. To this end, services organizations, product vendors and user groups are developing automated means to reveal and connect these indicators of compromise across systems for better visibility.
The Role of Centralized Intelligence

Once an organization has established baselines for its information systems, it can start centralizing intelligence feeds that draw in new information from internal and external sources to help identify new patterns and indicators of attack. Figure 2, taken from the SANS Analytics and Intelligence survey, shows the sources that organizations are gathering intelligence from and the tools they are using.

How is your threat intelligence data gathered and used for detection? Select all that apply.

There are two stages to the cyberthreat intelligence information collection process. First, the malicious/anomalous data trail or IoC must be generated. Then the information must be collected in a central repository (usually a SIEM or log management system, according to the SANS CSC and Analytics/Intelligence surveys) to facilitate analysis and take action. The following case study shows how connecting the dots between systems and layering intelligence on the actions observed can result in a faster, more cost-effective response to events on the network.

---

Applying Intelligence to Response: A Case Study

Imagine that malicious software has accidentally been installed on a workstation by an end user who visits a website that downloads malicious code to his workstation without his knowledge. Assuming the organization has established system baselines already and is looking for deviations to that baseline, several things should immediately occur within the automated detection and response system:

1. The organization's whitelisting app detects the presence of a new software application that is not on the approved list of applications gathered during baseline assessment.

2. At the same time, the organization's antimalware or endpoint protection system (host IPS) detects the presence or attempted execution of malicious software and blocks it.

3. At this point two localized detection events have occurred. However, if these events remain distributed, responders may remain unaware. So these detection sensors should alert a central intelligence system to the presence of the anomalies on the workstation in conjunction with the IPS alert.

4. Now, with two anomalies registered in the repository, it is easier for staff to validate that a threat exists and respond. This could even be automated to the point that the combination of these two events occurring simultaneously would generate an action, such as additional dynamic file analysis or blocking network access from the infected system.

5. Additionally, if the malicious code has spread to other systems, then the baseline comparison, combined with the IPS alerts, can help staff identify the location of all affected systems more rapidly than trying to hunt them down individually through manual log analysis.

6. To facilitate this level of automated response, central collection points gather alerts and anomalies, usually through the SIEM, which correlates and analyzes the data, and then alerts incident handlers to Events of Interest or IoCs.

If the tools aren’t automated and making connections between their findings, the odds of identifying an incident during an attack such as this are low to nonexistent.
Given their lack of visibility into events in their networks, SANS survey respondents repeatedly indicate that many organizations still lack automated baselines, initial detection capabilities or the ability to aggregate intelligence gathered through dispersed sensors.

Yet organizations are moving in the right direction, automating what they can. According to the SANS Analytics and Intelligence survey, the majority of respondents felt they were “fairly” automated, but only 9% felt they had fully automated these functions. Those who are attempting these processes are primarily doing so through a combination of in-house developed processes and services organizations, according to the Analytics and Intelligence Survey. See Figure 3.

**How automated are your security analytics and intelligence processes (such as combining pattern recognition, whitelists, blacklists and reputational libraries)?**

*Select the most appropriate.*

![Figure 3. Level of Automation](http://example.com/figure3.png)

---

9 Unpublished data from the “Analytics and Intelligence Survey 2014,”
What, in particular, is vexing to organizations today with their automated response programs? According to the SANS Critical Security Controls survey, 66% of respondents indicate they need a clearer picture to present, manage and report on security risk posture, while another 58% lack the ability to prioritize response.\(^\text{10}\)

Part of the problem is the sheer number of tools used to follow up on incidents. According to the SANS Incident Response survey, organizations are using network sensors, decrypters, agents, UTMs, endpoint controls, third-party intelligence, and internal and third-party digital forensics tools, as well as traditional screen captures and other hard-to-automate processes for incident response. In Figure 4, the red line shows the response functions they’ve automated most often—including network scans, host intrusion detection (HIDS), IPS/UTM and network flow tools, while the blue line shows what is handled mostly manually, starting with user notification, log analysis and use of third-party digital forensics tools.

How does your organization identify impacted systems, and how automated are these processes of identification?

![Figure 4. Multiple Tools Used in Response with Varying Degrees of Automation\(^\text{11}\)](image)

---

\(^{10}\) “Critical Security Controls: From Adoption to Implementation,” www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-adoption-implementation-35437, p. 13, Figure 9.

Pulling these tools together and connecting the dots is critical in making a full-scale response to a multifaceted incident.

Figure 5, taken from the SANS Analytics and Intelligence survey, shows the capabilities that investigators already integrate and those they want to integrate as they perform their detection and response workflows.

What types of detective technologies do you need your analytics and intelligence capabilities to interface with?

Please indicate which ones are currently integrated into your environment and those that are planned but not integrated yet.

The top planned interfaces are network-based antimalware and network access control. A centralized advanced malware analysis system can provide detailed insights into the nature, intent and capabilities of a malware payload. This detail, such as contacted IP addresses, altered registry values and other evasive behaviors, enables an investigator to more effectively pursue the attacker.

---

12 “Analytics and Intelligence Survey 2014,” www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507, p. 11, Figure 8.
Automating Responses to Aggregated Intelligence (CONTINUED)

If advanced malware tools identify a malicious IP address, that destination and reputation can be fed back into host and perimeter IPS to automatically block the traffic and actively reset the network connections of any systems talking to that connection to ensure the connection does not continue. Logs can be mined to trace back interactions with the address and identify reconnaissance, command and control, and exfiltration activities.

The Incident Response survey reinforces the importance of connecting these dots. In it, lack of visibility across systems, endpoints, configurations and vulnerabilities was a top inhibitor of response (following lack of time to review, lack of budget and lack of team). Nearly 40% of respondents cited difficulties with correlation, followed by silos between response and operations groups. See Figure 6.

What do you believe are the key impediments to effective IR at your organization?

![Figure 6. Impediments to Effective, Timely Response](image)

Reusable Threat Intel

Identifying threats can be accelerated through automated reuse of new threat information combined with the correlation capabilities available in many SIEM systems. In the SANS Analytics and Intelligence survey, organizations had many different ways of gathering and correlating threat intelligence. Although 29% do not correlate event data with internal or external intelligence, 27% correlate manually, while another 27% rely on their SIEM vendors to handle intelligence gathering for them. Twenty-five percent use a security analytics system to perform correlation automatically, while the largest group (32%) leaves that function to third parties.14

Automated Actions

An incident response system could respond with a variety of automated actions after it identifies an event.

- If the incident occurs on a workstation, the system could:
  - Stop a malicious/dangerous process.
  - Delete an unwanted file.
  - Create forensic images for investigators.
  - Completely re-image a computer to a known good state based on automated rules programmed into the incident response system.
  - Revise policies and thresholds to increase sensitivity to risky activities.
  - Collect instance information to capture evidence of repeated activities.
  - Set a watch list to monitor for recurrence of the file.
  - Mine historical data for evidence of the file's appearance in the past.

- On a network, the system could:
  - Block the offending traffic.
  - Disallow all traffic from an offending IP address or system.
  - Block a specific port on a switch from communicating.
  - Begin a full packet capture of all relevant network traffic related to the incident for later investigation.
  - Set a watch list to monitor for future communication attempts to or from the blacklisted address.

Automating and integrating many of these practices is achievable today. Based on several SANS surveys discussed in this paper, such automation is already occurring in steps. And those who are automating to connect the dots across their detection and response systems are experiencing improvements.

For example, 58% of the SANS Analytics and Intelligence survey respondents say their use of analytics and intelligence automation is improving their performance and response time: 55% claim improved ability to correlate events, and 50% are experiencing fewer false positives. Another 46% are very satisfied with reusing their threat intelligence.\(^\text{15}\)

Together, these improvements have a powerful impact on the cost of response. The sooner the breach is detected, ideally at the company gateway, the lower the cost of response. However, with so many mobile and nontraditional devices connecting to the network, detecting everything is, so far, an unattainable goal. So in addition to prevention technologies, IT leaders should see automated response and remediation as a way to more effectively allocate technology resources and lower the organization’s overall exposure to loss.

**Recommendations**

The Council on CyberSecurity takes a holistic view of automation, aligning it with policy, practice, and intake and response to threat data. See Figure 7.

---


\(^{16}\) www.counciloncybersecurity.org/critical-controls
Specifically related to response, the Council on CyberSecurity recommends that organizations implement threat data collection sensors as soon as possible. In the first five controls, the CSCs recommend collecting data for the following purposes:

- Network access control
- Application whitelisting
- Vulnerability management systems
- Host- and network-based antimalware systems

These processes give IT staff the data necessary (and the visibility needed) to properly address incidents as they occur. And they provide the data needed to follow up and remediate the vulnerabilities that allowed the breach in the first place, resulting in an improved risk posture.

SANS recommends that organizations start with their inventory or baseline and then follow these practical steps to create a defensible IT architecture that includes automated response actions:

1. Acknowledge that these tools (SIEM systems, security analytics systems or threat intelligence systems) will not implement themselves. These tools have not reached their full potential, and yet they are the starting place for coordinating detective-response actions. Have a plan for continued improvement, count on spending money over time to integrate and automate in steps, and push vendors and integrators for more cross-platform solutions.

2. Don’t expect to decrease IT staff as a result of initial implementations. Although organizations are experiencing faster response as a result of their automated processes, IT staff—whether insourced or outsourced as a service—will be needed to manage, fine tune and challenge automated systems according to the events in their specific environments.

3. Build a long-term incident handling program to serve the organization and expand to manage new threats and detective/response capabilities.
4. Remember that automation can even help you get started by mapping systems and providing answers to important startup questions, such as:

- Do we know every device currently connected to our network, and has every device been documented in an easily accessible form?
- Do we know every software application (executable and code library) present on our systems, and are they documented in an easily accessible form?
- Do we have a baselining platform to document and detect deviations from our established information system baselines?
- Do we have a SIEM or security analytics system that is currently aggregating threat data and correlating it to other events to flag a “high interest” event?
- Does our incident response team have access to the analytics system, and are they training it to automatically respond to known threats?

If the answers to any of these questions is “No” or “We don’t know,” then it’s time to determine whether that capability is desired, required and worth investing in.

Defenses will rarely be 100% effective, and there will always be a need for monitoring and reactive controls to respond when incidents occur. By proactively implementing systems for incident response, organizations give themselves the best chance of minimizing loss through an effective, well-planned response. By feeding insights collected in the incident response process back into the defensive system, organizations can become truly adaptive with security defenses that learn from past experience.
Responsibility for breaches and computer security incidents is no longer assigned only to technical staff. Boards of directors and executive leadership are increasingly being held accountable by industry, regulators and shareholders for the security of digital assets such as intellectual property and confidential customer data. Detection and response, then, must catch up with the threats—and that means automating the processes that staff and consultants are handling manually.

SANS surveys show that automation doesn’t just happen by itself; it takes planning and costs money to improve visibility and response by automating and interconnecting detection and response systems. The best way to accomplish this is to know the core business requirements in this area, including the ability to:

- Generate thorough baselines of all technology systems
- Detect deviations from established baselines
- Aggregate alerts on anomaly detection
- Contextualize data and alerts to separate signal from the noise
- Automatically respond to detected anomalies
- Learn and evolve based on threats that have been detected

Through the use of baselining systems, generating automated alerts to system anomalies and aggregation of system intelligence, organizations can build a platform to empower incident handlers to respond to incidents in a timely manner and reduce the organization’s exposure to unnecessary loss and risk.

The sky is not falling, but organizations must prepare for information system security incidents. Not every company will be targeted by a nation state or by organized crime, but one thing is certain: A cyber incident will occur in every organization. Executives should ask themselves: Have we properly allocated the necessary financial and manpower resources needed to respond to cyberthreats? Have we discussed this possibility with staff? Will we be prepared when the time comes?
James Tarala is a principal consultant with Enclave Hosting, LLC and is based out of Venice, FL. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many of its auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, email, terminal services and wireless technologies. James has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.
## 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 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>Online TXUS</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>