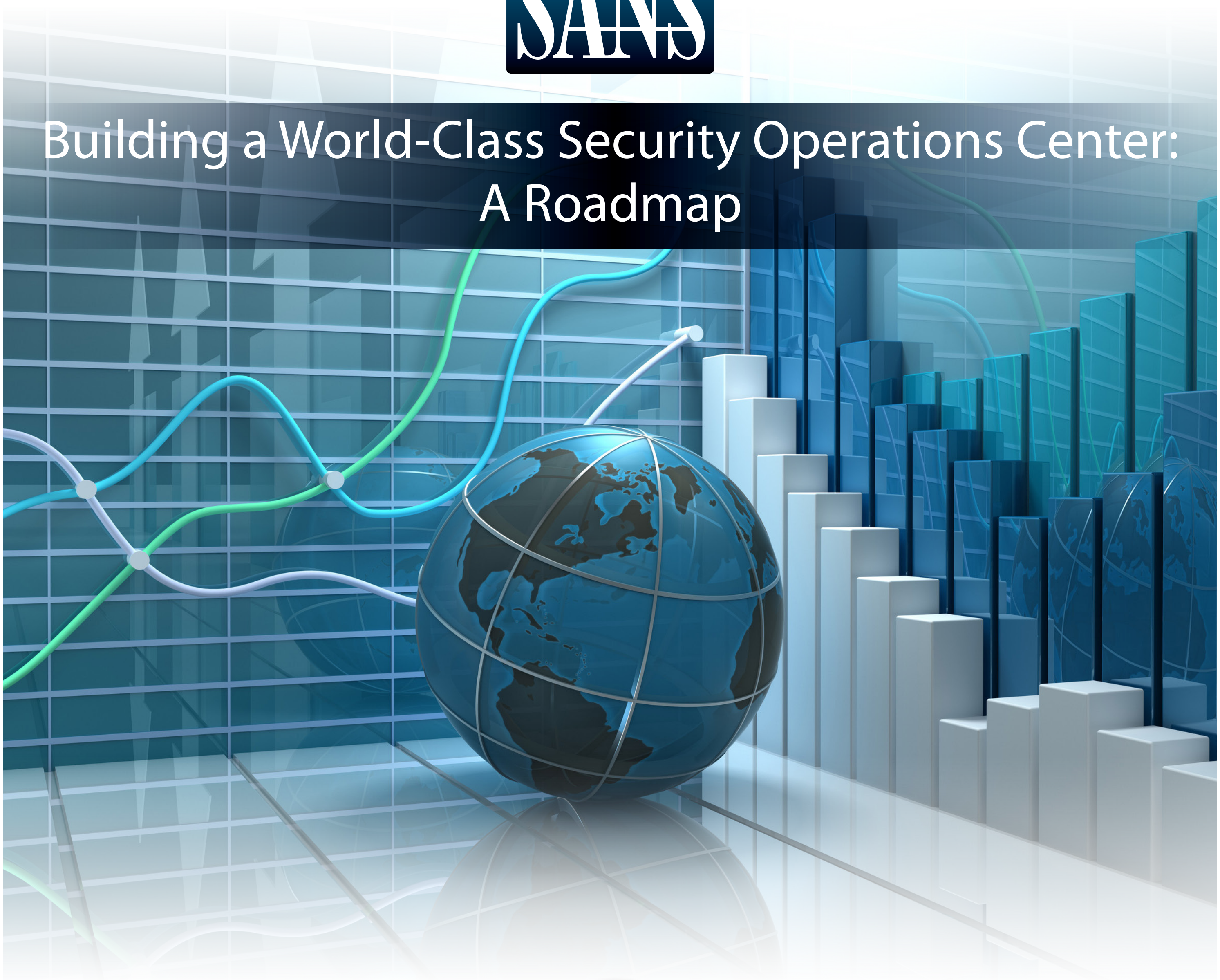
Building a World-Class Security Operations Center: A Roadmap

Explore how you can build a world-class security operations center (SOC) by focusing on the triad of people, process and technology.

Building a World-Class Security Operations Center: A Roadmap



A SANS Whitepaper

Written by Alissa Torres

May 2015

Sponsored by
RSA

Investing in Security

If you are reading this paper your most pressing concern undoubtedly is protecting your organization's intellectual property and sensitive customer data.

Highly visible breaches and attacks have brought an intense focus on organizations' incident detection, investigation and mitigation capabilities. After all, if you can't prevent a security incident, you had better be able to detect and respond to it quickly. But just increasing security spending does not guarantee more protection. Achieving the goal of better security depends on how that budget is allocated; what people, procedures and infrastructure are put into place; and how the security program is managed and optimized over the long term.

For organizations without a formalized incident-handling capability, the creation from scratch of a security operations center that enables centralized visibility, alerting and investigation can be a daunting task. But fortunately organizations don't need a room full of security experts and an investment of millions of dollars in security systems to make progress here. In this paper we look at how to develop an effective security operations center (SOC) and provide a roadmap for continuously evolving this capability to keep pace with the tactics of the adversaries.

Percentage of respondents to the 2014 SANS Incident Response Survey who reported that no portion of their organization's security budget is currently allocated to incident response[1]

Creating the Roadmap

Because you can't build a world-class security operations center (SOC) overnight no matter how much money you are willing to invest, the task is more of a marathon than a sprint. Creating a plan for incremental phases of implementation is critical to success. But what goes into such a roadmap? What comes first and what next?

The goal of planning should be to execute regular incremental improvements based on your completed gap analysis and to establish a series of prioritized milestones that lead the organization toward optimized security and improved incident detection and response. The gaps you uncover in that analysis can be translated into goals. Budget, personnel and cultural constraints require that new processes and technologies be implemented in stages.

[1] www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

Once you've identified what you need, what will work in your organization's culture and the way to get there, it is important to realize that building a SOC requires collaboration and communication among multiple functions (people), disparate security products (technology), and varying processes and procedures (processes), as shown in Figure 1.

Triad of Security Operations: People, Process and Technology

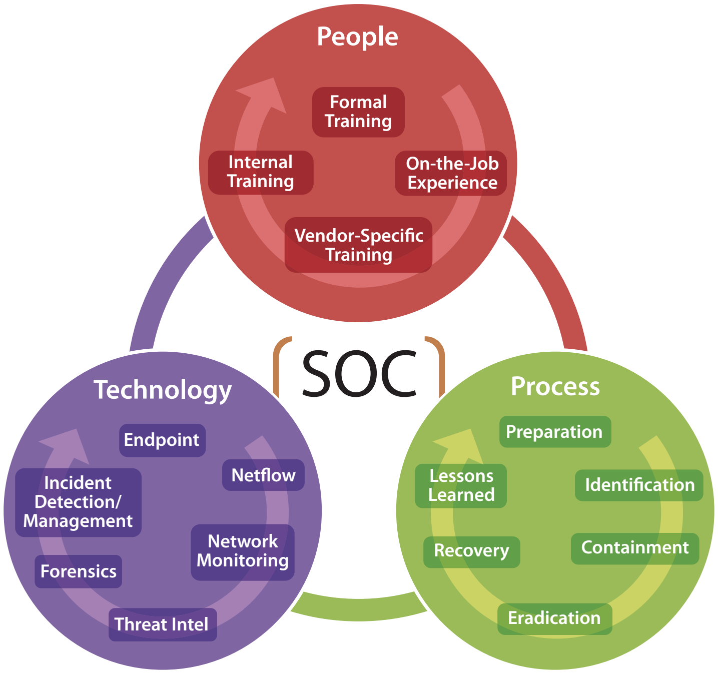


Figure 1. Building Blocks of a SOC

People

Your organization may have employees ready to step in to fill the role of incident responders and SOC analysts, or it may need to evaluate other options, such as outsourcing (via managed security service providers, or MSSPs) or contracting specialists to provide surge incident response (IR) support. For some security teams, a hybrid mix of these options works well. According to the 2014 SANS Incident Response survey,[2] 61% of respondents call upon surge staff to handle critical incidents and 58% have a dedicated response team. It is clear that organizations rarely cover incident response needs completely with in-house staff or completely outsource it. Regardless of your staffing structure, SOC staff must have the necessary training to deal with the constantly changing and often quite challenging job of a security analyst, incident investigator, subject matter expert or SOC manager (see Table 1).

[2] www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

Table 1. SOC Duties and Training Needs

Job Title	Duties	Required Training
Tier 1 **Alert Analyst**	Continuously monitors the alert queue; triages security alerts; monitors health of security sensors and endpoints; collects data and context necessary to initiate Tier 2 work.	Alert triage procedures; intrusion detection; network, security information and event management (SIEM) and host-based investigative training; and other tool-specific training. Certifications could include SANS SEC401: Security Essentials Bootcamp Style.
Tier 2 **Incident Responder**	Performs deep-dive incident analysis by correlating data from various sources; determines if a critical system or data set has been impacted; advises on remediation; provides support for new analytic methods for detecting threats.	Advanced network forensics, host-based forensics, incident response procedures, log reviews, basic malware assessment, network forensics and threat intelligence. Certifications could include SANS SEC501: Advanced Security Essentials - Enterprise Defender; SANS SEC503: Intrusion Detection In-Depth; SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling.
Tier 3 **Subject Matter Expert/ Hunter**	Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure; acts as an incident "hunter," not waiting for escalated incidents; closely involved in developing, tuning and implementing threat detection analytics.	Advanced training on anomaly-detection; tool-specific training for data aggregation and analysis and threat intelligence. Certifications could include SANS SEC503: Intrusion Detection In-Depth; SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling; SANS SEC561: Intense Hands-on Pen Testing Skill Development; SANS FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques.
SOC Manager	Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; communicates with management; serves as organizational point person for business-critical incidents; provides overall direction for the SOC and input to the overall security strategy.	Project management, incident response management training, general people management skills. Certifications include CISSP, CISA, CISM or CGEIT.

In addition to SOC analysts, a security operations center requires a ringmaster for its many moving parts. The SOC manager often fights fires, within and outside of the SOC. The SOC manager is responsible for prioritizing work and organizing resources with the ultimate goal of detecting, investigating and mitigating incidents that could impact the business. A typical SOC organization is illustrated in Figure 2.

Security Operations Center: Organization Chart

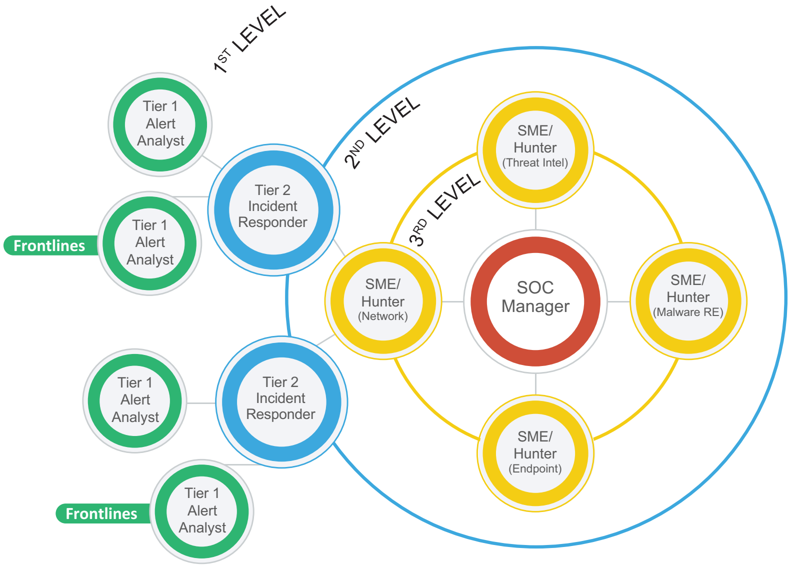


Figure 2. Organization of the SOC

The SOC manager should develop a workflow model and implement standardized operating procedures (SOPs) for the incident-handling process that guides analysts through triage and response procedures.

Processes

Defining repeatable incident triage and investigation processes standardizes the actions a SOC analyst takes and ensures no important tasks fall through the cracks. By creating repeatable incident management workflow, team members' responsibilities and actions from the creation of an alert and initial Tier 1 evaluation to escalation to Tier 2 or Tier 3 personnel are defined. Based on the workflow, resources can be effectively allocated.

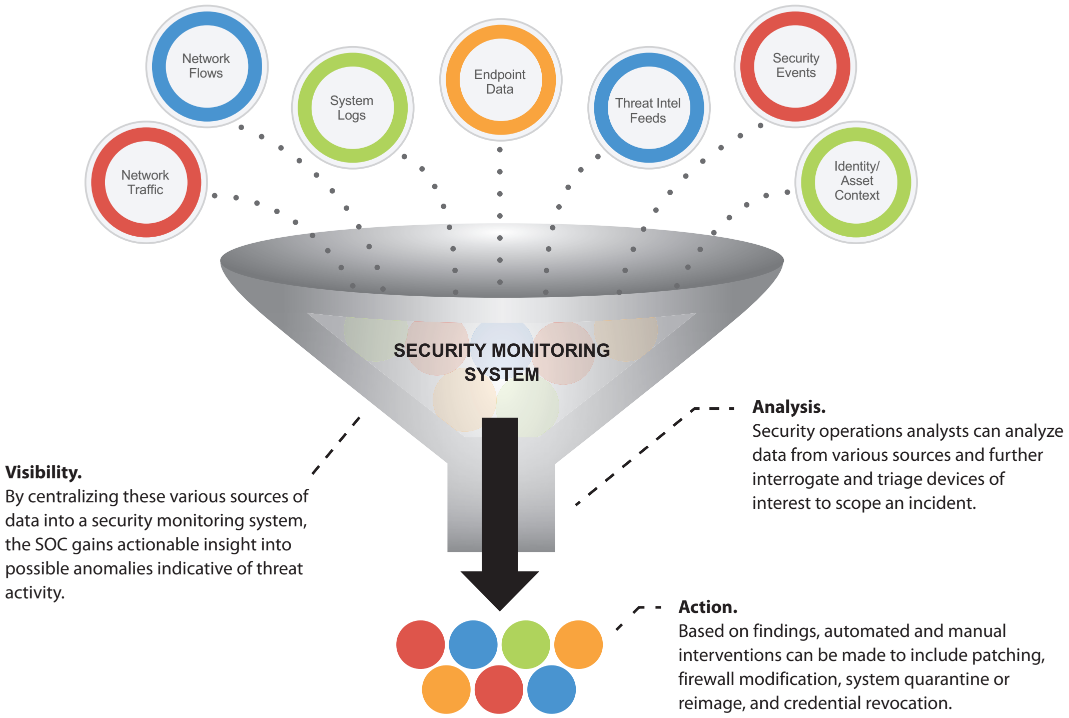
One of the most frequently used incident response process models is the DOE/CIAC model, which consists of six stages: preparation, identification, containment, eradication, recovery and lessons learned. In addition, NIST SP800-61 Revision 2, "Computer Security Incident Handling Guide"[3] provides excellent guidance in developing IR procedures.

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Technology

An enterprisewide data collection, aggregation, detection, analytic and management solution is the core technology of a successful SOC. An effective security monitoring system incorporates data gathered from the continuous monitoring of endpoints (PCs, laptops, mobile devices and servers) as well as networks and log and event sources. With the benefit of network, log and endpoint data gathered prior to and during the incident, SOC analysts can immediately pivot from using the security monitoring system as a detective tool to using it as an investigative tool, reviewing suspicious activities that make up the present incident, and even as a tool to manage the response to an incident or breach. Compatibility of technologies is imperative, and data silos are bad—particularly if an organization has an existing security monitoring solution (SIEM, endpoint, network or other) and wants to incorporate that tool's reporting into the incident management solution (see Figure 3).

Data Aggregation for Improved Incident Handling



Analysis.
Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Visibility.
By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

Action.
Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

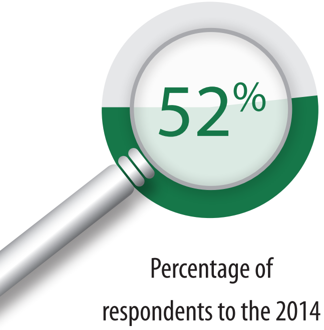
Figure 3. Compatible Technologies Aid Detection

Adding Context to Security Incidents

The incorporation of threat intelligence, asset, identity and other context information is another way that an effective enterprise security monitoring solution can aid the SOC analyst's investigative process. Often, an alert is associated with network or host-based activity and, initially, may contain only the suspicious endpoint's IP address. In order for the SOC analyst to investigate the system in question, the analyst generally needs other information, such as the owner and hostname of the machine or DHCP-sourced records for mapping IP and host information at the time of the alert. If the security monitoring system incorporates asset and identity information, it provides a huge advantage in time and analyst effort, not to mention key factors the analyst can use to prioritize the security incident—generally speaking, higher-value business assets should be prioritized over lower-value assets.

Defining Normal Through Baselining

The ability to create a baseline of activity for users, applications, infrastructure, network and other systems, establishing what normal looks like, is one advantage of aggregated data collected from various enterprise sources. Armed with the definition of "normal," detecting suspicious behavior—activities that are in some way outside of the norm—becomes easier. A properly baselined and configured security monitoring system sends out actionable alerts that can be trusted and often automatically prioritized before getting to the Tier 1 analyst.[4] However, according to the SANS 2014 Log Management Survey, one of the top challenges in utilizing log data cited by respondents is the inability to discern normal from suspicious activity.[5] The lack of such a baseline is a common obstacle organizations face in implementing an enterprise security monitoring system.



Percentage of respondents to the 2014 SANS Incident Response Survey[6] who cited "Little visibility into endpoints/ system configurations and vulnerabilities" as an obstacle for incident response efficiency

A best practice is to use platforms that can build baselines by monitoring network and endpoint activity for a period of time to help determine was "normal" looks like and then provide the capability to set event thresholds as key alert drivers. When an unexpected behavior or deviation of normal activity is detected, the platform creates an alert, indicating further investigation is warranted.

Threat Intelligence

Mature SOCs continually develop the capability to consume and leverage threat intelligence from their past incidents and from information-sharing sources, such as a specialized threat intelligence vendor, industry partners, the cybercrimes division of law enforcement, information-sharing organizations (such as ISACs), or their security monitoring technology vendors. According to the 2015 SANS Cyberthreat Intelligence (CTI) Survey, 69% of respondents reported that their organization implemented some cyberthreat intelligence capability, with 27% indicating that their teams fully embrace the concept of CTI and integrated response procedures across systems and staff.[7] A security monitoring system's capability to operationalize threat intelligence and use it to help spot patterns in endpoint, log and network data, as well as associate anomalies

[4] www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755

[5] www.sans.org/reading-room/whitepapers/analyst/ninth-log-management-survey-report-35497

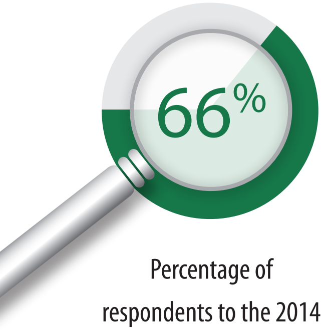
[6] www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

[7] www.sans.org/webcasts/cyberthreat-intelligence-how-1-definitions-tools-standards-99052

with past alerts, incidents or attacks, can enhance an organization's capability to detect a compromised system or user prior to it exhibiting the characteristics of a breach. In fact, 55% of the respondents of the CTI Survey are currently using a centralized security management system to aggregate, analyze and operationalize their CTI.

Obstacles to Efficient SOC Incident Handling

To achieve efficient incident handling, the SOC must avoid bottlenecks in the IR process that moves incidents through Tier 1, into Tier 2, and finally through Tier 3. Bottlenecks can occur due to too much "white noise," alerts of little consequence or false-positives that lead to analyst "alert fatigue." This phenomenon is a common experience among responders, as seen in the 2014 SANS Incident Response Survey results, where 15% reported responding to more than 20 false-positive alarms originally classified as incidents.[8] When choosing an enterprise security monitoring tool, look for such features as alert threshold customization and the ability to combine many alerts into a single incident. Also when incidents include additional context, analysts can triage them more quickly, reducing the layers of evaluation that must take place before an issue can be confirmed and quickly mitigated.



Percentage of respondents to the 2014 SANS Incident Response Survey[9] who identified false alarms as one of the types of incidents they are responding to

[8] www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

[9] www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342

Summary

As you tackle the challenge of building a security operations center (SOC), your ability to anticipate common obstacles will facilitate smooth startup, build-out and maturation over time. Though each organization is unique in its current security posture, risk tolerance, expertise and budget, all share the goals of attempting to minimize and harden their attack surface and swiftly detecting, prioritizing and investigating security incidents when they occur. Working within the constraints of your organization, while pushing the boundaries and striving to achieve its critical security mission, your SOC can be a critical and successful venture—and a key contributor to your organization's continuously improving security posture.

For a more graphic view of building a SOC, be sure to check out the related infographic.

About the Author

Alissa Torres is a certified SANS instructor specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as an incident handler and working on an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic and corporate environments, and she holds a bachelor's degree from University of Virginia and a master's from University of Maryland in information technology. Alissa has served as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

Sponsor

SANS would like to thank this paper's sponsor:

RSA®

Last Updated: July 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	**San Antonio, TXUS**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MAUS**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Hyderabad 2017	**Hyderabad, IN**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Prague 2017	**Prague, CZ**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS New York City 2017	**New York City, NYUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Salt Lake City 2017	**Salt Lake City, UTUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, ILUS**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, AU**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VAUS**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS San Francisco Fall 2017	**San Francisco, CAUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Tampa - Clearwater 2017	**Clearwater, FLUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NVUS**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS Dublin 2017	**Dublin, IE**	**Sep 11, 2017 - Sep 16, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**The Hague, NL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Oslo Autumn 2017	**Oslo, NO**	**Oct 02, 2017 - Oct 07, 2017**	**Live Event**
SANS DFIR Prague 2017	**Prague, CZ**	**Oct 02, 2017 - Oct 08, 2017**	**Live Event**
SANS Phoenix-Mesa 2017	**Mesa, AZUS**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS October Singapore 2017	**Singapore, SG**	**Oct 09, 2017 - Oct 28, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, AU**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
Secure DevOps Summit & Training	**Denver, COUS**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS Tysons Corner Fall 2017	**McLean, VAUS**	**Oct 14, 2017 - Oct 21, 2017**	**Live Event**
SANS Tokyo Autumn 2017	**Tokyo, JP**	**Oct 16, 2017 - Oct 28, 2017**	**Live Event**
SANS Brussels Autumn 2017	**Brussels, BE**	**Oct 16, 2017 - Oct 21, 2017**	**Live Event**
SANS Berlin 2017	**Berlin, DE**	**Oct 23, 2017 - Oct 28, 2017**	**Live Event**
Security Awareness Summit & Training 2017	**OnlineTNUS**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**