Interested in learning more about security?

SANS Institute InfoSec Reading Room

Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems

SANS ANALYST PROGRAM

Sponsored by ArcSight, an H-P Company

Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems

A SANS Whitepaper – April 2011

Written by James Tarala

Goals and Philosophies of the Top 20 Critical Controls

Evaluating the Relationship between the Controls

Critical Controls and SIEM

Post-Implementation Value of SIEM in Light of the Controls

Abstract and Introduction

There is much debate over the reality of cyber war, cyber espionage, the advanced persistent threat (APT). The reality of the current situation is that there are those who intend to violate the confidentiality, integrity or availability of critical data sets. The threat is real, causing damage to systems and leakage of valuable data, and it is difficult to defend against.

Because of this current state of affairs, the Center for Strategic and International Studies (CSIS) and the SANS Institute have collaborated with more than 200 U.S. government agencies and information assurance professionals to develop the the Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines.[1]

These controls were updated in April 2011 to reflect changes in the threat landscape and to introduce additional controls that have been found to be most effective at stopping today's threats. For example, left to operate in silos, security systems take more effort to maintain and potentially leave the organization vulnerable to gaps in their correlation. So an important new recommendation in the April update is the listing of security information and event management (SIEM) systems as a necessary control for visibility and attribution. Because one of the key goals of these 20 critical controls is automation, there must be a central "brain" that can synthesize raw security data feeds: This is the primary function of a SIEM.

As organizations have begun to implement the 20 controls, they are looking for practical guidance on where to start and how to achieve best results in their implementations. This involves prioritizing controls against systems already in place and ultimately implementing a central hub for processing and correlating data sets from information security tools. This paper examines the top 20 controls, with advice on how to get started and an explanation of how SIEM systems can provide a central role in implementing the 20 critical controls effectively.

[1] www.sans.org/critical-security-controls

Goals and Philosophies of the Top 20 Critical Controls

Overall, the 20 critical controls have four main philosophies for implementing security controls that will combat the most significant threats to information systems. The guidelines, posted at SANS.org, describes these philosophies as:

- Defenses should focus on addressing the most common and damaging attack activities occurring today and those anticipated in the near future.
- Enterprise environments must ensure consistent controls across an enterprise to effectively negate attacks.
- Defenses should be automated where possible and periodically or continuously measured using automated measurement techniques where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.[2]

To truly understand the controls, IT managers must read them in light of these four philosophies. There are two controls that are of interest specifically for this discussion:

1. "Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future"
2. "Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible"

Most importantly, these controls must be automated in order to reduce mistakes and complexity. An organization cannot rely on people to perform these tasks manually, yet this is precisely the situation organizations find themselves in today.

When individuals are left to collect and interpret data manually and respond to threats or implement appropriate defensive controls, they often fail in their efforts, leaving systems they're supposed to be protecting vulnerable to attack. Common security principles teach us that if there is a weakness (vulnerability) in a system, then that weakness should be repaired so it no longer represents a risk. With manually implemented controls, the weaknesses are the humans tasked with the responsibility of correlating, interpreting, and responding to threats. An upgraded, automated system, implemented and managed correctly, can remove these human-based weaknesses and system control failures. This does not mean those machines will be infallible. Over time humans will need to fine-tune systems to better interpret and respond to the threats that are discovered. But this is the direction and philosophy that must be entertained.

[2] www.sans.org/critical-security-controls/guidelines.php

Evaluating the Relationship between the Controls

To better understand which approach to take to implement the controls, organizations should consider how the controls interact with each other. Such an undertaking helps better formulate a strategy for implementation. As with planning any other project, begin with the project's end goals in mind before taking the first implementation steps.

A good place to start would be evaluating the overlaps between multiple projects, where resources can be prioritized and reused and efficiencies can be discovered. For instance, imagine an organization was planning on implementing a payroll system and a sales system. Most likely each of those technical systems would require authentication and access control management in order to ensure that only authorized individuals were able to access the information in each system. One approach would be to have each project team implement its own authentication database (resulting in separate databases for the payroll system and the sales system). The second, more efficient, option would be for the teams to utilize a common authentication database that could be extended to future projects as well.

If an organization has a high-level view of all the controls, they would be able to identify overlapping system requirements between each of the 20 controls. One way that application developers often accomplish this task is by using a tool known as the Unified Modeling Language (UML).[3] The Object Management Group (OMG) defines UML in this way:

"The Unified Modeling Language is a visual language for specifying, constructing, and documenting the artifacts of systems. It is a general-purpose modeling language that can be used with all major object and component methods, and that can be applied to all application domains (e.g., health, finance, telecom, aerospace) and implementation platforms."

There are 14 different UML diagram types that are defined by the OMG, all of which can be divided into two categories of diagrams — structural diagrams and behavioral diagrams. Entity relationship diagrams (ERDs) or class diagrams are commonly used to define classes of objects and the attributes associated with each class.

[3] www.omg.org/spec/UML/2.2/

For the sake of this discussion, this concept has been translated from the development world to be used by security engineers to create a holistic view of the 20 critical controls. Diagramming the controls using this methodology reveals the commonalities and overlaps between each of the controls. This will not only help improve efficiencies and reuse, it will also help identify high-priority controls, which are foundational or prerequisite controls used for multiple purposes.

For example, in satisfying Critical Control 1, "Inventory of Authorized and Unauthorized Devices," you might develop an entity relationship diagram (ERD) similar to the one shown in Figure 1.

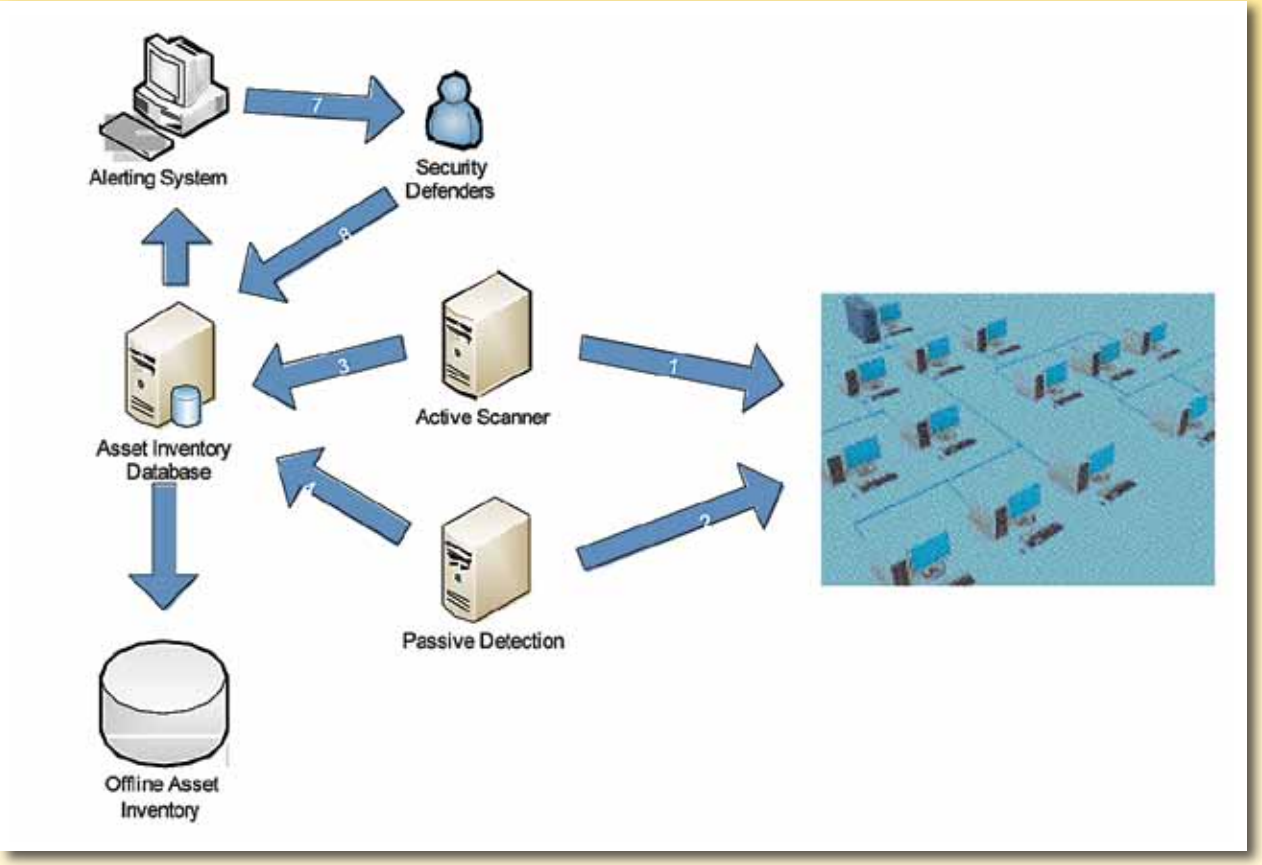

Figure 1. Entity Relationship Diagram for Device Monitoring

A tool such as Microsoft Visio gives organizations the ability to include all of the objects necessary to implement this control. Then, arrows can be used to illustrate the interaction between each of the objects necessary for implementing the control. A security architect could then perform this process for each of the 20 critical controls, which would show all of the objects necessary to successfully implement each control. Once an ERD had been created for each of the 20 critical controls, the architect could lay each of the ERDs side-by-side, as in Figure 2, to look for commonalities.

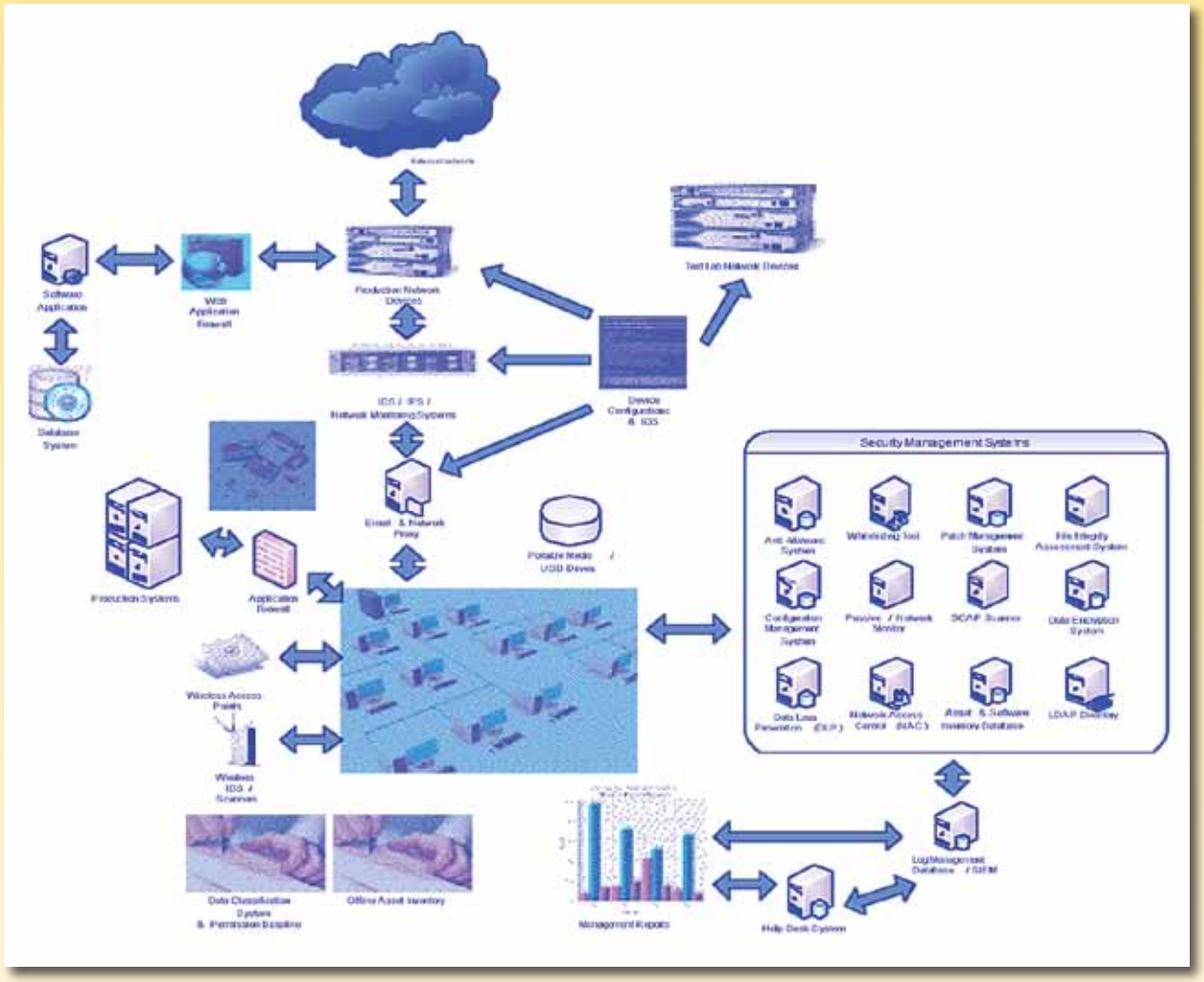

Figure 2. ERDs for the 20 Critical Controls

When the systems required to achieve the goals of each of the 20 critical controls are combined into one ERD, it allows an organization to focus on those systems that are necessary to making the entire program successful. The individual controls that are required for implementing several of the 20 critical controls should be the priority for laying the foundation as a whole. Therefore, these higher priority controls should be attempted prior to other controls.

As you look at the diagram above, organizations will discover that the following systems are repeated throughout the 20 critical controls:

- Security information and event management (SIEM) systems
- Security content automation protocol (SCAP) scanners
- Network traffic capture and monitoring sensors
- Anti-malware whitelisting or file integrity assessment tools

When an organization makes a plan to implement the 20 critical controls as a whole, SIEM should be one of the first controls implemented. Vulnerability scanners (based on SCAP), whitelisting tools, and other specific controls are important, but no specific control is more relied upon for effective control implementation than a SIEM. That's because SIEM can take data from all these tools and more to help organizations understand their vulnerabilities, detect and troubleshoot security incidents and help improve security posture. The next section shows how and where SIEM intersects with 15 of the top 20 controls calling for automation.

Critical Controls and SIEM

Specifically, if you look at the first 15 controls (the controls that are most easily automated) one at a time, you will see that SIEM products can quickly be made to interact with many of them, as illustrated Table 1.

Critical Control	Relationship to SIEM Tools
Critical Control 1: Inventory of Authorized and Unauthorized Devices	SIEM should be used as the inventory database of authorized asset information. SIEMs can use the awareness of asset information (location, governing regulations, data criticality, and so on) to detect and prioritize threats.
Critical Control 2: Inventory of Authorized and Unauthorized Software	As in Control 1, SIEM should be used as the inventory database of authorized software products for correlation with network and application activity.
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Known vulnerabilities are still a leading avenue for successful exploits. If an automated device scanning tool discovers a misconfigured network system during a Common Configuration Enumeration (CCE) scan, that misconfiguration should be reported to the SIEM as a central source for these alerts. This helps with troubleshooting incidents as well as improving overall security posture.
Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	As with Control 3, any misconfiguration on network devices should also be reported to the SIEM for consolidated analysis.
Critical Control 5: Boundary Defense	Network rule violations, like CCE discoveries, should also be reported to one central source (a SIEM) for correlation with authorized inventory data stored in the SIEM solution.
Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	Control 6 is basically a control about SIEMs, which are a leading means for collecting and centralizing critical log data; in fact, there is even a subcontrol for analysis that studies SIEM specifically. SIEMs are the core analysis engine that can analyze log events as they occur.
Critical Control 7: Application Software Security	Like CCE scan results, vulnerabilities that are discovered in software applications should also be reported to a central source where these vulnerabilities can be correlated with other events concerning a particular system. SIEMs are a good place to store these scan results and correlate the information with network data, captured through logs, to determine whether vulnerabilities are being exploited in real time.
Critical Control 8: Controlled Use of Administrative Privileges	When the principles of this control are not met (such as an administrator running a web browser or unnecessary use of administrator accounts), SIEM can correlate access logs to detect the violation and generate an alert.

Table 1: Mapping Controls to SIEM

Table 1 continued on next page

Critical Control	Relationship to SIEM Tools
Critical Control 9: Controlled Access Based on Need to Know	SIEM can correlate user activity with user rights and roles to detect violations of least privilege enforcement, which is required by this control.
Critical Control 10: Continuous Vulnerability Assessment and Remediation	SIEM can correlate vulnerability context with actual system activity to determine whether vulnerabilities are being exploited.
Critical Control 11: Account Monitoring and Control	Abnormal account activity can only be detected when compared to a baseline of known good activity. The baseline to meet this control should be recorded by the SIEM; and, as future snapshots or baselines are recorded, they can be compared to the approved baseline in the SIEM.
Critical Control 12: Malware Defenses	Malware that is discovered should be recorded according to this control. Centralized anti-malware tools should report their findings to a SIEM, which correlates against system and vulnerability data to determine which systems pose greater risk due to the malware discovered on that system.
Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services	Like CCE scan results, if a system has a running port, protocol, or service that has not been authorized, it should also be reported to a central source where these vulnerabilities can be correlated with other events concerning a particular system. SIEMs can monitor log data to detect traffic over restricted ports, protocols, and services. Organizations can use these controls to determine which ports and services are useful for business, which are not, and which types of traffic and ports to limit.
Critical Control 14: Wireless Device Control	Device misconfigurations and wireless intrusions should be reported to a central database for incident handling purposes. A SIEM is a perfect candidate to consolidate this information and use it for correlation or detection of threats to wireless infrastructure.
Critical Control 15: Data Loss Prevention	As with Control 5, data loss rule violations, like CCE discoveries, should also be reported to one central source such as a SIEM, which can correlate data loss events with inventory or asset information as well as other system and user activity to detect complex breaches of sensitive data.

Table 1: Mapping Controls to SIEM

In short, a SIEM, when properly configured, has the capacity to become the central nervous system of a network, collecting and processing data feeds that are given to it and therefore meets many of the top 20 requirements for automation. This allows organizations to leverage an intelligent, continuous monitoring system that can take responsibility for the securing networks from the physical layer to the application layer 24/7/365.

Post-Implementation Value of SIEM in Light of the Controls

The business benefits integrating SIEM with the 20 critical controls are significant. SIEM implementations enable organizations to better manage risk, gather actionable security metrics, and audit the effectiveness of their control implementations.

Risk Management

Regardless of the risk model that an organization subscribes to, they will always encounter two common elements: vulnerabilities and threats. SIEMs can show an organization where the vulnerabilities exist and whether they are being actively exploited by internal or external threats. The consolidation and correlation of alerts from widely used security tools (firewalls, intrusion detection/prevention tools, data leakage protection tools, and so on) with event logs from base infrastructure (for example, hosts, databases and applications) enables SIEM to detect the sophisticated and complex threats facing modern enterprises.

In addition, SIEM—when integrated into vulnerability, whitelisting, end point and security monitoring systems—gives a better picture of the organization's risk posture. In this context, the controls are like a mirror that reflects the organization's information security maturity. By supporting the trending of security information, SIEM gives visibility into the organization's risk posture for ongoing improvements.

Ongoing, Actionable Metrics

Built into version 2.3 and later versions of the 20 critical controls are a set of metrics meant to help an organization to implement the critical controls. The metrics are written in such a way as to measure how effectively an organization is meeting the spirit of the controls.

For example, the goal of Control 1 is to allow only authorized devices to connect and utilize the organization's network. Therefore, the metric and evaluation are to add unapproved devices to the network, see if they are able to access resources, and measure how long it takes before these devices are isolated and are no longer able to access the network. If the SIEM is configured to keep an inventory of all authorized devices and information regarding new devices is reported to the SIEM, then the SIEM should be able to record when these devices were first discovered and how long they were actually on the network. Thus, the SIEM is able to record metrics on how well an organization is meeting the goals of the controls. Ultimately this is meant to facilitate continuous process improvement and help business owners establish thresholds for levels of acceptable risk in the organization.

[9] www.us-cert.gov/control_systems/pdf/Catalog%20of%20Recommendations%20March%202010.pdf

Auditing the Effectiveness of Controls

If the above goals have been met, then this leads to a third post-implementation goal that SIEMs have the opportunity to provide: assisting with effective auditing of the organization's controls. The hope is that by establishing risk thresholds and appropriate metrics based on the 20 critical controls, auditors will be able to measure an organization on those aspects of risk that actually impact the security of the systems.

Today many auditors know that how long unauthorized devices are on a network would be valuable data to have, particularly if this device connection information can be gathered over a long period of time. However, most auditors have no way to perform this type of assessment in the scope of a given audit; therefore, although most would agree this information is important, it is rarely if ever measured. A SIEM, properly configured to the 20 critical controls, can record this information, save it over long periods of time, and report that information to auditors. Auditors can then use this information to evaluate the risk level of the organization's systems and whether appropriate controls exist. Only after the SIEM is implemented does this information become available.

Things to Keep in Mind

Organizations that leverage SIEM to monitor the enforcement of the 20 critical controls can gain value from their SIEM systems. However, here are some important things about SIEM to keep in mind:

1. Most SIEM products have not been designed with the 20 critical controls in mind.
2. SIEMs are useful only if they are configured and able to handle all the relevant event data feeds.
3. Consolidated data feeds are useful only if the SIEM can automate the business logic and analysis required to detect sophisticated threats and evaluate risk.
4. Alerts from business analytics in any SIEM are only worth the investment if they are acted upon.

SIEM that is truly adaptable to an organization's business model and metrics will be the most valuable.

Conclusion

Security threats are dynamic in nature and exploits are constantly evolving as attackers grow ever more organized, precise and persistent. Therefore, the controls used to protect information systems also need to be dynamic enough to respond to the evolving nature of today's threats. This is the purpose of the 20 critical security controls.

No matter how the threats evolve, the collection and correlation of system, network, user, and application activity will continue to play pivotal roles in the 20 critical controls guidelines. As threats and security events evolve, SIEM vendors and the information security community must work together to build relevant and actionable business analytics into their systems. By continuously improving recommendations and the controls to support those recommendations, SIEM products can become true information security hubs that not only automate audits, but also provide proactive means to protect the organization.

If implemented properly, SIEM can provide the visibility that organizations need to trend and improve their risk postures over time—which is the ultimate goal of the 20 critical controls. As such, SIEM or SIEM-like technologies for centralization and consolidation of an organization's security data will continue to be important investments for organizations wanting to accurately respond to threats and ultimately improve their risk and compliance postures.

About the Author

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent a large amount of time assisting organizations in their security management, operational practices and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing 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.

SANS would like to thank this paper's sponsor

Last Updated: May 24th, 2017

Upcoming SANS Training

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

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced