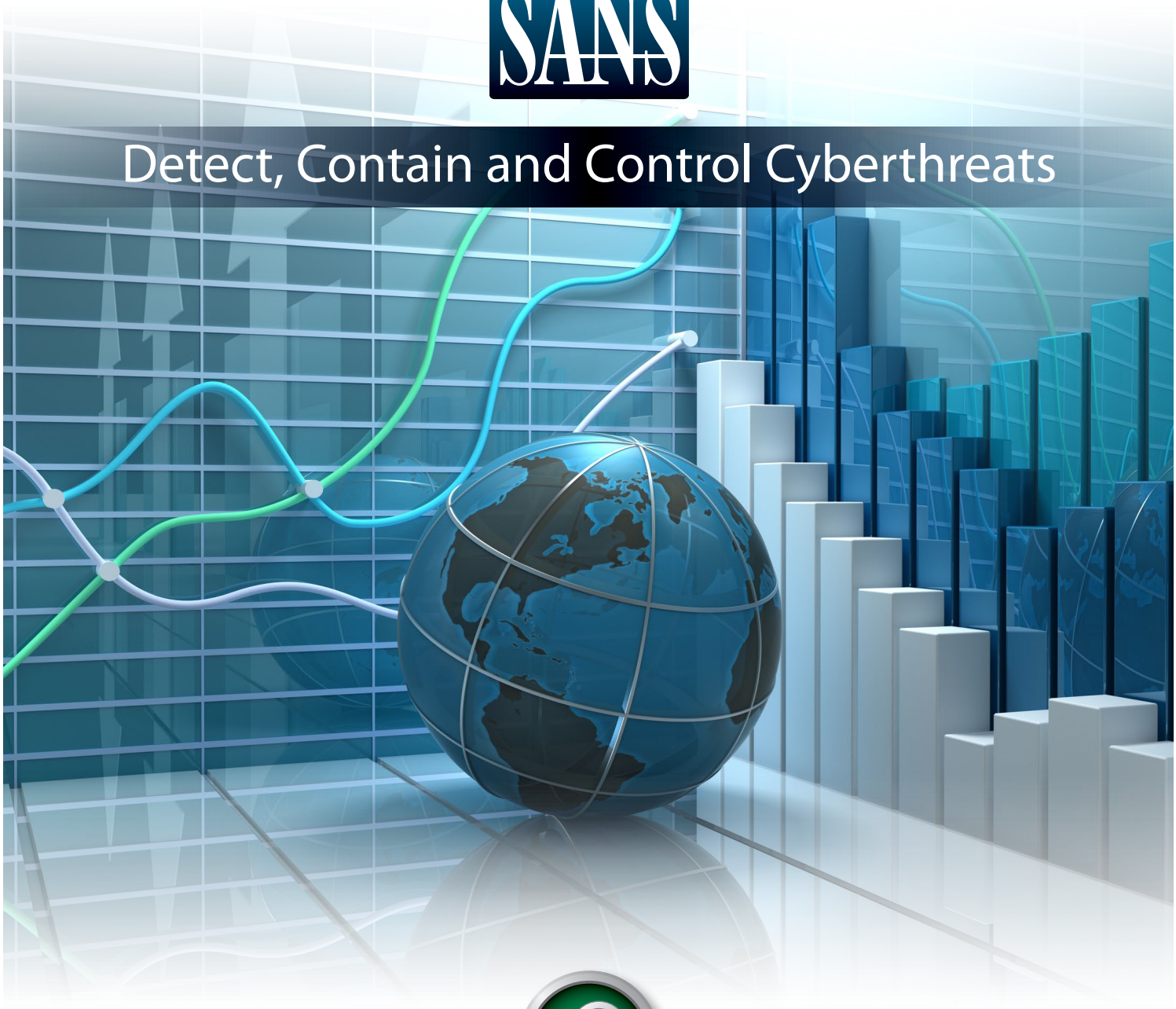
Detect, Contain and Control Cyberthreats

Eric Cole, PhD

Detect, Contain and Control Cyberthreats



A SANS Whitepaper

Written by Eric Cole, PhD

June 2015

Sponsored by
Raytheon|Websense

Introduction

Today, every organization is a target and attackers can compromise any organization. Large-scale compromises used to be a surprise, but now they are a reality that is often accepted. The means, methods and techniques that adversaries use to target and ultimately compromise organizations have caused a shift in mind-set. It is not a matter of *if* an attacker will compromise an organization, but *when* an attack will occur.

DWELL TIME
Relates to damage because the longer a system is compromised, the bigger the impact.

Although prevention is ideal, not all attacks can be prevented, making compromise inevitable. Therefore, a better approach to security is timely detection of the attack—detection that will contain and control the damage. Organizations that cannot detect and control the damage of an attack will cease to exist, while those that can implement effective security to minimize the impact of attacks will be the successful entities of the future.

In recognizing that attackers will succeed, the goal becomes minimizing the exposure and damage. This correlates into two key metrics:

LATERAL MOVEMENT
Is closely tied to dwell time. An adversary will try to cause more damage by trying to move within an organization, similar to the way cancer spreads in the body, compromising as many systems as possible.

- **Dwell time.** This includes the time from when someone clicks (you are compromised) until the time the malware is no longer effective, whether that be by blocking command and control so it cannot communicate or by taking the compromised box(es) off the network. This directly relates to damage, because the longer a system is compromised, the bigger the impact. This is a very similar approach to disease, where the goal is prevention and early detection, because the longer disease can exist within a body, the more damaging and lethal it is to the individual. Controlling dwell time means early detection with appropriate response.
- **Lateral movement.** Closely tied to dwell time and in a fashion similar to cancer spreading in a body, an adversary will try to cause more damage by trying to move within an organization, compromising as many systems as possible.

As organizations build mature security programs, it is critical that they detect attacks early (reduce dwell time) and control the damage (limit lateral movement).

When designing, deploying and building networks, organizations must assume that the networks will be compromised. Trying to fix every vulnerability within an organization is an unreasonable goal, but prioritizing mitigation efforts based on known risks and high-value targets can lead to success.

Organizations also need to focus on two key characteristics of risk: likelihood and impact, because not all threats are equal. An organization should prioritize threats that are likely to occur and in the process cause great damage.

To help keep your organizations aligned on containment and control, before you spend a dollar of budget or an hour of time on security problems, you should always ask three questions:

- What are my high-value targets—data, machines and personnel?
- What are the risks if these high-value targets are compromised?
- What are the most cost-effective ways of reducing risks?

The answers to these questions will help you prioritize risks and deploy appropriate defenses. This paper will help define strategies and tactics for this approach.

The Changing Threat Landscape

Over the past several years, the means and methods that attackers use to compromise an organization have changed dramatically. In the past, attacks were visible and opportunistic, targeting low-hanging fruit and operating on a large scale. Therefore, many of the security technologies and solutions developed in response to such attacks focused on looking for specific ways an attacker worked, typically through signature-based detection. However, today's organizations are grappling with advanced threats that are stealthy, targeted and data-focused, rendering traditional security defenses ineffective.

Traditional attacks targeted servers in an organization's so-called demilitarized zone (DMZ), or perimeter network—typically hosting outward-facing services such as email and web—and exploited vulnerabilities in those systems. Even if attackers were able to compromise such a server, the machine was isolated on a separate network and did not contain sensitive data. Today's attackers target insiders within a network and employ victims as points of compromise.

Although this sounds like the work of sophisticated attackers, in reality the *tools* have become more capable, while the people behind the tools no longer need to be experts to take advantage of vulnerable systems. The increasing sophistication of cyberthreats is depicted in Figure 1.

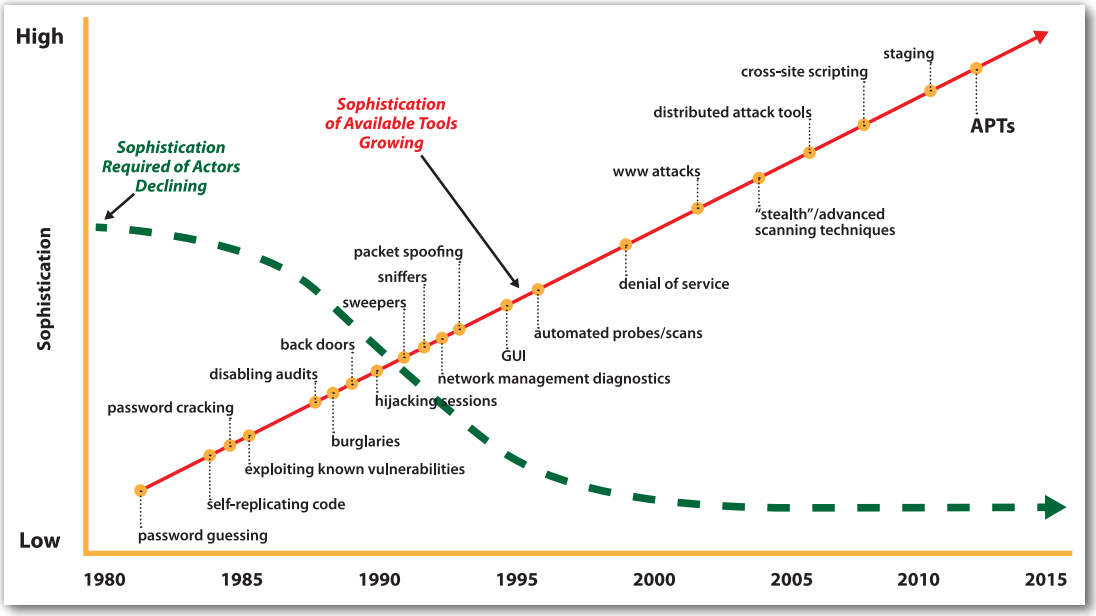


Figure 1. Evolution of Cyberthreats

When people think about computer attacks, they often visualize them as external threats. Although this is often true, it is important to differentiate between the source of a threat and the cause of damage. Although the source of most threats may be external, internal threats are increasingly real and on the minds of security analysts and IT managers. The 2015 SANS survey on insider threats showed that threats from malicious and negligent employees concern most organizations: 74 percent of respondents cited employees, rather than contractors, as their greatest headache.[1]

When people hear *insider threat*, many initially think of malicious threats such as an embezzler or data thief—someone within the organization who deliberately and maliciously wants to cause harm. Although that certainly is one form of insider threat, more likely threats come from accidental insiders, people an attacker tricks or manipulates into doing something they normally would not do if they knew the true intent. Modern security solutions must address such accidental insiders.

[1] "Insider Threats and the Need for Fast and Directed Response," www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892, pg. 6, Figure 4.

Current Challenges

If an organization cannot detect an attack in a timely manner and limit the dwell time, the damage an attack causes will be significant. Modern IT security means putting more focus on internal detection and controlling the damage.

Organizations that focus on external prevention continue to struggle with security. Although they can prevent some attacks, many others can easily slip past preventive measures and compromise internal systems. If an organization cannot detect an attack in a timely manner and limit the dwell time, the damage an attack causes will be significant. Modern IT security means putting more focus on internal detection and controlling the damage.

As attacks continue, organizations are willing to invest more money toward the security budget, but finding the correct types of skilled personnel remains one of the most significant challenges. Given this constraint, the goal for almost every IT department is to automate security and present information in an intuitive, easy-to-use manner that facilitates timely and appropriate action to mitigate risks within the organization. Automating this processing and analysis with proper tools allows the security operations center (SOC) to see just the information that security teams need for damage control, keeping the noise in the background where it belongs. Table 1 compares automated and manual approaches.

Table 1. Automated Versus Manual Approaches to Processing and Analysis

	Pros	Cons
Automated	• Fast • Predictable • Scalable • Able to process large amounts of information	• Must be properly configured • Cannot perform detailed analysis • Could miss critical information
Manual	• Able to perform high-end analysis • Enables in-depth correlation • Facilitates ad hoc analysis and discovery	• Slow • Not scalable • Limited ability to process large amounts of information

Contextual visualization and filtering are two ways to provide security teams with useful intelligence that is both intuitive and actionable. The saying "a picture is worth a thousand words" is especially true when it comes to security; visual formats can simplify the processing of large amounts of information and threat alerts. Meanwhile, filtering ensures that the information the security team receives is of high value, with as little "noise" as possible. Every device on a network generates traffic, which can be overwhelming from an analysis perspective. Only through proper filtering can information of value be discovered.

Ultimately, the security team will benefit from a more efficient way to visualize data and metrics. Clear visualization and prioritization enables staff to better use valuable intelligence, which in turn leads them to make decisions in a timely manner. Although a comprehensive dashboard helps, multiple dashboards will hinder the security team's ability to focus on the most valuable data. Ultimately, what matters most is the data feeding the dashboard.

Dashboards must combine automated and manual information; they cannot just provide data, but must facilitate cognitive reasoning and quick response. This in turn requires sophisticated visualization features that include high-end data aggregation, scrubbing and correlation. Such capabilities will enable incident responders to make proper decisions while offering them an intuitive visual console. A "single pane of glass" view of relevant data will enable security analysts to drill down and discover insights and patterns.

The typical gated community reflects traditional approaches to designing and implementing IT security, with a defined perimeter and controlled access through it. Such communities may keep some "undesirables" out of the development, but they are vulnerable to anyone the guards recognize or who can jump over the fence. Likewise, an organization may have the best firewall available, but attackers who bypass it might find themselves in a network that is wide open because of a flat design, which makes it easy for them to access any information they want.

Instead, let's look at the example of the residences within the gated community, each with an alarm system and locks of its own: there is a clear division of control between each home. If burglars hit one house, they do not find it easier to rob another, which means the amount of damage is managed and controlled. In a similar vein, networks within an organization should be highly segmented, thereby limiting the reach of any single machine. This way, if attackers compromise one system, they find it no easier to compromise others. Such segmentation also helps catch attacks early and control lateral movement into more sensitive areas in the network.

If an organization does not know what devices are on its network and how they are configured, is unable to manage change or does not know where its critical data is located, its security is doomed to fail.

Although highly segmented networks are one of the more practical defensive tactics to follow, organizations must have proper foundational items in place for any defensive effort to succeed. The four components of a solid cybersecurity foundation are shown in Figure 2.

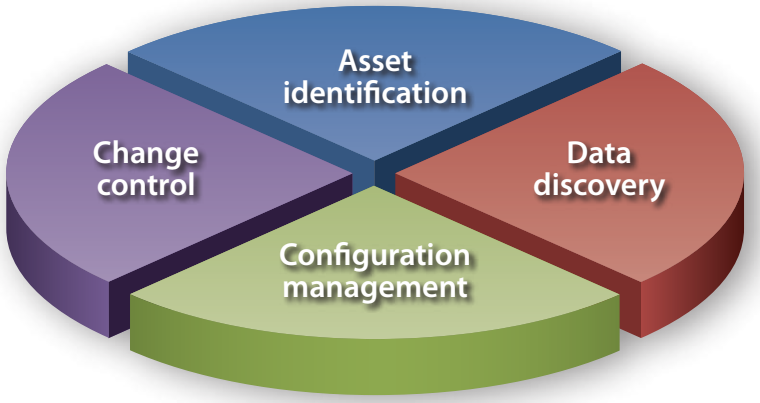


Figure 2. Components of a Sound Cybersecurity Foundation

If an organization does not know what devices are on its network and how they are configured, is unable to manage change or does not know where its critical data is located, its security is doomed to fail. Although no solution on its own will stop attackers—they will always find a way into a system—a layered approach to security can provide a sound foundation.

Prioritizing and focusing on high-quality information in an appropriate contextual perspective leads to useful intelligence. Consequently, contextual awareness leads to appropriate and timely decisions, which reduces dwell time and controls overall damage.

Proper IT security is not about the *quantity* of information; it is about its *quality*. Large amounts of useless information can distract the security team, but prioritizing and focusing on high-quality information in an appropriate contextual perspective leads to useful intelligence. Consequently, contextual awareness leads to appropriate and timely decisions, which reduces dwell time and controls overall damage. Ultimately, a smarter approach to security requires a single visual interface with integrated metrics, one that visually allows an IT security team to quickly understand what is happening across the enterprise network, discover patterns, derive insights, and make effective and informed decisions.

For information to be truly useful, understanding the context of the information and what is actually occurring is essential. Security analysts can then prioritize and focus on the information that really matters, in turn enabling fast and decisive action; a clear visual interface is an essential tool for such work.

Detect, Contain and Control—Pillars of Success

Effective security solutions must align with how attackers work and focus on controlling the amount of damage an organization will experience. If compromise is inevitable, then the next best approach is to contain and control threats so damage is limited. One way to approach this problem is to think of three pillars, as we see in Figure 3.

Figure 3. Pillars of Cybersecurity Success

These five points expand on the three pillars of success: detection, containment and control:

1. **Use security tools with end-to-end visibility across the entire organization.** Correlating the universe of activity is essential to a full understanding of what is happening during an attack. Advanced threats are stealthy by design; if a security device is looking at only one aspect, it will most likely miss the attack. Point solutions alone are not effective. An all-encompassing view of the network with visibility into what is transpiring across the enterprise is necessary when attempting to detect and contain harmful activity.

2. **Beware of information overload; too much visibility is almost as bad as too little.** Understanding the context of data is critical because attackers will try to mimic the patterns of normal user activity. Filtering out noise and focusing on the activities that really matter are the ways to a better understanding of contextual awareness, which requires correlating current activities with "known good" behavior to gain intelligence on what an adversary is doing and how. Gathering information on user activity helps provide proper contextual awareness of what is happening. For example, a user copying a 500MB file on a Saturday could be a problem, but understanding the context requires knowledge of the user's other activities. Combining this intelligence with analytical capabilities provides specific insight into what a potential adversary is doing, which can be a basis for early detection, thereby containing a potential attack and controlling the overall damage to the organization.

3. **Get security solutions that perform real-time analysis.** Speed is essential when fighting an attack, and there's just no substitute for real-time analysis. Of course, the success of such analysis requires the filtering of noise, so the security solution can work with just the information that is likely to detect an attack. Data-driven intelligence is the key to quickly identifying, controlling and minimizing the damage caused by an attacker. This information needs to be presented to SOC analysts in a manner that enables them to make proper decisions. An intuitive visual interface based on cognitive research clearly displays what is happening, with proper context.

4. **Reduce the dwell time an adversary spends within a network.** The longer an organization is compromised, the greater the overall damage. Therefore, this is the most important point of all. Early detection and controlling the adversary are vital to reducing overall dwell time—and thereby reducing damage and related costs.

5. **Implement an in-depth defense.** Because adversaries often cannot directly break into the system they want to compromise, they will look for one that can be compromised and use it as a pivot point to go deeper into the network. Such lateral movement allows an adversary to cause more damage, which makes it even more surprising that many organizations focus on perimeter protection and completely miss internal activity. Effective security solutions must monitor the internal network, detect when systems are compromised, and be able to recognize the attacker's lateral movements.

The most important point of all: Early detection and controlling the adversary are vital to reducing overall dwell time—and thereby reducing damage and related costs.

In each case, the three pillars of successful defense represent challenges and opportunities for both evolving and mature security models.

Monitoring and Metrics

Recognizing the speed and persistence with which adversaries break into systems, security is no longer just about setting up some devices at the network edge. It instead requires continuous monitoring with timely response—the most effective ways to minimize dwell time. Meeting this requirement has led many businesses to hire security analysts, or even establish a SOC. In the simplest sense, a SOC is responsible for monitoring and responding to the intelligence the organization's security devices generate.

Many IT departments struggle when standing up their SOCs with establishing an appropriate focus for their work and defining the information that analysts can have; in other words, how to monitor. From an analyst's perspective, the most important part of monitoring—with or without a SOC—is to have an effective, properly designed visual interface. It should be easy to use and must be able to show the analysts what is happening within the organization, providing situational awareness across the network and—given the growing use of cloud services—beyond. The visual interface must enable analysts to drill down into events, to better understand what is happening and verify the accuracy of the information to make effective and actionable decisions.

Visual Interfaces

From an analyst's perspective, the most important part of monitoring is to have an effective, easy to use and properly designed visual interface that:

- Provides the right metrics for analysts to know what is happening within the organization
- Provides situation awareness across the network and beyond
- Integrates with other systems

The most important part of visual interface design is the data it measures and displays to the analyst. The single-pane-of-glass approach is critical if analysts are to discover abnormal activity in a timely fashion. Any visual interface must be properly integrated with other systems and provide accurate and clear information. The problem is not that security teams need more metrics. Instead, they need the *right* metrics: data they can easily measure and act upon. Any monitoring interface must be dynamic, constantly tracking the adversary and providing information in a manner that leads to prompt and appropriate decisions.

If the security dashboard is to clearly show deviations from normal activity, the metrics behind the dashboard must quantify the difference between normal and hostile activity. Security analysts need an intuitive, easy-to-use interface with visualization capabilities, so they can quickly see what is happening in their environment. The most critical metrics are those that are associated with data flows, both within a network and outbound. Monitoring suspicious connections—and the amount of information flowing over them—makes it possible to identify deviations caused by adversaries and take proper action.

Conclusion—A Path for the Future

Many people try to minimize the frequency of illness, but when they do get sick—because we all do—their goal is to minimize the impact of the illness. In cybersecurity, the goal is the same: minimizing the frequency in which an organization is compromised and, when a compromise occurs, responding swiftly to minimize the damage and exposure to the organization.

A key component of a successful security program is a SOC that can monitor and respond to attacks in a timely manner. An effective SOC relies on key metrics such as reducing dwell time and minimizing lateral movement, information that feeds into a dashboard and gives security analysts visibility into what is happening within an organization. By focusing on useful intelligence and implementing tools that enable real-time analytics, organizations can ensure analysts get the information they need, when they need it, to maintain proper security across the organization.

About the Author

Eric Cole, PhD, is a SANS Faculty Fellow, course author and instructor who has served as CTO of McAfee and chief scientist at Lockheed Martin. He is credited on more than 20 patents, sits on several executive advisory boards and is a member of the president's Commission on Cyber Security. Eric's books include *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible* and *Insider Threat*. As founder of Secure Anchor Consulting, Eric puts his 20-plus years of hands-on security experience to work to help customers build dynamic defenses against advanced threats.

Sponsor

SANS would like to thank its sponsor:

Raytheon | websense®

Last Updated: July 22nd, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2019	Riyadh, SA	Jul 28, 2019 - Aug 01, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Melbourne 2019	Melbourne, AU	Aug 05, 2019 - Aug 10, 2019	Live Event
Security Awareness Summit & Training 2019	San Diego, CAUS	Aug 05, 2019 - Aug 14, 2019	Live Event
SANS London August 2019	London, GB	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Crystal City 2019	Arlington, VAUS	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Prague August 2019	Prague, CZ	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Minneapolis 2019	Minneapolis, MNUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS San Jose 2019	San Jose, CAUS	Aug 12, 2019 - Aug 17, 2019	Live Event
Supply Chain Cybersecurity Summit & Training 2019	Arlington, VAUS	Aug 12, 2019 - Aug 19, 2019	Live Event
SANS Virginia Beach 2019	Virginia Beach, VAUS	Aug 19, 2019 - Aug 30, 2019	Live Event
SANS Amsterdam August 2019	Amsterdam, NL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Chicago 2019	Chicago, ILUS	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS MGT516 Beta Three 2019	Arlington, VAUS	Aug 19, 2019 - Aug 23, 2019	Live Event
SANS New York City 2019	New York, NYUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, DK	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Hyderabad 2019	Hyderabad, IN	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Philippines 2019	Manila, PH	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Brussels September 2019	Brussels, BE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Canberra Spring 2019	Canberra, AU	Sep 02, 2019 - Sep 21, 2019	Live Event
SANS Munich September 2019	Munich, DE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Network Security 2019	Las Vegas, NVUS	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, NO	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS Dubai September 2019	Dubai, AE	Sep 14, 2019 - Sep 19, 2019	Live Event
SANS Raleigh 2019	Raleigh, NCUS	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Paris September 2019	Paris, FR	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Rome September 2019	Rome, IT	Sep 16, 2019 - Sep 21, 2019	Live Event
Oil & Gas Cybersecurity Summit & Training 2019	Houston, TXUS	Sep 16, 2019 - Sep 22, 2019	Live Event
SANS Bahrain September 2019	Manama, BH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
DFIR Summit & Training 2019	OnlineTXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced