What Security Practitioners Really Do When It Comes to Security Testing

Matt Bromiley

SANS

A SANS Spotlight

What Security Practitioners Really Do When It Comes to Security Testing

(Part 2 of Are Your Security Controls Yesterday's News?)

Written by **Matt Bromiley**

October 2019

Sponsored by:

Cymulate

Introduction

Take a moment to consider your current security control testing procedure(s). Do you perform scheduled, scope-limited penetration tests because you're required to? Do you simply let the vulnerability scanner do its thing and hope the attackers don't do the same? Or are you unsure about how you're testing your controls?

In the first of this duo of spotlight papers,[1] we discussed why security controls testing should not be constrained by scope-limited penetration tests or tests using attacks that do not mimic true threat actor activities. In conjunction with that paper (which we will call Part One), SANS ran a poll asking respondents to provide data about their current security control testing procedures. We explore that data in this paper.

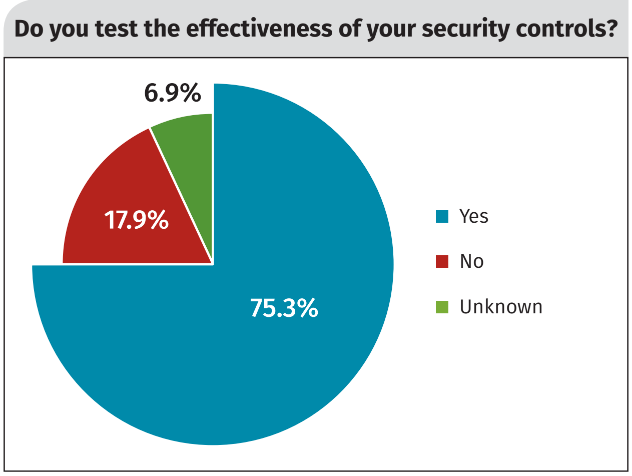


Figure 1. Poll Responses to Question About Effectiveness of Security Controls

Across our 366 poll respondents from the security community, approximately 75% indicated they do in fact test the effectiveness of their security controls, as illustrated in Figure 1. The rest of this paper will discuss additional details provided by this majority, but that still leaves us with approximately 25% who either do not test or are unsure if they do.

> Whether you're testing your security controls or not, one truth remains: Attackers don't care about scope.

[1] "Are Your Security Controls Yesterday's News?" www.sans.org/reading-room/whitepapers/analyst/security-controls-yesterday's-news-39065. Registration required.

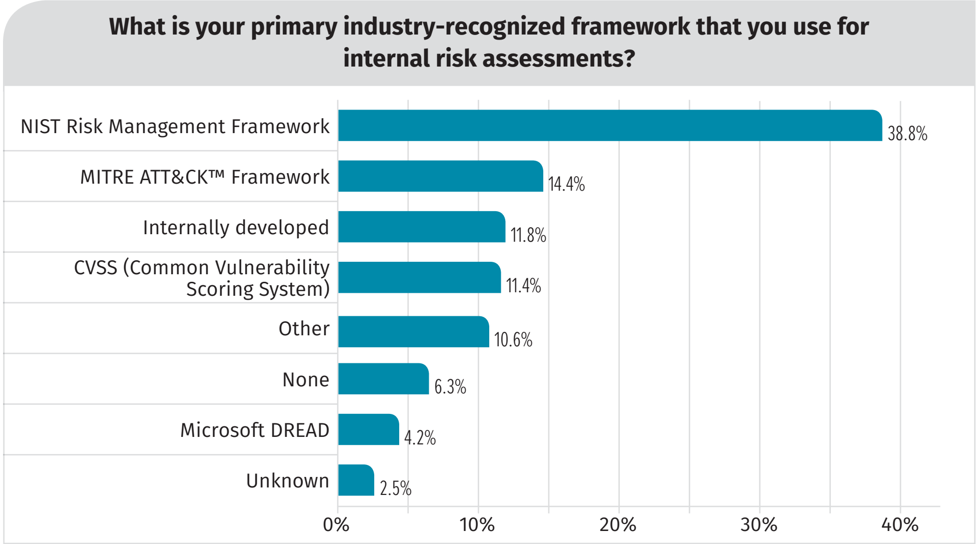
Although it's the theme of this spotlight series, it bears repeating: You should be testing your controls! If you are not testing your security controls, there's a chance someone else is. And they don't produce a pretty report at the end.

> *If you are not testing your security controls, there's a chance someone else is. And they don't produce a pretty report at the end.*

Getting It Right

Effective security control testing doesn't occur overnight; organizations will typically align their testing with various security frameworks that provide a useful scope of reference. In this survey, approximately 39% of our respondents indicated that they use NIST's Risk Management Framework,[2] with MITRE's ever-popular ATT&CK™ Framework coming in at just under 15%. As seen in Figure 2, organizations also utilize internally developed frameworks, CVSS and others.

Choosing the right framework for security control testing contributes significantly to the success of the testing. Typically, security teams and/or organizations may gravitate to compliance-type frameworks, ones with checkboxes that can represent a false sense of security and defense. Threat actors have shown repeatedly that they do not care about compliance standards or hypothetical defenses.



What is your primary industry-recognized framework that you use for internal risk assessments?

Figure 2. Poll Responses to Question About Which Primary Framework Respondents Use for Internal Risk Assessments

Instead, we recommend aligning with a framework that provides the foundation to identify and test against "real-world" threats, whether they are employed by a particular threat actor or something that is commonly exploited. MITRE's ATT&CK™ Matrix can start your security team thinking about the many methods by which a threat actor may escalate privileges, for example. By being able to test and verify against those techniques, you can start to limit what a "real" threat actor could do if they breached the environment.

This type of scenario-based testing may not necessarily be threat-actor based, but you will find yourself mitigating a lot of commonly used techniques by attackers of all skill levels. On the topic of relevant scenarios, we also asked our respondents to rank scenarios in terms of criticality with respect to their organization. The top-ranked critical scenario, as shown in Figure 3 on the next page (where the lower the score, the higher the criticality) was an attack on consumer-facing applications. A close second and third place were the ability to detect file-less and signature-less attacks and spear-phishing, respectively.

[2] "Risk Management," https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

Rounding out our ranked threat actor scenarios were concerns such as exfiltration of data, unsafe browsing habits, ransomware and compromise of critical assets. Given the recent wave of highly targeted and coordinated ransomware attacks, we've seen that these attacks can potentially cause more technical and financial damage than other types of attacks.

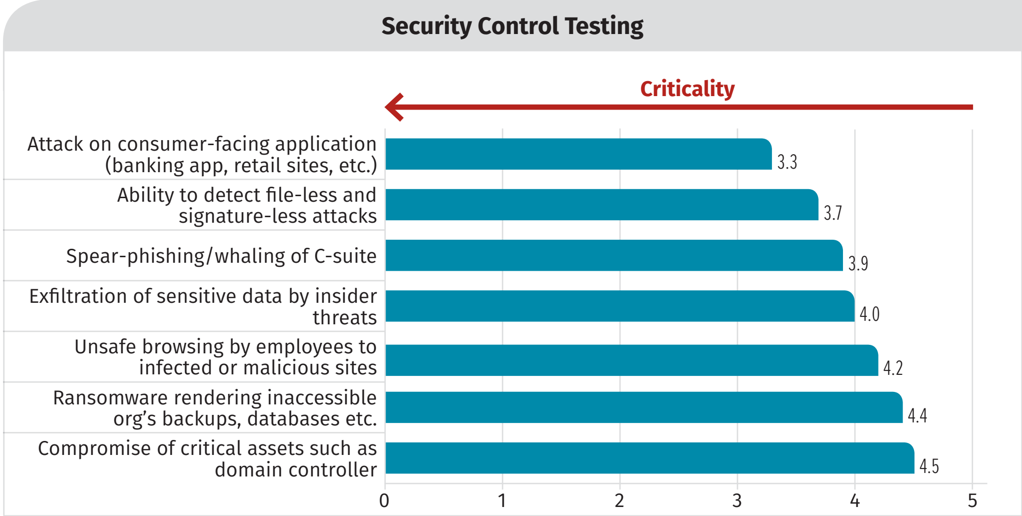


Figure 3. Ranking of Scenarios According to Perceived Criticality

However, organizations that utilize technique-based frameworks for their security control testing can rest easier; many of our top-concerning scenarios employ multiple techniques. For example, advanced malware may utilize an application vulnerability to deploy signatureless attacks. This blending of multiple critical techniques into one scenario highlights the need to tune security controls based on a combination of techniques, not a simple scenario.

These results brought to the surface other concerns for us: Are organizations testing their security controls in line with the highest concerns—or greatest fears? Are they limiting the success of security control testing via scope definitions or environment segmentation? In the next section, we examine just how testing is being performed.

TAKEAWAY

Security control testing can ensure that you have some controls or detections in place for some of the more advanced threat actor techniques, but these will often cover some of the basic techniques as well. Utilize a framework that focuses on *attacker techniques*. After all, they're the ones you need to defend against!

Getting It Done

It's likely that your security controls are being tested. Hopefully, the party doing the testing is one you're aware of! To the 76% of our full respondent base that perform testing, we inquired about the methods used to test the effectiveness of their security controls (see Figure 4). Leading the pack was penetration testing, at a whopping 84%. Vulnerability scanning came in second, nearly 20% behind. As shown in Figure 4, Red/Blue/Purple teaming activities[3] were in fourth place, at approximately 44%.

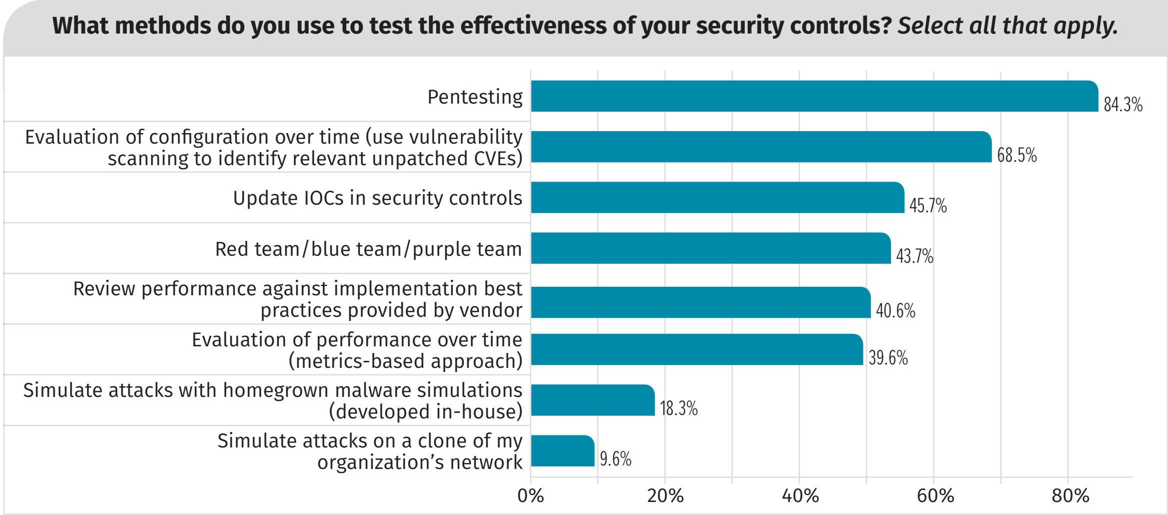


Figure 4. Poll Results About Methods Used to Test Security Controls Effectiveness

[3] While we did not expand on the concept of blue/red/purple teaming within this survey, we'll classify that as activities performed in unison by a blue and red team, who are trying to defend and attack, respectively.

We hypothesized in Part One of this spotlight series that penetration tests and vulnerability scans were the primary security control effectiveness test, and unfortunately, they possess inherent weaknesses. Penetration tests, while useful for identifying pathways into an environment, are often dependent on the skill level of the penetration tester. Furthermore, penetration tests may do little to replicate the toolsets that a "real" threat actor may employ, thus providing a false sense of security. Lastly, and perhaps most importantly, penetration testing may be limited in scope and/or performed on a periodic, well-known schedule. This does little to take into account all the moving pieces of a complex organization—ones that an attacker may jump on and take advantage of.

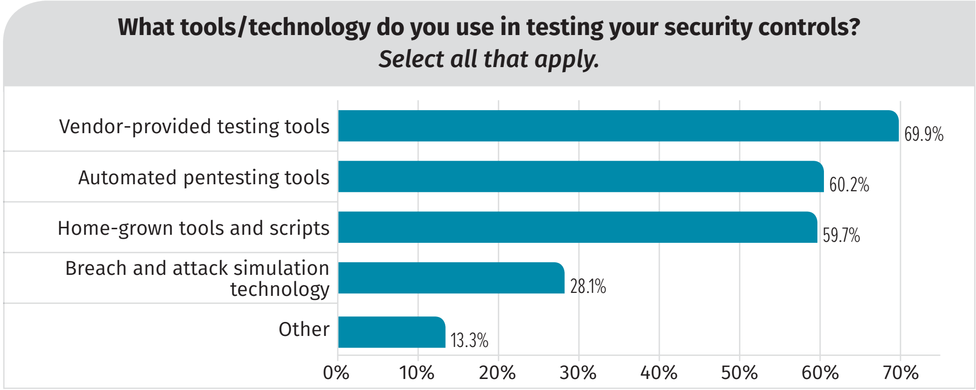


Figure 5. Poll Results in Response to Question About What Technology Respondents Employ in Testing Their Security Controls

To follow up on the notion of effectiveness, we also asked our respondents what technology they employ in testing their security controls. As shown in Figure 5, approximately 70% utilize vendor-provided testing tools. The top three responses were rounded out with automated penetration testing tools and home-grown tools/scripts, respectively.

In addition to the tools present, we also wanted to get an idea of how frequently security control testing happens. According to approximately 68% of our respondents, security control testing occurs at best case monthly and worst case annually. As shown in Figure 6, nearly 16% of our respondents indicated that testing occurred occasionally—yet another dangerous precedent.

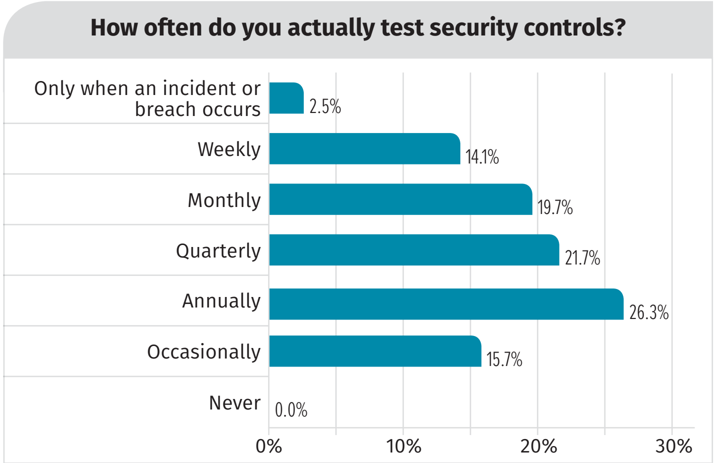


Figure 6. Poll Results in Response to Question About How Frequently Respondents Test Security Controls

Security control testing should be *ongoing*. It should be performed in response to events and done continuously. How do you do that? We'll discuss that next.

Making It Better

Lastly, we asked our respondents how they are utilizing security control testing in their day-to-day activities. In short, is testing making their organization better or worse? As shown in Figure 7, approximately 75% of our respondents indicated that security control testing has a primary objective of identifying gaps that require remediation, with misconfiguration and poor policies a close second at 63%.

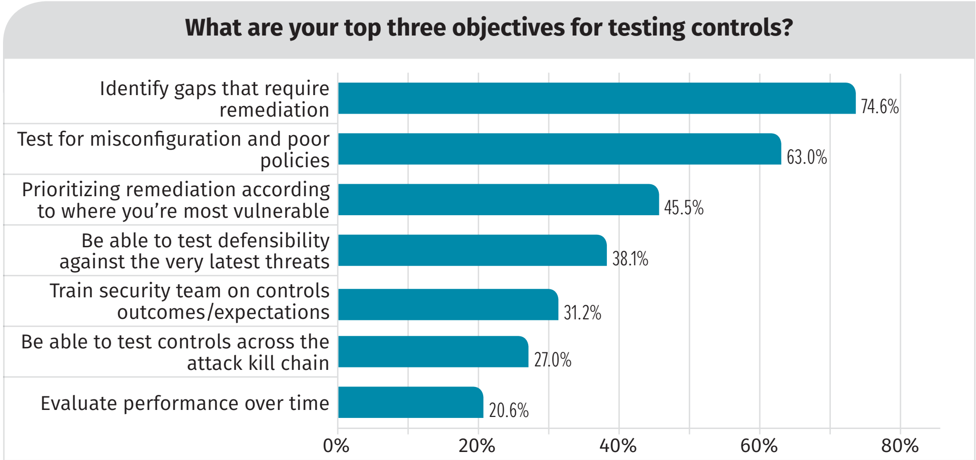


Figure 7. Poll Results in Response to Question About Objectives for Testing Controls

These statistics are encouraging. When security controls are used to identify and make immediate improvements in the environment, they are truly serving their unique purpose. Another area to give particular attention to is our fourth-place objective: testing defensibility against the very latest threats. We hope this objective means your organization is analyzing, documenting and testing against true threat actor activities.

Even with the best-laid plans, organizations still run into issues that may prevent them from achieving the level of success that they seek. In a near four-way tie, as shown in Figure 8, our respondents indicated that limitations and a lack of approach, knowledge and visibility in the use of automation are their top barriers.

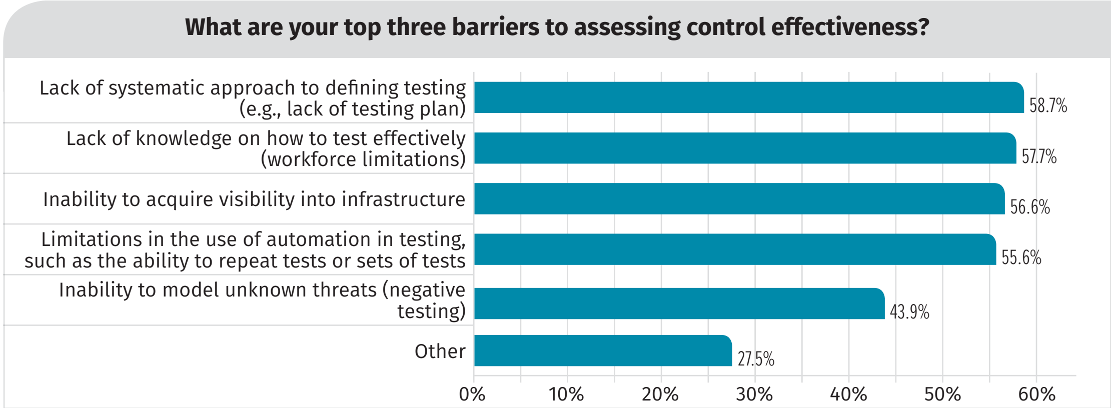


Figure 8. Poll Responses to Question About Top Three Barriers to Assessing Control Effectiveness

Limitations in the use of automation in testing are one area where we expect organizations to grow the most in the coming months. Thanks to solid foundational frameworks and integrated environments, automation can be the key that replaces periodic testing with increased, continuous, almost real-time security control testing with environment-wide scope.

Closing Thoughts

Many organizations rely very heavily on their security controls to protect their environments. A lot of security work is typically done behind the scenes, and users simply go about their day, oftentimes without knowledge of the complexities going on in the background. For the information security team, it's an ongoing task to not only implement security controls, but also test their effectiveness. Without testing controls, we can never be sure they are working properly to defend the organization.

In this two-part SANS spotlight series,[4] we discussed why security control testing is so crucial. Furthermore, we also discussed how oftentimes, penetration tests and simple vulnerability scans do not effectively test your implemented security controls. Threat actors who have your organization in their crosshairs will employ *whatever technique necessary* to achieve their objective. It's tough for your penetration testing team to emulate all the possibilities. Thus, we *must have a better way to test our security controls.*

Without testing controls, we can never be sure they are working properly to defend the organization.

Focus your security control testing on techniques and paths that can be exploited by multiple types of threat actors. By utilizing technique-based frameworks, your organization can effectively test and neutralize multiple types of attacks simultaneously, providing a sense of security that defends against real-world threats, not the limited scope of a penetration test. It's time to make your security controls do their job—defend the organization against realistic rather than hypothetical threats.

[4] Part One: "Are Your Security Controls Yesterday's News?" www.sans.org/reading-room/whitepapers/analyst/security-controls-yesterday's-news-39065. Registration required.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

Cymulate
Breach & Attack Simulation

Last Updated: November 15th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

European Security Awareness Summit 2019	London, GB	Nov 18, 2019 - Nov 21, 2019	Live Event
SANS Austin 2019	Austin, TXUS	Nov 18, 2019 - Nov 23, 2019	Live Event
SANS Munich November 2019	Munich, DE	Nov 18, 2019 - Nov 23, 2019	Live Event
SANS SEC401 Madrid November 2019 (in Spanish)	Madrid, ES	Nov 18, 2019 - Nov 23, 2019	Live Event
SANS Atlanta Fall 2019	Atlanta, GAUS	Nov 18, 2019 - Nov 23, 2019	Live Event
Pen Test HackFest Summit & Training 2019	Bethesda, MDUS	Nov 18, 2019 - Nov 25, 2019	Live Event
SANS November Singapore 2019	Singapore, SG	Nov 18, 2019 - Nov 23, 2019	Live Event
SANS Tokyo November 2019	Tokyo, JP	Nov 25, 2019 - Nov 30, 2019	Live Event
SANS Cyber Threat Summit 2019	London, GB	Nov 25, 2019 - Nov 26, 2019	Live Event
SANS Bangalore 2019	Bangalore, IN	Nov 25, 2019 - Nov 30, 2019	Live Event
SANS Paris December 2019	Paris, FR	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Security Operations London 2019	London, GB	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS San Francisco Winter 2019	San Francisco, CAUS	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Nashville 2019	Nashville, TNUS	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Frankfurt December 2019	Frankfurt, DE	Dec 09, 2019 - Dec 14, 2019	Live Event
SANS Cyber Defense Initiative 2019	Washington, DCUS	Dec 10, 2019 - Dec 17, 2019	Live Event
SANS Austin Winter 2020	Austin, TXUS	Jan 06, 2020 - Jan 11, 2020	Live Event
SANS Threat Hunting & IR Europe Summit & Training 2020	London, GB	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Miami 2020	Miami, FLUS	Jan 13, 2020 - Jan 18, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VAUS	Jan 20, 2020 - Jan 27, 2020	Live Event
SANS Amsterdam January 2020	Amsterdam, NL	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Tokyo January 2020	Tokyo, JP	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CAUS	Jan 20, 2020 - Jan 25, 2020	Live Event
MGT521 Beta Two 2020	San Diego, CAUS	Jan 22, 2020 - Jan 23, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NVUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CAUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Vienna January 2020	Vienna, AT	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Security East 2020	New Orleans, LAUS	Feb 01, 2020 - Feb 08, 2020	Live Event
SANS London February 2020	London, GB	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Northern VA - Fairfax 2020	Fairfax, VAUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS New York City Winter 2020	New York City, NYUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Gulf Region 2019	OnlineAE	Nov 16, 2019 - Nov 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced