Effectively Addressing Advanced Threats

Matt Bromiley
Executive Summary

There seems to be a never-ending abyss of cyber threats plaguing organizations these days. From ransomware to crypto-mining to state nexus threat actors, it feels like every day a new group is labeled or malware family is discovered. Keeping up with these threats can be daunting—until we consider what it takes to defend against them. Not all threats are created equal—however, not all defenses are created equal either.

The defenses your organization employs to combat these threats likely contain various capabilities and can hopefully scale accordingly. In this survey, we teamed up with IBM Security to understand how large, mature organizations deal with advanced threats. By advanced threats, we are referring to ones typically representing highly capable threat actors with specific, targeted actions. While threats of all shapes and sizes can cause concern for an organization, responding to advanced threats typically involves more resources, technology and time.

In this survey, we got right to the heart of the matter to determine just how much success, if any, organizations are having when they combat advanced threats. We wanted to focus on core concepts such as whether organizations are responding to advanced threats, what their top limitations are and what the future of advanced threat handling looks like.

Some key takeaways from this survey indicated:

- Visibility is a key concern for many organizations, whether it's the type of data being processed within the infrastructure or uncertainty of data location.
- Organizations are concerned with privileged user and/or credential abuse.
- Endpoint alerts and network access devices are the top sources of incident information, providing alerts and investigation support, respectively.
- Many organizations (74%) have a blend of on-premise and cloud environments, in many cases using multiple cloud providers.

As we worked through our survey results, we also looked for areas organizations can work on improving sooner rather than later. As you read through, watch for our “Take Action Now” call-outs, where we provide opportunities to look for immediate or short-term improvements within your organization.
In this survey, we maintained a healthy representation from multiple countries, multiple industries and positions within those industries. Our respondent pool of 366 organizations had the largest share in banking and finance, and government and technology, respectively, but we also saw representation from healthcare, education and manufacturing. Figure 1 provides a breakdown of our respondent pool by industry.

Organization size, another potential contributor to resource availability and maturity of security program, ranged from small organizations (fewer than 10 employees) to massive organizations with more than 100,000 employees. Our most popular respondent pool, approximately 20% as shown in Figure 2, was between 101 and 1,000 employees.

We also saw a good mix of respondent positions represented in this survey. We typically prefer to see a blend of management and analysts, which helps combine both long-term strategies (as we’ll explore later) as well as “boots on the ground” visibility. As shown in Figure 3, the top four positions included security analysts, managers/directors, incident response team members and IT managers. We also saw responses from penetration testers, engineers and threat intelligence analysts.
Lastly, we also wanted to understand what types of environments our respondents were tasked with protecting. As we explore detecting and defending against advanced threats, one key consideration is where those threats might materialize. After all, attackers don’t care where your data lives—they just want access to it! A whopping 77% of our respondents have their operations either entirely within the cloud, or in a mix of on-premise and cloud hybrid environments, as shown in Figure 4.

While there is no “easy” environment to defend (except, perhaps, one that is offline), hybrid environments present unique challenges that may not be present in entirely on-premise environments, which 19% of our respondents selected. The cloud can introduce threat vectors that on-premise organizations may not realize. Note this does not make the cloud insecure; it simply changes how an organization should structure its ability to detect and respond to threats.

With these data points in mind, we’ll begin to explore how and where organizations need to improve and where we identified elements of success in advanced threat detection and defense.

**Blind Spots**

Organization-wide visibility—meaning from the network to the endpoints—offers organizations a tremendous advantage over advanced threats. However, given the speed at which organizations are growing, visibility can be a challenge. Furthermore, your endpoints aren’t always online or connected to the corporate network. Respondents to our survey identified a number of blind spots hindering their ability to effectively secure the organization.

The most significant blind spot from our respondents, at slightly more than 48%, was a lack of visibility into what and where data is being processed within the organization. However, our “less popular” categories are the ones that concern us—such as access to sensitive data by insecure, unmanaged devices or unauthorized individuals, misuse by insiders and a lack of data geolocation with respect to where sensitive data is located or stored, as seen in Figure 5.
These visibility gaps likely increase the difficulty of detection within these organizations; after all, you cannot defend against what you cannot see! Another significant concern when we see a lack of visibility stems from how quickly some advanced threat actors can shift from intrusive or disruptive to destructive. Recently, active state nexus groups, such as those with ties to Iran, have been known to deploy “wiper” malware that can obliterate infected systems or an entire network! The security team simply cannot afford to think only in reactive terms with such looming advanced threats.

Oddly enough, despite our theory that lack of visibility serves as a major issue for organizations, our survey respondents actually leaned toward other issues as their primary barriers to detecting advanced threats and subsequently responding to or remediating them. As shown in Figure 6, the number one concern for organizations was an inability to understand and baseline normal behavior. A close second was a shortage of funding and resources, followed by a shortage of skills.

Lack of visibility into endpoints, users and location-based data and/or network traffic and logs yielded only approximately 21% and 20%, respectively.

We were surprised by these results, primarily because the top three barriers to detection, response and remediation don’t necessarily solve the major visibility gaps within the organization. Sure, baselining and visibility go hand in hand, however an organization likely needs the latter before the former. We’d highly encourage organizations focus on visibility before attempting to baseline their environment; these two concepts work in concert with one another, as baselining requires environmental know-how.

Given the prevalence of cloud-based operations within our respondent base, we also asked our respondents to discuss gaps within their cloud-based infrastructure. Cloud infrastructure presents unique challenges to organizations; we would expect unique gaps with regards to security analytics as well. Unfortunately, the results still centered around a lack of visibility.

---

Our respondents’ top two concerns were integration of data with security analytics tools and combining data across multiple cloud environments, at approximately 55% and 52% respectively. Third place, at approximately 48% of our respondents, was a lack of visibility into the cloud environment. Figure 7 details these results.

These results can speak to challenges arising specifically in cloud environments. For example, combining data across multiple clouds is certainly unique, but we’re concerned that these results continue to display patterns of gaps in overall visibility, which may be unnecessarily exposing the organization or limiting the security team’s abilities. In fact, five of the top six responses have to do with either a lack of data, integration or understanding of the cloud. Keep in mind that visibility is key—obtaining data from the cloud may be different than collecting from on-premise hosts—but this doesn’t diminish its importance. **We have to work on visibility.**

The only threat-related response from Figure 7—which we actually think is an area where organizations can make quick improvements—is a lack of insights into threats targeting cloud environments, at approximately 43%. This gives a nod toward the importance of integrating threat intelligence within your security program. Your threat preparedness and knowledge should be focused on your infrastructure, and you should receive data that helps you protect your organization.

On the topic of visibility, another area where we encourage organizations to maintain visibility is on themselves. Tracking internal metrics helps your security team assess its effectiveness, improve the security posture of the organization, and measure the team’s ability to detect, respond to and remediate threats. In this survey, without specification, we simply wanted to know if our respondents track metrics. As Figure 8 shows, approximately 61% of our respondents indicated that they did—we love seeing this! There is room for improvement, as nearly 26% indicated they did not track metrics.
Approximately 89% of our respondents indicated that they track the number of incidents detected—this was our most popular metric. Rounding out the top five, organizations are also keeping track of how many incidents they close (70%), the time to respond (58%), assets at risk (51%), and the time spent on investigations (49%). Figure 9 provides the results from this question.

As we analyzed some of the less frequently selected results, we noticed some organizations are really measuring their analysts’ effectiveness via metrics. Approximately 41% measured volume of alerts per analyst and approximately 43% track service-level related metrics. As mentioned, tracking these types of details can be very crucial to determining how effective your security program is.

Approximately 44% indicated they track the number of false positives encountered, another metric we consider extremely important. While this may seem an odd data point to keep track of, it’s actually a great way to measure the effectiveness of your security tools and analytics. Teams that chase too many false positives might have to reassess the source of those false positives, and either tune or replace noisy signals within the environment.

At approximately 31%, the time to respond to an incident is the primary driver for our respondents. This is a good metric, as it allows the rest of the security team to measure how well their security controls are working. The second-highest driver for our respondents was the number of incidents closed, at approximately 28%.

The topic of visibility often presents many ups and downs for organizations. This is a common problem we’ve been experiencing for years—organizations grow in size, either horizontally and/or vertically, and end up with significant gaps in visibility. The cloud does not prevent or exclude this problem—in fact, it may amplify it.

**Action Items**

Metrics allow your security team to benchmark and measure its effectiveness. Start tracking metrics—even via something simple as a spreadsheet—just so you have a reference point. Collecting data will allow the team to demonstrate value, something that is a constant battle for internal security teams. The team will enjoy having something to compare against, and management will appreciate seeing improvements over time.
This survey not only showed us issues into visibility, but also provided us with insight into the types of threats organizations are handling. When asked about major threats or risks realized within their environments, our respondents found that account and/or credential hijacking is the top concern, at approximately 52% of our respondents. A close second, and perhaps a similar type of threat, is privileged user abuse at 49%. Figure 10 provides the results for this question.

This came as no surprise; advanced attackers will often move quickly to identify, steal and misuse legitimate account credentials. The higher the privilege of these accounts, the more targeted they are. Some of the largest reported breaches—such as Target, Yahoo or Starwood—involved the theft and misuse of legitimate credentials.

While we can spend an entire paper focusing on account credential protection, we hope that organizations are wrapping enhanced security measures around these privileged accounts.

Narrowing our focus on advanced threat actors, approximately 35% responded they have experienced one or more advanced threats within their environment. As shown in Figure 11, nearly 30% indicated that they were uncertain. This is not an uncommon finding. While we defined advanced threats in the survey, it is tough for an organization to always know whether a particular incident or threat will materialize into an “advanced” threat.

Looking to break this down further, we also asked our respondents just how many advanced threats they faced in the past 12 months. A slim majority of our respondents (approximately 53%) indicated they have only faced a handful of threats. Conversely, we did have a handful of respondents, approximately 3%, that dealt with more than 100 advanced threats in the past 12 months. Phew! Experience has shown us that some industries are targeted more often than others, however these figures are hardly reason to ever think your industry is safe from an advanced threat. Figure 12 provides insight into these responses.
Keeping track of the number of realized threats is only half the game—useful metrics also identify the unique characteristics of advanced threats.

Taking the largest share of our respondent pool, approximately 53% of realized advanced threats contained malware infections. This also comes as no surprise—it is one of the most common characteristics of advanced actors. Whether it’s custom, single-use or widespread malware, attackers will often travel with and use their various toolkits consistently.

Other key characteristics included unauthorized access (30%), persistent, multi-stage attacks (30%) and the theft of sensitive data (29%). See Figure 13.

Lastly, we wanted to know what types of data sources were utilized in uncovering advanced threats. Network access devices, such as firewalls, proxies and VPN appliances, were the most useful in supporting investigation of advanced threats at nearly 70% of our respondents. SIEM technologies and network-based firewalls were second and third, at 68% and 60% respectively (as shown in Figure 14).

We were very pleased to see network devices represent such an important data source, especially in organizations that may suffer endpoint visibility issues. Network-based data can often serve as a unique vantage point, as it usually represents a smaller quantity of devices than

What were the characteristics of these advanced threats? Select all that apply.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infections</td>
<td>53.4%</td>
</tr>
<tr>
<td>Unauthorized access by external party</td>
<td>30.1%</td>
</tr>
<tr>
<td>Advanced persistent threat or multistage attack from an unknown threat group</td>
<td>29.5%</td>
</tr>
<tr>
<td>Data breach (stealing sensitive data)</td>
<td>28.8%</td>
</tr>
<tr>
<td>Advanced persistent threat or multistage attack from known threat group</td>
<td>22.7%</td>
</tr>
<tr>
<td>Unauthorized access by trusted insider</td>
<td>21.5%</td>
</tr>
<tr>
<td>Malicious activities within legitimate traffic</td>
<td>19.0%</td>
</tr>
<tr>
<td>Encrypted malicious traffic</td>
<td>19.0%</td>
</tr>
<tr>
<td>DDoS attack as the main attack</td>
<td>19.0%</td>
</tr>
<tr>
<td>Attack impacting data integrity</td>
<td>18.4%</td>
</tr>
<tr>
<td>Unauthorized privilege escalation for lateral movement</td>
<td>17.0%</td>
</tr>
<tr>
<td>Destructive attack (aimed at damaging systems)</td>
<td>14.1%</td>
</tr>
<tr>
<td>DDoS attack as a diversion</td>
<td>11.0%</td>
</tr>
<tr>
<td>Unauthorized access by external party</td>
<td>3.3%</td>
</tr>
</tbody>
</table>

What are the data sources (e.g., types of systems, services and applications) that support the investigation and detection of potential advanced threats in your organization?

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network access devices (firewall, VPN, web proxy, network sessions)</td>
<td>69.5%</td>
</tr>
<tr>
<td>SIEM technologies and systems</td>
<td>68.1%</td>
</tr>
<tr>
<td>Network-based firewalls/IPS/IDS/unified threat management (UTM) devices</td>
<td>60.3%</td>
</tr>
<tr>
<td>Host-based anti-malware</td>
<td>57.5%</td>
</tr>
<tr>
<td>Vulnerability management tools (scanners, configuration and patch management)</td>
<td>56.0%</td>
</tr>
<tr>
<td>Application information (event logs, audit logs)</td>
<td>52.5%</td>
</tr>
<tr>
<td>Endpoint protection (MDM, network access control [NAC], log collectors)</td>
<td>51.8%</td>
</tr>
<tr>
<td>Forensics tools (network, endpoint)</td>
<td>49.7%</td>
</tr>
<tr>
<td>Host-based IPS/IDS</td>
<td>44.7%</td>
</tr>
<tr>
<td>Dedicated log management platforms</td>
<td>35.5%</td>
</tr>
<tr>
<td>Asset inventory systems</td>
<td>35.5%</td>
</tr>
<tr>
<td>Identity and access management (IAM) systems</td>
<td>32.6%</td>
</tr>
<tr>
<td>DNS/Dig and other internet lookup tools</td>
<td>31.9%</td>
</tr>
<tr>
<td>Third-party intelligence platforms or services</td>
<td>28.4%</td>
</tr>
<tr>
<td>Relational database management systems (transactions, event logs, audit logs)</td>
<td>27.7%</td>
</tr>
<tr>
<td>Network-based malware sandbox platforms</td>
<td>27.7%</td>
</tr>
<tr>
<td>Network behavior analysis</td>
<td>27.0%</td>
</tr>
<tr>
<td>User and entity behavior analytic platforms</td>
<td>24.1%</td>
</tr>
<tr>
<td>Specialized threat hunting tools</td>
<td>23.4%</td>
</tr>
<tr>
<td>Cloud infrastructure activity and security information (instrumentation data)</td>
<td>21.3%</td>
</tr>
<tr>
<td>Deception and honey pot technologies</td>
<td>14.2%</td>
</tr>
<tr>
<td>Management tools for unstructured data sources (NoSQL, Hadoop)</td>
<td>7.8%</td>
</tr>
<tr>
<td>Other</td>
<td>2.1%</td>
</tr>
</tbody>
</table>
endpoints, but can offer amazing, enterprise-wide visibility. However, host-based mechanisms, specifically host-based anti-malware, came in at fourth place, representing a significant data source for nearly 58% of our respondents.

These results lined up with what we’re seeing in the industry these days: a shift to include multiple types of data points when it comes to threat activity detection and analysis. However, all the right data points mean nothing if they’re not properly analyzed.

**Hot on the Trail**

Even with network and host-based data available for security teams, data must be harnessed and effectively correlated and/or analyzed to serve a purpose. Typically, organizations will push data points to some sort of centralized analytics solution or service, as just over 50% of our respondents indicated they do with their various data points. Nearly a quarter of respondents do not utilize a central solution, and as shown in Figure 15, approximately 27% were unsure.

Centralized analytics are often game changers for security teams, primarily because they allow for data points to be correlated and investigations to move more quickly. However, the scale and capability of a centralized analytics service depends heavily on the type of solution being used. Some organizations can fill up in an hour what others can do in a year! Within the survey, we also wanted to know how many of our respondents utilize in-house or cloud-based analytics solutions.

Of those using a centralized approach, approximately 46% indicate they use an in-house commercial platform. This does not come as a surprise to us. Centralized systems are typically large undertakings and are often deployed in-house. However, the industry has recently seen a shift toward cloud-based analytics services, which approximately 16% of our respondents utilize. Our survey results also showed some organizations rely on homegrown or open-source solutions, which accounted for approximately 37% combined. See Figure 16.

Looking at reliance on a centralized solution from a different lens, we are also curious to know if our respondents utilized a cloud-based infrastructure for their centralized solution. Again, one of our key goals from this survey is understanding how

**Action Items**

Network- and/or host-based data can provide useful detection of advanced threats but may not provide the whole picture when standing on their own. Are you collecting and/or analyzing both types of data? If not, then look to see if there are ways your organization can quickly gain additional visibility. You may already have the means available, just not enabled.

**Figure 15. Centralized Analytics Usage**

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.6%</td>
<td>23.0%</td>
<td>50.4%</td>
</tr>
</tbody>
</table>

**Figure 16. Centralized Analytics Approaches**

<table>
<thead>
<tr>
<th>In-house commercial platforms</th>
<th>In-house open-source systems</th>
<th>In-house custom-developed (homegrown) systems</th>
<th>Cloud-based analytics services</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.7%</td>
<td>15.7%</td>
<td>14.3%</td>
<td>22.9%</td>
<td>1.4%</td>
</tr>
</tbody>
</table>
organizations incorporate the cloud into their security posture, and usage of cloud for analytics solutions is certainly an extension of that. See Figure 17.

Approximately 31% indicated they use cloud-based infrastructure, while just under half do not. There are multiple reasons why an organization may or may not move toward utilizing the cloud: regulations, lack of environment support or lack of available resources. We polled our respondents for particular reasons for avoiding a centralized or cloud-based analytical platform, and their open-ended responses included:

“Lack of vision and need for such software”

“Money”

“Cloud-based analytics... is not where we want to be right now in the government.”

“No suitable product”

And perhaps our favorite:

“Need to get basic fundamentals under control first”

These open-ended responses exemplify that our organizations are not only battling advanced threats, but also internal pressures and regulations to move toward centralized platforms—if they are even interested in doing so. These comments and responses also continue to drive home why organizations need to be collecting and focusing on the data points that help them detect threats most effectively.

With that in mind, we were curious about the various data points our respondents relied on when it came to the investigation of advanced threats. The results surprised us, primarily because they continue to highlight a bridge between host- and network-based data points. Approximately 62% of our respondents indicated their primary source of potential incident identification comes from endpoint monitoring alerts. This result, coupled with earlier findings, shows that organizations alert off of endpoint data but utilize network data to complete their investigations. We love the combo approach! See Figure 18.
Other sources include automated alerts from SIEMs (a close second place at 60%), perimeter defense alerts (57%) and—our absolute favorite—user reports (56%). SIEMs can be some of the most useful tools within any organizations security arsenal, as they allow for correlation across multiple data sets and an ability to view the environment holistically. That’s one way to tackle visibility!

We absolutely love seeing organizations utilize user reports at such a high level. Your users are often the first line of defense for your organization, especially from advanced threat techniques such as targeted spear phishing and/or malicious links.

Looking Ahead

As always, we’re curious about what’s in store for the future of our survey respondents. As we’ve analyzed in previous sections, there is plenty of room for improvement in visibility, and it’s clear our organizations need to work to get their arms around their cloud assets and data.

Despite the need for visibility and better data management, nearly half (46%) of our respondents plan to invest the most in personnel and training within the near future. While we don’t disagree with an investment in personnel and training, we hope that investments made will help increase security posture and provide better insight into available data, not simply increase headcount. Our respondents’ results are provided in Figure 19.

From a technology perspective, rounding out our top five areas of investment include SOC upgrades (31%), SIEM tools or systems (30%), IR integration (29%) and automated workflow management (26%). This is perhaps the most promising result from this particular question: Organizations are aware they need to invest in technology in order to increase their security awareness. Some of the less-common investments are also data-centric, including big data analytics, automated mitigation solutions and security intelligence products. Overall, we’re pleased to see a good blend of our respondents understand the need for better, enhanced technology.

### Figure 19. Security Analytics and Security Intelligence Investment Plans

<table>
<thead>
<tr>
<th>What are your top three areas for future investment in security analytics and security intelligence, in order to strengthen posture against advanced threats? Select the top three, not in any order.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel/Training</td>
</tr>
<tr>
<td>Detection/Security operations center upgrades</td>
</tr>
<tr>
<td>SIEM tools or systems</td>
</tr>
<tr>
<td>IR integration</td>
</tr>
<tr>
<td>Automated workflow management</td>
</tr>
<tr>
<td>Integration among disparate sources of security information</td>
</tr>
<tr>
<td>Big data analytics engines and tools (reduced cost around data management)</td>
</tr>
<tr>
<td>Security intelligence products, platforms or services</td>
</tr>
<tr>
<td>Automated mitigation solutions for known bad threats</td>
</tr>
<tr>
<td>Managed security service providers</td>
</tr>
<tr>
<td>Convergence technologies (middleware/APIs)</td>
</tr>
<tr>
<td>Standalone analytics platforms</td>
</tr>
</tbody>
</table>

Effectively Addressing Advanced Threats
In this advanced threat survey, we set out to uncover how large and/or mature organizations handle advanced threats. By advanced threats, we intended to focus on those extending beyond typical “commodity” malware and that are the result of a threat actor who is highly capable and often has specific, targeted intentions.

This survey identified several areas where we see success and/or need to continue seeing progress:

- Visibility continues to remain a major problem for most organizations, whether it’s on-premise or cloud-based infrastructure. **Poor visibility leaves holes in a security program that your teams simply cannot defend against.**

- Our survey showed a bridge established between host- and network-based artifacts. **For years we’ve been recommending that teams harness both data sets, as they offer true insight into the activity within your networks.**

- Self-detection, automated alerting and user-reporting are some of the most common sources of potential incident identification. **Utilizing your internal barometers helps your security team keep the advantage—a crucial step in defeating advanced attackers!**

We introduced an additional complexity to this survey, as we also wanted to get an idea of how much our organizations are utilizing the cloud within their infrastructure. We hypothesized that usage of cloud shouldn’t lower security defenses; instead, it should **provide additional opportunities** for detection and data insight. This is another area where organizations can improve their security practices.

However, regardless of where your organization’s data “is,” one thing remains the same: **An advanced, targeted threat simply doesn’t care where data lives.** The issues we see in cloud environments are the same we see in on-premise environments as well. If they want to come after your organization, the “where” of your data may simply be another step for them, not necessarily a blocker.
About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, 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 survey’s sponsor:

IBM Security
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oil &amp; Gas Cybersecurity Summit &amp; Training 2019</td>
<td>Houston, TXUS</td>
<td>Sep 16, 2019 - Sep 22, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rome September 2019</td>
<td>Rome, IT</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Raleigh 2019</td>
<td>Raleigh, NCUS</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain September 2019</td>
<td>Manama, BH</td>
<td>Sep 21, 2019 - Sep 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TXUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Fall 2019</td>
<td>San Francisco, CAUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Kuwait September 2019</td>
<td>Salmiya, KW</td>
<td>Sep 28, 2019 - Oct 03, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Fall- Reston 2019</td>
<td>Reston, VAUS</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cardiff September 2019</td>
<td>Cardiff, GB</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh October 2019</td>
<td>Riyadh, SA</td>
<td>Oct 05, 2019 - Oct 10, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha October 2019</td>
<td>Doha, QA</td>
<td>Oct 12, 2019 - Oct 17, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cairo October 2019</td>
<td>Cairo, EG</td>
<td>Oct 19, 2019 - Oct 24, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Santa Monica 2019</td>
<td>Santa Monica, CAUS</td>
<td>Oct 21, 2019 - Oct 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Orlando 2019</td>
<td>Orlando, FLUS</td>
<td>Oct 28, 2019 - Nov 02, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2019</td>
<td>Houston, TXUS</td>
<td>Oct 28, 2019 - Nov 02, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai September 2019</td>
<td>OnlineAE</td>
<td>Sep 14, 2019 - Sep 19, 2019</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>