Detecting a Targeted Data Breach with Ease: A SANS Product Review

Jake Williams
Detecting a Targeted Data Breach with Ease

A SANS Product Review

Written by Jake Williams

October 2015

Sponsored by
LightCyber
Let’s face it: It’s impossible to stop every attacker from gaining a foothold in your network. In fact, the SANS 2015 Endpoint Security Survey found that more than half of respondents are operating under the assumption that attackers are already operating in their networks.¹

With that in mind, we evaluated LightCyber Magna, a security tool designed to integrate network and host monitoring and thereby minimize the time between when attackers gain access and when they are detected, a period often referred to as *dwell time*. Our review of Magna focused on its effectiveness in detecting reconnaissance, lateral movement, data exfiltration and other threats.

To form the outline of our test plan, we used Lockheed Martin's Cyber Kill Chain model. Introduced in 2011, it defines common steps of network-based attacks.² After gaining access to a network, attackers will normally take the following steps, which are components of the Cyber Kill Chain’s “command and control” and “actions on objectives” phases:

- Scan from their bridgehead to locate other hosts on the network
- Guess passwords or exploit vulnerabilities found on remote systems
- Map file shares to copy malware and find data for exfiltration
- Execute commands on remote machines
- Exfiltrate data to remote servers under the attackers’ control

We evaluated Magna’s effectiveness in detecting these attacks using a lab representative of a corporate network and mimicked the actions of attackers during a compromise. The only problem we encountered was our testbed’s lack of background network traffic, which would have enabled Magna’s anomaly-based detection to perform at its peak.³ Even in this constrained environment, Magna performed well, detecting all attacks as designed. Had these attacks been real, any one of our findings would have jump-started an investigation.


³ The more baseline traffic there is in a sample, the more likely it is that anomalies will stand out.
Magna doesn’t focus on detecting or preventing endpoint threats. Instead, it uses a proprietary blend of endpoint and network data to detect threats that traditional security solutions are doomed to miss because they look at network or endpoint data in isolation. Magna, following the later phases of the Cyber Kill Chain model, detects the activities that attackers are certain to perform after the initial compromise.

We found three key attributes that set Magna apart from traditional endpoint management tools. First, during testing, it reduced the time between compromise and detection, limiting the damage attackers can inflict. Second, Magna increases operational efficiency by minimizing false positives and ensuring that alerts provide real, actionable intelligence to analysts. Too often, security products provide a large number of alerts with high false positive rates and minimal value. With Magna, however, the alerts received during testing were true positives and included context that would be critical to beginning a real-world investigation.

Finally, Magna uses a unique blend of network- and host-based indicators to help expedite investigations. It automatically provides context around alerts that other products offer only after lengthy—and expensive—manual investigation.

Capturing Data

To capture network data, the Magna Detector—a network or virtual appliance that deeply inspects network traffic and parses it into metadata—must be connected to a network tap, a network packet broker or a switch’s physical port that supports port mirroring, or “spanning.” The port must be able to monitor traffic from appropriate devices, including domain controllers and file servers. After two or three weeks—the soak (or learning) phase, which involves little more than minor tuning of the Detector—Magna can identify deviations from established network behavior.

To capture host information, Magna uses an agentless technology. Analysts configure Magna with privileged credentials so they can connect it to a remote machine and query it for additional data related to a suspicious event. Magna’s ability to integrate host data collected on demand with anomalous network data into a comprehensive, one-window view is a powerful tool for analysts investigating suspected compromises.

4 “Spanning” refers to Cisco’s implementation of port mirroring (also known as port monitoring) in its Switched Port Analyzer (SPAN) feature. This sends all traffic received on the switch to the SPAN port, facilitating centralized monitoring.
Finding the Adversary

As noted in the introduction, attackers follow a pattern once they establish toeholds in their target networks. Recognizing this behavior is Magna’s bread and butter, as it attempts to detect deviations from the normal behavior of network hosts. This stands in contrast to the most advanced antivirus and malware tools, which usually don’t baseline normal behavior before triggering an alarm, making false positives, as well as missed threats, much more likely.

Magna goes a step beyond traditional network monitoring tools by integrating host information in its Pathfinder feature. Although other network detection tools tell the analyst a host transmitted suspicious traffic, Magna can actually identify which host application or process (LightCyber uses the term artifact to embrace both) was responsible.

Once Pathfinder locates the suspicious artifact, it can optionally upload it to LightCyber’s Cloud Expert System, which automatically examines it further using a number of antivirus products, sandboxing and reputation data sources.5 Pathfinder can also determine whether a particular artifact is prevalent throughout the network (a possible indicator that it is benign) and whether it was scheduled or configured to run automatically at boot. Pathfinder is especially effective at discovering “riskware” and presenting the investigative data to analysts, thanks to its ability to analyze the unique characteristics and prevalence of common attack tools.

With its fusion of network and endpoint data, Magna truly demonstrates that the whole is greater than the sum of its parts. Several attacks we detected with Magna are difficult or impossible to detect when using only endpoint sensors, leaving network detection as the best available option. However, Magna also stands apart from competitors that only inspect network traffic, adding value and reducing false positives by synthesizing data from the endpoint with what it sees on the network. Other tools ask analysts to do the impossible by querying this data from multiple sources and manually correlating the results, but Magna provides them with data already correlated.

5 This is a fee-based annual subscription service.
We tested Magna for its ability to detect multiple classes of malicious behavior. As part of our evaluation, we ran a number of simulated attacks from a compromised host in the test network. This section details the attack classes against which we tested Magna and how they relate to the typical attack's life cycle.

### Mapping the Target Network

Attackers wishing to move laterally throughout the network typically seek information about the environment, including endpoints and users. This reconnaissance includes port scanning and collection of user information.\(^6\)

### Port Scanning

Attackers worth their salt will often begin gathering intelligence through port scanning, which can identify the services running on endpoints. Port scanning is notoriously difficult to detect, and many analysts find that they receive an unacceptable number of false positive results.\(^7\) Because Internet-facing hosts are scanned on a regular basis—just “business as usual”—security analysts often cringe at the idea of responding to port scans without considering the nature of the systems being scanned. Although scans of Internet-facing hosts may be commonplace, port scans of internal hosts are a different matter, because such scans can indicate a compromised system. If analysts can determine from which host a port scan originated, they need to start digging.

Security analysts must be able to detect two types of port scans to identify malicious scanning in the network. The first, where an attacker scans many ports on the same host, can be detected if the destination host is monitored through host-based firewall logs or similar tools. Attackers typically use such scans to identify what services are available on the host.

In the second type of port scan, the attacker scans the same port on many hosts. This scanning method allows an attacker to identify hosts that are vulnerable to a particular exploit. Alternatively, the attacker may be looking for a particular type of host, such as a database server listening on a particular port. In either case, it is unlikely that the compromised host has exhibited this behavior before, and as such, anomaly detection with Magna is relatively trivial.

---

\(^6\) Penetration testers refer to this phase as *enumeration*, but that word hardly describes the amount of intelligence that some attackers compile.

\(^7\) “Avoid these five common IDS implementation errors,” TechRepublic, July 20, 2005, www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors
Figure 1 shows Magna’s detection of port scanning.

Magna identified the machine in the center of Figure 1 (red) as infected; the other machines (in green) are the port scan’s targets. Magna also showed the baseline recording for the same machine, designated by the blue arrow in Figure 1.

**Collecting User Information**

A directory service such as Microsoft Active Directory (or any LDAP-based service) can be a gold mine for attackers wishing to “pivot” from one system to others. Many organizations use these services as an organizational phone book, containing specific information about users, such as phone numbers, departments or supervisors—making this a valuable target for attackers.
For this phase of our test, we performed standard directory queries against an Active Directory domain controller. Even in this relatively small domain, our testbed’s compromised machine created 1,224 LDAP sessions in a single hour, as seen in Figure 2.

![Figure 2. Hostile Directory Services Inquiry](image)

However, the baseline of activity for the host is only six sessions per hour, an obvious anomaly. Magna provided contextual information to the investigator about the attacker’s activity, saving valuable time in investigating the incident. The same data might be available in audit logs, depending on machine settings, but discovering and analyzing that data would require manual effort.

**Expanding Access and Pivoting**

After attackers have a picture of the hosts and services on the targeted network, they often move laterally, expanding their access to those assets. This phase is an especially important time to catch attackers, for two reasons:

- Lateral movement is usually followed by data exfiltration.
- If the attack can be detected and contained before lateral movement is achieved, remediation efforts may be less burdensome.

We tested Magna to determine if it could effectively detect common lateral movement techniques, including password guessing, password spraying and use of administrative tools.

**Password Guessing**

Attackers often gain access to the targeted network by exploiting a user with limited permissions. One way they may elevate those privileges is to guess the password of a privileged user and assume that identity. Attackers will typically use an automated tool to attempt many connections, which is why “best practices” for authentication processes allow a limited number of attempts before resetting a connection or locking out the account. Magna can detect abnormally large numbers of connections, whether to one or multiple hosts.
We used a password-guessing tool for Remote Desktop Protocol (RDP) environments to replicate this popular attack. Because the compromised host did not normally exhibit this pattern of large numbers of connections in a short period, Magna flagged these connections as suspicious “port exhaustion” activity in the GUI. In our testbed’s normal condition, there were at most two RDP sessions per hour between the compromised machine and the remote server. However, when this number rose to 320 sessions per hour, Magna alerted us through the console. Antivirus tools on the compromised machine did not detect the infection, but Magna was able to point investigators to not only the compromised machine, but to the attacker’s target as well.

Figure 3 shows our password-guessing attack. Again, the red machine in the figure is our compromised host, and the green one is our target.

Not only does Magna detect anomalies in RDP logins, it can also detect them for other protocols, including Windows file sharing (Server Message Block, or SMB) and SQL connections. When we tested this by guessing logins to a MySQL server, Magna detected our attack with ease. Figure 4 depicts this attack.

Our compromised host generated a MySQL login session every second, which stood out like a sore thumb against our baseline of zero MySQL logins.

**Password Spraying**

Password spraying attacks, in which attackers try the same one or two passwords against a large number of accounts, are common when the attacker simply wants to gain access to any account without choosing a specific target. This is in contrast to a brute-force attack, where an attacker tries many passwords against a single user.
Attack Classes Tested (CONTINUED)

Attackers often use password spraying in environments where account lockouts come into effect after a defined number of unsuccessful login attempts. The attacker can try a common password against all accounts, assuming that one or more users in the environment have chosen this password. If unsuccessful, the attacker will usually try again after waiting long enough to presume that no accounts will be locked out. Figure 5 shows Magna’s detection of password spraying.

![Figure 5. Detecting Password Spray Attacks](image)

Magna detected all tested instances of password spraying, identifying not only the machine that attackers were using for the password spraying (the compromised host from which the attackers are attempting to pivot), but also the accounts that the password spraying compromised. Figure 6 shows (at top) the accounts our attack correctly guessed.

![Figure 6. Guessing Account Passwords](image)

Again, Magna detected the intrusion, listing both the accounts whose passwords the attacker guessed correctly and those for which it did not. In a real investigation, the next step would be to enhance the monitoring of these accounts and force password changes (using Magna’s integration with Active Directory), denying the attacker access.
Use of Administrative Tools

Systems administrators don't have the activity patterns of normal users. Instead, they use a number of administrative tools, such as SSH, administrative shares and remote PowerShell, that end users rarely, if ever, touch. However, attackers regularly use these same tools to explore and pivot throughout a network. A host suddenly displaying signs of administrative tool usage may indicate compromise of that host if there's no trouble ticket requiring hands-on support. Figure 7 shows how attackers would typically use administrative tools to compromise systems on a network.

![Figure 7. Compromising Systems with Administrative Tools](image)

We used several administrative tools to connect to machines in our testbed. During traffic profiling, the compromised machine displayed no administrative share or SSH use—when such activity began, Magna detected the activity as an intrusion and alerted us. Such information can accelerate the launch of an investigation, providing much more context than a typical antivirus alert by telling analysts about the remote targets to which the attacker attempted to pivot.

TAKEAWAY:
Attackers often use password guessing and password spraying to escalate privileges by compromising privileged accounts. Attackers then use the credentials and administrative tools to move laterally within the network. Magna detects such attacks with ease.
Stealing Sensitive Data

The goal of many attackers—if not the overwhelming majority of them—is to steal data from the compromised organization. The theft, like all such capers, has two main phases: reconnaissance and exfiltration. We tested Magna to determine if it could detect common activities related to data theft, including SMB share access and exfiltration via network services. Although typical employees have little free time to search file servers for directories and files outside their jobs, this search is a critical step for attackers—because before attackers can exfiltrate sensitive data, they must first locate it.

SMB Share Access

Most organizations have critical data on file servers that use the SMB protocol for Windows file sharing. Forensic investigators often find after a compromise that infected machines were making connections to SMB shares looking for data to exfiltrate.

Magna can detect attack behavior by examining the SMB shares to which a particular host is connecting, something simple analysis of network traffic flows (or netflow) can’t do. In most cases, the attackers are simply connecting to the same file servers to which the compromised machine would normally connect, but accessing different file shares on the same server.

Attackers will also test for weak permissions and try to access interesting looking shares (for example, “IT” or “finance”) using their established access. This may result in failed logins to some shares, which could reveal the attackers’ presence, but only if the security team monitors event logs closely enough. (More commonly, event log monitoring never happens, and even if it does, false positives abound.)

To identify the use of new shares, Magna must first establish a baseline of normal SMB share activity for each endpoint and then monitor for behavior that is outside the baseline. Obviously, this means that the Magna Detector must have a view of file share traffic; the Detector is most effective when connected to a tap or SPAN port that includes workstation-to-server traffic. By identifying unusual file share usage, Magna not only detects attackers gathering data for exfiltration, but also malicious insiders attempting to steal data. During testing, Magna provided us the names of shares the compromised test machine accessed. In real-world operations, this would help analysts determine the types of data being exfiltrated and possibly give some indication of an attacker’s motive.
Figure 8 shows Magna’s detection of SMB share use by a compromised machine.

![Figure 8. Detecting Anomalous SMB Share Use](image)

Figure 9 shows a detailed view of odd file shares.

![Figure 9. Unusual File Shares](image)

Listing both the IP and the physical addresses associated with the traffic helps analysts confirm they’re investigating the right machine.

**Data Exfiltration**

Once attackers pivot to a target inside the network and obtain confidential data, they need to exfiltrate that data from the network. Many IDS products attempt to discover confidential data leaving the network, but the inherent complexities of signature creation and encryption often limit their effectiveness for this purpose.

As much as attackers may try to hide in plain sight, it is unlikely that the compromised machine will have previously used the specific servers and/or services an attacker uses for data exfiltration. Because Magna profiles machines for normal behavior, the abnormalities of data exfiltration traffic stand out.
For our test, we exfiltrated data to an Amazon Web Services (AWS) server. Attackers frequently take advantage of AWS’ high tenant turnover and dominant role as a cloud service provider, which forestalls any reputation-based IP address blocking. Magna detected the exfiltration quickly, identifying not only the compromised host, but also the server in the AWS cloud. Figure 10 shows Magna’s depiction of data exfiltration.

Immediate identification of the attacker’s server is especially helpful in situations where other network locations (e.g., remote offices) may not have their networks monitored by Magna. Investigators can block the IP address and domain of the remote server at egress firewalls, preventing further data leaks to that server. Attempts by other hosts to contact the IP address or domain of the remote server may then lead to the detection of additional compromised machines. In this scenario, Magna facilitates not only the investigation, but also the containment and remediation.

**Detecting Other Malware**

Beyond the detection capabilities outlined so far, Magna has several general-purpose malware detection capabilities. These backstop traditional malware and riskware detection techniques, implementing a defense in depth. Recommendation 5-8 of the Critical Security Controls states, organizations should “ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection.” Magna meets this need by providing anomaly-based detection of post-exploitation activities.

---

**TAKEAWAY:**

When attackers and insiders collect data for exfiltration or theft, they often exhibit unusual access patterns with SMB shares. Magna detects these deviations from baseline activity and alerts the analyst. Likewise, by detecting exfiltration servers that an attacker uses, Magna provides threat intelligence that analysts can use to increase the efficacy of other tools in their portfolios.

---

DNS Query Failures

When attackers use a single domain for command and control (C2) of malware, blocking that domain removes the ability to control the malware. Malware authors often use domain generation algorithms (DGA) to make it more difficult and costly for defenders to block C2 channels. Of these, attackers must only have a few domains actively registered at one time in order to control the malware. Because the malware does not know which domains will actually be registered on a particular day, it will likely make numerous requests (potentially thousands) to unregistered domains before finding a working C2 domain. Requests to unregistered domains fail and return an NXDOMAIN error. By looking for excessive numbers of DNS query failures from a single host, Magna can detect hosts infected with DGA-based malware. Figure 11 shows Magna’s display of DNS query failures and randomized DNS domains.

Figure 11. Detecting DNS Query Failures

We tested Magna for its ability to detect DGA-based malware, and it correctly identified the compromised machine. Monitoring for excessive DNS query failures is an effective technique for detecting malware, but an obscure one, perhaps because the process often involves manually examining DNS server logs. Magna automatically profiles mail servers, as they typically generate a pattern of DNS use (and thus, failures) from other hosts, to avoid false positives and enhance visibility into these attacks.

**Random-Looking Domain Names**

In addition to detecting excessive failed DNS queries, Magna detects DNS queries for suspicious domain names that appear randomly generated. Such queries are another sign that an attacker has infected a machine with malware that uses DGA. Figure 12 shows Magna’s detection of random-looking domain names.

By implementing multiple algorithms for detecting malware and C2 traffic (we tested DNS query failures and random domains), Magna maximizes its chances of identifying such traffic while signature-based antivirus is constantly playing catch-up with each new malware variant.
Ransomware Encryption Attacks

Magna also supports detection of “ransomware” encryption attacks, such as those used by CryptoLocker. In these attacks, adversaries encrypt files on local machines and remote file shares and demand payment before providing a decryption key. In essence, the attacker reads an existing file, then encrypts it and replaces the original with the unreadable encrypted version. The ransomware then moves on to the next file, repeating the process. Magna classifies the encryption of remote files as a “bulk rewrite” operation, one that is easy to distinguish from normal file manipulation because of the number of files involved.

Magna does not perform detection in real time; it alerted us only after our attack tool encrypted some files on the remote file share. However, in a real-world environment, it could take days to encrypt a sufficiently large file share, meaning Magna still provides value by potentially notifying the analyst before an attacker completely encrypts the share’s contents. By detecting the threat early, Magna helps defenders identify and isolate the infected machine, reducing the number of files that responders must restore from backup and shortening remediation time. Figure 13 shows Magna’s detection of bulk rewrite operations.

Figure 13. Detecting Bulk Rewrite Operations

Magna also tells the analyst specifically which machine was involved in the encryption process, ensuring that administrators do not try to restore from backup before the infected machine is remediated. Although this feature is not its strongest selling point, Magna is a good addition to any defense-in-depth strategy against ransomware infections.
Riskware

Magna’s Pathfinder technology can also detect some riskware programs that communicate on the network. Attackers frequently use these programs after compromising a machine, to map the network and pivot to other machines.

During our test, Magna easily detected `nmap`, a popular network scanning and vulnerability discovery tool. It not only detected port scanning, but also observed characteristics unique to the `nmap` tool, which gave investigators specific information about the specific tools our simulated attack used and minimized false positives.

Network traffic analysis also helped Magna detect `ncrack` and `PsExec` activity. `Ncrack` is a popular brute-force login utility that attackers favor because it runs well on Windows. It is also open source, which allows attackers to modify it to easily avoid detection by signature-based endpoint tools such as antivirus. Magna detected the use of `ncrack` on the network, notifying us of the compromised machine from where `ncrack` was run and the remote machines on which `ncrack` attempted brute-force logins. Figure 14 shows Magna’s detection of `ncrack` in the test environment.
Another test used the **PsExec** tool, which executes commands on remote Windows machines and is commonly used by systems administrators as well as attackers.\(^\text{11}\)

Systems administrators use this to help automate administration of remote machines, while attackers use it to pivot to new machines by running malware on them. Magna detects **PsExec** riskware by monitoring network traffic, notifying analysts of both the compromised machine from which **PsExec** was run and the machines where **PsExec** executed malware.

Simply detecting and blocking **PsExec** at every endpoint isn’t feasible, for two main reasons. First, **PsExec** used to be open source, and attackers can easily modify it to avoid signature-based endpoint tools. Meanwhile, **PsExec** has many legitimate uses in day-to-day IT operations.

Magna’s network anomaly detection makes these arguments moot. It won’t generate alerts for **PsExec** on legitimate (that is, baselined) systems administrator machines but will do so for machines where it has not been observed previously. Meanwhile, although the on-disk signatures of PsExec are easily avoided, its network traffic signatures are much more difficult to modify without breaking functionality. In our tests, Magna detected all uses of PsExec from the compromised machine.

---

\(^{11}\) Microsoft TechNet hosts the Sysinternals suite; **PsExec** is available at [https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx](https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx)
Advanced Features

Beyond the findings discussed in the previous section, LightCyber Magna has advanced features that allow it to operate effectively in large-scale environments.

**Process-Level Context**

Magna goes a step beyond traditional network monitoring tools with what LightCyber calls Network-to-Process Association (N2PA) for suspicious traffic. Although other network detection tools tell the analyst a host transmitted suspicious traffic, Magna can actually identify which host process was responsible.

N2PA changes the game for incident responders. Most network detection products require follow-up investigation to understand the nature of an alert. Endpoint imaging and investigation is typically disruptive to the end user, which in turn is disruptive to the business. N2PA presents analysts with process-level context for the alert, enabling them to decide whether to take action. In the event that the appropriate action is simply to terminate the suspicious process, Magna enables remote process termination with a single click, through its Malicious File Termination (MFT) feature. In the test environment, Magna supported the entire incident response cycle from detection to remediation.

**Pathfinder Host Profiling**

When Magna detects suspicious network traffic, it profiles the hosts looking for processes that are uncommon to the environment. When low-prevalence processes turn up, Magna can automatically send them to LightCyber’s malware analysis cloud, in time providing the analyst with additional context to begin investigating the suspect host.

**Scalability**

In larger network environments where one Magna Detector can’t monitor all traffic sources of interest, Magna’s clustering capabilities—a Master-Detector-Probe model—will be helpful. This contrasts favorably with a number of tools that do not scale, thereby forcing the organization to deploy multiple installations across the network. The ability to manage a Magna cluster as such saves analysts the work of managing widely dispersed Detectors or Probes.
Our testing of LightCyber Magna demonstrated its effectiveness in detecting reconnaissance, lateral movement, data exfiltration and other threats in the network environment. It complements existing detection products, uncovering what real-time technologies may miss. Magna was particularly effective in providing actionable intelligence with minimum false positive alerts. This focus on high-quality, actionable intelligence helped to jump-start the investigation in every case tested. The unique blend of network and endpoint data made investigation and remediation of threats much easier compared with using traditional security tools.
Jake Williams is a SANS analyst, certified SANS instructor, course author and designer of several NetWars challenges for use in SANS’ popular, “gamified” information security training suite. Jake spent more than a decade in information security roles at several government agencies, developing specialties in offensive forensics, malware development and digital counterespionage. Jake is the founder of Rendition InfoSec, which provides penetration testing, digital forensics and incident response, expertise in cloud data exfiltration, and the tools and guidance to secure client data against sophisticated, persistent attack on-premises and in the cloud.

SANS would like to thank this paper’s sponsor:

LightCyber
### Upcoming SANS Training

**Click here to view a list of all SANS Courses**

<table>
<thead>
<tr>
<th>SANS Training</th>
<th>Location</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>