GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Case Study: How CIS Controls Can Limit the Cascading Failures During an Attack

GIAC (GSEC) Gold Certification

Author: Bill Knaffl, bill.knaffl@gmail.com
Advisor: Adam Kliarsky
Accepted: April 23, 2016

Abstract

It seems that every day a new and more frightening data breach goes public. These attacks seem to run the gamut; everything from International Banks, Government Agencies, private companies, educational institutions, and even non-profit organizations are targets. With each attack the confidentiality, integrity and availability of our data is diminishing. The use of the "Critical Controls" is one part of the defense in depth approach to data security. By approaching security from the perspective of these controls, we can reduce the threat vectors, reduce detection time, and expose attacks to the overall security posture. This paper reviews one such attack and shows how implementation of the critical controls would have reduced the impact to the company.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Every day it seems that new information becomes public about the latest data breach. Millions of records (read also as personal data) are lost annually and dutifully reported by the nightly news. For example, Forbes reported that the Anthem breach alone allowed the compromise of over 78 million records ("Forbes Welcome," n.d.). However, not all breaches occur because of "elite hackers" breaking into digital networks. Sometimes (as the ACME case below illustrates), the attack can be unintentional and without the knowledge or even participation of the computer user. Sometimes a simple mistake is all that is required to open the door for damage to take place.

Attacks these days can vary greatly between the tools, the techniques and the methods used by the attacker (threat actor). The use of "Trojan software" allows the attacker to embed malware within a seemingly legitimate product. In recent years, a new term has come to the market; "Malware as a service". History of this term is a bit convoluted, but it seems to begin in the Verizon 2011 Data Breach Investigations Report (Verizon, 2011). Similar to selling Platform as a Service (PaaS) and Software as a Service (Saas), it is possible to purchase malware designed for a specific intent. As easily as it is to acquire and deploy malware the growth in the open market has been exponential. Panda Security published an article stating that they had analyzed and neutralized:

> **"84 million new malware samples** throughout 2015. This is nine million more than the year previous, according to the corresponding data. The figure means that there were **230,000 new malware samples produced daily** over the course of the year." (Panda, 2016)

As far as the loss, it was reported, "in 2014, the Internet Crime Complaint Center (IC3) received 269,422 complaints with an adjusted dollar loss of $800,492,073" (FBI, 2015). Worse, due to under-reporting of damage from malware, the total cost of malware may never be clear. Many times these numbers show only the larger corporate losses rather than the individual costs. To say that the attacks are very expensive to governments, private companies, and even individuals is quite the understatement.

For years, the security teams at these agencies worked with various concepts of how they should direct protections; typical security measures never

© 2015 The SANS Institute Author retains full rights.

seemed to provide the complete answer. As the attacks became more and more common, the defenses started analyzing these attacks and used that to create new solutions. Instead of simply addressing the discovered vulnerabilities, these researchers were looking to understand the methodologies and anticipate future attack vectors.

In 2000, the Center for Internet Security, Inc. (CIS) formed to "enhance the security readiness and response of public and private sector entities, with a commitment to excellence through collaboration" (Center for Internet Security, 2015, p. 05). Since that time, they have been working with various industries worldwide to help enhance the concept of shared information. By allowing the offense to drive defense, they take actual attack experiences within the industry and develop a prioritized list of controls to help bolster the overall defensive measure. The Critical Security Controls (CSC) "are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions" (Tarala, J.)

The CIS includes control families "that can be shown to stop known real-world attacks". (Center for Internet Security, 2013, p. 03). By focusing on these real events and the specific environment for that company or group, the security team can develop security controls that will address the current high priority items as well as methods to address existing issues. Rather than replacing company policy or procedure, these controls can be used by security management teams as a framework used to evaluate risks across the board and then reprioritize as necessary. There are no silver bullets in security. There are no 'one-size-fits-all' solutions. The goal is to give the responding teams the opportunity to review the current posture, review applicable controls and address the gaps between current posture and control framework.

The below attack summary is a case study of how the CIS controls could have prevented or limited exposure during an attack; it is not meant to explain how the information was detected nor is this a timeline of the events. This is also not a forensic review of the activity. This is merely a review of the high-level activities, describing failures and showing how controls would have enhanced the security posture. Also added are the remediations suggested to management in order to prevent or reduce the probability that this activity from being a problem in the future.

© 2015 The SANS Institute Author retains full rights.

Ladies and gentlemen, the story you are about to read is true. The names have been changed to protect the innocent.

2. Attack Summary

An ACME Inc. employee brought a personal laptop into the facility infected (albeit unknowingly) with Poison Ivy and connected it to the corporate network via a wireless access point (AP). The system obtained an IP Address using Dynamic Host Configuration Protocol (DHCP) addressing provided by the core corporate network services. Upon connection, the infected system made an Internet connection to the command and control server (wile.e.coyote.com). Once connected, the threat actor provided the command for the system to scan the local network for available services. While the user noticed that the machine was running slowly, it was late on Friday starting a three-day weekend. The user left the machine powered on with plans to look at it again on Tuesday. The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. The threat actor, still using the compromised machine, logged into the FTP server, compressed the contents and then transferred the data to the control server (over the internet) using an encrypted outbound VPN connection.

Over the weekend, the Network Operations Center (NOC) tracked a large amount of data over an encrypted channel. While able to identify both the source and destination, without the encryption keys, they were unable to decrypt the traffic to identify the content. The destination was not on the current list of known malicious sites (the list was out of date by four months). The help desk technician then opened a work ticket for the local desktop services to investigate.

Early Tuesday morning the user noticed that this was still acting erratic even after a reboot. The user then called the help desk to open a ticket. The helpdesk technician was able to tie IP address of this machine to the traffic identified over the weekend. When the desktop technician arrived, it was determined that the machine in question is not a corporate machine and does not have all the standard protection software. A quick scan using a boot time tool found the Poison Ivy signature. At this point, the technician confiscated the machine for forensic investigation and the tickets closed.

Bill Knaffl, bill.knaffl@gmail.com

© 2015 The SANS Institute Author retains full rights.

The forensics team determined a known malware tool named Poison Ivy compromised the machine. They also found a temporary file, left over by the scanning, that included the directory listing of the FTP site. Many of the folders within the directory we named after previous high-value programs. These files included parts lists, price quotes and even proprietary drawings. Included in the information, were patents from the current Chief Executive Officer (Mr. R. Runner) as well as legal documents describing the purchasing and legal aspects of these programs.

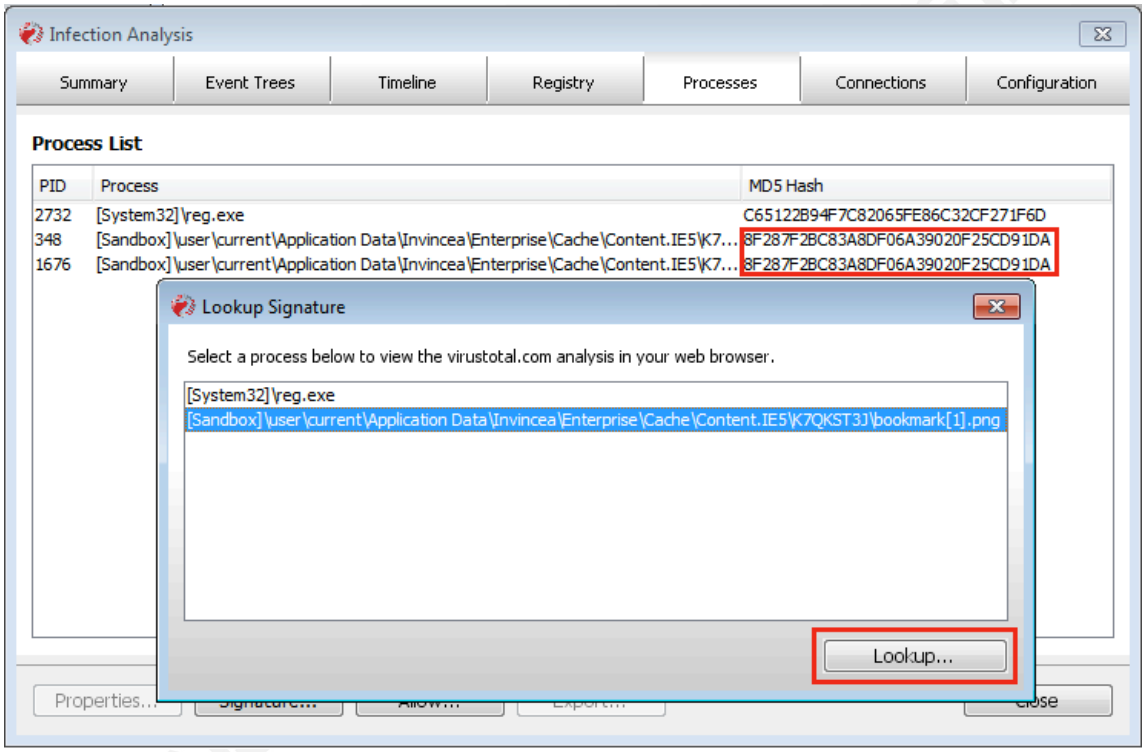

Figure 1 - Infection Analysis

3. Which Controls could have helped

3.1. Inventory of Authorized and Unauthorized Devices (CSC 1)

3.1.1. Why this control is important

While there are six sub controls within this control, the main concept is to ensure that the organization knows what devices are connected to the network. Without controlling the access to the network, unauthorized devices can expose

© 2015 The SANS Institute Author retains full rights.

the organization to a multitude of risks. Unauthorized devices can bring malware or other vulnerabilities to the internal areas of the network. Further, unauthorized devices will not have the standard software, configurations, and tools. As a result, the enterprise defenses are either nonexistent. The key controls for this event were CSC1.1, CSC 1.2, and CSC 1.5.

3.1.2. What controls should have been in place and why

The first sub control requires the use of an automated discovery tool. By knowing that an unauthorized device connected, the organization could have implemented corrective controls to remove access from this device. By moving this device logically to a separate quarantine virtual local area network (VLAN), an external device would be isolated from any other network resources as well as alerts sent to staff regarding the unauthorized connection.

Another issue is DHCP. The purpose of DHCP is to ensure that devices can quickly and effectively obtain an IP address and communicate on the network. While static addressing is certainly more labor intensive, it does allow for a level of control that DHCP does not. Machines that enter the network without the proper addressing and subnet information would not be able to communicate immediately. By allowing DHCP without other compensating controls, the organization was not able to control access of this machine from the rest of the network.

Another sub control that could have prevented this attack would be network level authentication or even the use of certificates to authenticate the machine. In this case, the machine would not be able to authenticate without the user providing credentials. This type of control would block the connection without the proper authentication.

3.2. Limitation and Control of Network Ports (CSC 9)

3.2.1. Why this control is important

The purpose of this control is to ensure that any port, protocol or network service has a business purpose. Secondarily, any service that is in user needs to be up to date and secured to the greatest degree possible. Unpatched services allow for weaknesses that require additional remediation. Sub controls

© 2015 The SANS Institute Author retains full rights.

9.1 and 9.3 address confirming the ports in use and ensuring that these align to business needs.

3.2.2. What controls should have been in place and why

In this case, the main vulnerability is the existence of an FTP Server. By default, FTP passes user names and passwords in the clear. It is possible to run the FTP services through a tunnel in order to mitigate the default vulnerability and the possible risk of clear text password transfer.

Routine scanning and collecting of known port baselines can help ensure knowledge of which services are used. Had the organization been doing routine scanning the presence of an FTP server on the network would have been apparent. While FTP is no longer a default package on most modern Windows Internet Information Services (IIS) installations, administrators may still install it. Specifically looking for this weak protocol requires active scanning. If the FTP service is required, there should be effort used to move to one of the more secure methods for FTP operation.

3.3. Boundary Defense (CSC 12)

3.3.1. Why this control is important

The goal of boundary defense is to validate traffic between the external and internal networks. Part of the validation process is to use rules to evaluate the legitimacy of the traffic. While there are 10 sub controls for this area, the controls that are most important to this scenario are 12.1, 12.3, 12.4, and 12.5.

3.3.2. What controls should have been in place and why

Sub control 12.1 states to deny communications with known malicious IP addresses. In the scenario above, the firewall rules should have prevented the outbound command and control channel connection. Had the blocking been in place, the infected device would not have been successful in reporting to the remote server, leaving the malware in a dormant state. When the helpdesk reviewed the encrypted traffic, the list they were using was out of date and thus did not indicate a malicious connection.

Control 12.3 and 12.4 address the use of Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS) to review traffic for malicious traffic signatures and execute rules based upon that analysis. Had either the IDS or IPS been in place or configured appropriately, alerts on the inbound traffic

© 2015 The SANS Institute Author retains full rights.

(control channel to and from the infected device) as well as detected and or stopped the outbound flow of encrypted data to a malicious site.

Another issue is the missing element from sub control 12.5. This control requires that all traffic route through at least one proxy firewall. If the traffic is unable to be decrypted with the corporation's escrowed keys, then the traffic is not legitimate. By preventing unauthorized encrypted traffic, the data exfiltration is not possible.

3.4. Data Protection (CSC 13)

3.4.1. Why this control is important

Data protection begins by identifying and understanding where critical data is stored and who has access. Understanding the location of the data is one of the primary aspects of this control (CSC 13.1). One of the chief data protection mechanisms is Data Backup and recovery. Backup systems will protect by copying specific data from specific location. All too often users will store data outside of the normal channels and only discover a gap in backup processes after the data is corrupt.

Another method of protecting data is by the use of Data Loss Prevention (DLP) suites. While many DLP solutions are host based in nature, there are tools that are able to monitor the network traffic looking for pattern changes. A network based DLP solution can stop the data from leaving the company if the sensor detects that the outbound traffic has unknown encryption or has a destination that blocked.

Finally, encryption is a key aspect to ensuring the proprietary nature of the data. Concerning data, data has two states: data at rest and data in motion. Data at rest is data that is stored on a medium (e.g. a network share, an external drive, a SharePoint repository, etc.). Data at rest encryption is simply the act of providing an encrypting that data prior to storage. By encrypting that data prior to writing to disk, the data will be restricted to only those with the appropriate decryption key. Just as data at rest encryption is important, data in transit is a critical control. If the data transferred takes place without strong protection, confidentiality is at risk. For effective encryption, both parts are equally important.

© 2015 The SANS Institute Author retains full rights.

3.4.2. What controls should have been in place and why

Most importantly, the data that taken resided on an FTP server allowing anonymous login. Anonymous access to any service is curious; access to critical data without authentication is a serious infraction. Why the data was stored here is not important. That the data was stored with anonymous access is a critical failure with this specific case. As part of the critical control 13.1, the goal is to do an assessment of data to identify sensitive information. Had the organization known that critical and sensitive data was stored on this server; the data could be moved to a more secure location or additional controls placed to protect this system.

In this case, the data was sent from the FTP service to an external server. Had the proper protection been in place, the anomalous traffic would have been detected, and the proper alerts issued. By using a network based DLP solution, the traffic would likely have been detected and prohibited.

Also of concern is the failure of CSC 13.7. This sub control states the organization should monitor all traffic leaving the organization and detect any unauthorized use of encryption. Part of an effective network design is having encrypted channels well documented. Forcing external connections through a proxy is a check as well to ensure that any encryption uses the appropriate keys. As the outbound connection was encrypted with an external key, the control failed.

3.5. Wireless Access Control (CSC 15)

3.5.1. Why this control is important

The growth of wireless access at many businesses has been both a blessing (access for customers at no charge) and a curse (adding wireless to business infrastructure with little to no understanding of how wireless works or the concerns of such a connection). As a result, wireless attacks are relatively common these days. Many times the wireless is set up as a convenience. The fact that wireless access points (AP) can be set up and operational in minutes with very little technical knowledge poses a risk to networks. An employee just “trying to get the job done” can unwittingly open the network to complete exposure. Understanding who is connecting to your wireless infrastructure is just as important as understanding who and what devices are connecting to your more traditional wired networks.

© 2015 The SANS Institute Author retains full rights.

3.5.2. What controls should have been in place and why

The first sub control for wireless is that each access point connected to the network matches a defined need and is has a predetermined configuration. In this case, that did not happen. This was a lab based access point brought from home by the lab manager. The devices purchased for use within this lab had all included both wired and wireless options. As such it was just easier and faster (and neater) to simply use wireless. A common problem with any networking equipment is using factory defaults. These settings are publicly accessible and designed with operation in mind rather than securing the setup.

Wireless rogue detection, while used as an enterprise default, was not installed in this area, as this was previously a classified environment. Therefore, while the network supported rogue detection, this was not active in the area.

Another failure regarding wireless was the lack of encryption. Since the AP was using a default configuration, there was no encryption required between the lab AP and the devices connecting. The proper setting would be to require at least require AES-256 with Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).

The key aspect that makes wireless access so preferable to wired access is ease of use. In many cases, it is difficult if not impossible to run wires everywhere an information device is located. It can be difficult to run wires to and from shop floor environments, airport maintenance shops or lab areas where there are many people moving about and wires can be a hazard. On the other hand, wireless makes connection of a foreign device that much more dangerous. Often a connection runs from a switch to a patch panel and from the panel to a floor jack. Knowing the location of the floor jacks one can reasonably ascertain the location of any given device. With wireless, the device only needs to be within range of that signal. Absent any authentication on the AP, this is a real problem for security as a whole.

3.6. Account Monitoring and Control (CSC 16)

3.6.1. Why this control is important

In any given IT system, the concepts of confidentiality, integrity and availability are primary concerns. Confidentiality and integrity imply knowing who has access and who has changed the content. Using anonymous access discards the “need to know”, and bypasses normal access controls.

© 2015 The SANS Institute Author retains full rights.

Furthermore, anonymous changes the efficacy of auditing and logging. Any activity done under an anonymous login is non-attributable.

3.6.2. What controls should have been in place and why

The primary control violation was the anonymous access. The use of anonymous accounts allow anyone access to the data. The controls for this section actually are the opposite of the concept of anonymous access. Logging is required for proper auditing and allowing anonymous access is essentially non-authenticated. Further accounts that are accessing sensitive data should be using multifactor authentication (CSC 16.11) or at the very least use long passwords (CSC 16.12).

4. Corrective Actions

4.1. Inventory of Authorized and Unauthorized Devices (CSC1)

While the primary problem was the unauthorized equipment, (both the laptop and access point) the reason that these were able to operate was due to the switch configured as a DHCP server. A configuration change set the DHCP service to disabled and MAC address filtering installed. The current plans for network level authentication are still under review, but this change will remove the opportunity for unauthorized devices to connect in the future.

4.2. Limitation and Control of Network Ports (CSC 9)

FTP is a protocol that has no built in security and transmits data in the clear. The correction for this is removal of the FTP service and replace with a more modern file storage system. There is a process in place to review the data stored on this server and determine the appropriate placement in other areas. In addition, the ftp server is scheduled for decommission.

4.3. Boundary Defense (CSC 12)

The general direction for boundary defense is to ensure that only appropriate traffic enters or leaves the network. The network team has installed both a new IDS and IPS. The goal of this new system is to ensure that sensors can review the traffic at multiple points. The helpdesk also has updated the knowledge base to ensure that the technicians are able to validate out bound

© 2015 The SANS Institute Author retains full rights.

traffic. Network Engineering is performing a redesign of the DMZ to ensure that all traffic exiting the company has the appropriate encryption.

4.4. Data Protection (CSC 13)

While the concept of data protection is a very broad control, the goal is to ensure protection from unauthorized disclosure, destruction or alteration. As FTP passes user credentials in the clear, this violates all of the tenets of information security. While it is possible to push FTP through an encrypted tunnel, this was a legacy system and the team is scheduling this system for retirement. Management issued briefings to all employees regarding the issues caused by data stored in services that are not production, and not protected and backed up.

4.5. Wireless Access Control (CSC 15)

Wireless networks can be configured to operate with security as an underlying principle. The situation described above was an unauthorized access point. Not only is the access point be removed, but also steps taken to ensure that the users are given the appropriate security training and the network configured such that this situation cannot be repeated. Port security will be configured on all lab network segments.

4.6. Account Monitoring and Control (CSC 16)

Account monitoring was a problem with the anonymous access. With the retirement of the FTP Server, this control is met. Although the data was sensitive, the chief issue was the anonymous access that the FTP service allowed. Shutting this service off will address all of the issues.

© 2016 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

5. Conclusion

After the incident review concluded, the incident response team briefed the Chief Information Security Officer (CISO) as well as senior management with the findings. The CEO charged the CISO with implementing new controls or updating existing controls found at fault. Regretfully, the situation started with an employee bringing an unauthorized machine, and connecting to an unauthorized wireless access point. The malware then made a call to an external site to initiate the command and control traffic. The infected machine then did a port scan. When the adversary discovered the anonymous FTP server, the data captured and sent to an exfiltration server. The help desk did not recognize the traffic as malicious due to out of date IP data and a lack of IDS and IPS. Later, the team discovered that sensitive data was stored on the FTP site and that it was part of the exfiltration.

While the proximate cause of the issue was the malware, the chief failure was the ability of the malware-infected machine to connect to the network. Given that the wireless access point was an attempt to circumvent configuration control, the secondary issue is that of user education and security awareness training.

©2016 SANS Institute, Author retains full rights.

Bill Knaffl, bill.knaffl@gmail.com

© 2015 The SANS Institute Author retains full rights.

References

Center for Internet Security. (2013). *Critical controls for effective cyber defense v4.1*. Retrieved from https://www.cisecurity.org/documents/CriticalControlsv4.1.pdf

Center for Internet Security. (2015). *2014 annual report*. Retrieved from https://www.cisecurity.org/about/documents/2014report.pdf

Federal Bureau of Investigation. (n.d.). *Internet crime report*. Retrieved from http://www.ic3.gov/media/annualreport/2014_ic3report.pdf

Forbes Welcome. (n.d.). Retrieved from http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#7fe2be667fd5

Panda Security. (n.d.). 27% of all recorded malware appeared in 2015 - Panda Security Mediacenter. Retrieved from http://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/

Tarala, J. (n.d.). SANS SEC566: Implementing and Auditing the Critical Security – In Depth.

Verizon. (2011). *Verizon 2011 Data Breach Investigations Report*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Bill Knaffl, bill.knaffl@gmail.com

© 2015 The SANS Institute Author retains full rights.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event