Global Information Assurance Certification Paper

Leveraging the Asset Inventory Database

GIAC (GCCC) Gold Certification

Author: Tim Straightiff, t_straightiff@mastersprogram.sans.edu
Advisor: Adam Kliarsky
Accepted: December 29, 2016

Abstract

A well maintained Asset Inventory Database can aid in building a more comprehensive security program based on the CIS Critical Security Controls (CSC). Adding inputs and outputs to the database workflow will help the organization with several of the Critical Security Controls. The Critical Security Controls define a list of prioritized controls that, when followed, can improve the security foundation of an organization. The controls are most effective when implemented in order. Keeping an integrated and well maintained Asset Inventory Database with the proper inputs and outputs can serve as a foundational element in any comprehensive security program.

1. Introduction

The Center for Internet Security (CIS) has documented a series of controls, the CIS Critical Security Controls (CSC), based on real world actual attacks and proven effective defensive actions against those attacks. The controls are documented in a series of security actions, which when followed, can reduce exposure to risk. Currently, these twenty controls are designed to be implemented in a prioritized order. Some major themes of the CIS CSC are continuous monitoring and automation. Periodic checks only capture point in time conditions and may miss events happening between capture points. Continuous monitoring is much more effective than periodic time point checks since it captures all conditions and not just those at the scheduled intervals. Automating processes creates greater consistency and ties into the continuous monitoring recommendation since it can provide the ability to monitor continuously without adding staff.

The first two Critical Security Controls focus on understanding what is authorized to run in an environment and establishing procedures and tools to detect and report what is running. Listing these controls first emphasizes that in order to defend an environment you must first understand it. Knowing expected (normal) behavior will help identify unexpected (abnormal) behavior so the network so rogue devices or applications can be identified. Expected behavior, through thorough documentation and performance data, is crucial in detecting anomalies. The first step in most computer attacks is reconnaissance so the attackers can understand the network.

At the heart of the first two controls is an asset inventory database. The Asset Inventory Database contains information about what (software, applications, etc.) is running and where (devices). Many items in the Asset Inventory Database can be discovered through automated scanning. Once identified through the automated scanning process, additional information can be added such as asset owner, relationships to other assets, maintenance contracts, support numbers, external access requirements and application criticality. The database can then be used as a checkpoint to determine whether a running device or application is authorized. Alerts or reports can be produced

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

indicating unexpected behavior when a device or application is running which is not in the database. Action can then be taken on these alerts investigating and mitigating, if required, the unexpected application or devices to reduce risk.

In addition to using the database to check whether devices or applications are permitted, feeds to and from other systems can be developed to leverage the database for additional uses. By extending the information in the database and developing links to other related systems, the Asset Inventory Database can serve as a crucial element in most of the other controls. Having a robust Asset Inventory Database is a foundational item and can be beneficial in determining remediation priorities (CSC 4), data protection (CSC 13) requirements; the inventory also plays a role in incident response (CSC 19).

Expanding the inputs and outputs of the Asset Inventory Database from what the CIS CSC 1 and CSC 2 defines can provide additional information for use in the other controls and be a crucial element in any cyber defense program. Adding data fields and relationship information will create a more comprehensive database which can help with the implementation of the remaining security controls (CSC 3 through CSC 20).

2. Overview of the CIS Critical Security Controls

2.1. CIS Critical Controls Defined

The Center for Internet Security (CIS) Critical Security Controls (CSC) define a list of prioritized controls that can improve the security foundation of an enterprise. The controls are designed to be most effective when implemented in order.

In the development of the controls there were several guiding tenets (CIS, 2016, p.3):

- Offense informs defense: use knowledge from actual events which have been documented and review lessons learned to build effective defenses for those events
- Prioritization: implement controls in an order which provides the greatest risk reduction first

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

- Metrics: establish a way to measure and communicate the effectiveness of the controls
- Continuous diagnostics and mitigation: measurement should be continuous to validate the effectiveness of the controls
- Automation: where possible automate actions, so results are consistent, reliable and scalable.

The guiding tenets were developed to make sure the controls were focused on providing a consistent method to both block initial compromises of systems and to also detect and address existing compromises.

2.2. Control Groupings

The Critical Security Controls are separated into three control priorities; System, Network and Application Controls. The current (version 6.1) list of Critical Security Controls grouped into their control priorities are:

- System Controls
    1. Inventory of Authorized and Unauthorized Devices
    2. Inventory of Authorized and Unauthorized Software
    3. Secure Configurations for Hardware and Software
    4. Continuous Vulnerability Assessment and Remediation
    5. Controlled Use of Administrative Privileges
    6. Maintenance, Monitoring, and Analysis of Audit Logs
    7. E-mail and Web Browser Protections
    8. Malware Defenses
    9. Limitation and Control of Network Ports
    10. Data Recovery Capability
- Network Controls
    11. Secure Configurations for Network Devices
    12. Boundary Defense
    13. Data Protection
    14. Controlled Access Based on the Need to Know

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

15. Wireless Access Control

- Application Controls
    16. Account Monitoring and Control
    17. Security Skills Assessment and Appropriate Training to Fill Gaps
    18. Application Software Security
    19. Incident Response and Management
    20. Penetration Tests and Red Team Exercises

2.3. Cyber Hygiene Controls

The National Campaign for Cyber Hygiene identified Critical Security Controls 1 through 5 as essential priorities and refers to them as "Foundational Cyber Hygiene." These are identified to help provide a plain-language approach to the CIS Critical Security Controls by providing a list of simple questions that should be answered (CIS, 2016, p.80):

- What is connected to systems and networks? (CSC 1)
- What software is running on systems and networks? (CSC 2)
- Is monitoring of the systems done continuously, managing against "known good" configurations? (CSC 3)
- Is there a continual search for "known bad" software? (CSC 4)
- Are people/accounts with administrative privileges restricted and logged to determine if they can or have changed, bypassed, or over-ridden security settings? (CSC 5)

2.4. CIS CSC #1 and #2

Control 1, Inventory of Authorized and Unauthorized Devices, and Control 2, Inventory of Authorized and Unauthorized Software, focus on actively detecting and monitoring what is connected and running on the network to compare against what is authorized or expected. Detecting unauthorized devices or applications is necessary when identifying potential issues. CSC 1 recommends to "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices

are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." (CIS, 2016, p.6)

The business goal of CSC 1 is to assure that only authorized systems are on a network (SANS, 2016, p.1-62). Assuring that only authorized systems are present on a network the risk is lowered by identifying and prohibiting rogue devices from being present.

The System Entity Relationship Diagram (ERD) for CSC 1 shows the automated inputs into the Asset Inventory Database for devices and the outputs from the database for alerts and reports.

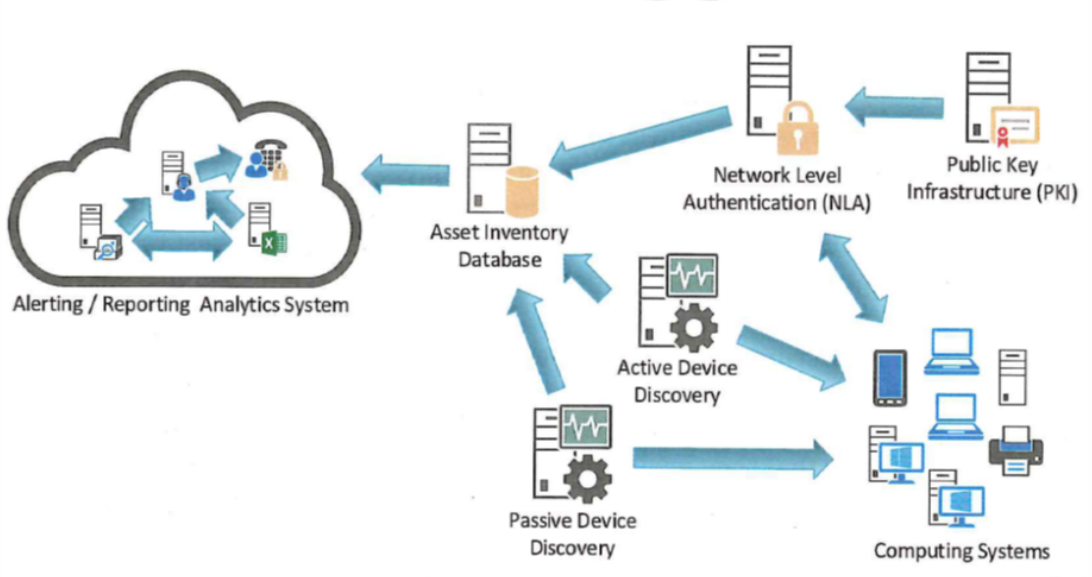

Figure 1: CSC 1 System Entity Relationship Diagram (CIS, 2016, p.9)

CSC 1 deals with hardware devices, CSC 2 references software applications. The business goal of CSC 2 is to assure that only authorized software is installed in the environment. (SANS, 2016, p.1-90). By ensuring that only authorized applications are present on a network risk is lowered by identifying and prohibiting rogue software from being present.

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

The System Entity Relationship Diagram (ERD) for CSC 2 shows the automated inputs into the Asset Inventory Database for software and the outputs from the database for alerts and reports.

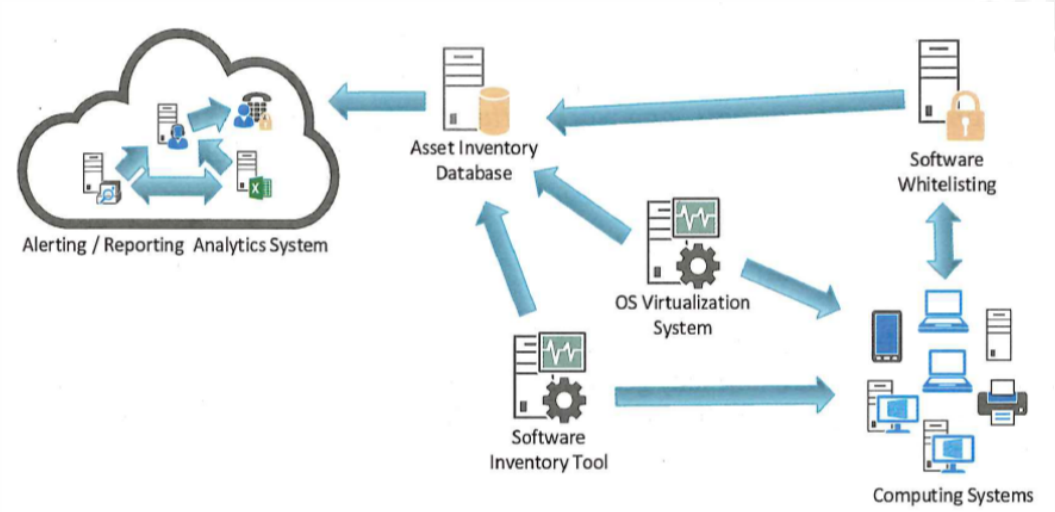

Figure 2: CSC 2 System Entity Relationship Diagram (CIS, 2016, p12)

Controls 1 and 2 focus on gaining an understanding of what is installed and running in the environment. This knowledge will help in implementing and managing the remaining controls. Both controls gather information about the environment to document what is authorized and where it is present. The Asset Inventory Database is used as a common database to record the information. The Asset Inventory Database becomes the focal point for information about all the devices and applications authorized to run on a network.

3. The Need for Knowledge

3.1. Operations Requirements

Operation and application support teams manage the corporate environments. Running day to day activities associated with any IT organization requires an understanding of what you are managing. As complexity grows, the network becomes larger, or changes are made, the importance of documentation increases. The Asset

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

Inventory Database can serve as a starting point for system documentation including network diagrams, application architecture documents, run books and problem resolution procedures. With the addition of new fields in the Asset Inventory Database knowledge of the network can be enhanced and the additional data can be used in some of the remaining CSC's 3 through 20. Having a better-documented environment helps in the strategy, design and management of support systems like the backup environment, external access systems, security systems and disaster recovery plans. Increasing the data fields available within the Asset Inventory Database can help the operational teams fulfill their duties.

3.2. The Attacker's Perspective (Cyber Kill Chain)

Understanding a network, the devices on it, and the applications installed is critical in both organizationally supporting an environment and also in attacking an environment. Understanding what is being defended is the first step in defense, and it is also the first step many attackers take. The Intrusion Kill Chain described by Lockheed Martin identifies the processes attackers can use for computer network attacks and computer network espionage, including seven kill chain phases (Hutchins, Cloppert, & Amin, n.d.):

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

Once attackers identify a target, they want to build knowledge about that target so they can plan the attack. Knowledge of the environment is critical when deciding whether to manage the computer environment, defend the environment or to attack the environment. The Asset Inventory Database is foundational in understanding a

computing environment. Properly managed and kept up to date, the database can help in the process of maintaining and protecting assets by serving as a repository of known good devices and applications. This repository can then be checked by monitoring systems detecting devices and/or applications to determine if they have been previously identified and authorized. When unauthorized devices or applications are detected, alerts can be created so the activity can be investigated.

Robert Joyce, head of NSA's Tailored Access Operations stated in 2016 at the USENIX Enigma security conference that the NSA is successful because "We put the time in …to know [that network] better than the people who designed it and the people who are securing it," he went on to say "You know the technologies you intended to use in that network. We know the technologies that are actually in use in that network. Subtle difference. You'd be surprised about the things that are running on a network vs. the things that you think are supposed to be there." (Zetter, 2016). As an attacker, understanding the network is critical.

The Penetration Testing Execution Standard documents seven main sections for a penetration testing execution standard (PTES, n.d.):

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

Under this standard, gaining knowledge about the target is the first step once permission is granted.

Whether you are attacking a network or supporting and defending a network, knowledge of what is authorized and normal should be one of the first steps in your work. With detailed knowledge about a network and what is normal, you can identify what is

out of the ordinary and a potential issue. The Asset Inventory Database can be the key repository of information about the network and help with this knowledge.

4. Asset Inventory Database

4.1. The Base Components

The first two controls, Inventory of Authorized and Unauthorized Devices, and Inventory of Authorized and Unauthorized Software, rely heavily on the Asset Inventory Database. The procedures and tools in these two controls are focused on building and maintaining the Asset Inventory Database and then utilizing that data to report and alert on deviations and utilize the information to know what is on the network.

CSC 1.4 states the Asset Inventory Database must maintain the following, network addresses, machine name(s), asset and department owner(s). CSC 2.3 notes the software inventory system should be tied into the hardware asset inventory, so all devices and associated software are tracked from a single location to allow a centralized source for information about the computer network. Having a centralized source of information can aid in problem solving, incident response and system design. (CIS, 2016)

Components are outlined in the CSC controls for the Asset Inventory Database at minimal levels. Procedures and tools are described to build and maintain the database at those levels. The database can be expanded to contain information that could help with many of the remaining controls. The database created and updated in the first two controls documents core information about the environment such as device name, IP address, asset owner, application name and department owner.

4.2. Software and Hardware Inventory Relationship

In evaluating what is running in the environment, a critical piece is knowing what software is running on which devices. Applications running in a company provide a benefit to the business. The applications run on or through the hardware devices. It is important to know the relationships between them and document where applications are running and what dependencies they have. When an event affects a hardware

component, what applications can potentially be affected? Fully developing knowledge of the environment should go well beyond applications running on servers, if a switch, router or firewall fails what devices are attached to it and what applications do they support? Tracking these relationships helps resolve problems and evaluate risk. The information obtained from these relationships can be used to identify critical components and then design and implement compensating controls.

Applications have levels of criticality to the business and the security of the environment as a whole. Tracking the criticality in the Asset Inventory Database can aid in developing focus areas for some of the remaining CSC's. Criticality can aid in remediation prioritization when working on CSC 4, Continuous Vulnerability Assessment and Remediation as well as on backup controls referenced in CSC 10, Data Recovery Capability.

The relationship between software and hardware needs to be tracked in the database so the environment can be better understood and maintained. By tracking hardware and software dependencies, the Asset Inventory Database can be linked to other sources of information to make current and up to date information accessible. The database can be expanded to include additional fields such as criticality. Adding criticality to Asset Inventory Database can further aid in implementing additional CSC's by allowing better prioritization of devices and applications.

4.3. Expanding Inputs: Asset Owner

As noted in CSC 1.4 there should be an asset owner listed for each hardware device. The procedures and tools noted in CSC 1 focus on creating automated feeds through passive and active scanning of the environment. Procedures and tools noted in CSC 1.4 center on the asset itself and may miss some of the associated information such as asset owner. The asset owner can be manually entered either in the Asset Inventory Database or entered into an asset record in Active Directory or a similar type system, but the key is that it has to be entered manually at least once.

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

Once the asset owner is inputted, it becomes a static entry. Creating a process to maintain the asset owner will make sure the field stays current. The procedures and tools outlined in CSC 1 do not address maintaining the asset owner field specifically. As with all the controls, automation, and continuous monitoring is best because asset owner is a required point of contact in events affecting the asset. Support or incident management teams do not want to be trying to find out who owns an asset when there is an event such as a failure, they need to know who the contact is. Many events happen outside business hours and having current information can save valuable time by not having to contact people to update information that has become out of date.

Maintenance and updating of an asset owner field must be done on a consistent basis. As personnel in organizations change, roles and responsibilities change, therefore, these changes need to be noted in the Asset Inventory Database when they occur. Documenting updates can be done manually by sending confirmations to asset owners on a scheduled basis or, in the spirit of the CIS Critical Security Controls, reports, could be generated when changes are made to Active Directory or the HR system. Automating either the alerting or the updating of asset owners in the database can help maintain the integrity of the Asset Inventory Database.

4.4. Asset Additions and Retirements

Changes to assets in an environment should be identified through automated monitoring by the procedures and tools deployed; however, having an additional record of additions and deletions through the asset management process will verify the results of the automated tools. In addition to verification of the changes, having a record when the activity takes place will keep the inventory up to date, aid in filling in the additional fields required, and noting relationships between assets.

In larger companies, there can be separate teams involved in the build, maintain and retirement phases of assets. Developing feeds from these work groups is recommended in order to keep the inventory up to date. Current information is critical for the operational teams and incident response teams to be able to respond quickly and efficiently while working on an issue.

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

4.5. Additional Fields: External Access

Some applications or devices may be required to be externally available because external customers, prospects, clients, vendors or support staff may need access from remote locations. When an application or device is externally available, additional fields can be entered into the asset record:

- How is the application or device accessed (ex. VPN, Citrix Gateway, NAT through the firewall, DMZ)?
- Is there a direct external address?
- Is there an external DNS entry?
- Is there a certificate installed?
- Is there a firewall involved?

By adding fields for external access (Y/N), external DNS entries, external IP addresses, firewalls (device and rule), and external customer or vendor contacts will add pertinent information to the asset inventory and again aid in problem resolution and incident management. With the added fields, communication and coordination with the teams managing firewalls, DNS, certificates and communications with external parties will be easier. Automating reports from the firewall, DNS, management, and other teams involved will help in the maintenance of the inventory. Keeping track of these items in the inventory will consequently improve communications with other teams when assets are added or retired.

Communication between various teams managing components of the multiple technologies is the key to keeping all records and systems updated. When an asset with external access is added or retired, the associated access rules and DNS records must be updated. Tracking certificates installed will also be important to report expirations if a separate certificate management system is not in place.

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

4.6. Coordination with Change Management Systems

Updating the Asset Inventory Database is initiated through automated scans. The automated scans can detect a wealth of information including memory, disk space, and CPUs. These items can be updated either physically or, in the case of a virtual machine, by changing parameters. Detecting these changes is important in managing the environment. All changes need to be authorized. In companies where a change management system is in place, a link between the Asset Inventory Database and the change management system will enable verification that changes were authorized. In larger environments, the change management system may be able to be linked to the Asset Inventory Database. In smaller environments reports could be produced showing changes for manual verification.

4.7. Additional Outputs

Enhancing the reporting functions of the Asset Inventory Database can be facilitated using more fields. By adding linkage between AD and HR systems, reports can be created to show assets with owners changing roles and responsibilities or leaving the company. The addition of external DNS/IP information can enable alerting to firewall and DNS teams if an asset is retired or changed. Changes in assets can be reported out and verified against approved changes in the change management system.

The use of automation to schedule reports or to run matching programs will further enhance the impact of the asset inventory database.

4.8. Impact on Other Controls

The Asset Inventory Database is a foundational element of the CIS Critical Security Controls. A case can be made that the Asset Inventory Database can be utilized in each and every control with the proper information kept in the database. The data contained in the database can be used by many teams and extends well beyond ascertaining and verifying only approved and authorized devices and applications that are running in the environment. The database could be important in the initial diagnosis of an incident or equipment failure. While the database is foundational, it's impact can be

far reaching if enhanced to contain additional information and linkage with other sources of information.

An alternative way to approach the fields required in the Asset Inventory Database would be to look at each control and then determine if additional data in the Asset Inventory Database could help fulfill the requirements of that control. For example, the listing of a criticality field could help prioritize remediation in CSC 4, Continuous Vulnerability Assessment and Remediation. The addition of fields identifying and listing external access information could help in identifying assets which should be securely hardened (CSC 3) and protected by boundary defenses (CSC 12).

The diagram below lists some proposed additional fields and areas of impact they can have. The diagram also shows the proposed connection between the asset owner and the HR/Active Directory systems designed to keep the information current.

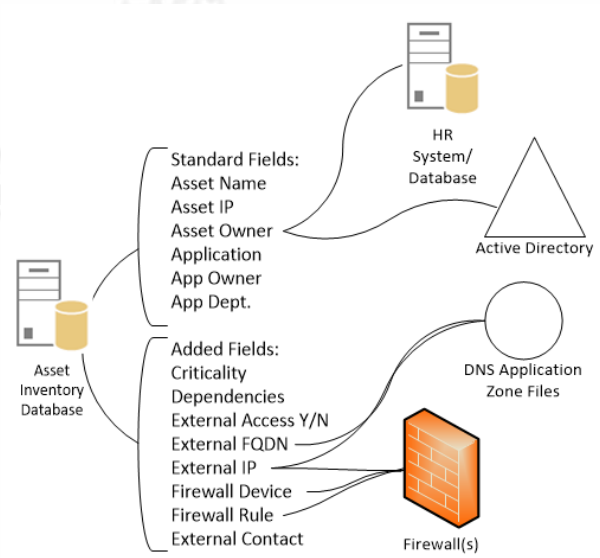

Figure 3: Additional Fields and System Impact

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

5. Conclusion

Implementation of the CIS Critical Security Controls can improve organizational security and lower risk levels. While listing the controls in a series of twenty security actions, the first two focus on understanding the environment. Developing an understanding of the environment is a foundational item, without that understanding the remaining controls are not as effective. The first two controls introduce the importance of an Asset Inventory Database and establish some required fields.

The Asset Inventory Database is the primary collection of information upon which assets are evaluated to understand if they are authorized. The initial information in the Asset Inventory Database can be acquired through active and passive scanning as discussed in the CIS CSC document. The required fields listed in the first two controls define what is required to fulfill these controls.

By adding additional fields to the Asset Inventory Database, it can have an impact on many of the subsequent controls. By reviewing each of the additional controls and determining what information could be added to the database to help with those controls, the Asset Inventory Database could be expanded to serve as a foundational element in many controls. Building a highly useful asset database requires looking at the individual fields and determining where does this data come from, what is the impact to other systems, and how do we keep the information current. This information will help support teams structure additional fields in the database and create links with other systems to enhance the value. This additional information will provide enhanced data and can then serve as a foundation to build a successful operating environment which is up to date and defensible.

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

References

Center for Internet Security (CIS). (2016). *The CIS Critical Security Controls for Effective Cyber Defense Version 6.1*

Hutchins, E. M., Cloppert, M. J., Amin, R. M. (n.d.). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

The Penetration Testing Execution Standard (PTES). (n.d.). Retrieved from http://www.pentest-standard.org/index.php/Main_Page

The SANS Institute. (2016). Security 566: *Implementing and Auditing the Critical Security Controls – In-Depth (Book 1)*

Zetter, K. (2016). *NSA Hacker Chief Explains How to Keep Him Out of Your System*. Retrieved from https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

Tim Straightiff,
t_straightiff@mastersprogram.sans.edu

Last Updated: June 23rd, 2017

Upcoming Training

SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
Community SANS Scottsdale SEC566	Scottsdale, AZ	Aug 14, 2017 - Aug 18, 2017	Community SANS
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Toronto SEC566	Toronto, ON	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZ	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced