IMPLEMENTING CIS CRITICAL SECURITY CONTROLS FOR ORGANIZATIONS ON A LOW-BUDGET

A thesis

Presented to

The Faculty of the Department of Information and Logistics Technology

University of Houston

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

Information System Security

By

Bashar Shamma

December 2018

IMPLEMENTING CIS CRITICAL SECURITY CONTROLS FOR ORGANIZATIONS ON A LOW-BUDGET

Bashar Shamma

APPROVED

Wm. Arthur Conklin, PhD
Committee Chair
Associate Professor
Information and Logistics Technology

Christopher Bronk, PhD
Committee Member
Assistant Professor
Information and Logistics Technology

Stuart Wagner, MBA
Committee Member
Enterprise Products Partners L.P.

George Zouridakis, PhD
Associate Dean for Research and Graduate Studies
College of Technology

Enrique Barbieri, PhD
Department Chair, Information
and Logistics Technology

Acknowledgment

I would like to express my deepest gratitude to Dr. Wm. Arthur Conklin. Words cannot describe how much of my career I owe to his guidance and encouragement. There is no doubt that taking his classes as an undergraduate student planted the seed for my career and my passion for this field. Dr. Conklin’s recommendation along with my hunger for his wisdom; were the reasons I returned to school to earn a master’s degree. To me, Dr. Conklin was not only a professor teaching information security principles, but he was also a wise and intelligent person teaching a mindset on the way to look at problems and analyze them. I took every chance to learn from his wisdom and knowledge and applied it to my life and career. This acknowledgment will not do Dr. Conklin any justice so I will take it upon myself to show my appreciation and my respect to Dr. Conklin by paying it forward to helping and guiding others and share everything he has taught me.

I also wish to thank my committee members, Dr. Christopher Bronk and Mr. Stuart Wagner for taking the time to review and provide recommendations for this thesis. I am honored to present before you and very thankful for sharing your invaluable knowledge and experience to make this research better.

I must express my gratitude to my parents for their continuous support and encouragement. Thank you for teaching me responsibility and discipline, it has definitely paid off. Thank you for everything you have done to make me who I am today. My continuous career and educational growth is proofing that your pains and struggle to raise me did not go to waste. I hope I made you proud today.

Finally, I would like to express my gratitude to my wife, Mariam. Thank you for believing in me. Thank you for being there for me every time I needed you. Thank you for the unconditional support throughout this journey. I couldn’t make it to the finish line without you.

Abstract

Small and medium size businesses have a lower chance of detecting and preventing cyber-attacks due to the high cost associated with adopting the latest security solutions and frameworks. This thesis presents a potential approach to implement most of the CIS Critical Security Controls without the need to dedicate a large budget to acquire commercial security solutions. An organization can adopt open source security solutions along with Windows built-in tools to cover most of the CIS controls if the organization implemented the policies and procedures necessary for each control. Any organization including small and medium size business can start improving their security posture by utilizing the cost-effective solutions mentioned throughout this research.

Table of Contents

Table of Tables

Abbreviations

ACLs	Access Control Lists
AD	Active Directory
AD FS	Active Directory Federation Services
AD CS	Active Directory Certificate Services
AES	Advanced Encryption Standard
APs	Access Points
ASLR	Address Space Layout Randomization
AV	Antivirus
CaaS	Crime-as-a Service
CIS	Center for Internet Security
CSC	Critical Security Controls
DCs	Domain Controllers
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
EAP/TLS	Extensible Authentication Protocol-Transport Layer Security
GPOs	Microsoft Group Policy Objects
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IEC	Information Security Management
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Dictionary Access Protocol
MAC	Media Access Control
MFA	Multi-Factor Authentication
NAC	Network Access Control
NFC	Near-field communication
NICE	National Initiative for Cybersecurity Education
NIDS	Network Intrusion Detection Systems
NIPS	Network Intrusion Prevention Systems
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol

OSS	Open Source Software
OSSS	Open Source Security Software
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
QA	Quality Assurance
RDP	Remote Desktop Protocol
S-SDLC	Secure Software Development Lifecycle Project
SANS	SysAdmin, Audit, Network, Security
SCT	Microsoft Security Compliance Toolkit
SIEM	Security Incident and Event Management
SMBs	Small and Medium Size Businesses
SSH	Secure Shell
TPM	Trusted Platform Module
URL	Universal Resource Locator
USB	Universal Serial Bus
VLANs	Virtual Local Area Networks
VNC	Virtual Network Computing
WAFs	Web Application Firewalls
WIDS	Wireless Intrusion Detection System
WMIC	Windows Management Instrumentation Commandline

Introduction

During the past decade, organizations have witnessed an increased number of cyber-threats. In 2017, there were 1,579 million recorded data breaches which contributed to the exposure of about 180 million records.[1] Furthermore, the financial impact of cyber attacks is huge; according to recent estimates by the Ponemon Institute in 2018, the average total cost of a data breach is $3.86 million.[2] The total cost of a data breach has increased by 6.4% in 2018 when compared with 2017 cost.[2] Furthermore, the probability of a breach recurring within a 2-year timeframe is almost 30%.[2]

Attacks are becoming easier and cheaper to carry especially after the creation of Crime-as-a Service (CaaS) model. The CaaS is a complex and organized model that provides attackers with high-performance tools and services at a relatively low cost as low as $100 per 1000 installs for their infection/spreading services.[3] Cyber attacks affect the operation of organization across all sectors. No company is completely immune from potential cyber threats. The potential risk for cyber threat is unavoidable, but, vulnerabilities can be significantly reduced by implementing security controls which can eventually lead to a decreased risk.[4]

The impact of cyber attacks was recognized by the majority of business leaders.[5] According to the Global State of Information Security Survey in 2018, a successful cyber attack could lead to losses or damages to operations loss of high-value data, lower quality of products and services, and physical damages.[5] On average, it takes 191 days for a company to detect the presence of a data breach.[6] With such timeframe, the impact of a successful breach may eventually lead to loss of time and money, loss of business reputation and loss of business value in the market. [7]

A plan to secure the company information and assets is needed regardless of the size of the company.[8] Small and medium size businesses (SMBs) do not usually put enough effort to secure their network and data due to the lack of awareness, resources, and budget; which makes SMBs the perfect target to access bigger companies' network. The best example for this scenario is the famous retailer "Target" hack and credit cards breach. The attackers compromised the Heating, Ventilation, and Air Conditioning (HVAC) service provider's network and then pivoted to Target network. This breach has cost Target $162 million in expenses.[9]

SMBs also have valuable information that must be protected to maintain the company credibility and business function including product information, financial information, customer information. SMBs are at risk of attacks from competitors who could steal their customers, protocols, pricing information, contracts, and other valuable data.[10] Any breach that compromises the company's data and information assets may lead to significant losses in the company assets and functionality and legal liabilities that may eventually lead to a complete loss of the company.[8]

Literature Review

Center for Internet Security (CIS) Controls

Although there are other developed security frameworks such as the International Organization for Standardization (ISO)/Information Security Management (IEC) 27001 and ISO/IEC 27002 and the National Institute of Standards and Technology (NIST) 800-53.[11, 12], these frameworks require a great effort to implement and understand because of the wide range of controls that these frameworks provide. The CIS controls were designed to provide organizations with a smaller number of actionable controls to gain effective, immediate and high impact security outcomes; which makes the CIS controls a good fit for SMBs [12, 13].

The primary focus of the CIS controls is to improve the organization's ability to prevent and stop attacks before these attacks are declared as incidents. The CIS controls do not focus on providing detailed guidelines for incident detection, mitigation or response but rather provide guidelines on reducing the number of incidents by preventing successful breaches and exploitations against the organization. Thus, when comparing the CIS controls to other frameworks, the CIS controls can provide the foundation to build upon the previously mentioned security frameworks.

Definition

SysAdmin, Audit, Network, Security (SANS) Institute has defined the CIS controls as "A recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks."[14]

Another definition to better understand the functionality of the CIS Controls has been provided by the CIS is "The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks."[15]

Brief History

In 2008, the Department of Defense (DoD) has requested from the National Security Agency (NSA), CIS, the SANS Institute and multiple private sectors to develop a framework that helps organizations identify and address their security gaps.[13] The initial goal of the CIS controls was to prioritize a list of main controls to prevent the majority of potential attacks.[13] The initial draft of the CIS controls was published in early 2009 and multiple organizations and information technology (IT) specialist has evaluated the initial draft and submitted their input for a final validation by the State Department.[13]. When this initial draft was validated and the initial security controls were implemented, the State Department has witnessed a significant decrease in attacks numbers in 2009.[13] More than 88% of cyber vulnerabilities was reduced across 85 thousand systems in the State Department.[13] Back then, the CIS controls were known as the "Consensus Audit Guideline". A few years later, the ownership of CIS controls was transferred to SANS in 2013 and was called the SANS Top 20 Critical Security Controls. It was in 2015 when the ownership was moved to the CIS, and now it is known as the "CIS Critical Security Controls". [16]

Version 7

After almost 3 years of the release of Version 6, the Center for Internet Security has released Version 7 of the CIS controls on March 19, 2018. The major change in version 7 is the change of controls' categorization. The CIS has moved from Foundational and Advanced categories in version 6 to Basic, Foundational, and Organizational categories in version 7. The new version also recommends immediate implementation of the first six controls instead of the first five in version 6. There are still 20 controls in version 7 with some controls rearranged but the number of sub-controls has increased from 139 to 171 sub-controls. [15]

Open Source Software (OSS)

Definition

Open source software (OSS) is software developed by individuals or organizations who publish the original underlying code for the software publicly for other individuals or organizations to view, alter, modify or re-distribute.[17]

Open Source Security Software (OSSS) and Distributions

There are dozens of OSSS and distributions that offer defensive security capabilities and protect systems and network form potential cyber-attacks. Some popular open sources security tools and distributions are:

Security Onion

Security Onion is a free and open source Linux distribution.[18] It includes multiple open source tools for network security monitoring and log aggregation to name a few. The distribution has grown and improved tremendously over the years and is largely used in enterprises today.

OpenVAS

Open VAS (Stands for Open Vulnerability Assessment System) is a free and open source framework developed by Greenbone network in 2009.[19] It is an online, free, automated vulnerability scanner. It can be installed on any Linux system or be deployed as a standalone using a virtual machine.

Wazuh

Wazuh is an open source, intrusion detection system that can monitor and analyze the internal system as well as the hosts on the network.[20] It is integrated with other potent tools such as OSSEC, OpenSCAP and ELK Stack for an optimal monitoring and management solution.[21-23] It provides a various set of capabilities, including log management and analysis, file integrity monitoring, host based intrusion, and anomaly detection, policy and compliance monitoring.[20]

Kolide Fleet

Kolide Fleet is an open source software that gives organizations a better view of their endpoints by providing the ability to collect live information from the endpoint.[24] This information is gathered by running SQL-like queries using Osquery.[25]

pfSense

pfSense is an open source firewall and router developed by Nergate.[26] It includes a web interface that allows hardware management without installing any software to manage.

Problem Definition

SMBs are the drivers of the economic growth in the United States. There are more than 30 million SMBs in the United States.[27] About 50 % of all employees in the United States work in SMBs.[27] Almost half of the cyber attacks target SMBs that consist of fewer than 250 employees.[10] In 2017, 61 % of breach victims were SMBs with less than 1000 employees.[28] Meanwhile, only one-fourth of SMBs are prepared for potential cyber attacks.[29] Almost 60% of SMBs reported that lack of budget is the main obstacles they face to secure their data. [29] The majority of SMBs does not have an adequate budget to buy and deploy security monitoring tools and equipment. According to a recent evaluation of 50 systems in Captera's network security directory, the average cost for one network security software for SMBs is around $1,400.[30] The average cost per license for one year is $1,000-$2,000.[30] Companies usually need multiple software to secure their company and need multiple licenses for multiple endpoints or servers. Many of SMBs do not have the capacity to purchase and deploy the necessary security software in their organization. This makes SMBs more prone to cyber-attacks and business loss.

Furthermore, SMBs may face major challenges to choose the appropriate security solutions for its environment even if they know their security requirements. Choosing the right solution to cover a certain control is challenging since the information and research to map OSSS solutions to certain controls is limited today. SMBs have limited resources and budget to investigate and determine the suitable security solution needed. Even if the company is aware of the software needed to secure its environment, the company maybe at a stage where it does not have the budget or the investment capacity for such software. The utilization of OSSS provides organizations with an alternative solution to protect their systems.

Purpose, Scope, and Goal

The aim of this thesis is to propose five OSSS and distributions that along with Windows built-in tools can cover most of the CIS controls.

The scope of this thesis will be limited to proposing solutions for the Windows operating system. Linux and macOS will not be covered throughout this research. This thesis will neither discuss the technicality of implementing the proposed solution nor provide a step by step guide to cover the CIS controls. But rather, the thesis will propose an approach to cover the CIS controls using OSSS and standard Windows-built-in tools that do not require additional Microsoft licenses. Estimating the cost associated with additional hardware or staffing needed to implement the proposed solutions is outside the scope of this thesis.

The goal is to help SMBs cover any missing gaps for a certain CIS control or to start planning the overall security roadmap to implement all the CIS controls without the need to buy expensive commercial security software and using solutions that can be implemented in a timely manner.

Methodology

This research started by analyzing the sensors for each sub-control of the CIS controls (version 7).[31] The CIS controls, sub-controls, and sensors are listed in Appendix 1. A sensor is considered as the baseline or the technical process that is necessary to implement a specific sub-control. Initially, the sensors of the first six CIS control were analyzed. The first six CIS controls are considered as the “Basic Controls” and have the highest implementation priority according to the CIS recommendation.[15] Thus, ensuring the coverage of the first six CIS controls is a priority.

During the initial sensor analysis, each sub-control of the first six CIS control was analyzed. Then, if the sub-control does not require a technical tool to be implemented and can be covered by implementing a policy or a process, it was assigned a policy/process as the primary tool.

Next, only the sensors that require a technical tool were aggregated to identify the most required sensors across the first six CIS controls. The result of this analysis is shown in Table 1.

Table 1: Aggregated count of sensors for Basic Controls (CSC 1 to 6)

Sensor	Sensor Frequency
Log Management System / SIEM	7
Software Whitelisting System	4
Software Application Inventory	4
SCAP Based Vulnerability Management System	3
Patch Management System	2
Network Level Authentication (NLA)	1
System Configuration Enforcement System	1
Passive Device Discovery System	1
Public Key Infrastructure (PKI)	1
Active Device Discovery System	1
Asset Inventory System	1

After that, the potential technical solution that will cover each sensor was identified. The popularity of the tool, features, and functions, integrations, available modules, and add-ons, as well as strong documentation and online support, were some of the criteria considered when choosing the solutions. Windows built-in tools were also considered in this research as these tools are usually available in the organization and can be implemented easily and do not require additional licensing.

Based on the mentioned criteria, the following five OSSS and distributions were chosen for this research:

- **Security Onion:** is considered as a distribution and not a solo tool. Thus, it provides many OSSS out of the box such as ELK Stack, Snort, Bro and Suricata, to name few.[32-34] This makes Security Onion a perfect candidate to cover as many CIS controls as possible very quickly.
- **OpenVAS:** will cover most of the requirements regarding network vulnerability scan and risk assessment and with the available virtual machine image, an organization can start scanning their environment in no time.
- **Wazuh:** provides a great integration with OSSEC and OpenSCAP to give an organization a very useful insight into their assets' compliance with organization's security standards as well as file integrity monitoring, log monitoring, rootcheck, and process monitoring capabilities. All from a single dashboard.
- **Kolide Fleet:** provides the ability to centrally control and overview a collection of Osquery agents across the enterprise and collect live information from endpoints at any time. Organizations can query any endpoint for open ports or programs installed using Osquery. Osqery even gives the ability to collect a hash value for any file on the system.
- **pfSense:** is a software distribution that an organization can utilize as a firewall or a router. Since pfSense usually sets at the perimeter as a firewall device, many modules can be utilized for more functionality without the need to implement new systems or devices.

Once the OSSS were identified and picked for each sub-control, another analysis was done against all the sensors across all sub-controls excluding sensors for the sub-controls that can be implemented using a policy or a process. This analysis re-confirmed the initial findings; the most common sensors for the first six CIS controls are also among the top for the most common sensors for the 20 CIS controls. The results are shown in Table 2.

Table 2: Aggregated count of sensors for all controls (CSC 1- 20)

Sensor	Count of Sensors
Log Management System / SIEM	12
Network Firewall / Access Control System	8
SCAP Based Vulnerability Management System	7
System Configuration Enforcement System	7
Software Whitelisting System	6
Endpoint Protection System	6
Software Application Inventory	4
Anti-Spam Gateway	3
Identity & Access Management System	3
Multi-Factor Authentication System	3
Network Device Management System	3
Network URL Filtering System	2
Host Based Data Loss Prevention (DLP) System	2
Patch Management System	2
Network Based Data Loss Prevention (DLP) System	2
DNS Domain Filtering System	2
Backup / Recovery System	2
Data Inventory / Classification System	1
Host Based Firewall	1
Active Device Discovery System	1
Network Level Authentication (NLA)	1
Web Application Firewall (WAF)	1
Network Packet Capture System	1
Application Aware Firewall	1
Network Based Intrusion Prevention System (IPS)	1
Software Vulnerability Scanning Tool	1
Wireless Intrusion Detection System (WIDS)	1
Asset Inventory System	1
Network Based Intrusion Detection System (NIDS)	1
Whole Disk Encryption System	1
Penetration Testing Plans	1

Sensor	Count of Sensors
Public Key Infrastructure (PKI)	1
Passive Device Discovery System	1

Next, a research through each proposed tool's documentation was conducted to verify the sub-control coverage. If the documentation did not lead a strong evidence of coverage, a basic testing of the tool was conducted to ensure that the tool offers a feature or a module that can cover the sub-control requirements. If the tool was able to cover all the requirements for the sub-control, it was assigned as a “primary tool”. If multiple tools were needed to cover the sub-control, a second technical solution was assigned as “secondary tool” to complement the primary tool’s coverage. If the sub-control requirements cannot be covered by the primary five OSSS or Windows built-in tools and needed an additional out-of-band tool, that out-of-bound tool was assigned as “Other Options”. The “Other Options” column was also assigned additional optional tools as an alternative.

Finally, a statistical analysis was performed to determine the overall proposed tool's coverage per control; aggregated by the coverage of the control's sub-controls.

Implementing CIS 20 Critical Security Controls

Basic Security Controls

The first six CIS controls are considered the “Basic Controls” because they are the ground to build the rest of the controls on. They are considered the minimum necessary controls to start improving the organization’s security posture.

CSC 1: Inventory of Authorized and Unauthorized Devices

The very first CIS control on the list requires the organization to be aware of the devices on their network. There is a reason why this control is listed first in the CIS controls list; the rest of the CIS controls will build upon this very essential control because simply put “You can't protect what you can't see”. This CIS control has eight sub-controls shown in Table 3.

Table 3: CSC 1 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
1.1	Utilize an Active Discovery Tool	OpenVAS		Nmap / ndiff
1.2	Use a Passive Asset Discovery Tool	Security Onion	PRADS/ Bro	
1.3	Use DHCP Logging to Update Asset Inventory	Policy/Process		Security Onion ELK Stack
1.4	Maintain Detailed Asset Inventory	Kolide Fleet	Policy/Process	
1.5	Maintain Asset Inventory Information	Kolide Fleet	Policy/Process	
1.6	Address Unauthorized Assets	Policy/Process		
1.7	Deploy Port Level Access Control			OpenNAC/ PacketFence
1.8	Utilize Client Certificates to Authenticate Hardware Assets	PKI/AD FS		PacketFence

CSC 1.1: Utilize an Active Discovery Tool

The first sub-control starts the process of identifying devices by actively scanning the network. A properly configured network scan will reveal all the devices connected to the network at the time of the scan. OpenVAS can be utilized to implement this sub-control. OpenVAS will probe the network to find live hosts and depending on the scan settings, OpenVAS will try to fingerprint the host to collect more information.

CSC 1.2: Use a Passive Asset Discovery Tool

A passive scan does not require probing for live hosts. It simply identifies hosts by analyzing which hosts are talking on the network. Organizations can utilize Security Onion with an interface on monitor mode to analyze the traffic passing through the interface using Bro and PRADS to identify assets.[35]

CSC 1.3: Use DHCP Logging to Update Asset Inventory

Enabling Dynamic Host Configuration Protocol (DHCP) logging will allow the organization to identify which Media Access Control (MAC) address or host was assigned which Internet Protocol (IP) at a certain time. Most DHCP servers will offer such feature. Organizations can implement this sub-control by having a process to ensure all DHCP servers are sending detailed logging data to the organization’s SIEM such as ELK Stack.

CSC 1.4: Maintain Detailed Asset Inventory

The previous sub-controls should provide an organization with a good picture of the organization’s asset inventory. This sub-control focuses on documenting and maintaining the information that has been collected. Once new assets have been identified, the asset inventory list should be updated. Wazuh and Kolide Fleet’s Osquery agents can be installed on the new assets to track endpoints. A spreadsheet can also be used to track assets that are offline or does not have an agent running.

CSC 1.5: Maintain Asset Inventory Information

The inventory spreadsheet should provide more details about each system, such as Host Name, IP address, business function, and the department responsible for the device. Kolide Fleet will allow the organization to tag or label the assets to group them under a certain department or business function. Kolide Fleet dashboards will also provide information about the assets' operating system, MAC address, IP, host specs, and last time seen.

CSC 1.6: Address Unauthorized Assets

The organization can define a policy to address unauthorized devices on the network. If an active or passive scan discovered an unauthorized device on the network, a policy can specify to remove or quarantine the device. The policy can also specify how to properly add the device to the network and update the inventory list.

CSC 1.7: Deploy Port Level Access Control

To decrease the threat of unauthorized devices connected to the network, an organization can use a network access control system to quarantine unauthorized new devices and prevent these devices from connecting to the network. PacketFence is an open-source network access control system which can be integrated with an AD to use Lightweight Dictionary Access Protocol (LDAP) for the user and machine authentication.[36-38]

CSC 1.8: Utilize Client Certificates to Authenticate Hardware Assets

This sub-control adds an additional authentication requirement for remote users or devices outside the organization's network. This could be done by utilizing Windows Active Directory

Federation Services (AD FS) and PKI to generate hardware certificates for each device.[39, 40]. PacketFence does also include an optional PKI service to be installed.[41]

CSC 2: Inventory of Authorized and Unauthorized Software

Moving on to the second CIS control which focuses on the visibility of the software running in the environment. After getting a good grip on the security of the devices running in an organization, the next natural and logical step is understanding what kind of software is running on these devices. An organization can inventory all authorized and unauthorized software to better understand its threats and vulnerabilities. This CIS control has ten sub-controls shown in Table 4.

Table 4: CSC 2 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
2.1	Maintain Inventory of Authorized Software	Policy/Process		
2.2	Ensure Software is Supported by Vendor	Policy/Process		
2.3	Utilize Software Inventory Tools	Kolide Fleet		Wazuh
2.4	Track Software Inventory Information	Kolide Fleet	Policy/Process	Wazuh
2.5	Integrate Software and Hardware Asset Inventories	Kolide Fleet		Wazuh
2.6	Address Unapproved Software	Kolide Fleet		Wazuh
2.7	Utilize Application Whitelisting	AppLocker	GPO	
2.8	Implement Application Whitelisting of Libraries	AppLocker	GPO	
2.9	Implement Application Whitelisting of Scripts	AppLocker	GPO	
2.10	Physically or Logically Segregate High Risk Applications	Policy/Process	pfSense	OPNsense

CSC 2.1: Maintain Inventory of Authorized Software

This sub-control requires building and maintaining an inventory list of all organization’s approved software. The list can include all software used for business purposes installed on an organization’s device or system. This will help create a baseline for standard software used across the organization and it will help identify deviations from the organization’s standards.

CSC 2.2: Ensure Software is Supported by Vendor

Organizations can implement this sub-control by having a policy and a process to regularly ensure that all their devices and systems are kept up to date by installing the latest updates and operating system patches. If the organization discovers a device or a system running an unsupported software or operating system, the device can be tagged and device’s patching priority can be increased. If the software is no longer supported by the vendor, the organization can plan to replace or upgrade the device.

CSC 2.3: Utilize Software Inventory Tools

This sub-control can be implemented by having a policy and a process to ensure the organization’s software inventory list is up to date, all software installed on organization’s assets can be audited and updated on a regular basis. To automate this task, an organization can use Kolide Fleet to schedule pre-defined query packs to query all the agents installed on the company’s systems or a list of software installed.

CSC 2.4: Track Software Inventory Information

When collecting software information from devices across the network, the organization can track the name, version, publisher, and install date for all software and operating systems to enrich the inventory data. This also can be accomplished by running queries using Kolide Fleet Osquery agents.

CSC 2.5: Integrate Software and Hardware Asset Inventories

It is important to combine software and hardware asset inventories into one list to understand each asset’s vulnerabilities. These vulnerabilities can be from an open port or running service or an outdated software installed. Kolide Fleet provides a nice dashboard to oversee all the assets and can produce the information needed by running queries across the environment.

CSC 2.6: Address Unapproved Software

Unapproved software can be addressed using the organization's policy. The policy can specify the criteria needed to define a software as an unapproved software. The device running an unapproved software can be isolated or blocked from accessing the corporate network. The policy can specify a process to immediately remove the unapproved software.

CSC 2.7: Utilize Application Whitelisting

The requirement of this sub-control could be achieved by implanting a software whitelisting system to ensure only authorized and trusted software is able to execute and run on company approved devices. This can be accomplished using Microsoft AppLocker to specify which software is approved and then push out this policy to the endpoint using Microsoft Group Policy Objects (GPOs).[42-44]

CSC 2.8: Implement Application Whitelisting of Libraries

This follows the previous sub-control. When applying software whitelisting policies, organizations can also block the systems' processes from loading any unauthorized software libraries. AppLocker and GPOs can be utilized here also.

CSC 2.9: Implement Application Whitelisting of Scripts

AppLocker and GPOs can also be used to block any unauthorized or unsigned scripts from running of organizations' devices.

CSC 2.10: Physically or Logically Segregate High Risk Applications

This sub-control requires using a Demilitarized Zone (DMZ) or separating applications with a high risk or threat profile from the rest of the network. This could be accomplished by either connecting servers to different physical switches on different networks or virtually by using Virtual Local Area Networks (vLANs) or Access Control Lists (ACLs) on firewalls such as pfSense or OPNsense.[45]

CSC 3: Continuous Vulnerability Assessment and Remediation

Just like the first two CIS controls would provide visibility and understanding of the organizations' overall software and hardware assets, the third control would allow the organization to understand and address the vulnerabilities these assets might possess. This CIS control has seven sub-controls shown in Table 5.

Table 5: CSC 3 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
3.1	Run Automated Vulnerability Scanning Tools	OpenVAS		Nmap / Ndiff
3.2	Perform Authenticated Vulnerability Scanning	Policy/Process		
3.3	Protect Dedicated Assessment Accounts	Policy/Process		
3.4	Deploy Automated Operating System Patch Management Tools	WSUS		Chef / Ansible
3.5	Deploy Automated Software Patch Management Tools	WSUS		
3.6	Compare Back-to-back Vulnerability Scans	Policy/Process		
3.7	Utilize a Risk-rating Process	Policy/Process		

CSC 3.1: Run Automated Vulnerability Scanning Tools

Being aware of your assets may not be sufficient to determine the risk associated with these assets. Thus, an organization can scan their assets for vulnerabilities on a defined and approved schedule. This can be accomplished by utilizing OpenVAS for networking scanning to discover which services are running on devices and the risk associated with these services. Organizations can also script Nmap to scan the environment then use Ndiff to compare the scan results.[46, 47]

CSC 3.2: Perform Authenticated Vulnerability Scanning

When using a network scanner, a dedicated, special service account can be used to authenticate to systems. Using an authenticated scan can help with providing more accurate results regarding the services installed and running on each system. Organizations can utilize a process to configure a scan to run with the service account designated for this task in order to cover this sub-control.

CSC 3.3: Protect Dedicated Assessment Accounts

To implement this sub-control, an organization can set up the dedicated, special service account mentioned in the previous sub-control with the least privileges needed to run scans successfully.

CSC 3.4: Deploy Automated Operating System Patch Management Tools

After every scan, the scan results can be reviewed to determine the patches needed to be deployed to the affected systems. An organization may have a system in place to automate pushing out the missing patches to all affected systems. An organization can determine the patching schedule based on the vulnerability severity. This can be accomplished by utilizing Microsoft Windows Server Update Services (WSUS), which is available at no cost on all Windows Server 2012 and up.[48] Other options can include Chef or Ansible.[49, 50]

CSC 3.5: Deploy Automated Software Patch Management Tools

This follows the principles to the previous sub-control. Outdated software can also be added to patching cycle based on the vulnerability and risk severity.

CSC 3.6: Compare Back-to-back Vulnerability Scans

An organization can verify that the missing patches have been applied successfully by comparing the results of the most recent scan to the previous scan when the vulnerability was identified and start a process to expedite pushing patches to any system that was not patched successfully.

CSC 3.7: Utilize a Risk-rating Process

As discusses in the previous sub-control, an organization's vulnerability remediation efforts can be focused on patching the vulnerabilities with the highest risk or severity. Prioritizing the remediation efforts can help organizations reduce their threat landscape more effectively in a timely manner.

CSC 4: Controlled Use of Administrative Privileges

The fourth control focuses on the principle of least privilege and separation of duties. This control will help decrease the impact of a successful attack using compromised user's credentials to limit the attacker's ability to execute malicious software, escalate privileges or login into critical servers. This CIS control has nine sub-controls shown in Table 6.

Table 6: CSC 4 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
4.1	Maintain Inventory of Administrative Accounts	Policy/Process		PowerShell / WMIC

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
4.2	Change Default Passwords	Policy/Process		
4.3	Ensure the Use of Dedicated Administrative Accounts	Policy/Process		
4.4	Use Unique Passwords	Policy/Process		
4.5	Use Multifactor Authentication For All Administrative Access	Policy/Process	PKI / AD FS	privacyIDEA / LinOTP / gluu
4.6	Use of Dedicated Machines For All Administrative Tasks	Policy/Process		
4.7	Limit Access to Script Tools	AppLocker	GPO	
4.8	Log and Alert on Changes to Administrative Group Membership	Security Onion	ELK Stack	
4.9	Log and Alert on Unsuccessful Administrative Account Login	Security Onion	ELK Stack	

CSC 4.1: Maintain Inventory of Administrative Accounts

This sub-control requires organizations to create an inventory list of all accounts with administrative rights in the environment. Once this baseline list has been created, the organization can have a process in place to compare and audit the list regularly to ensure that only the approved personnel have admin access to company's systems and resources. To automate this step, a PowerShell script could be scheduled to run Windows Management Instrumentation Command line (WMIC) to get a list of users and then compare it to a previous list.[51] The results can be reviewed and any unauthorized account may be investigated.

CSC 4.2: Change Default Passwords

The next sub-control requires implementing a policy to change the default password on any device that belongs to the organization. These devices include but not limited to: printers, security cameras, routers, switches and any other device that is shipped with a default password. This sub-control will help to reduce the success rate of a brute-force attack.

CSC 4.3: Ensure the Use of Dedicated Administrative Accounts

Organizations can have a policy and a process to ensure creating two separate accounts for administrators of the environment. Personnel with admin accounts may be aware of where and when to use the admin account. Administrative accounts can be used for the sole purpose of administrating organization’s assets and devices and running scripts.

CSC 4.4: Use Unique Passwords

If a Multi-Factor Authentication (MFA) is not feasible to use for certain accounts such as local admin accounts or service accounts, an organization can have a policy to prevent using the same password for different accounts or devices. Every account may have a password that is unique to that system or device.

CSC 4.5: Use Multifactor Authentication for All Administrative Access

Organizations can implement this sub-control by having a policy and a process ensuring that administrative accounts are using encrypted channels to authenticate to different systems. The policy can prohibit using unsecure Virtual Network Computing (VNC) and permit secure Remote Desktop Protocol (RDP) or Secure Shell (SSH) instead.[52-54]

The process can also restrict administrators to using MFA when authenticating. Organizations can implement MFA by utilizing Windows AD FS and PKI to generate certificates as a form of second factor authentication as discussed in CSC 1.8 or can use a dedicated open source solution such as privacyIDEA, LinOTP, gluu.[55-57]

CSC 4.6: Use of Dedicated Machines for All Administrative Tasks

Organizations may have a policy in place to ensure that administrative activities can be done from a dedicated machine or “jump box”. The jump box is preferably connected on a separate network and has limited access to the internet. Personnel with admin accounts can avoid using the admin account for browsing the internet or for accessing their emails. An account with fewer privileges may be used for such activities.

CSC 4.7: Limit Access to Script Tools

PowerShell scripts are a staple in every hacker's toolbox. Thus, only certain accounts across the organization can have the ability to run scripts. AppLocker and GPOs can help block certain accounts or endpoints from running PowerShell and batch files. [51, 58]

CSC 4.8: Log and Alert on Changes to Administrative Group Membership

Admin accounts can be limited and well documented across the organization. Any modification to the administrator's group can be logged and alerted on. These changes include adding or removing an account from the administrator's group or changing the privileges of any administrator account. If the organization is forwarding all the authentication logs to ELK Stack as indicated in CSC 6.5 and CSC 6.6, this sub-control can be implemented by configuring ELK Stack to alert on certain Windows Event IDs or alert on certain commands for Linux. [59-61]

CSC 4.9: Log and Alert on Unsuccessful Administrative Account Login

Administrative accounts are highly targeted by attackers. An abnormal number of failed logins for an admin account might indicate a brute-force attempt. Thus, any failed login for an admin account can be logged and alerted on. Just like the previous sub-control, this can be implemented by alerting on certain event IDs for Windows and certain logs or Linux.[62, 63]

CSC 5: Secure Configurations for Hardware and Software

The fifth CIS control covers secure configuration. The key focus for this CIS control is to establish a configuration baseline and utilize it for all new system deployments as well as auditing and monitoring current systems' configurations. This CIS control has five sub-controls shown in Table 7.

Table 7: CSC 5 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
5.1	Establish Secure Configurations	Policy/Process	CIS Benchmark	SCT
5.2	Maintain Secure Images	Policy/Process		
5.3	Securely Store Master Images	Policy/Process		
5.4	Deploy System Configuration Management Tools	GPO		Chef / Ansible
5.5	Implement Automated Configuration Monitoring Systems	Wazuh		

CSC 5.1: Establish Secure Configurations

Operating systems and software usually come with default settings and configurations out of the box. Default configurations usually are not designed according to security best practices. Organizations may need to implement a policy and process to harden their systems by enforcing more secure configurations. Organizations can also use CIS Benchmarks as guidelines.[64]

CIS Benchmarks provides very detailed PDF guides to secure different operating systems and software's configuration. Another resource for secure configuration is Microsoft Security Compliance Toolkit (SCT).[65] Microsoft-recommended security configuration baselines for Windows and other Microsoft products include automation scripts and spreadsheets for manual process.[65]

CSC 5.2: Maintain Secure Images

Once a secure baseline has been established, the organization can use a policy to create and store a golden image securely. The golden image may be used for any new system deployment or for imaging a compromised system.

CSC 5.3: Securely Store Master Images

To ensure and maintain the integrity of the organization's golden images, a policy and a process can be in place to keep a record of the hash value of the golden image file and schedule a script to retrieve that hash value and compare it on a regular basis to ensure the image has not been tampered with. Organizations can also keep a copy of these images offline on a physical external hard drive or Universal Serial Bus (USB) drive in case the backup server becomes compromised or unreachable.

CSC 5.4: Deploy System Configuration Management Tools

This sub-control can be implemented by addressing systems that have deviated from the company-standard configuration settings. Microsoft GPO can be utilized to automatically enforce and redeploy configuration settings.[66]

CSC 5.5: Implement Automated Configuration Monitoring Systems

Organizations can monitor and identify any system that has deviated from organization's standard configuration. Wazuh along with OpenSCAP wodle integration can be utilized to perform specialized configuration assessments to ensure compliance with organization policy.[67]

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

This CIS control is very useful for incident response and intrusion detection as well as root cause analysis for operational issues. Organizations may collect all critical systems' logs in a centralized location and the logs may be reviewed daily. This CIS control has eight sub-controls shown in Table 8.

Table 8: CSC 6 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
6.1	Utilize Three Synchronized Time Sources	Policy/Process	AD / DC / GPO	
6.2	Activate Audit Logging	Policy/Process		
6.3	Enable Detailed Logging	Policy/Process		
6.4	Ensure Adequate Storage for Logs	Policy/Process		
6.5	Central Log Management	Security Onion	ELK Stack / Filebeat	GrayLog
6.6	Deploy SIEM or Log Analytic Tool	Security Onion	ELK Stack	GrayLog
6.7	Regularly Review Logs	Policy/Process		
6.8	Regularly Tune SIEM	Policy/Process		

CSC 6.1: Utilize Three Synchronized Time Sources

Establishing a timeline is essential for investigating any intrusion. Organizations can implement this sub-control by verifying all their systems are pointing to the same Network Time Protocol (NTP) server across the enterprise. This is especially important if the organization have assets in different time zones. Organizations can define specific NTP servers in all Domain Controllers (DCs) and ensure all devices on the network are time synchronized using AD and GPOs.[68]

CSC 6.2: Activate Audit Logging

This sub-control requires organizations to enable local logging on all systems and network devices. Organizations can have a policy in place to enable local logging on all systems and network devices. This policy is important to trace certain events or issues on any system.

CSC 6.3: Enable Detailed Logging

Following on the previous sub-control, when enabling logging on systems across the network, the collected logs can be reviewed to ensure all necessary metadata is included in the logs. This can be a part of the policy developed by the organization in the previous sub-control.

CSC 6.4: Ensure Adequate Storage for Logs

An organization can also prepare enough storage space to store logs for the period defined by the organization's log retention policy mentioned in the previous sub-control. Older logs can be compressed and archived to lower storage costs.

CSC 6.5: Central Log Management

This sub-control requires collecting all systems' logs centrally. Collecting all logs in one place will help organizations make more sense of the data and make it easier to analyze, correlate and aggregate the logs. ELK Stack can be utilized to cover this sub-control by either using Beats agents or by using syslog.[69, 70] Beats agents can ship logs from windows hosts and other devices where syslog is not available.

CSC 6.6: Deploy SIEM or Log Analytic Tool

As mentioned in the previous sub-control, collecting all logs in one place will make it easier to analyze, correlate and aggregate the logs. A Security Incident and Event Management (SIEM) solution will make this process easier and more effective. ELK Stack is included in Security Onion and can be used to cover this sub-control. Another option is GrayLog which is also open source and comes with a security focused dashboard and enrichment. [71]

CSC 6.7: Regularly Review Logs

Once an organization has deployed a SIEM solution, a process can be defined to review collected logs regularly. Analysts can look for abnormal events or behaviors and any alerts that have been generated.

CSC 6.8: Regularly Tune SIEM

SIEMs are not set up to operate as “set it and forget it” mode. Organizations can implement a policy to regularly tune their SIEM solution to reduce false positives and increase visibility and detection rate. Any un-necessary or noisy logs can be tuned.

Foundational Security Controls

Foundational controls will focus on many technical aspects of securing an organization. These controls can help an organization improve the security and availability of its systems, networks, data, and infrastructure significantly.

CSC 7: Email and Web Browser Protections

After implementing the first six controls, an organization should have a better understanding of its infrastructure and assets. The next step is to focus on today’s most common types of attacks; manipulating users to open a phishing email or click on a malicious link. This control will go over how to secure Emails and web browsers and it has ten sub-controls shown in Table 9.

Table 9: CSC 7 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	GPO		

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	GPO		
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	GPO		
7.4	Maintain and Enforce Network-Based URL Filters	pfSense	Squid	
7.5	Subscribe to URL-Categorization Service	pfSense	Squid ufdbGuard E2Guardian	
7.6	Log All URL Requests	pfSense	Squid Security Onion	
7.7	Use of DNS Filtering Services	pfSense	Unbound	OpenDNS, CleanBrowsing Quad9
7.8	Implement DMARC and Enable Receiver-Side Verification	pfSense	MailScanner	Postfix SpamAssassin
7.9	Block Unnecessary File Types	pfSense	MailScanner	
7.10	Sandbox All Email Attachments	pfSense	MailScanner	ClamAV

CSC 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients

This sub-control can be a combination of a policy and an enforcement. Users can be aware of the approved list of software by the organization and may not try to use or download un-approved software. This also can be enforced using GPOs policies to push or remove software packages.

CSC 7.2: Disable Unnecessary or Unauthorized Browser or Email Client Plugins

The same discussion for the previous sub-control applies to this sub-control also.

CSC 7.3: Limit Use of Scripting Languages in Web Browsers and Email Clients

Same as the previous two sub-controls, disable certain scripting languages can be achieved using GPOs.

CSC 7.4: Maintain and Enforce Network-Based URL Filters

Using pfSense firewall along with Squid proxy integration can allow the organization to prevent users from visiting certain sites that belong to a certain category defined by the organization.[72] Both pfSense and Squid can allow or block traffic to certain website or IP.

CSC 7.5: Subscribe to URL-Categorization Service

Universal Resource Locator (URL) Categorization service will dynamically update the proxy's blacklist to block users from landing on known malicious sites. There are multiple free URL-Categorization services that integrate with Squid including ufdbGuard and E2Guardian.[73, 74]

CSC 7.6: Log all URL Requests

Collecting which sites were visited by a certain endpoint will provide a tremendous value in an incident investigation or containment. URL-request logs usually include information such as the time, date, Hypertext Transfer Protocol (HTTP) method, visited site name, URL and the HTTP response code. Organizations can enable this feature in Squid and configure Squid to send all its logs to ELK Stack in Security Onion.

CSC 7.7: Use of DNS Filtering Services

In concept, this is similar to CSC 7.4. DNS filtering will allow organizations to block malicious domains by returning a non-routable IP address to the Domain Name System (DNS) query requester. pfSense provides a module to enable Unbound DNS server. An organization can use Unbound DNS server to block its own list of malicious IPs or domains.[75] The organization can also point this DNS server to query public DNS servers such as OpenDNS, CleanBrowsing or Quad9 which will block phishing and malicious sites for free automatically.[76-78]

CSC 7.8: Implement DMARC and Enable Receiver-Side Verification

Verifying the identity and the origin of an email can help to reduce the amount of spam, phishing and spoofed emails an organization receives. pfSense offers an open source email gateway module: MailScanner.[79] MailScanner has multiple add-ons such as Postfix and SpamAssassin which will enable checking for the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards and Reporting and Conformance (DMARC) policy.[80, 81] These standards and protocols will verify the identity and the origin of the email received by the gateway. Organizations can also check with their online email service provider to enable these features.

CSC 7.9: Block Unnecessary File Types

Organizations can specify which file types are allowed through the email gateway. There is no reason for users to send and receive executables and scripts through emails. MailScanner can provide the ability to block unnecessary or suspicious file types at the gateway.

CSC 7.10: Sandbox All Email Attachments

If an email has a suspicious attachment, the attachment can be checked and verified before landing in a user’s email box. MailScanner has a built-in anti-virus: ClamAV[82]. It can scan the attachment for known viruses and malware before sending to the end user.

CSC 8: Malware Defenses

Malware attacks are very common today as they can cause a lot of damage very quickly. This control will focus on detecting, containing and preventing malware and virus attacks against an organization. This CIS control has eight sub-controls shown in Table 10.

Table 10: CSC 8 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
8.1	Utilize Centrally Managed Anti-Malware Software	Wazuh	Windows Defender	
8.2	Ensure Anti-Malware Software and Signatures are Updated	Policy/Process	GPO	
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	GPO	Windows Defender	
8.4	Configure Anti-Malware Scanning of Removable Devices	Wazuh	Windows Defender	
8.5	Configure Devices Not To Auto-Run Content	GPO		
8.6	Centralize Anti-Malware Logging	Wazuh		
8.7	Enable DNS Query Logging	pfSense	Unbound / Security Onion	
8.8	Enable Command-Line Audit Logging	GPO		

CSC 8.1: Utilize Centrally Managed Anti-Malware Software

It is important for organizations to be aware of any infection or known exploit used in their environment. Thus, having a centrally managed anti-malware software is essential. While this research will not provide a ready to be deployed solution for this sub-control; organizations can use Wazuh along with Windows Defender and a custom ruleset to generate an alert for Windows Defender detections on Wazuh.[83]

CSC 8.2: Ensure Anti-Malware Software and Signatures are Updated

This sub-control is more of a policy, regardless of which Antivirus (AV) solution is being utilized across the enterprise. Organizations can ensure that the AV used is up-to-date by pushing put a configuration policy using GPOs.

CSC 8.3: Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enabling anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) will help an organization minimize the number of successful exploits. These features are available in Windows Defender and can be pushed out to all windows hosts using GPOs.[84]

CSC 8.4: Configure Anti-Malware Scanning of Removable Devices

Removable devices such as USB flash drives possess high threat risk due to its nature of being plugged into multiple systems that might be outside the organization's network or systems that do not follow the organizations secure standards. Windows Defender scans removable devices for viruses and malware automatically on Windows 10 Pro and up.[85] Wazuh can be utilized to determine where USB drives have been plugged into on an organization's system.[86]

CSC 8.5: Configure Devices Not To Auto-Run Content

To prevent malware and viruses from auto-running once a removable device has been plugged into a system, a policy using GPOs can be deployed to block such action.[87]

CSC 8.6: Centralize Anti-Malware Logging

This sub-control can be covered using the workaround in CSC 8.1. Another approach can be used if an organization is already shipping logs to ELK Stack, a custom alert can be created to alert on detection events.

CSC 8.7: Enable DNS Query Logging

This sub-control goes hand in hand with CSC 7.7. If an organization has a DNS server or system implemented, it can configure the DNS system to send all query logs to ELK Stack for analysis and storage. If a system queries a known bad hostname, it can be investigated for infection.

CSC 8.8: Enable Command-Line Audit Logging

Most of today’s attackers use the command line to execute their code and move laterally around the environment. Enabling command-line logging will enable the organization to track and follow the attacker’s footprints. Organizations can implement this sub-control by enabling logging for command-line for Windows.[88]

CSC 9: Limitation and Control of Network Ports

Hackers usually start their attack by looking for open ports, services or protocols. And will then start fingerprinting these services to identify any vulnerabilities. This control will help organizations understand and secure open ports and running services in their environment. This CIS control has five sub-controls shown in Table 11.

Table 11:CSC 9 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	OpenVAS		Wazuh / Kolide Fleet
9.2	Ensure Only Approved Ports, Protocols and Services Are Running	Policy/Process		
9.3	Perform Regular Automated Port Scans	OpenVAS		nmap
9.4	Apply Host-based Firewalls or Port Filtering	GPO	Windows Firewall	
9.5	Implement Application Firewalls	pfSense	ModSecurity	

CSC 9.1: Associate Active Ports, Services and Protocols to Asset Inventory

If an organization has successfully implemented CSC 2.5, then this sub-control can be also covered, OpenVAS will provide the ability to associate ports, services, and protocols to systems and devices. If either Wazuh or Kolide Fleet agent is installed on a system, it can also determine and present this information.

CSC 9.2: Ensure Only Approved Ports, Protocols and Services Are Running

An organization can have a policy to approve ports, protocols, and services before they are enabled. A process can also be placed to address unapproved ports, protocols, and services which might require an immediate termination of the service or isolating the system running it.

CS 9.3: Perform Regular Automated Port Scans

This sub-control depends on the previous sub-control. In order to address unapproved ports, protocols, and services, organizations need to discover them first. Thus, an organization can have a policy and a process to schedule these scan on regular basis and review the results. This sub-control can be covered using OpenVAS or Nmap.

CSC 9.4: Apply Host-based Firewalls or Port Filtering

Enabling a host-based firewall on endpoints will reduce the attacker's chance of moving laterally across the network. It will also reduce the chance of a ransomware spreading around the network because users' workstations do not need to talk to other workstations and such communication can be blocked. Windows Firewall can be utilized to cover this sub-control.[89]

CSC 9.5: Implement Application Firewalls

External facing applications and servers are usually highly targeted because they offer a foot in the door to the organization's network. Web Application Firewalls (WAFs) inspect the traffic to identify and block abnormal traffic. ModSecurity can be used to implement this sub-control.[90] ModSecurity is an open source, cross-platform WAF. It can be configured under pfSense.[91]

CSC 10: Data Recovery Capabilities

This control focuses on systems and data backups to prepare organizations to recover from incidents and minimize the downtime needed to get systems back online. This CIS control has five sub-controls shown in Table 12.

Table 12:CSC 10 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
10.1	Ensure Regular Automated Back Ups	Windows Backup and Restore		
10.2	Perform Complete System Backups	Windows Server Backup/ Windows Backup and Restore		UrBackup/ Amanda/ Bacula
10.3	Test Data on Backup Media	Policy/Process		
10.4	Ensure Protection of Backups	Policy/Process	BitLocker	
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Policy/Process		

CSC 10.1: Ensure Regular Automated Back Ups

This sub-control is crucial. If all the security controls in an organization have failed to stop an attacker or a malware spread, an organization will always go back to the data backups to restore the data. Hence, organizations can always verify that all scheduled backups have been completed and investigate any error or incomplete backup. Organizations can utilize multiple Windows built-in features such as File history, Windows Backup and Restore or OneDrive for employees' critical files up to 5 GB.[92-94]

CSC 10.2: Perform Complete System Backups

If a critical system gets wiped or compromised, an organization may need to recover the operating system and configuration files along with the data stored. Thus, only backing up data

will not be sufficient for a server to come back online in a timely manner. Organizations may need to utilize a software that will back up the server entirely as an image or using a similar process to ensure a quick recovery. The organization can utilize Windows Backup and Restore, Windows Server Backup or Windows System Restore to implement this sub-control.[92, 95, 96]
Organizations can also use a dedicated system imaging a backup open source solutions such as UrBackup, Amanda or Bacula.[97-99]

CSC 10.3: Test Data on Backup Media

An organization can have a process in place to regularly test to restore the data to avoid last minute surprises. This process will help identify any issues with backup data before the data is really needed.

CSC 10.4: Ensure Protection of Backups

Ransomware can infect the backup server and cripple the organization's ability to restore the data. Organizations may need to ensure that backups are secured and encrypted while moving and at rest. A Windows built-in tool, BitLocker, can be used to encrypt the drive where the backups are stored.[100]

CSC 10.5: Ensure Backups Have At least One Non-Continuously Addressable Destination

Following the previous sub-control, an organization can have a policy in place to use an additional destination for backups that is not part of the network such as external hard drives or media tapes.

CSC 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

This control goes over network devices as they cannot be ignored. Network devices are the core element to any organization Information Technology (IT) infrastructure and they also need to be secured. This CIS control has seven sub-controls shown in Table 13.

Table 13: CSC 11 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
11.1	Maintain Standard Security Configurations for Network Devices	Policy/Process	CIS Benchmark	
11.2	Document Traffic Configuration Rules	Policy/Process		
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes			Nipper/ Nipper-ng
11.4	Install the Latest Stable Version of Any Security-related Updates on All Network Devices	Policy/Process		
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions		PKI / AD FS	privacyIDEA/ LinOTP/gluu
11.6	Use Dedicated Machines For All Network Administrative Tasks	Policy/Process		
11.7	Manage Network Infrastructure Through a Dedicated Network	Policy/Process		

CSC 11.1: Maintain Standard Security Configurations for Network Devices

This sub-control may require the organizations to have a policy and a process to securely configure network devices. Just as mentioned in CSC 5.1, refer to CIS Benchmarks for recommendations on hardening network devices.

CSC 11.2: Document Traffic Configuration Rules

This sub-control requires documenting details when adding or disabling firewall rules. Documentation can include business justification, change number, the duration the rule needed and the business unit responsible. The organizations can use a spreadsheet to implement this sub-control. pfSense provides the ability to add a description to each rule or the ability to group rules by a visual rule separator that can divide the rules logically.[101]

CSC 11.3: Use Automated Tools to Verify Standard Device Configurations and Detect Changes

An organization may regularly compare network devices' security configuration to the organization's approved security configuration. This sub-control will help the organization identify any network device with a security configuration that deviated from the organization's standard. Open source tool Nipper can be used to implement this sub-control.[102]

CSC 11.4: Install the Latest Stable Version of Any Security-related Updates on All Network Devices

This sub-control is to ensure that organizations have a process and a policy in place to verify all network devices are updated and operating the latest stable version. This sub-control will help minimize the risk of successfully exploiting a network device that has not updated with the latest security updates.

CSC 11.5: Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions

This sub-control follows the same recommendation for CSC 4.5. To implement this sub-control, network admins may need to use MFA and encrypted sessions to administrate network devices. This sub-control can be covered using the same tools discussed in CSC 4.5

CSC 11.6: Use Dedicated Machines for All Network Administrative Tasks

If an organization has implemented CSC 4.6, this sub-control should be a quick win. Organizations can have a policy in place to use a dedicated system to manage all devices across the organization including network devices. There is no OSSS recommendation for this sub-control.

CSC 11.7: Manage Network Infrastructure Through a Dedicated Network

Building upon the previous sub-control, a policy that emphasizes on using dedicated interfaces and networks for managing network devices will reduce the risk of the device being exposed to attackers and malware since the dedicated network should mostly carry administration traffic. There is no OSSS recommendation for this sub-control.

CSC 12: Boundary Defense

This control focuses on protecting and monitoring the network ingress and egress points. Data entering and leaving the organization can be examined to detect anomalies and monitor attackers. This CIS control has 12 sub-controls shown in Table 14.

Table 14: CSC 12 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
12.1	Maintain an Inventory of Network Boundaries	Policy/Process	OpenVAS	Nmap
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	OpenVAS		
12.3	Deny Communications with Known Malicious IP Addresses	pfSense		
12.4	Deny Communication over Unauthorized Ports	pfSense		
12.5	Configure Monitoring Systems to Record Network Packets	Security Onion		Moloch
12.6	Deploy Network-Based IDS Sensor	Security Onion	Snort/ Suricata/ Bro	
12.7	Deploy Network-Based Intrusion Prevention Systems	Security Onion pfSense	Snort/ Suricata	
12.8	Deploy NetFlow Collection on Networking Boundary Devices	Security Onion		ElastiFlow SOF-ELK / nfcapd / ntopng
12.9	Deploy Application Layer Filtering Proxy Server	pfSense	OpenAppID/ ModSecurity	
12.10	Decrypt Network Traffic at Proxy	pfSense	Squid	
12.11	Require All Remote Login to Use Multi-factor Authentication	pfSense	Windows PKI/ OpenVPN/ FreeRADIUS	privacyIDEA / LinOTP/ gluu
12.12	Manage All Devices Remotely Logging into Internal Network		Wazuh / PacketFence	

CSC 12.1: Maintain an Inventory of Network Boundaries

The first sub-control requires organizations to stay up-to-date with network boundary devices. If an organization implemented CSC 1.1, it can use OpenVAS to track and identify boundary devices. This also can be accomplished using a Nmap scan.

CSC 12.2: Scan for Unauthorized Connections across Trusted Network Boundaries

Following on the previous sub-control, organizations can scan outside and inside each network to eliminate blind spots or missing any devices behind a router or a firewall. This also can be accomplished using OpenVAS.

CSC 12.3: Deny Communications with Known Malicious IP Addresses

If a bad or malicious IP was identified, it can be blocked at the perimeter firewall to eliminate any further attack attempts. This sub-control can be implemented using pfSense firewall rules.

CSC 12.4: Deny Communication over Unauthorized Ports

Organizations can have a list of authorized or approved ports and protocols across the enterprise and at the perimeter. Any unapproved port or protocol cannot be allowed to communicate and dropped immediately. This sub-control can also be implemented using pfSense.

CSC 12.5: Configure Monitoring Systems to Record Network Packets

This sub-control requires the implementation of a packet capture system. Capturing live packet will provide a wealth of information and can be invaluable for identifying o containing incidents. Security Onion can be used to implement this sub-control. Organizations can also implement Moloch which is an open source, full packet capturing and indexing system.[103]

CSC 12.6: Deploy Network-Based IDS Sensor

Implementing this sub-control can help organizations detect network-based attacks. Network Intrusion Detection Systems (NIDS) are usually noisy and produce a decent amount of false positive alerts. Organizations can tune NIDS to make it more efficient. This sub-control can be implemented using Security onion which has Snort or Suricata working out of the box. pfSense also has the ability to act as a NIDS system.[104] Bro IDS is also included in Security Onion and can also be used to detect abnormal traffic behavior.

CSC 12.7: Deploy Network-Based Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) will not only detect an intrusion but will also automatically block the attacking IP address. An organization can use NIPS when they have high-confidence that the originating IP is malicious. Otherwise, legitimate IPs might be auto-blocked. This sub-control can be implemented by using pfSense scripts or API call from Snort or Suricata in Security Onion. Or by enabling Snort or Suricata as part of pfSense.[105]

CSC 12.8: Deploy NetFlow Collection on Networking Boundary Devices

Depending on the size of the organization, this sub-control can provide additional visibility to devices talking internally if not being captured by CSC 12.5. NetFlow can be very useful to understand traffic traveling across endpoints without leaving the parameter. ntopng can be installed on Security Onion to enable NetFlow collection.[106] NetFlow can also be captured directly from the monitoring interface using nfdump.[107] Organizations can also use ElastiFlow or SOF-ELK as an alternative solution[108, 109]

CSC 12.9: Deploy Application Layer Filtering Proxy Server

As discussed in CSC 9.5, using pfSense along with ModSecurity will help determine application layer traffic and attacks. Another available option that can be used is OpenAppID, which focuses on application layer analysis and attack detection. It works as a Snort module.[110]

CSC 12.10: Decrypt Network Traffic at Proxy

Many of the sub-controls in this control will render useless if the traffic is encrypted. IDSs are signature based will not detect any attacks since the packets are not readable. Organizations can use Squid proxy to decrypt traffic by installing Squid certificate on all endpoints pointing to the Squid proxy. An organization can place IDS or IPS sensors internally before the traffic gets encrypted at the egress point.

CSC 12.11: Require All Remote Login to Use Multi-factor Authentication

This sub-control will help reduce the threat of attackers using compromised credentials to connect remotely to an organization's network. There are multiple ways to implement this sub-control. An organization can use pfSense, OpenVPN, RADIUS or FreeRADIUS, and Windows PKI. [111-114]. It also can be implemented by using pfSense, OpenVPN and the solutions mention previously: privacyIDEA, LinOTP, and gluu.

CSC 12.12: Manage All Devices Remotely Logging into Internal Network

This sub-control recommends ensuring that devices that have left the organization's network are scanned and verified of being infection-free before allowed to enter the network. While there are no OSSS to cover this sub-control entirely, Wazuh can be used to alert of infection or configuration change and then an admin can block the device manually using a Network Access Control (NAC) solution such as PacketFence.

CSC 13: Data Protection

Sensitive information is the organization's most valuable asset. It must be protected, secured, and tracked. This control focuses on reducing the risk associated with data leakage or breach. This CIS control has nine sub-controls shown in Table 15.

Table 15: CSC 13 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
13.1	Maintain an Inventory Sensitive Information	Policy/Process		

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Policy/Process		
13.3	Monitor and Block Unauthorized Network Traffic			MyDLP
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	pfSense		
13.5	Monitor and Detect Any Unauthorized Use of Encryption	Security Onion	Bro / Suricata	MyDLP / pfSense Squid
13.6	Encrypt the Hard Drive of All Mobile Devices.	Policy/Process		
13.7	Manage USB Devices	Policy/Process	GPO	
13.8	Manage System's External Removable Media's Read/write Configurations	GPO		
13.9	Encrypt Data on USB Storage Devices	BitLocker		

CSC 13.1: Maintain an Inventory Sensitive Information

This sub-control focuses on the need to identify and locate sensitive information across the organization. Sensitive information can be identified and tracked in a secure spreadsheet or a system. The spreadsheet or system utilized can be encrypted, password protected and is accessible by an authorized personnel only. This will add an extra layer of protection. This sub-control can be achieved by an organization by implementing a process. If an organization implemented a Data Loss Prevention (DLP) system, the system can be used to identify and track such data.

CSC 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Removing sensitive data from the network and making it available only via offline methods can greatly reduce the risk associated with losing or compromising the sensitive data. An organization can implement a policy or a process to take sensitive data offline after a certain period of time. There is no recommended OSSS to implement this sub-control.

CSC 13.3: Monitor and Block Unauthorized Network Traffic

This sub-control protects the organization's pre-defined sensitive data from leaving the organization by monitoring network traffic. This sub-control can be covered by utilizing MyDLP Community Edition.[115]

CSC 13.4: Only Allow Access to Authorized Cloud Storage or Email Providers

Organizations usually have limited visibility to a cloud storage and external emails due to the encryption capabilities of an external cloud storage or an email provider. Since external cloud storage or external email can be the primary method for sensitive data leakage or extraction, an organization can limit which providers are allowed using pfSense firewall rules.

CSC 13.5: Monitor and Detect Any Unauthorized Use of Encryption

Encrypted attack traffic or sensitive data can pass through most detection mechanism with being detected. Thus, an organization can monitor any abnormal or unauthorized use of encryption to detect suspicious activities. This sub-control can be implemented using MyDLP or using Security Onion along with Bro or Suricata and JA3 hash lookup.[116]

CSC 13.6: Encrypt the Hard Drive of All Mobile Devices.

When assigning mobile devices to employees, organizations can have a policy and a process to ensure that hard drive of the mobile devices is encrypted. This policy will help reduce the risk of sensitive data leakage if the phone is lost or stolen. iPhones can be encrypted using a built-in tool.[117] Android phones can also be encrypted using a built-in tool.[118]

CSC 13.7: Manage USB Devices

This sub-control requires organizations to only allow approved USB devices to be used in the environment. Organizations can have a policy and a process specifying what type of devices can be used and block all other devices such as flash drives or external hard drives if the organization can function without the need to use of such devices. This sub-control can be implemented using Microsoft Windows GPOs.

CSC 13.8: Manage System's External Removable Media's Read/write Configurations

This sub-control helps organizations to control a potential data infiltration using USB drives when the business process requires using USB drives for a necessary business function. Microsoft Windows GPOs can be used to allow read-only from external drives and block users' attempts to copy data to a USB drive.[119]

CSC 13.9: Encrypt Data on USB Storage Devices

This sub-control shares the same principles as CSC 13.6. Any sensitive information stored on a portable device including USB drives can be encrypted to prevent leakage if the device is lost or stolen. Windows BitLocker along with Microsoft Windows GPOs can be used to implement this sub-control.[120, 121]

CSC 14: Controlled Access Based on the Need to Know

This CIS control follows the previous CIS control to secure critical systems and sensitive information. This CIS control helps the organization limit an attacker's ability to access sensitive data by moving laterally. Implementing this CIS control can also help with tracking changes to sensitive data. This CIS control has nine sub-controls shown in Table 16.

Table 16: CSC 14 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
14.1	Segment the Network Based on Sensitivity	Policy/Process		
14.2	Enable Firewall Filtering Between VLANs	pfSense		
14.3	Disable Workstation to Workstation Communication	pfSense		
14.4	Encrypt All Sensitive Information in Transit	Policy/Process		
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data			MyDLP
14.6	Protect Information through Access Control Lists	Policy/Process	AD Group Policy	
14.7	Enforce Access Control to Data through Automated Tools			MyDLP
14.8	Encrypt Sensitive Information at Rest	BitLocker		
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Wazuh		Elk Stack MyDLP

CSC 14.1: Segment the Network Based on Sensitivity

The first sub-control encourages classifying network segments based on data sensitivity within the network. This sub-control focuses on the logical side of network segmentation. An organization can use a policy or a process to ensure networks are segmented properly. Organizations can group assets with the same function or the level of data access needed in the same segment. This sub-control requires a policy implemented to ensure coverage.

CSC 14.2: Enable Firewall Filtering Between VLANs

Firewall rules are not only useful at the perimeter, but they are also very useful inside the network too. pfSense firewall rules can be used to specify how VLANs' traffic should be allowed or denied. An example of this implementation would be denying any traffic from the marketing department VLAN to the research and development VLAN. pfSense can be used to implement this sub-control.

CSC 14.3: Disable Workstation to Workstation Communication

The same principles and discussion for CSC 14.2 also apply to this sub-control.

CSC 14.4: Encrypt All Sensitive Information in Transit

This sub-control will limit an attacker's ability to intercept traffic by eavesdropping once inside the network. Organizations can implement a policy or process to ensure all the traffic is encrypted while in transit. A specific software or process can be used based on the traffic type.

CSC 14.5: Utilize an Active Discovery Tool to Identify Sensitive Data

We have previously touched on a similar sub-control (CSC 13.3). This sub-control requires identifying all sensitive data anywhere and on any system; not the ones on the network only. MyDLP can be used to implement this sub-control.

CSC 14.6: Protect Information through Access Control Lists

This sub-control focuses on using ACLs to determine who can access the sensitive data. This sub-control can be implemented against files stored on systems, network shares, databases, and applications access. This sub-control recommends organizations to grant access to users based on their business need and functionality. Even though this sub-control is more of a process, Microsoft Active Directory along with Windows GPOs can be used to implement this control.

CSC 14.7: Enforce Access Control to Data through Automated Tools

This control compliments CSC 14.5 by encouraging the use of host-based DLP solutions. This sub-control adds another layer of detection and protection by actively tracking sensitive data on endpoints. This sub-control can be covered by installing MyDLP's Windows or Linux agents on endpoints. The Windows agent can also be pushed out using Microsoft Windows GPOs.[122]

CSC 14.8: Encrypt Sensitive Information at Rest

This sub-control requires adding another layer of protection to decrypt sensitive data at rest by using a secondary authentication mechanism not integrated into the operating system. An organization can use BitLocker along with Trusted Platform Module (TPM) devices or USB drives to implement this sub-control.[123, 124]

CSC 14.9: Enforce Detail Logging for Access or Changes to Sensitive Data

Tracking who and when someone accessed or changed sensitive information is very important to any organization. An organization can use a Wazuh to monitor such activities.[125]

CSC 15: Wireless Access Control

This control focuses on reducing the risks associated with wireless network devices, access points, and wireless clients. Wireless access can possess major risks since its attack surface is broader and easier to reach than traditional networks. This CIS control has 10 sub-controls shown in Table 17.

Table 17: CSC 15 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
15.1	Maintain an Inventory of Authorized Wireless Access Points	Policy/Process		
15.2	Detect Wireless Access Points Connected to the Wired Network			RogueScanner
15.3	Use a Wireless Intrusion Detection System			RogueAP Detector/ OpenWIPS-ng
15.4	Disable Wireless Access on Devices if Not Required	Policy/Process	GPO	
15.5	Limit Wireless Access on Client Devices	Policy/Process		

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
15.6	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients	Policy/Process	GPO	
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Policy/Process		
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Windows PKI	AD DS	
15.9	Disable Wireless Peripheral Access of Devices	Policy/Process		
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Policy/Process		

CSC 15.1: Maintain an Inventory of Authorized Wireless Access Points

This sub-control focuses on documenting the authorized Access Points (APs) to establish a baseline. This baseline can be used to identify any rogue or unauthorized access point. This sub-control can be implemented using a policy and process to keep track of all APs utilized by the organization.

CSC 15.2: Detect Wireless Access Points Connected to the Wired Network

This sub-control focuses on finding rogue access points by scanning wired networks. If an organization have multiple physical sites or offices, it will not be easy to travel to different sites to scan for rogue APs. Organizations can detect rogue access points be scanning the wired network. RogueScanner can be used to implement this sub-control.[126]

CSC 15.3: Use a Wireless Intrusion Detection System

This sub-control recommends using a Wireless Intrusion Detection System (WIDS) to detect and alert on rogue APs automatically. An organization can implement this sub-control by utilizing RogueAP Detector or OpenWIPS-ng.[127, 128] Organizations can also build a custom solution using multiple open source tools.[129, 130]

CSC 15.4: Disable Wireless Access on Devices if Not Required

This sub-control requires an organization to have a policy or process to disable wireless access on devices without business justification. This also can be implemented using Microsoft Windows GPOs for endpoints running Windows systems.

CSC 15.5: Limit Wireless Access on Client Devices

This sub-control requires a policy or a process to allow wireless clients to connect to specific wireless networks based on the client's business need. For example, tablets might have a different business use than laptops, an organization can configure each device category to connect to a different network.

CSC 15.6: Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients

Just as the CSC 14.3 which focuses on limiting peer to peer communication over a wired network, the same principle should be applied for wireless communication. This control can also be implemented by pushing a policy using Microsoft Windows GPOs.

CSC 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

This sub-control recommends organizations to use strong encryption algorithms for wireless data transmission. The suggested algorithm is Advanced Encryption Standard (AES).[131] Organizations can implement this sub-control by having a policy or process to ensure all organization's APs are using AES for encryption.

CSC 15.8: Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication

Just like the previous sub-control, this sub-control focuses on using the strongest standards for encryption and authentication. It recommends using Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) along with multi-factor authentication.[132] Organizations can implement this sub-control by implementing Password-Based 802.1X Authenticated Wireless Access on Windows Server.[133]

CSC 15.9: Disable Wireless Peripheral Access of Devices

This sub-control encourages organizations to disable other wireless communication technologies such as Bluetooth and Near-field communication (NFC) if it is not needed for any business function. An organization can implement this sub-control by having a policy or process to disable these technologies on all devices.

CSC 15.10: Create Separate Wireless Network for Personal and Untrusted Devices

Wireless personal and untrusted devices possess a higher risk to an organization because these devices are not configured according to the organization security standards and might have connected to hostile networks before connecting to an organization's network. Thus, wireless personal devices can be isolated and contained in a separate wireless network that cannot reach the internal organization's network. This sub-control can be implemented using a policy or a process.

CSC 16: Account Monitoring and Control

This control focuses on securing credentials and authentication mechanisms. This control is important to reduce the chance of using legitimate credentials by an attacker to avoid detection. This CIS control has 13 sub-controls shown in Table 18.

Table 18: CSC 16 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
16.1	Maintain an Inventory of Authentication Systems	Policy/Process	Kolide Fleet	
16.2	Configure Centralized Point of Authentication	Windows AD	LDAP RADIUS	
16.3	Require Multi-factor Authentication			privacyIDEA / LinOTP / gluu
16.4	Encrypt or Hash all Authentication Credentials	Policy/Process		
16.5	Encrypt Transmittal of Username and Authentication Credentials	Policy/Process		
16.6	Maintain an Inventory of Accounts	PowerShell Scripting		OpenIAM / gluu
16.7	Establish Process for Revoking Access	Policy/Process		
16.8	Disable Any Unassociated Accounts	Policy/Process		
16.9	Disable Dormant Accounts	Policy/Process		
16.10	Ensure All Accounts Have An Expiration Date	Policy/Process		
16.11	Lock Workstation Sessions After Inactivity	Policy/Process	GPO	
16.12	Monitor Attempts to Access Deactivated Accounts	Security Onion	ELK Stack	
16.13	Alert on Account Login Behavior Deviation	Security Onion	ELK Stack	

CSC 16.1: Maintain an Inventory of Authentication Systems

As discussed in previous controls, this sub-control will help to create a baseline and aid the efforts of identifying the most critical systems to monitor and protect. This sub-control can be implemented using a policy or a process to keep track of authentication systems. These systems can also be tagged or labeled in other inventory systems such as Wazuh or Kolide Fleet.

CSC 16.2: Configure Centralized Point of Authentication

This sub-control focuses on minimizing the number of authentication systems utilized across an organization. Having fewer systems to monitor and configure can increase the organization’s ability to prevent and detect attacks. Organizations can use Windows AD along with RADIUS or PKI to implement this sub-control.

CSC 16.3: Require Multi-factor Authentication

This sub-control takes the previous sub-controls a step further by requiring MFA and applying this authentication mechanism to all accounts across the enterprise and not only admin accounts as recommended in sub-controls CSC 11.5 and CSC 4.5. An organization can implement this sub-control by utilizing privacyIDEA, LinOTP, and gluu. Organizations can also take advantage of MFA when it is offered for free and as part of the service by a cloud application or service such as Microsoft Office 365 and G Suite for business email.[134, 135]

CSC 16.4: Encrypt or Hash all Authentication Credentials

This sub-control can be applied to both operating systems and databases storing credentials. Most recent versions of operating systems and AD can cover this sub-control by default. If an organization uses a custom or in-house application, it can implement this control by ensuring credentials are encrypted and stored as hashes with salt. This sub-control can be implemented using a policy or a process.

CSC 16.5: Encrypt Transmittal of Username and Authentication Credentials

This sub-control can be implemented using a policy or process to verify that all organization’s systems are configured to encrypt all credentials before transmitting.

CSC 16.6: Maintain an Inventory of Accounts

This sub-control requires an organization to keep track of all user accounts in the environment. Maintaining this list over time can help identify when an account was changed or modified. This sub-control can be implemented using PowerShell scripts or by using an open source Identity and Access Management (IAM) system such as OpenIAM.[136, 137] gluu can also be used if it is already implemented.

CSC 16.7: Establish Process for Revoking Access

This sub-control can be implemented by having a process to disable any user account that is no longer needed such as contractor' or vendors' previous employees' accounts.

CSC: 16.8: Disable Any Unassociated Accounts

This sub-control can be implemented by having a process to disable any user account that cannot be associated with a legitimate existing owner.

CSC 16.9: Disable Dormant Accounts

This sub-control can be implemented by having a process to disable any user account if it has not been used for a specific time period.

CSC 16.10: Ensure All Accounts Have an Expiration Date

This sub-control can be implemented by having a process to enforce an expiration date for every user account in the organization. If the organization does not have a tool in place to automate this process such as AD, a manual process can be utilized to review all accounts on a daily, weekly or monthly basis to ensure only needed accounts are still active.

CSC 16.11: Lock Workstation Sessions After Inactivity

This sub-control can be implemented by having a policy pushed out to all endpoints to lock the screen after a certain period of inactivity. This can be implemented using GPOs.[138, 139]

CSC 16.12: Monitor Attempts to Access Deactivated Accounts

Trying to access deactivated accounts is a sign of an abnormal behavior. An organization can implement this control by setting up an alert for such activities when collecting logs from AD and then aggregating these alerts in ELK Stack. Certain Windows event IDs can be utilized to identify this type of abnormal activity.[140]

CSC 16.13: Alert on Account Login Behavior Deviation

This sub-control can be implemented by creating custom alerts in ELK Stack to identify any user login during abnormal business hours, or from a unique workstation or location if using VPN.

Organizational Security Controls

The following set of controls are categorized as Organizational Control. They focus more on people and processes rather than technical implementation and tools. Thus, organizations can decide on the priority and the need to address their controls based on the organization's security roadmap and priorities.

CSC 17: Implement a Security Awareness and Training Program

The first organizational security control focuses on identifying the missing skills in the workforce and raising security awareness across the organization. This CIS control has nine sub-controls shown in Table 19.

Table 19: CSC 17 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
17.1	Perform a Skills Gap Analysis	Policy/Process	NICE Cybersecurity Workforce Framework	
17.2	Deliver Training to Fill the Skills Gap	Policy/Process		cybrary.it opensecuritytraining.info
17.3	Implement a Security Awareness Program	Policy/Process		NIST SP800-50 SANS
17.4	Update Awareness Content Frequently	Policy/Process		OUCH! Newsletter
17.5	Train Workforce on Secure Authentication	Policy/Process		cybrary.it opensecuritytraining.info
17.6	Train Workforce on Identifying Social Engineering Attacks	Policy/Process		Gopshish
17.7	Train Workforce on Sensitive Data Handling	Policy/Process		
17.8	Train Workforce on Causes of Unintentional Data Exposure	Policy/Process		
17.9	Train Workforce Members on Identifying and Reporting Incidents	Policy/Process		

CSC 17.1: Perform a Skills Gap Analysis

This control requires a policy for implementation. Understanding the security team's weak points will help improve the organization's security posture. Organizations can use the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to identify missing skills.[141, 142]

CSC 17.2: Deliver Training to Fill the Skills Gap

After identifying the missing skills' gaps, an organization can have a process to fill these gaps by providing training to the security team. There are many free resources online to implement this control. Cybrary provides a complete course training for various cyber security topics for free.[143] Other available free training resources include Sams Class and Open Security Training.[144, 145]

CSC 17.3: Implement a Security Awareness Program

This sub-control requires organizations to implement a process for training all organization's employees to be aware of online threats and phishing attacks. Organization's employees are the organizations' first line of defense so they should be trained regularly. An organization can utilize NIST SP800-50 Infosec Awareness Training to implement this control.[146] SANS also provide great resources and ready to use templates for the community.[147]

CSC 17.4: Update Awareness Content Frequently

This sub-control also requires a process to constantly update the security awareness materials. Organizations can utilize SANS OUCH! Newsletter which is published monthly to implement this sub-control.[148]

CSC 17.5: Train Workforce on Secure Authentication

This sub-control can be implemented by enforcing a policy to regularly train the workforce to use secure authentication to connect to the organization's resources and intranet.

CSC 17.6: Train Workforce on Identifying Social Engineering Attacks

This sub-control can be implemented by enforcing a policy to regularly train the workforce on identifying phishing emails and other social engineering attacks such as impersonating phone calls. Organizations can use Gopshish to establish an internal phishing campaign.[149]

CSC 17.7: Train Workforce on Sensitive Data Handling

This sub-control can be implemented by enforcing a policy to regularly train the workforce on how to store and transfer sensitive data internally and externally.

CSC 17.8: Train Workforce on Causes of Unintentional Data Exposure

This sub-control can be implemented by enforcing a policy to regularly educate the workforce about indirect sensitive data exposure. This can include using a public computer or insecure networks to access the organization's data; or losing devices with organization's sensitive data.

CSC 17.9: Train Workforce Members on Identifying and Reporting Incidents

This sub-control can be implemented by enforcing a policy to regularly educate the workforce to report any suspicious or abnormal behavior.

CSC 18: Application Software Security

This control focuses on securing internally developed applications. There is a higher chance of an internally developed application to be more vulnerable due to the lack of resources for proper security testing before releasing the application. This CIS control has 11 sub-controls shown in Table 20.

Table 20: CSC 18 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
18.1	Establish Secure Coding Practices	Policy/Process		OWASP S-SDLC
18.2	Ensure Explicit Error Checking is Performed for All In-house Developed Software	Policy/Process		
18.3	Verify That Acquired Software is Still Supported	Policy/Process		
18.4	Only Use Up-to-date And Trusted Third-Party Components	Policy/Process		
18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Policy/Process		
18.6	Ensure Software Development Personnel are Trained in Secure Coding	Policy/Process		
18.7	Apply Static and Dynamic Code Analysis Tools	Policy/Process		OWASP
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Policy/Process		
18.9	Separate Production and Non-Production Systems	Policy/Process		
18.10	Deploy Web Application Firewalls (WAFs)	pfSense	ModSecurity	
18.11	Use Standard Hardening Configuration Templates for Databases	Policy/Process	GPO / CIS Benchmarks	

CSC 18.1: Establish Secure Coding Practices

This sub-control requires an organization to establish a policy and process to ensure secure coding process is followed by the development team members. An organization can refer to the Open Web Application Security Project (OWASP) Secure Software Development Lifecycle Project (S-SDLC) for guidelines and best practices.[150]

CSC 18.2: Ensure Explicit Error Checking is Performed for All In-house Developed Software

Application errors usually provide valuable information to attackers. Some errors might reveal certain configuration settings or configuration files' location. Organizations can implement this sub-control by enforcing a policy and a process to sanitize any application error with a generic message instead of verbose one.

CSC 18.3: Verify That Acquired Software is Still Supported

This sub-control is very similar to CSC 2.2. Organizations can implement this control by utilizing a policy and a process to check the version of an externally acquired software for vendor support.

CSC 18.4: Only Use Up-to-date and Trusted Third-Party Components

Many internally developed applications will utilize third-party components. Organizations can implement this sub-control by utilizing a policy and a process to ensure all third-party have supported updates from the vendor and are updated as soon as the components are integrated with the internal application.

CSC 18.5: Use Only Standardized and Extensively Reviewed Encryption Algorithms

Organizations can implement this sub-control by utilizing a policy and a process to ensure that developers refrain from using any specially developed internal algorithms for internal applications. Instead, developers can use a well-known algorithm to reduce the risk of breaking the algorithm.

CSC 18.6: Ensure Software Development Personnel are Trained in Secure Coding

Organizations can implement this sub-control by utilizing a policy and a process to train in-house developers on secure coding. Depending on the primary programming language used to develop the application, an organization can find many guidelines on how to code securely using that programming language.

CSC 18.7: Apply Static and Dynamic Code Analysis Tools

Organizations can implement this sub-control by utilizing a policy and a process to use static and dynamic code analysis tools when developing applications. OWASP has a great reference to some of the tools that can be used to cover this sub-control. Also, the community has compiled a list of tools that can be utilized to cover this control.[151-153]

CSC 18.8: Establish a Process to Accept and Address Reports of Software Vulnerabilities

Organizations can implement this control by utilizing a policy and a process to start a bug bounty program or other similar programs to allow external entities to test an organization's application. While it will not be easy to implement this sub-control using OSSS, organizations can allow different internal Quality Assurance (QA) teams to test different applications that the QA teams never tested before.

CSC 18.9: Separate Production and Non-Production Systems

Organizations can implement this sub-control by utilizing a policy and a process to enforce developers to use separate systems and even networks for testing application before releasing to production.

CSC 18.10: Deploy Web Application Firewalls (WAFs)

WAFs can significantly reduce the risk associated with vulnerable web applications. WAFs has the ability to verify user input and sanitize the web application server output. Organizations can implement this sub-control by utilizing pfSense and ModSecurity.

CSC 18.11: Use Standard Hardening Configuration Templates for Databases

Just as mentioned in CSC 5.1, secure configurations should be applied to all organization's assets including databases. Databases are usually targeted for the amount of valuable data stored and a wide range of vulnerabilities. Organizations can implement this sub-control by utilizing CIS Benchmarks as a guideline to securely configure different types of databases. GPOs can also be used to ensure that secure configurations are enforced and not changed over time.

CSC 19: Incident Response and Management

Given the threat landscape today, any organization might be a potential victim of a cyber-attack. This control will focus on preparing organizations to respond and contain an attack by ensuring the proper policies and processes are implemented. Thus, this control will focus on policies and processes primarily. This CIS control has eight sub-controls shown in Table 21.

Table 21: CSC 19 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
19.1	Document Incident Response Procedures	Policy/Process		NIST SP 800-61
19.2	Assign Job Titles and Duties for Incident Response	Policy/Process		
19.3	Designate Management Personnel to Support Incident Handling	Policy/Process		
19.4	Devise Organization-wide Standards for Reporting Incidents	Policy/Process		
19.5	Maintain Contact Information For Reporting Security Incidents	Policy/Process		

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Policy/Process		
19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Policy/Process		
19.8	Create Incident Scoring and Prioritization Schema	Policy/Process		

CSC 19.1: Document Incident Response Procedures

This sub-control can be implemented by having a procedure defining the roles needed to handle the incident along with a guideline to identify the incident handling phase. An organization can use NIST Computer Security Incident Handling Guide as a guideline to implement this sub-control.[154]

CSC 19.2: Assign Job Titles and Duties for Incident Response

In an event of an incident, organizations can hit the ground running by having a policy that identifies the key personnel to handle and address the incident. The policy or procedure can also specify the tasks assigned to each person. This sub-control can be covered by implementing the policy mentioned.

CSC 19.3: Designate Management Personnel to Support Incident Handling

Organizations can implement this sub-control using a process to identify the management personnel responsible to make decisions when handling an incident and including this personnel in the incident handling procedure.

CSC 19.4: Devise Organization-wide Standards for Reporting Incidents

Organizations can implement this sub-control by ensuring the procedures to report incidents by any organization’s employee is included in the incident handling procedures.

CSC 19.5: Maintain Contact Information for Reporting Security Incidents

Organizations can implement this sub-control by including contact information for helpful third-party like law enforcement or vendors in the incident handling procedures.

CSC 19.6: Publish Information Regarding Reporting Computer Anomalies and Incidents

This sub-control follows CSC 19.4. Organizations can use a policy to involve all the organization’s employees to be part of the incident response process to detect and report abnormal activities as they happen.

CSC 19.7: Conduct Periodic Incident Scenario Sessions for Personnel

Organizations can implement this sub-control by having a routinely table-top exercise to identify weak points and potential improvements for the overall security posture.

CSC 19.8: Create Incident Scoring and Prioritization Schema

This sub-control can be implemented by using a scoring system to prioritize the organization’s efforts when handling multiple incidents at the same time. The procedure can also include how often an update should be provided to upper management based on the incident’s threat-level and impact.

CSC 20: Penetration Tests and Red Team Exercises

The last control focuses on identifying vulnerabilities and weaknesses before the attackers do. It covers testing different elements by following the malicious attacker thought-process. This CIS control has eight sub-controls shown in Table 22.

Table 22: CSC 20 coverage per sub-control

CSC	Sub-Control Title	Primary Tool	Secondary Tool	Other Options
20.1	Establish a Penetration Testing Program	Policy/Process		
20.2	Conduct Regular External and Internal Penetration Tests	Policy/Process		Kali Linux
20.3	Perform Periodic Red Team Exercises	Policy/Process		Kali Linux
20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Policy/Process		
20.5	Create Test Bed for Elements Not Typically Tested in Production	Policy/Process		
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	OpenVAS		
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Policy/Process		SCAPTimony
20.8	Control and Monitor Accounts Associated with Penetration Testing	Policy/Process		

CSC 20.1: Establish a Penetration Testing Program

This sub-control can be implemented by starting a process to build the organization’s penetration testing program. The plan can include which areas or technologies to be tested and accounts for full or partial coverage based on the testing scope.

CSC 20.2: Conduct Regular External and Internal Penetration Tests

Organizations can implement this sub-control by performing internal and external penetration tests. While these tests might require extra bodies or expertise, there are many tools with a wide range of tutorials on how to get started. Organizations can utilize Kali Linux distribution’s tools to perform these tests.[155]

CSC 20.3: Perform Periodic Red Team Exercises

Organizations can implement this sub-control by performing red team exercises regularly to test the blue team ability to detect and respond to attacks. This sub-control is a blend of a policy, process and tools. Kali Linux can also be used to conduct red team exercises.

CSC 20.4: Include Tests for Presence of Unprotected System Information and Artifacts

If an organization implemented CSC 13.1 successfully, then this control can be implemented by having a policy and a process to search for sensitive information identified in CSC 13.1 in un-secure systems. This can include unencrypted password files, network diagrams, and configuration files to name a few.

CSC 20.5: Create Test Bed for Elements Not Typically Tested in Production

Many authorized and approved penetration tests can result in production systems downtime. Organizations can duplicate the production systems in a separate environment for testing these systems without affecting the business. This sub-control can also be covered by a process.

CSC 20.6: Use Vulnerability Scanning and Penetration Testing Tools in Concert

Organizations can implement this sub-control by using the results of a vulnerability scan as a starting point for penetration testing. This process will aid on focusing the penetration testing efforts on the obvious weaknesses. This sub-control can also be covered by a process.

CSC 20.7: Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards

Organizations can implement this sub-control by using the same format for all penetration testing results. This way the organization can have the ability to go back and compare the results. If an organization is utilizing SCAP standards, SCAPTimony can be used to store SCAP results in a database.[156]

CSC 20.8: Control and Monitor Accounts Associated with Penetration Testing

Organizations can implement this sub-control by having a policy to track user accounts used during penetration tests as well as a procedure to remove these accounts after the engagement is over.

The Missing Control – Secure Network Engineering

CIS has dropped control 19 “Secure Network Engineering” from version 6 and replaced it with CSC 7 in version 7 “Email and Web Browser Protections”. CIS did not bring back “Secure Network Engineering” in version 7. However, since the aim of control 19 in version 5 “Secure Network Engineering” has been embedded throughout version 7. An initial analysis of “Secure Network Engineering” sub-controls indicated that the missing sub-controls overlap with some of the sub-controls indicated in version 7. So, by implementing version 7, organizations can indirectly have coverage for the missing control “Secure Network Engineering”.

Coverage Matrix

As shown above, different tools can cover multiple sub-controls. To better understand the effectiveness of the proposed solution, a statistical analysis of each tool was conducted to calculate the percentage of each tool's coverage. The total coverage for the proposed solution was then calculated as well as the total coverage with additional OSSS which were listed under other options. Then, the average coverage for each category (Basic, Foundational, Organizational).

Basic Controls Coverage Matrix

As mentioned above, the first six controls are the "basic" controls and have the highest implementation priority. As shown in Table 23, using the proposed solution, the data shows a 97.9% coverage average for the first 6 controls. Organizations can achieve %100 coverage by utilizing one additional OSSS. The results show that implementing the proposed solution can provide organizations with a high coverage for the basic controls.

Table 23: Proposed solution coverage for each basic control.

	CSC 1	**CSC 2**	**CSC 3**	**CSC 4**	**CSC 5**	**CSC 6**	**Avg**
Security Onion	12.5%			22.2%		25.0%	
OpenVAS	12.5%		14.3%				
Wazuh					20.0%		
Kolide Fleet	25.0%	40.0%					
pfSense		5.0%					
Windows Tools	12.5%	30.0%	28.6%	16.7%	20.0%	6.3%	
Policy/Process	25.0%	25.0%	57.1%	61.1%	60.0%	68.8%	
Proposed Solution Coverage	**87.5%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**97.9%**
Additional OSSS	12.5%						
Total Coverage	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

Foundational Controls Coverage Matrix

The foundation controls are the controls that focus on the technical aspects of securing an organization. The foundational controls are from CSC 7 to CSC 16. As shown in Table 24, using the proposed solution; 90.1% coverage average for the 10 controls can be achieved. Organizations can achieve %100 coverage by utilizing additional OSSS. The analysis for this category also showed a high coverage percentage for the proposed solution.

Table 24: Proposed solution coverage for each foundational control.

	CSC 7	**CSC 8**	**CSC 9**	**CSC 10**	**CSC 11**	**CSC 12**	**CSC 13**	**CSC 14**	**CSC 15**	**CSC 16**	**Avg**
Security Onion	5.0%	6.3%				33.3%	11.1%			15.4%	
OpenVAS			40.0%			12.5%					
Wazuh		25.0%				4.2%		11.1%			
Kolide Fleet										3.8%	
pfSense	50.0%	6.3%	20.0%			33.3%	11.1%	22.2%			
Windows Tools	30.0%	56.3%	20.0%	50.0%	14.3%	4.2%	27.8%	16.7%	20.0%	19.2%	
Policy/Process		6.3%	20.0%	50.0%	71.4%	4.2%	38.9%	27.8%	60.0%	53.8%	
Proposed Solution Coverage	**85.0%**	**100.0%**	**100.0%**	**100.0%**	**85.7%**	**91.7%**	**88.9%**	**77.8%**	**80.0%**	**92.3%**	**90.1%**
Additional OSSS	15.0%				14.3%	8.3%	11.1%	22.2%	20.0%	7.7%	
Total Coverage	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

Organizational Controls Coverage Matrix

As discusses before, organizational controls focus more on policies and procedures and that has clearly reflected in the statistics' results. The organizational controls are from CSC 17 to CSC 20. As shown in Table 25, using the proposed solution, the data shows a 95.5% coverage average for the four controls. Organizations can achieve %100 coverage by utilizing one additional OSSS. Organizations can achieve over 70% coverage just by implementing the right policies and processes.

Table 25: Proposed solution coverage for each organizational control.

	CSC 17	**CSC 18**	**CSC 19**	**CSC 20**	**Avg**
Security Onion					
OpenVAS				12.5%	
Wazuh					
Kolide Fleet					
pfSense		9.1%			
Windows Tools		4.5%			
Policy/Process	94.4%	86.4%	100.0%	75.0%	
Proposed Solution Coverage	**94.4%**	**100.0%**	**100.0%**	**87.5%**	**95.5%**
Additional OSSS	5.6%			12.5%	
Total Coverage	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

As the field of information security develops, different solutions and tools may become more feasible to implement with the release of new features. On the other hand, other solutions and tools may become obsolete; developers might stop supporting the project and move on to other projects. If one of the proposed tools or solutions became obsolete or needed to be replaced with a better solution or tool, an organization can use Tables 23, 24 and 25 to determine which control has been affected by the replacement of the tool or the solution.

Discussion and Conclusion

This research was started to identify the potential of utilizing OSSS to cover CIS 20 CSC in order to help SMBs be more secure using cost-effective tools, software, and distributions. Understanding each sub-control and the purpose it is trying to serve; has helped to map the right tool, software or add-on needed to cover the sub-control. Breaking down each sub-control coverage per solution provided a more accurate result than just trying to cover the control at a high level. Even though the coverage for each control varied, the results show that a high percentage of CIS CSC can be implemented using five OSSS along with windows built-in tools.

The research has also revealed that implementing policies or processes can cover the majority of some controls and a significant portion of other controls. Policies and processes can be a quick win for some organizations or a good starting point to start implementing the CIS controls. Especially when an organization has some tools or software already implemented, applying the missing policies can lead to a total control coverage. The results also show that there is always a cost-effective tool or procedure to ensure coverage. However, these additional tools and procedures will require more efforts and additional resources to be utilized in order implement properly.

Researching the discussed tools and distributions showed that most of these tools and distributions require understanding the organization’s needs and gaps. It also requires organizations to research the associated cost with implementing such tools. While commercial solutions provide feature-rich tools and software as well as the ability to automate some tasks or processes; OSSS can deliver the same core functionality at the potential cost of human resources, minimal support, more time to implement and integrate as well as potentially higher maintenance costs. Organizations might need additional hardware or storage to utilize these tools. Organizations might also be able to utilize legacy systems for initial deployment, testing or even production use. A thorough research and testing must be conducted for each potential solution before deploying into production. The testing process can include testing the core functionality as well as the integrations with other existing or potential solutions.

While implementing all the proposed solutions to cover all the CIS controls might seem a tedious and impossible task for SMBs, organizations can take baby steps towards securing their environment by adopting one policy, process or proposed solution at a time. An organization can plan each implementation as part of the overall security roadmap to ensure enough testing and integration time is given for each implementation.

A limited financial budget should not stop any SMB from improving their security posture. Complicated and expensive security solutions can be substituted with simple cost-effective and ready to be deployed solutions to get the organization on the right security track. Even implementing the right policy or process can improve an organization's security posture tremendously.

Research Limitations

This thesis has the following assumptions and limitation:

- The results of this thesis are based on the current edition of the CIS 20 CSC version 7. Although the CIS 20 CSC contains well-defined, actionable security control. The CIS 20 CSC are updated frequently and organizations should continue to update their security measures accordingly.
- Implementing the proposed tools and controls do not guarantee that the organization will be breach-free nor that it will be %100 secure. However, the proposed tools and controls

will provide some level of security and help companies improve their overall security posture.

- This research focused primarily on Microsoft Windows as the primary type of operating system utilized across the organization. Other operating systems were not the focus of this research. However, the research included some solutions that inherently support multiple operating systems.
- Although OSS is mostly free to use, tool or distribution utilization may require an acquisition of additional hardware such as servers, storage space, peripherals, as well as hiring additional staff to manage and monitor the implemented solutions. So, there might be some costs associated with implementing these tools and controls.
- This research did not test the proposed solutions in a production environment. Integration ability as well solutions' collision should be accounted for while implementing the proposed solutions in a production environment.
- Most of the open source software suggested in this thesis provide free support through community forums and groups. Enterprise support is usually available at an additional cost.
- The proposed solutions suggested in this thesis may require the presence of a staff member who is familiar with the information security field to successfully implement the proposed solution. Getting the maximum benefit of a suggested solution might require a person with an extensive knowledge and experience in the information security field.

Future Research

This research has proposed potential low-cost solutions that can cover most of the CIS controls. Future research in this area could focus on the following questions:

- What is the estimated cost associated with additional hardware or staffing needed to implement the proposed solutions?
- What level of expertise is needed to successfully implement the proposed solution?
- What is the effectiveness of the proposed solutions in a Linux or macOS environment?
- How much of other security frameworks such as NIST 800-53 can be covered by implementing the proposed solution?
- What other features or capabilities does each proposed OSSS or distribution provide?
- What are the technical steps needed to implement each proposed solution?
- Will all the proposed solutions integrate well together?

References

1. The Statistics Portal. *Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)*. 2018 [cited 2018 November, 4]; Available from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
2. Ponemon Institute, ***2018 Cost of Data Breach Study: Global Overview***. 2018, Ponemon Institute LLC.
3. Manky, D., *Cybercrime as a service: a very modern business.* Computer Fraud & Security, 2013. **2013**(6): p. 9-13.
4. Watts, S., *IT Security Vulnerability vs Threat vs Risk: What's the Difference?*, in *BMC Blogs* 2017: Security & Compliance Blog
5. PwC, C.a.C., *The Global State of Information Security Survey 2018*. 2018.
6. Ponemon Institute, ***Cost of Data Breach Study: Global Overview***. 2017, Ponemon Institute LLC.
7. Richardson, S., *Ransomware Attacks: They'll Never Happen to You, Right?*, in *IT Managment*. 2017.
8. Applied Trust, *Every company needs to have a security program*, in *The Barking Seal*. 2008.
9. Lunden, I. *Target Says Credit Card Data Breach Cost It $162M In 2013-14*. 2015 [cited 2018 November 3]; Available from: https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/.
10. Symantec, *Internet Security Threat Report* 2016, Symantic.
11. SANS, *CIS Critical Security Controls:Maping the CIS Critical Security Controls*. 2016.
12. Trend Micro, *Addressing the SANS Top 20 Critical Security Controls for Effective Cyber Defense*, in *A trend Micro Whitepaper*. 2016.
13. SANS. *CIS Critical Security Controls: A Brief History*. 2018 [cited 2018 November, 7]; Available from: https://www.sans.org/critical-security-controls/history.
14. SANS. *The CIS Critical Security Controls for Effective Cyber Defense*. 2018 [cited 2018 November, 2]; Available from: https://www.sans.org/critical-security-controls.
15. Center for Internet Security, *CIS Controls, Version 7*. 2018.
16. Pescatore, J. and B. Filkins, *Back to Basics: Focus on the First Six CIS Critical Security Controls*. 2018 SANS Institute.
17. OpenSource. *What is Open Source?* [cited 2018 11,12]; Available from: https://opensource.com/resources/what-open-source.
18. Github. *Security Onion Solutions*. 2018 [cited 2018 11, 4]; Available from: https://github.com/Security-Onion-Solutions/security-onion.
19. OpenVAS. *Open Vulnerability Assessment System*. [cited 2018 October 10]; Available from: http://www.openvas.org.
20. Wazuh. *Wazuh: User Manual* [cited 2018 11, 4]; Available from: https://documentation.wazuh.com/current/user-manual/index.html.
21. OSSEC. *Open Source Host-based Intrusion Detection System (HIDS) SECurity* [cited 2018 11, 13]; Available from: https://www.ossec.net.
22. OpenSCAP. *Open Security Content Automation Protocol (SCAP)* [cited 2018 11, 14]; Available from: https://www.open-scap.org.

23. Elastic. *ELK Stack: Elasticsearch, Logslash, Kibana*. [cited 2018 11, 16]; Available from: https://www.elastic.co/elk-stack.

24. Kolide Fleet. *Kolide Fleet: Open Source Osquery Manager*. [cited 2018 November 10]; Available from: https://kolide.com/fleet.

25. Osquery. *Facebook/osquery: Performant endpoint visibility*. Available from: https://osquery.io.

26. PfSence. *pfSence: World's Most Trusted Open source Firewall*. [cited 2018 November 10]; Available from: https://www.pfsense.org.

27. U.S. Small Business Administration, *2018 Small Business Profile* 2018, U.S. Small Business Administration.

28. Verizon, *Data Breach Investigations Report- Excutive Summary* 2017, Verizon

29. William, D., *Only 1 in 4 Small Businesses Well Prepared for Cyber Attack*, in *Small Business Trends* 2017: Technology Trends

30. Anderson, K., *How Much Does Network Security Software Cost?*, in *IT Managment*. 2018, Capterra.

31. (CIS), C.f.I.S. *CIS Controls V7 Measures & Metrics*. 2018 [cited 2018 October 9]; Available from: https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/.

32. Snort. *Network Intrusion Detection & Prevention System*. [cited 2018 October 11]; Available from: https://www.snort.org.

33. Bro. *Bro Network Security Monitor*. [cited 2018 October 11]; Available from: https://www.bro.org/.

34. Suricata. *Suricata: Open Source IDS / IPS / NSM engine*. [cited 2018 October 11]; Available from: https://suricata-ids.org/.

35. prads. *Passive Real-time Asset Detection System*. [cited 2018 October 11]; Available from: https://github.com/gamelinux/prads.

36. PacketFence. *PacketFence: Open Source NAC*. [cited 2018 October 12]; Available from: https://packetfence.org.

37. Flores, J., et al. *Active Directory Domain Services Overview*. 2017 [cited 2018 11, 14]; Available from: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

38. Chandrasekaran, R. *Step by Step Guide to Setup LDAPS on Windows Server*. 2017 [cited 2017 11, 15]; Available from: https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/.

39. Chou, Y. *Enterprise PKI with Windows Server 2012 R2 Active Directory Certificate Services (Part 1 of 2)*. 2013 [cited 2018 11, 16]; Available from: https://blogs.technet.microsoft.com/yungchou/2013/10/21/enterprise-pki-with-windows-server-2012-r2-active-directory-certificate-services-part-1-of-2/.

40. Jones, P. *How to enable password + user certificate authentication in ADFS 3.0*. 2014 [cited 2018 November 11]; Available from: https://blogs.technet.microsoft.com/pauljones/2014/05/27/how-to-enable-password-user-certificate-authentication-in-adfs-3-0/.

41. Packerfence. *PKI Quick Installation Guide*. [cited 2018 November 14]; Available from: https://packetfence.org/doc/PacketFence_PKI_Quick_Install_Guide.html.

42. Lich, B., L. Poggemeyer, and J. Hall. *AppLocker*. [cited 2018 October 11]; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview.

43. Rouse, M. *Group Policy Object (GPO)*. [cited 2018 October 20]; Available from: https://searchwindowsserver.techtarget.com/definition/Group-Policy-Object.

44. Microsoft TechNet. *How to configure AppLocker Group Policy to prevent software from running*. [cited 2018 October 20]; Available from: https://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx.

45. OPNSence. *OPNsence: Open Source Firewall- High-end Security Made Easy*. [cited 2018 October 14]; Available from: https://opnsense.org.

46. Nmap. *Nmap: Network Mapper* [cited 2018 October 24]; Available from: https://nmap.org.

47. Nmap. *Ndiff: A utility for comparing Nmap scan results*. [cited 2018 October 10]; Available from: https://nmap.org/ndiff/.

48. WSUS. *WSUS: Windows Server Update Services* [cited 2018 October 23]; Available from: https://docs.microsoft.com/en-us/powershell/module/wsus/?view=win10-ps.

49. Chef. *Chef: Automate IT Infrastructure*. [cited 2018 October 23]; Available from: https://www.chef.io/chef/.

50. Ansible. *Ansible: Automatation for everyone* [cited 2018 october 23]; Available from: https://www.ansible.com.

51. Microsoft. *PowerShell Scripting*. [cited 2018 october 23]; Available from: https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6.

52. Richardson, T., et al., *Virtual Network Computing*. IEEE Internet Computing, 1998. **2**(1).

53. Microsooft. *Remote Desktop Protocol*. [cited 2018 October 25]; Available from: https://docs.microsoft.com/en-us/windows/desktop/termserv/remote-desktop-protocol.

54. The Internet Society, *The Secure Shell (SSH) Protocol Architecture*. 2006.

55. PrivacyIDEA. *privacyIDEA - Two Factor Authentication System*. [cited 2018 November 14]; Available from: https://www.privacyidea.org.

56. LinOTP. *LinOTP: The Open Source OTP Solution*. [cited 2018 November 14]; Available from: https://www.linotp.org.

57. gluu. *Gluu Server*. [cited 2018 November 14]; Available from: https://www.gluu.org.

58. Microsoft. *Using batch files*. [cited 2018 October 23]; Available from: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758944(v=ws.10).

59. Smith, R.F. *4732: A member was added to a security-enabled local group*. [cited 2018 October 23]; Available from: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4732.

60. Smith, R.F. *4728: A member was added to a security-enabled global group*. [cited 2018 October 23]; Available from: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4728.

61. Smith, R.F. *4729: A member was removed from a security-enabled global group*. [cited 2018 October 23]; Available from:

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4729.

62. Smith, R.F. *4625: An account failed to log on*. [cited 2018 October 23]; Available from: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4625.

63. Cezar, M. *How to Find All Failed SSH login Attempts in Linux*. 2017 [cited 2018 October 23]; Available from: https://www.tecmint.com/find-failed-ssh-login-attempts-in-linux/.

64. Center for Internet Security. *CIS Benchmarks*. [cited 2018 October 24]; Available from: https://www.cisecurity.org/cis-benchmarks/.

65. Microsoft. *Windows security baselines*. [cited 2018 October 25]; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines#where-can-i-get-the-security-baselines.

66. Microsoft. *Group Policy API*. [cited 2018 October 23]; Available from: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/Policy/group-policy-start-page.

67. Wazuh. *OpenSCAP*. [cited 2018 November 11]; Available from: https://documentation.wazuh.com/current/user-manual/capabilities/policy-monitoring/openscap/index.html.

68. Tawfik, M. *"It's Simple!" – Time Configuration in Active Directory*. 2013 [cited 2018 November 15]; Available from: https://blogs.technet.microsoft.com/nepapfe/2013/03/01/its-simple-time-configuration-in-active-directory/.

69. Elastic. *The Beats Family*. [cited 2018 October 23]; Available from: https://www.elastic.co/products/beats.

70. Eaton, I., *GIAC Security Essentials Certification (GSEC) Practical Assignment*. 2003, SANS Institute

71. GrayLog. *Graylog: Do more with your log data*. [cited 2018 October 23]; Available from: https://www.graylog.org/solutions/security.

72. Squid-Cache. *Squid: Optimising Web Delivery*. [cited 2018 October 20]; Available from: http://www.squid-cache.org.

73. URLfilterDP. *ufdbGuard, a URL filter for Squid*. [cited 2018 October 25]; Available from: https://www.urlfilterdb.com/products/ufdbguard.html.

74. E2guardian. *E2guardian Web filtering*. [cited 2018 October 24]; Available from: http://e2guardian.org/cms/index.php.

75. Netgate. *Configuring the DNS Resolver*. [cited 2018 October 25]; Available from: https://www.netgate.com/docs/pfsense/dns/unbound-dns-resolver.html.

76. OpenDNS. *Cloud Delivered Enterprise Security by OpenDNS*. [cited 2018 October 25]; Available from: https://www.opendns.com.

77. CleanBrowsing. *CleanBrowsing DNS - Protecting our families and kids when visiting the web*. . [cited 2018 November 11]; Available from: https://cleanbrowsing.org.

78. Quad9. *Quad9 DNS: Internet Security and Privacy in a Few Easy Steps*. [cited 2018 October 20]; Available from: https://www.quad9.net.

79. MailScanner. *MailScanner: The #1 Open Source Email Filter*. [cited 2018 October 23]; Available from: https://www.mailscanner.info.

80. MailScanner. *Using MailScanner with Postfix*. [cited 2018 November 11]; Available from: https://www.mailscanner.info/postfix/.

81. MailScanner. *Configuration Index - MailScanner v5.1.x*. Available from: https://www.mailscanner.info/MailScanner.conf.index.html#Check%20SpamAssassin%20If%20On%20Spam%20List.
82. ClamAV. *ClamAV*. [cited 2018 November 10]; Available from: https://www.clamav.net.
83. Github. *Windows Defender ASR in OSSEC*. [cited 2018 November 10]; Available from: https://gist.github.com/frcolumba/5a2518684ed4e2b18a386fa3647d5629.
84. Microsoft. *Customize Exploit Protection*. [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection.
85. Microsoft. *Windos 10 Commercial Edition Comparison*. [cited 2018 November 10]; Available from: https://wincom.blob.core.windows.net/documents/Windows10_Commercial_Comparison.pdf.
86. Martin, A. *Monitoring USB drives in Windows using Wazuh*. 2017 [cited 2018 November 11]; Available from: https://blog.wazuh.com/monitoring-usb-drives-in-windows-using-wazuh/.
87. Microsoft. *How to disable the Autorun functionality in Windows*. [cited 2018 November 10]; Available from: https://support.microsoft.com/en-us/help/967715/how-to-disable-the-autorun-functionality-in-windows.
88. Microsoft. *Command line process auditing*. 2017 [cited 2018 2018]; November 11]. Available from: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing.
89. Microsoft. *Windows Firewall Integration and Best Practices*. 2018 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices.
90. ModSecurity. *ModSecurity: Open Source Web Application Firewall*. 2018 [cited 2018 November 11]; Available from: https://www.modsecurity.org.
91. Pfsense Setup HQ. *ModSecurity: Part One*. 2014 [cited 2018 November 11]; Available from: http://pfsensesetup.com/modsecurity-part-one/.
92. Microsoft. *Back up and restore your PC*. [cited 2018 November 15]; Available from: https://support.microsoft.com/en-us/help/17127/windows-back-up-restore.
93. Microsoft. *File History in Windows*. [cited 2018 November 15]; Available from: https://support.microsoft.com/en-us/help/17128/windows-8-file-history.
94. Microsoft. *Microsoft OneDrive*. [cited 2018 November 14]; Available from: https://onedrive.live.com/about/en-us/.
95. Huculak, M. *How to use System Restore on Windows 10*. 2017 [cited 2018 November 15]; Available from: https://www.windowscentral.com/how-use-system-restore-windows-10.
96. Microsoft. *Set up or customize server backup*. 2016 [cited 2018 November 15]; Available from: https://docs.microsoft.com/en-us/windows-server-essentials/manage/set-up-or-customize-server-backup.
97. UrBackup. *UrBackup: Client/Server Open Source Network Backup for Windows*. [cited 2018 November 15]; Available from: https://www.urbackup.org.
98. Amanda. *Amanda: The Advanced Maryland Automatic Network Disk Archiver*. [cited 2018 November 14]; Available from: http://www.amanda.org.
99. Systems, B. *Bacula: Open Source Backup, Enterprise ready, Network Backup Tool*. [cited 2018 November 11]; Available from: http://blog.bacula.org/page/3/.

100. Microsoft. *BitLocker*. 2017 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

101. Netgate. *Introduction to the Firewall Rules screen*. [cited 2018 November 11]; Available from: https://www.netgate.com/docs/pfsense/book/firewall/introduction-to-the-firewall-rules-screen.html.

102. Github. *nipper*. [cited 2018 November 11]; Available from: https://github.com/arpitn30/nipper-ng/tree/master/0.11.10.

103. Moloch. *Moloch*. [cited 2018 November 11]; Available from: https://molo.ch.

104. Netgate. *Pfsence: IDS/ IPS*. [cited 2018 October 18]; Available from: https://www.netgate.com/docs/pfsense/ids-ips/index.html.

105. Github. *pfsense_fauxapi*. [cited 2018 October 11]; Available from: https://github.com/ndejong/pfsense_fauxapi.

106. Github. *so-ntopng-installer*. [cited 2018 October 11]; Available from: https://github.com/branchnetconsulting/so-ntopng-installer.

107. Github. *nfdump*. [cited 2018 October 11]; Available from: https://github.com/phaag/nfdump.

108. Github. *elastiflow*. [cited 2018 October 12]; Available from: https://github.com/robcowart/elastiflow.

109. Github. *SOF-ELK: Configuration files for the SOF-ELK VM, used in SANS FOR572*. [cited 2018 October 10]; Available from: https://github.com/philhagen/sof-elk.

110. Thompson, J. *Application Detection on pfSense® Software*. 2017 [cited 2018 October 12]; Available from: https://www.netgate.com/blog/application-detection-on-pfsense-software.html.

111. FreeRADIUS. *FreeRADIUS*. [cited 2018 November 11]; Available from: https://freeradius.org.

112. Cisco. *How Does RADIUS Work?* 2006 [cited 2018 November 11]; Available from: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html.

113. Microsoft. *Plan NPS as a RADIUS server*. [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-plan-server.

114. Netgate. *Authenticating OpenVPN Users with RADIUS via Active Directory*. [cited 2018 11, 15]; Available from: https://www.netgate.com/docs/pfsense/vpn/openvpn/authenticating-openvpn-users-with-radius-via-active-directory.html?highlight=certificate.

115. MyDLP. *MyDLP*. [cited 2018 November 11]; Available from: https://www.mydlp.com.

116. Github. *JA3 is a standard for creating SSL client fingerprints in an easy to produce and shareable way*. [cited 2018 November 11]; Available from: https://github.com/salesforce/ja3.

117. Surveillance Self-Defence. *How to: Encrypt Your iPhone*. 2018 [cited 2018 November 10]; Available from: https://ssd.eff.org/en/module/how-encrypt-your-iphone.

118. Microsoft. 2017 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/intune-user-help/encrypt-your-device-android.

119. Huculak, M. *How to enable write protection for USB devices on Windows 10*. 2016 [cited 2018 November 11]; Available from: https://www.windowscentral.com/how-enable-write-protection-usb-devices-windows-10.

120. Microsoft. *Prepare your organization for BitLocker: Planning and policies*. 2018 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies.

121. Microsoft. *BitLocker Group Policy settings*. 2017 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings.

122. MyDLP. *How to deploy MyDLP Endpoint Agent automatically on a Microsoft Active Directory domain*. 2018 [cited 2018 November 11]; Available from: https://www.mydlp.com/deploy-mydlp-endpoint-agent-automatically-microsoft-active-directory-domain/.

123. Microsoft. *Trusted Platform Module (TPM) and BitLocker Drive Encryption*. [cited 2018 November 11]; Available from: https://technet.microsoft.com/en-us/windows/dn653315(v=vs.92).

124. Hoffman, C. *How to Use a USB Key to Unlock a BitLocker-Encrypted PC*. 2016 [cited 2018 November 11]; Available from: https://www.howtogeek.com/262744/how-to-use-a-usb-key-to-unlock-a-bitlocker-encrypted-pc/.

125. Romero, R. *Configuring OSSEC to report file changes*. 2016 [cited 2018 November 11]; Available from: https://blog.wazuh.com/configure-ossec-to-report-changes-in-the-content-of-a-text-file/.

126. SourceForge. *RogueScanner*. [cited 2018 November 11]; Available from: https://sourceforge.net/projects/roguescanner/.

127. Github. *Rogue Access Point Detector*. [cited 2018 Novimber 11]; Available from: https://github.com/anotherik/RogueAP-Detector.

128. OpenWIPS-ng. *OpenWIPS-ng*. [cited 2018 November 11]; Available from: http://openwips-ng.org.

129. Champ, C. *Building Wireless IDS Systems Using Open Source* [cited 2018 November 11]; Available from: http://sagan.quadrantsec.com/papers/wireless-ids/.

130. Hutchison, K., *Wireless Intrusion Detection Systems*. 2004, SANS Institiue

131. Rouse, M. *Advanced Encryption Standard (AES)*. [cited 2018 November 11]; Available from: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard.

132. Intel. *Overview and EAP Types*. 2018 [cited 2018 November 11]; Available from: https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html.

133. Microsoft. *Deploy Password-Based 802.1X Authenticated Wireless Access*. 2018 [cited 2018 November 14]; Available from: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/wireless/a-deploy-8021x-wireless-access.

134. Microsoft. *Office 365 is built for your business.* [cited 2018 October 23]; Available from: https://products.office.com/en-us/business/office.

135. google. *G suite*. [cited 2018 October 25]; Available from: https://gsuite.google.com.

136. Script Center. *Get Active Directory - user information report summary Get-ADUser*. 2011 [cited 2018 November 10]; Available from:

https://gallery.technet.microsoft.com/scriptcenter/f3d907e4-2438-4aff-9370-238b7a787d35.

137. OpenIAM. *OpenIAM - Open Source Identity and Access Management*. [cited 2018 November 10]; Available from: https://www.openiam.com.

138. Microsoft. *Configure Windows Spotlight on the lock screen*. 2018 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/configuration/windows-spotlight.

139. Microsoft. *Interactive logon: Machine inactivity limit*. 2018 [cited 2018 November 11]; Available from: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit.

140. Smith, R.F. *Access Denied: Identifying Logon Attempts That Use Disabled Accounts*. 2004 [cited 2018 November 11]; Available from: https://www.itprotoday.com/windows-78/access-denied-identifying-logon-attempts-use-disabled-accounts.

141. Studies, N.N.I.f.C.C.a. *NICE Cybersecurity Workforce Framework*. [cited 2018 November 11]; Available from: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

142. Education, N.N.I.f.C. *Determining Current Cybersecurity Capabilities: Develop and maintain an unrivaled, globally competitive cybersecurity workforce*. [cited 2018 November 11]; Available from: https://www.nist.gov/sites/default/files/documents/2017/01/27/wed_determining-current-cybersecurity-capabilities_mkoehler.pdf.

143. Cybrary, *Cybrary - Online Cyber Security Training, Free, Forever*.

144. Bowne, S. *Sams Class: Sam Bowne Class Information*. [cited 2018 November 12]; Available from: https://samsclass.info.

145. Open Security Training. Open Security Training [cited 2018 November 11]; Available from: http://opensecuritytraining.info.

146. NIST National Institute of Standard and Technology, *Building an Information Technology Security Awareness and Training Program*. 2003, U.S. GOVERNMENT PRINTING OFFICE: Washington, DC.

147. SANS. *Security Awarness Resources*. [cited 2018 November 11]; Available from: https://www.sans.org/security-awareness-training/resources.

148. SANS. *OUCH! Newsletter*. [cited 2018 November 11]; Available from: https://www.sans.org/security-awareness-training/ouch-newsletter.

149. Gophish. *Gophish: Open-Source Phishing Framework*. [cited 2018 November 11]; Available from: https://getgophish.com.

150. OSASP. *OWASP Secure Software Development Lifecycle Project(S-SDLC)*. [cited 2018 November 11]; Available from: https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project.

151. Github. *Static analysis tools for all programming languages*. [cited 2018 November 11]; Available from: https://github.com/mre/awesome-static-analysis.

152. OWASP. *Source Code Analysis Tools*. 2018 [cited 2018 November 11]; Available from: https://www.owasp.org/index.php/Source_Code_Analysis_Tools.

153. Github. *A curated list of dynamic analysis tools for various programming languages*. [cited 2018 Novembe 11]; Available from: https://github.com/mre/awesome-dynamic-analysis.

154. NIST National Institute of Standard and Technology, *Computer Security Incident Handling Guide:Recommendations of the National Institute of Standards and Technology*. 2012.

155. Kali by Offensive Security. *Kali Linux: Penetration Testing and Ethical Hacking Linux Distribution*. [cited 2018 November 11]; Available from: https://www.kali.org.

156. OpenSCAP. *ScapTimony: OpenSCAP portal*. [cited 2018 November 11]; Available from: https://www.open-scap.org/tools/scaptimony/.

Appendix 1

The CIS Controls Version 7 Controls, Sub-Controls and Sensors

CIS	Title	Description	Sensor
1	**Inventory and Control of Hardware Assets**		
1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	Active Device Discovery System
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Passive Device Discovery System
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	Log Management System / SIEM
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Asset Inventory System
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Asset Inventory System
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	Asset Inventory System
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Network Level Authentication (NLA)
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Public Key Infrastructure (PKI)

CIS	Title	Description	Sensor
2	**Inventory and Control of Software Assets**		
2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	Software Application Inventory
2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	Software Application Inventory
2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Software Application Inventory
2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	Software Application Inventory
2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Software Application Inventory
2.6	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	Software Application Inventory
2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Software Whitelisting System
2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Software Whitelisting System
2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.	Software Whitelisting System
2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Network Firewall / Access Control System

CIS	Title	Description	Sensor
3	**Continuous Vulnerability Management**		
3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	SCAP Based Vulnerability Management System
3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	SCAP Based Vulnerability Management System
3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	SCAP Based Vulnerability Management System
3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	Patch Management System
3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	Patch Management System
3.6	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	SCAP Based Vulnerability Management System
3.7	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	SCAP Based Vulnerability Management System
4	**Controlled Use of Administrative Privileges**		
4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Privileged Account Management System

CIS	Title	Description	Sensor
4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	Privileged Account Management System
4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	Privileged Account Management System
4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	Privileged Account Management System
4.5	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	Multi-Factor Authentication System
4.6	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	Dedicated Administration Systems
4.7	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	Software Whitelisting System
4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Log Management System / SIEM
4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Log Management System / SIEM

CIS	Title	Description	Sensor
5	**Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**		
5.1	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.	System Configuration Baselines & Images
5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	System Configuration Baselines & Images
5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	System Configuration Baselines & Images
5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	System Configuration Enforcement System
5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	SCAP Based Vulnerability Management System
6	**Maintenance, Monitoring and Analysis of Audit Logs**		
6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	Network Time Protocol (NTP) Systems
6.2	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.	Log Management System / SIEM
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Log Management System / SIEM
6.4	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	Log Management System / SIEM

CIS	Title	Description	Sensor
6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Log Management System / SIEM
6.6	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Log Management System / SIEM
6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	Log Management System / SIEM
6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	Log Management System / SIEM
7	**Email and Web Browser Protections**		
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	Software Whitelisting System
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	Software Whitelisting System
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	System Configuration Enforcement System
7.4	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Network URL Filtering System
7.5	Subscribe to URL-Categorization service	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Network URL Filtering System
7.6	Log all URL requests	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	Log Management System / SIEM
7.7	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.	DNS Domain Filtering System

CIS	Title	Description	Sensor
7.8	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	Anti-Spam Gateway
7.9	Block Unnecessary File Types	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.	Anti-Spam Gateway
7.10	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Anti-Spam Gateway
8	**Malware Defenses**		
8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Endpoint Protection System
8.2	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	Endpoint Protection System
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	System Configuration Enforcement System
8.4	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	Endpoint Protection System
8.5	Configure Devices Not To Auto-run Content	Configure devices to not auto-run content from removable media.	System Configuration Enforcement System
8.6	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	Endpoint Protection System
8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	DNS Domain Filtering System

CIS	Title	Description	Sensor
8.8	Enable Command-line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.	Log Management System / SIEM
9	**Limitation and Control of Network Ports, Protocols, and Services**		
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.	SCAP Based Vulnerability Management System
9.2	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	SCAP Based Vulnerability Management System
9.3	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	SCAP Based Vulnerability Management System
9.4	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Host Based Firewall
9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Application Aware Firewall
10	**Data Recovery Capabilities**		
10.1	Ensure Regular Automated Back Ups	Ensure that all system data is automatically backed up on regular basis.	Backup / Recovery System
10.2	Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Backup / Recovery System
10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Backup / Recovery System
10.4	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Backup / Recovery System

CIS	Title	Description	Sensor
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.	Backup / Recovery System
11	**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**		
11.1	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.	Network Device Management System
11.2	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	Network Device Management System
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	Network Device Management System
11.4	Install the Latest Stable Version of Any Security-related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	Network Device Management System
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	Multi-Factor Authentication System
11.6	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	Dedicated Administration Systems
11.7	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate	Dedicated Administration Systems

CIS	Title	Description	Sensor
		VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	
12	**Boundary Defense**		
12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	Network Firewall / Access Control System
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	System Configuration Enforcement System
12.3	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	Network Firewall / Access Control System
12.4	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	Network Firewall / Access Control System
12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	Network Packet Capture System
12.6	Deploy Network-based IDS Sensor	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	Network Based Intrusion Detection System (NIDS)
12.7	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	Network Based Intrusion Prevention System (IPS)
12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	Network Device Management System

CIS	Title	Description	Sensor
12.9	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	Network Firewall / Access Control System
12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Network Firewall / Access Control System
12.11	Require All Remote Login to Use Multi-factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	Multi-Factor Authentication System
12.12	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	System Configuration Enforcement System
13	**Data Protection**		
13.1	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	Data Inventory / Classification System
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Data Inventory / Classification System
13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Network Based Data Loss Prevention (DLP) System
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	Network Firewall / Access Control System

CIS	Title	Description	Sensor
13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	Network Based Data Loss Prevention (DLP) System
13.6	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	Whole Disk Encryption System
13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	Endpoint Protection System
13.8	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Endpoint Protection System
13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	Endpoint Protection System
14	**Controlled Access Based on the Need to Know**		
14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	Network Firewall / Access Control System
14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	Network Firewall / Access Control System
14.3	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	Network Firewall / Access Control System
14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	System Configuration Enforcement System
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems,	Data Inventory / Classification System

CIS	Title	Description	Sensor
		including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	
14.6	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	System Configuration Enforcement System
14.7	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Host Based Data Loss Prevention (DLP) System
14.8	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Host Based Data Loss Prevention (DLP) System
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	Log Management System / SIEM
15	**Wireless Access Control**		
15.1	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	Network Device Management System
15.2	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	SCAP Based Vulnerability Management System
15.3	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Wireless Intrusion Detection System (WIDS)
15.4	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	System Configuration Enforcement System

CIS	Title	Description	Sensor
15.5	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	System Configuration Enforcement System
15.6	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.	System Configuration Enforcement System
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	Network Device Management System
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.	Network Device Management System
15.9	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	System Configuration Enforcement System
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	Network Device Management System
16	**Account Monitoring and Control**		
16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	Identity & Access Management System
16.2	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	Identity & Access Management System

CIS	Title	Description	Sensor
16.3	Require Multi-factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	Multi-Factor Authentication System
16.4	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	Identity & Access Management System
16.5	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	Identity & Access Management System
16.6	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	Identity & Access Management System
16.7	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	Identity & Access Management System
16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	Identity & Access Management System
16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	Identity & Access Management System
16.10	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	Identity & Access Management System
16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	Identity & Access Management System
16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	Log Management System / SIEM

CIS	Title	Description	Sensor
16.13	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Log Management System / SIEM
17	**Implement a Security Awareness and Training Program**		
17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	Training / Awareness Education Plans
17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	Training / Awareness Education Plans
17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	Training / Awareness Education Plans
17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	Training / Awareness Education Plans
17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	Training / Awareness Education Plans
17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	Training / Awareness Education Plans
17.7	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	Training / Awareness Education Plans
17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	Training / Awareness Education Plans
17.9	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	Training / Awareness Education Plans

CIS	Title	Description	Sensor
18	**Application Software Security**		
18.1	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	Secure Coding Standards
18.2	Ensure Explicit Error Checking is Performed for All In-house Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Secure Coding Standards
18.3	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	Secure Coding Standards
18.4	Only Use Up-to-date And Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	Secure Coding Standards
18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.	Secure Coding Standards
18.6	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	Training / Awareness Education Plans
18.7	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Software Vulnerability Scanning Tool
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Software Vulnerability Scanning Tool
18.9	Separate Production and Non-Production Systems	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	Secure Coding Standards

CIS	Title	Description	Sensor
18.10	Deploy Web Application Firewalls (WAFs)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Web Application Firewall (WAF)
18.11	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	System Configuration Enforcement System
19	**Incident Response and Management**		
19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.	Incident Management Plans
19.2	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	Incident Management Plans
19.3	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	Incident Management Plans
19.4	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	Incident Management Plans
19.5	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	Incident Management Plans
19.6	Publish Information Regarding Reporting	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	Incident Management Plans

CIS	Title	Description	Sensor
	Computer Anomalies and Incidents		
19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	Incident Management Plans
19.8	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	Incident Management Plans
20	**Penetration Tests and Red Team Exercises**		
20.1	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	Penetration Testing Plans
20.2	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	Penetration Testing Plans
20.3	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Penetration Testing Plans
20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	Penetration Testing Plans
20.5	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	Penetration Testing Plans
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	Penetration Testing Plans
20.7	Ensure Results from Penetration Test are	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method	Penetration Testing Plans

CIS	Title	Description	Sensor
	Documented Using Open, Machine-readable Standards	for determining the results of Red Team exercises so that results can be compared over time.	
20.8	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	Penetration Testing Plans