CYBERSECURITY

Presented by: PSA®

PSA Cybersecurity Committee

CIS CONTROLS WHITEPAPER

2020 EDITION

INTRODUCTION

PLAIN LANGUAGE EXPLANATION OF KEY INFORMATION SECURITY CONTROLS AND THEIR IMPLEMENTATION IN OUR RESPECTIVE ORGANIZATIONS

The implementation of a cybersecurity program can be a daunting task. Starting the process can be extremely difficult and time consuming. Where do I start? Which standard should I implement? How do I measure success? Often, there is too much information, not enough information, or very complicated standards to analyze. We can thank the folks from The Center for Internet Security (CIS) for developing a framework that is reasonably straightforward to implement, provides for verification of our processes, and allows us to implement new strategies when the need arises.

Security through obscurity is a thing of the past. As integrators, we must protect ourselves against constantly emerging threats. We owe it to our customers and our organization to maintain an adequate level of cyber security. This document is designed to provide a plain language explanation of key Information Security controls and their implementation in our respective organizations.

The Center for Internet Security has identified 20 of the top cyber security controls which, when fully implemented, are generally agreed to mitigate a high percentage of the cyber security vulnerabilities that are inherent to networked systems. These controls are commonly referred to as the CIS Controls V7.1 (CIS Controls™) and are a great starting place when trying to improve the cyber security of your network.

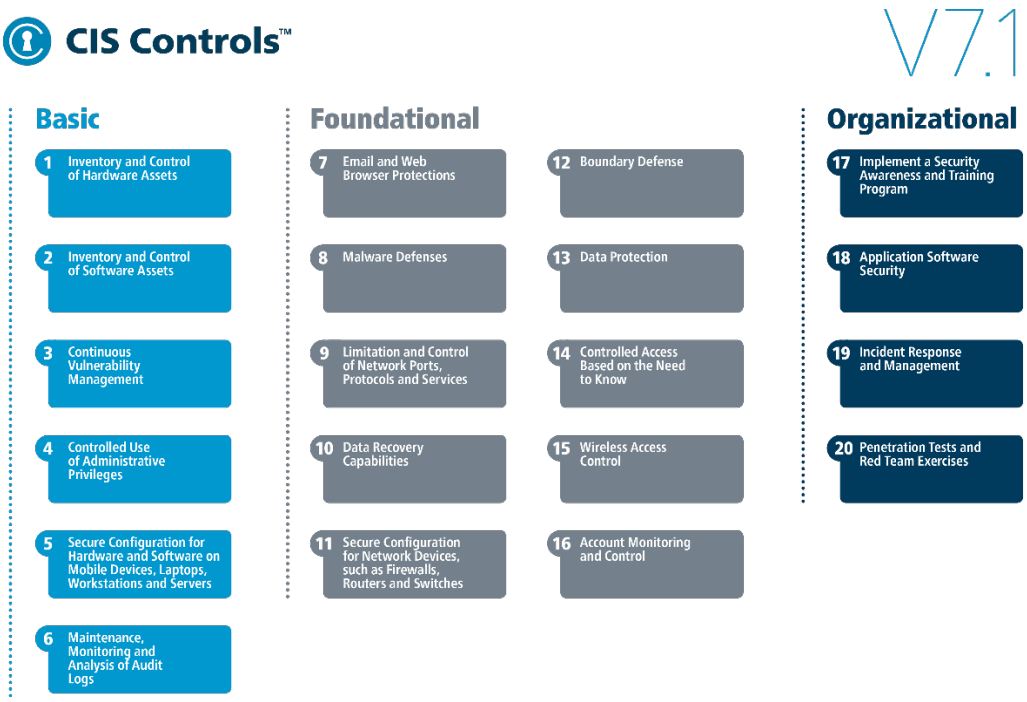
The CIS Controls™ are a great starting point for any organization. They provide actionable items and allow positive results to be realized upon implementation of these control measures. It has been said that by implementing the CIS Controls™, organizations can increase their cybersecurity security posture by over 90 per cent. This “living” PSA Cybersecurity Committee whitepaper demonstrates some of the ways that you could implement some of the top Center for Internet Security Controls, and it is the goal of the committee to add to this paper every year.

The Framework for the implementation of these controls defines activities that can be performed to achieve desired cybersecurity results. In addition, the framework provides references and examples to provide the guidance necessary to successfully achieve the Cyber Security goals of the organization.

What it 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. The CIS Controls are developed by a consensus-based community of cybersecurity experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. Within each of the 20 CIS Controls is a set of Sub-Controls focused on specific asset types and security functions. There is a total of 171 Sub-Controls. The CIS Controls fall into three categories:

- Basic - Contains controls that help an organization assess its current security and take simple steps to improve it.
- Foundational - Contains more advanced guidance to improve an organization's security.
- Organizational - Contains controls that make changes to an organization's policies to improve and maintain their cybersecurity.



While these three categories provide a rough ordering of the best risk mitigations as an organization matures, resource limitations may make some of Sub-Controls in the Basic category infeasible for an organization. To address this CIS introduced the concept of Implementation Groups (IGs) into v7.1, which was released on April 4, 2019. IGs provide a simple and accessible way for an organization to prioritize implementation of the Sub-Controls for specific types of risk profiles and available resources. CIS also refers to IG1 as basic cyber hygiene.

There are three IGs, each building upon the previous one, that identify which Sub-Controls are reasonable for an organization to implement if, for instance, they hold critical or sensitive data. By following the IG methodology guide and IG classifications, an organization can narrow down the CIS Sub-Controls that are most prudent to their cyber defenses. This ensures that the CIS Controls are viable for organizations of all sizes and implemented in the most effective manner possible.

Why does it matter

The CIS Controls are an effective tool for prioritizing risk-based cybersecurity. They provide effective approaches to mitigating risk, in contrast to tools like the NIST Cybersecurity Framework V1.1 (CSF), which focuses on assessing an organization's risk posture without directly providing mitigations for those risks. The Controls are aligned to NIST (see the NIST CSF to CIS Controls mapping) and several other common cybersecurity frameworks to help organizations document their compliance with whichever larger framework they have adopted.

TABLE OF CONTENTS

CIS #1: Inventory and Control of Hardware Assets

MAPPING THE CIS V7.1 Control 1 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets** ***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***			
1	1.1	Devices	Identify	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

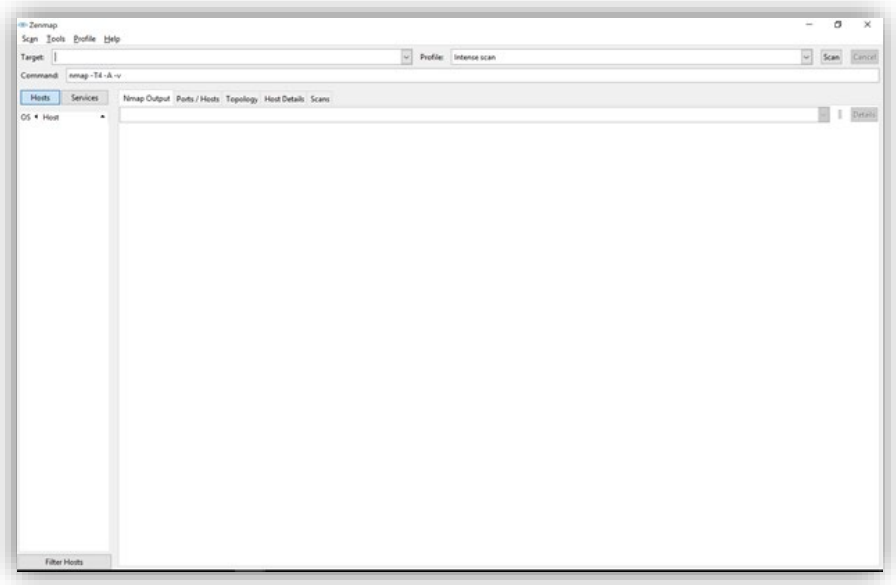
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #1 sub control 1 as follows:

- CSF Function: Identify
- CSF Category: Asset Management
- CSF Category Identifier: ID.AM -1
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 1 – Basic

GAP OR RISK ADDRESSED

The CSF ID.AM functional categories referenced above are defensive in nature. They are undertaken to establish a baseline of network assets which is necessary to detect if new (unauthorized) equipment is introduced to the network. The CSF PR.DS functional category referenced above is defensive in nature. It is undertaken to ensure that data contained on network assets is properly managed when assets (workstation, servers, storage devices, etc.) are moved to other network locations, or removed from the network for storage or destruction.

TOOLS TRIED/USED



To satisfy CIS #1.1, this example used a free program called Nmap. Nmap is a port scanning Linux software tool that also has a popular Windows-based variant called Zenmap. There are online versions of the Nmap tool available for use as a subscription service.

PROS AND CONS

Nmap is very useful for network reconnaissance. It is best known for the following features:

- Scan a range of IPs
- Detects Operating System and Active Services
- Versatile for TCP and UDP scanning
- Stealthy options available to bypass firewall or Intrusion Detections Systems
- Perform fast DNS lookup

Some difficulties are reported, and they could affect your CIS #1.1 efforts, so take notice of the first two:

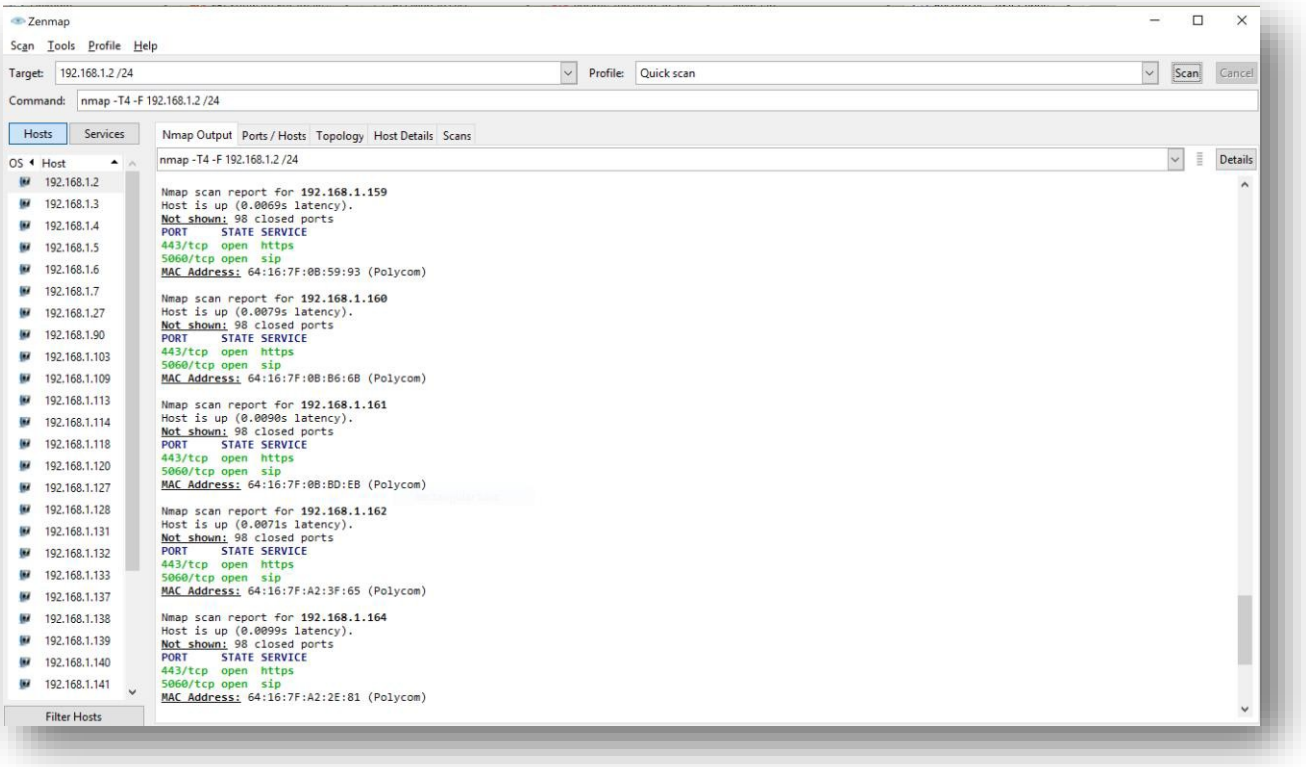
- Weak devices can be knocked offline by network scans
- Network scans create a lot of network traffic
- Customizing Nmap is difficult because it is written in LUA
- Scanning through proxies can be difficult, and proxy support is poor.

ANTICIPATED OUTPUT

Your output will depend on the type of scan you perform. You could scan a single IP address or hostname. You could also scan a range of addresses e.g., 10.10.1.1-50. For the purposes of CIS #1.1, I'm scanning an entire subnet, e.g., 10.10.0.0/24. You can also submit .csv lists of targets for scanning, and you must submit separate lists to scan IPv4 and IPv6 targets in bulk, a requirement of the CIS #1.1 control. 254 IP addresses are the max you can scan in a single profile.

ACTUAL OUTPUT

Here's a glimpse of the output, this becomes the baseline for our network assets:



AUTOMATION STEPS

There are many tools for automating NMAP scans, a good online example can be found at hackertarget.com, or simply search “Nmap automation.”

MONITORING STEPS

NMAP is a point in time scanner. You can choose to schedule automated scans, and receive reports comparing your most recent scans. You could opt receive monitoring reports via email with the same periodicity as the scans, daily for example. You could also opt to only receive a report if something has

changed between the most recent scans. The report would show you if different hosts responded as well as their port and service results.

REPORTING STEPS

You will want to note any new devices if you are doing automated scans. Here is an example of the executive summary output from an online NMAP automation tool

No Change	This indicates the previous two scans are identical.
Changed	This indicates there is a difference in results of the previous two scans.
No Data	There is not enough data to determine the status (there are not two results available for comparison).
Running	A Nmap scan is currently running, progress will be indicated in the table above.
Queued	The scan is currently queued to run when the next available server is available.
Error	There was a problem running the scan, try again or contact support if this continues

OVERALL PERCEIVED VALUE

NMAP is free, so the investment is really in time spent learning the tool. NMAP is a very basic tool and is used by nearly every network researcher for baseline reconnaissance, and more.

TIME SPENT

In a few days you can become very acquainted with the NMPA tool and its features. Additional tools that work with NMAP may be difficult to configure for many users, but to do baseline asset scans of your network could be a quite simple learning curve for many.

RETURN ON INVESTMENT

NMAP is excellent for a variety of tasks, and to satisfy the initial network asset inventory, there's not a simpler way to get started.

CIS #1.2: Audit your Network with Passive Scanning

MAPPING THE CIS V7.1 Control 1 Sub-Control 2 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***		
1	1.2	Devices	Identify	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

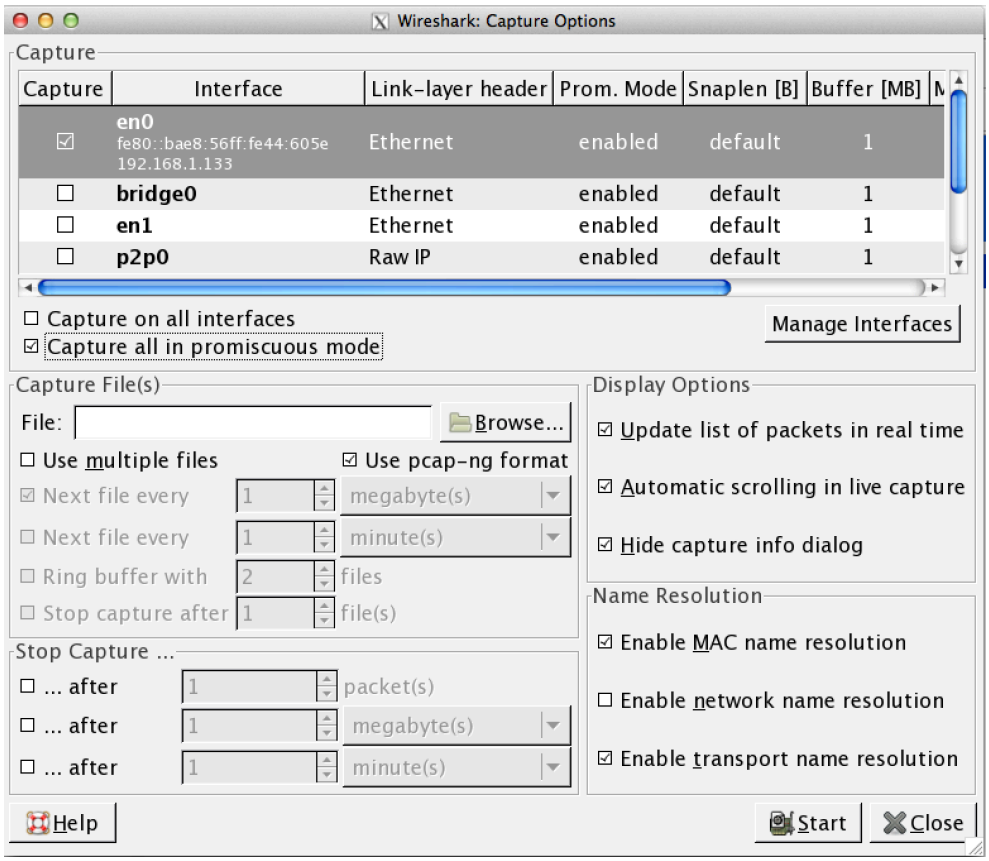
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #1 Sub-Control 2 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM
  - CSF ControlDE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 1 - Basic

Passive scanning (packet sniffing) allows for the detection of running services on a network without broadcasting packets onto the network, as is discussed with active scanning in CIS 1.1. Many types of equipment (IP Cameras, SCADA Controllers, Audio Controllers, etc.) are susceptible to unstable or unpredictable functionality when they are scanned with active scanning tools, so passive scanning on a production network may be your best available option.
Packet sniffing can reveal operating system information, network information, and protocol information running on known and unknown ports. There are a few with passive scanning that should be mentioned:

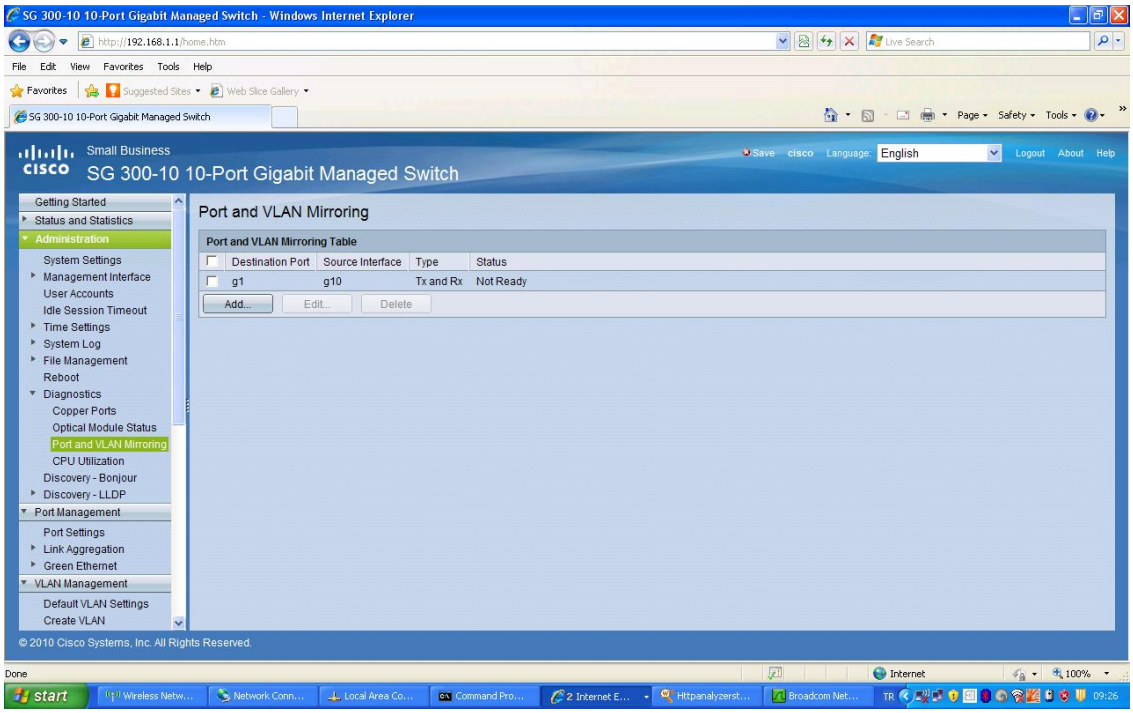
1. Packet sniffing is that it will only detect equipment that is actively sending or receiving packets on the network.
2. The extent of the detected packets depends on where the packet sniffing takes place on the network.
3. Malformed application data packets could be reported erroneously or ignored based on the type of packet sniffer used.

A packet sniffing tool can be attached to a network switch, but with managed switches, the sniffer will only record traffic between the host machine and the network. Network traffic packets on other switch ports will not be seen. Wireshark (shown below) is a popular, free packet sniffing tool that you can learn to use online.



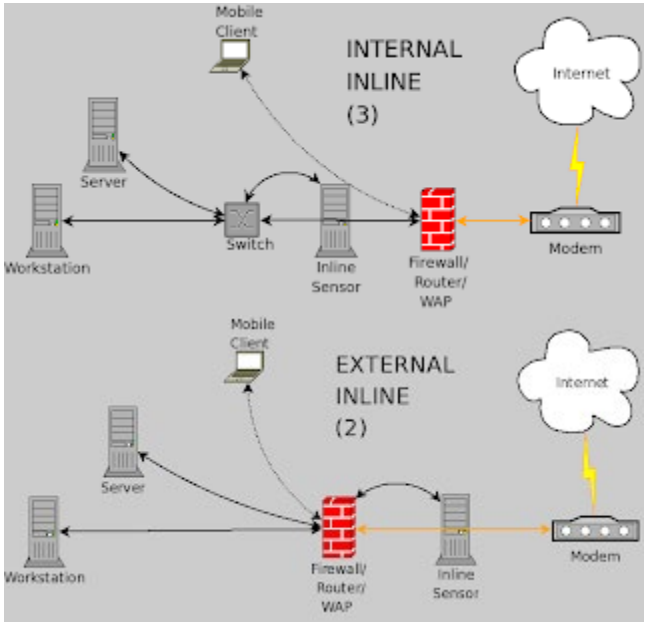
Many switches and routers allow for “port mirroring.” Port mirroring allows all traffic on a particular switch to be sent across the mirrored port. This may be useful depending on the topology you are scanning however, note that on a network with multiple VLAN’s (Virtual Local Area Networks), network packets from different VLAN’s will not be exposed on the mirrored port.

The port mirroring settings example for a Cisco SG 300 switch are shown below:

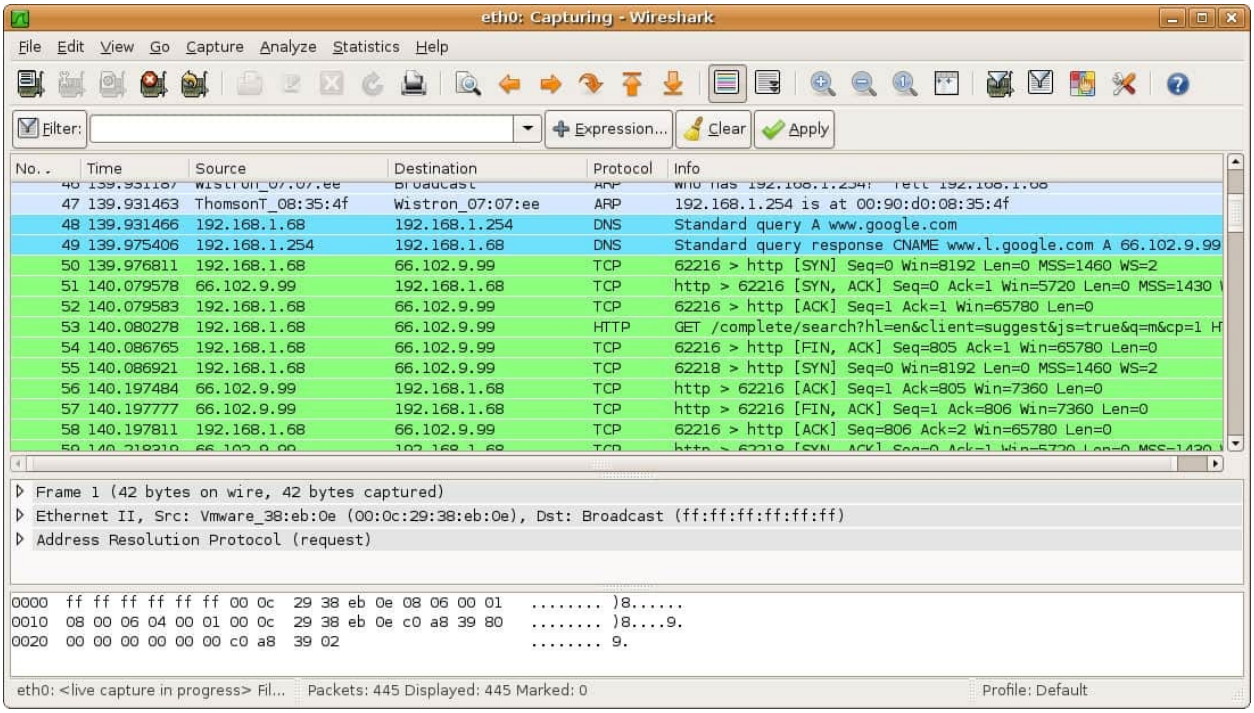


Another tactic is to insert the sniffer between the network switch layer and the network router, if possible. Also, many routers allow for a “promiscuous mode” configuration. In promiscuous mode, the router will capture the packets and record them in a log file that can be parsed to review the network information. Each router has a specific way of performing this task, but it may be the simplest way for you to passively scan a production network.

The following diagrams depict internal and external packet sniffing topology configurations.



Packet sniffing tools also do the data “parsing.” Parsing is simply analyzing the packets and presenting them into a form that is more easily consumed by the human brain.
Below is an example of a Wireshark tool data capture



Note there are 4 different protocols, ARP, DNS, TCP, and HTTP captured in this short session along with other host and target Machine Address Code (MAC), and Internet Protocol (IP) address information. There are a variety of free tools available to help you get familiar with passive scanning. Passive scanning can be used for vulnerability detection as well as auditing of systems. Here is a list of some of the more frequently used network scanning tools:

Network tools, including whois, ping, traceroute, NsLookup:
– https://www.robtex.com/
– https://whois.domaintools.com/
– https://mxtoolbox.com/
– https://centralops.net/co/
– https://ping.eu/

Scanning for DNS:
– http://www.dnsinspect.com/
– http://dnssec-debugger.verisignlabs.com/

Scanning for configuration and encryption:
– https://www.ssllabs.com/ssltest/
– mail server encryption: https://ssl-tools.net/mailservers
– configuration with PCI DSS, NIST and HIPAA guidelines and requirements:
https://www.htbridge.com/ssl/
– Dutch standards: https://internet.nl/

– securityheaders: https://securityheaders.io/
– HSTS: https://hstspreload.org/
– DMARC: https://dmarcian.com/dmarc-inspector/
– DOMXSS: http://www.domxssscanner.com/
– https://toolbar.netcraft.com/site_report
– https://observatory.mozilla.org/
– https://tls.imirhil.fr/

Scanning for SSL certificate:
– https://www.sslshopper.com/ssl-checker.html
– https://www.digicert.com/help/
– https://www.thesslstore.com/ssltools/ssl-checker.php
– https://cryptoreport.websecurity.symantec.com/checker/
– https://www.wormly.com/test_ssl
– https://sslanalyzer.comodoca.com/
– https://crt.sh/
– https://www.sslchecker.com/sslchecker

Scan for IPv6:
– https://ip6.nl/

Scanning your own client:
– for encryption: https://www.howsmyssl.com/
– for encryption: https://badssl.com/
– IPv6: http://test-ipv6.com/

Happy Scanning!

CIS #1.3: Use DHCP Logging to update asset inventory

MAPPING THE CIS V7.1 Control 1 Sub-Control 3 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***		
1	1.3	Devices	Identify	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #1 Sub-Control 3 as follows:

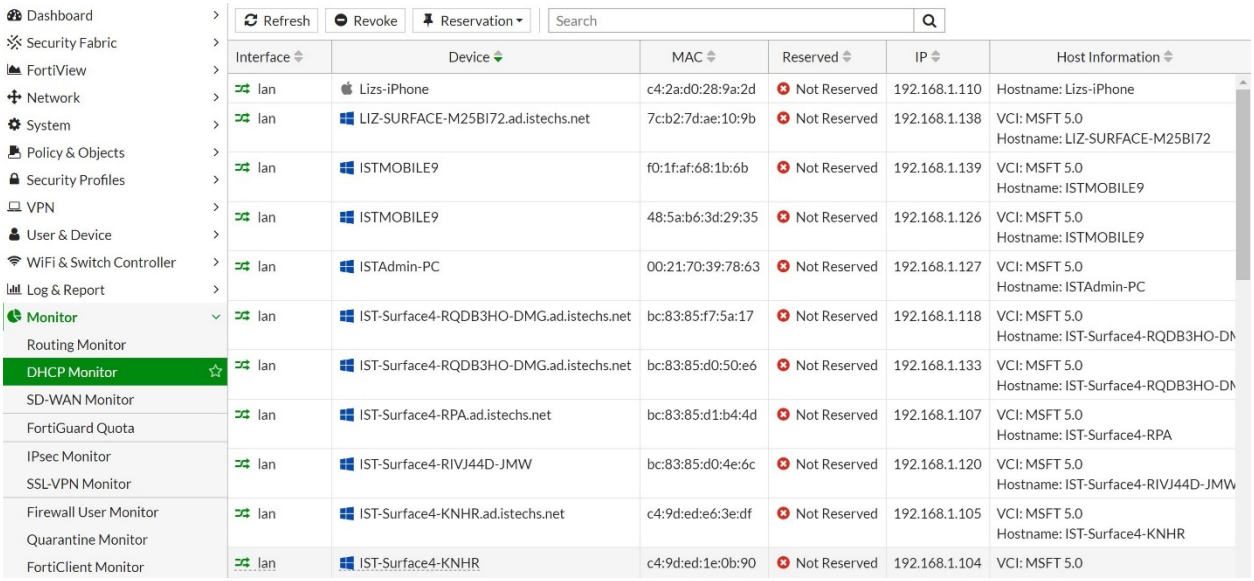
- CSF Function: Identify
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM
    - CSF ControlDE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 1 - Basic

The Dynamic Host Control Protocol (DHCP) is a service that automatically distributes network IP addresses, subnet masks, firewall gateway, and Domain Name Service server information to computers and devices that attempt to connect to a network.
There are 4 steps to the DHCP process.

1. Discover. The client, which does not yet have an IP address, broadcasts a series of DHCP Discover packets in order to locate DHCP servers.
2. Offer. Each DHCP server will respond with an IP address for the client to use. Note, for normal DHCP at Stanford, where the user gets the same address each time, both DHCP servers will reply with the same address. Note that clients do not send out Discovers (and no Offers are returned) when renewing a DHCP address.
3. Request. The client requests the use of one of the addresses provided. Note that, in the case of renewals, the client will contact the DHCP server who provided the address directly.
4. ACK/NAK. The server acknowledges (ACK) or denies (NAK) the use of the address requested by the user.

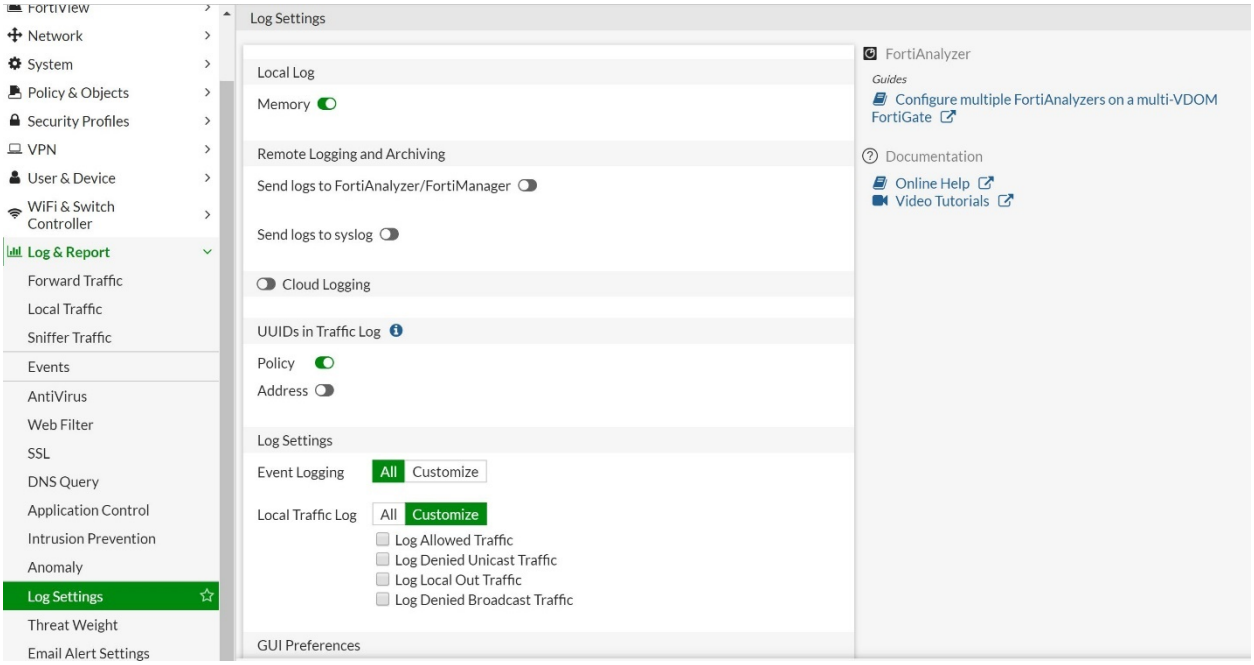
DHCP log files provide a useful inventory of devices that have successfully connected, and unsuccessfully attempted to connect, to a network. The DHCP log file report can be viewed dynamically and/or reported upon over a given time period.

Here is an example of a live DHCP monitoring report:



Your router will have configuration settings that define the length of time your DHCP log files reports will cover, where they will be viewed, and if they are integrated into a Security Event and Information Management (SEIM) system.

Here is an example of a log file(s) configuration screen:



Your DHCP log file report can also be searched. Here is an example output of a media access control address (MAC address) search. This could be useful for seeing the last time a device connected to your network:

Searching for hardware address 00:0d:93:b1:9e:d6

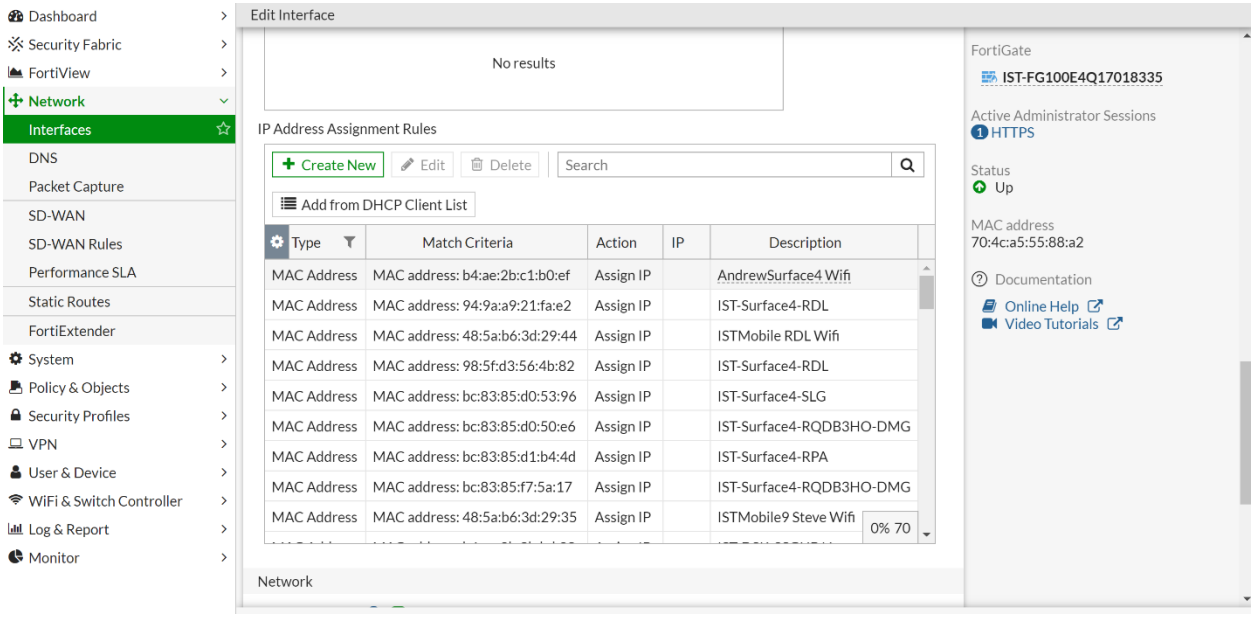
last request	: 2006-11-06 11:40:06
type	: dhcp
gateway	: direct
status	: found
ip	: 171.64.20.120

It is important to note that each DHCP message is reported by message type, then chronologically. The following example report shows a successful DHCP sequence of events:

server	count	most recent		first		IP address
DISCOVER:	1	14	10/13/06 11:48:26	05/26/05	09:58:07	171.64.20.1
	2	14	11:48:26		09:58:07	171.64.20.1
OFFER:	1	1	10/13/06 11:48:26	10/13/06	11:48:26	171.64.20.120
	2	1	11:48:26		11:48:26	171.64.20.120
REQUEST:	1	110	11/06/06 11:40:06	05/19/06	15:05:40	171.64.20.120
	2	82	11/02/06 11:40:24		15:05:40	171.64.20.120
	1	13	05/19/06 15:05:39	02/07/06	18:27:27	171.64.171.85
	2	126	15:05:39	12/16/05	11:06:19	171.64.171.85
	1	68	12/16/05 10:41:09	05/26/05	09:58:08	171.64.20.54
	2	136	10:41:09		09:58:08	171.64.20.54
ACK:	1	110	11/06/06 11:40:06	05/19/06	15:05:40	171.64.20.120
	2	82	11/02/06 11:40:24		15:05:40	171.64.20.120
	1	12	05/17/06 15:47:50	02/07/06	18:27:27	171.64.171.85
	2	124	15:47:50	12/16/05	11:06:19	171.64.171.85
	1	67	12/12/05 14:44:25	05/26/05	09:58:08	171.64.20.54
	2	135	11/30/05 14:45:18		09:58:08	171.64.20.54
RELEASE:	1	1	10/13/06 11:48:17	10/13/06	11:48:17	171.64.20.120

DHCP Log files offer a good check and balance for network connected assets on systems that do not have other authentication methods e.g., MAC filtering or 802.1x etc.

Below is an example of a MAC addressing assignment list. MAC filtering ensures that only authorized devices can connect to your DHCP network, however, MAC spoofing cyber attacks are still possible, so this is not an invulnerable network authentication method.



The time spent perusing DHCP log files can reveal authorized and/or unauthorized connected network devices that an administrator may not have been aware of previously.

CIS #1.4: Maintain detailed asset inventory

MAPPING THE CIS V7.1 Control 1 Sub-Control 4 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***		
1	1.4	Devices	Identify	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.	ID.AM-1	Physical devices and systems within the organization are inventoried
						PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition

The NIST Cyber Security Framework Version 1.1 (CSF) has 2 Mappings for CIS #1 Sub-Control 4 as follows:

- CSF Function: Identify
- CSF Category: Asset Management
- CSF Category Identifier: ID.AM-1
    - CSF Control: Physical devices and systems within the organization are inventoried
- Category: 1 - Basic

- CSF Function: Protect
- CSF Category: Data Security
- CSF Category Identifier: PR.DS-1
    - CSF Control: Assets are formally managed throughout removal, transfers, and disposition
- Category: 1 - Basic

Whether exported from your firewall logs into a SEIM tool, entered manually into a database or spreadsheet, or gathered via another network monitoring tool, it is imperative that you maintain an accurate working inventory of your network assets.
Assets include Firewalls, Network Monitoring Equipment, Wireless Access Points, Switches, Servers, Workstations, Mobile Devices, Printers, Storage, and all other hardwired or wireless network devices.
Below is an example of the information that you would want to collect from your network devices. Note that knowing the last time the device connected to the network "Last Discovery," may be an important indicator of device health.

Customer Name	Site	Device Class	Device Name
Integrated Security Technologies	No Site	Switch/Router	IST-FG100E4Q17018335.ad.istechs.net
Integrated Security Technologies	No Site	Windows Laptop	AndrewSurface4

Network Address	Make / Model	Serial Number	CPU (GHz)	CPU Description	RAM (MB)	Total Disk (GB)	OS and Service Pack	OS Installation	Last Logged in User	Warranty Expiry	Last Discovery
192.168.1.2	Fortinet / FGT_100E	FG100E4Q17018335				0	Other Operating System	Mar 07, 2018			May 29, 2018
192.168.1.48	Microsoft Corporation / Surface Pro 4	015147354053	2.5	Intel(R) Core(TM) i5-6300U @ 2.40GHz	4096	119	10 Pro	Jul 04, 2019	ISTECHS\andrew		Dec 20, 2019

CIS #1.5: Maintain Asset inventory information

MAPPING THE CIS V7.1 Control 1 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***		
1	1.5	Devices	Identify	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.	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #1 Sub-Control 5 as follows:

- CSF Function: Protect
- CSF Category: Data Security
- CSF Category Identifier: PR.DS-3
    - CSF Control: Assets are formally managed throughout removal, transfers, and disposition
- Category: 1 - Basic

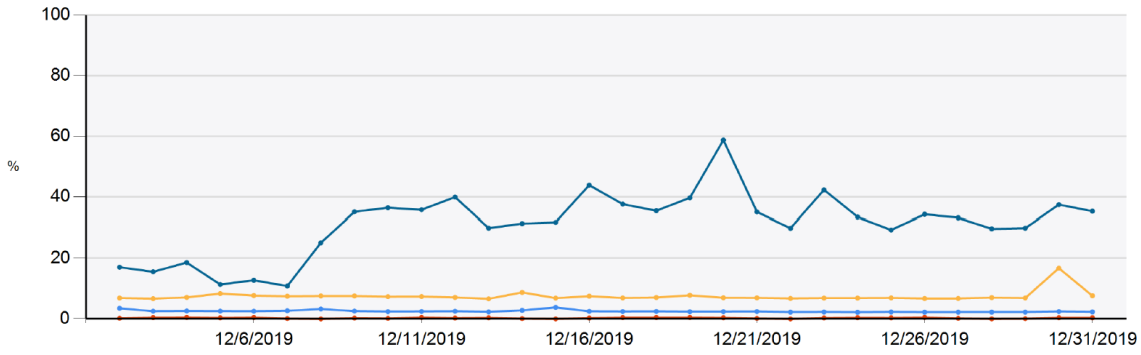
Once you've got a firm handle on your assets, and defined a way to review the asset inventory on a periodic basis that meets with your organizations risk appetite, you'll want to define some information parameters about each asset that is important for your organizations operational cybersecurity assurance.
Below is an example of a device software update information inventory for a Microsoft Surface laptop:

#	Device Name / Patch Name	Device Class	Product	Classification	Published Date	Approval Status	Installation Status
	IST-Surface4-RPA	Laptop - Windows					
1	2020-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for x64 (KB4532938)		Windows 10, version 1903 and later	Security Updates	2020-Jan-14	Approved for Install on 2020-Jan-14	Not Installed since 2020-Jan-14
2	2020-01 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4528760)			Security Updates	2020-Jan-14	Approved for Install on 2020-Jan-14	Not Installed since 2020-Jan-14
3	Windows Malicious Software Removal Tool x64 - January 2020 (KB890830)		Windows 10 Windows Server 2016 Windows Server 2012 Windows 8.1 Windows Server 2012 R2	Update Rollups	2020-Jan-14	Approved for Install on 2020-Jan-14	Not Installed since 2020-Jan-14

The following example of server CPU utilization is valuable for understanding the load performance of servers and firewall equipment:

CPU Usage

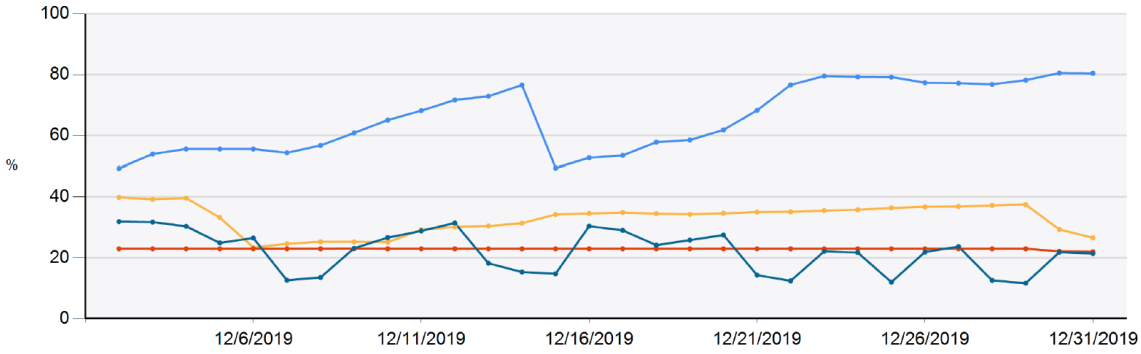
During business operating hours, if the average CPU utilization is below 30%, the server is operating within acceptable parameters and the server is well matched to the tasks it is assigned. An average CPU utilization of between 30% and 70% indicates that the machine is quite busy and performance may be impacted during peak operating times. An average CPU utilization of over 70% indicates that the machine's resources are overtaxed and require an upgrade or reassignment of tasks.



The following examples of server memory usage are valuable for understanding the physical and virtual memory load utilization of servers and firewall equipment.

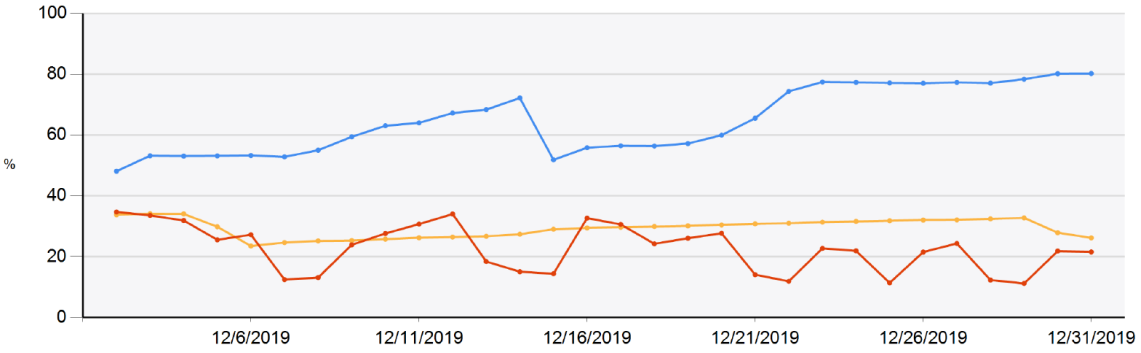
Physical Memory Usage

High physical memory usage is not necessarily an indicator of poor performance. Some applications, such as Microsoft Exchange Server and Microsoft SQL Server, will use as much physical memory as is available. When viewing memory utilization on these devices, virtual memory utilization is more indicative of issues. Overall, excessively high utilization of both physical & virtual memory indicates a need for memory to be added to the system.

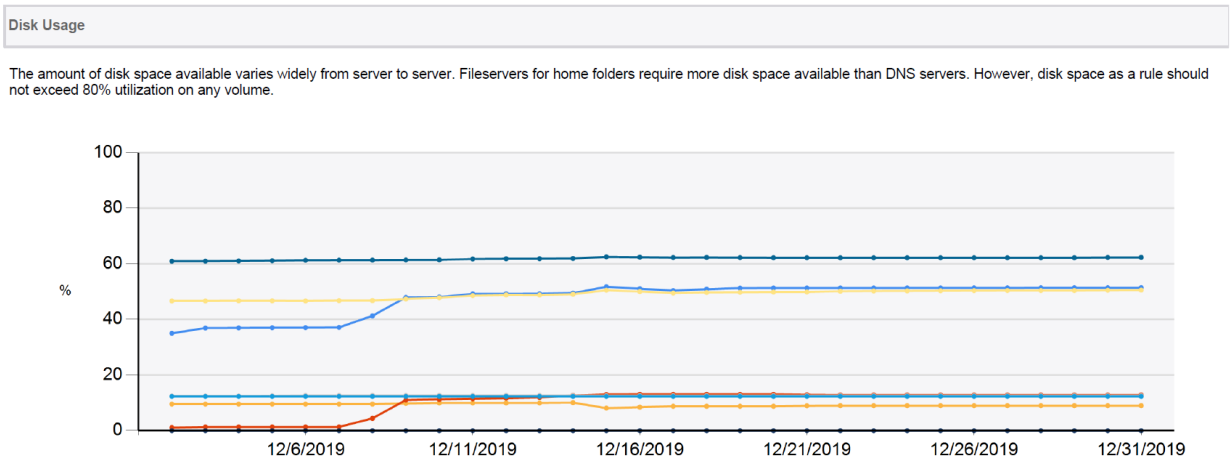


Virtual Memory Usage

High virtual memory utilization indicates that the system is busy paging to swap and it can reach the state in which it is not able to keep up with demand. Excessively high utilization of virtual memory indicates a need for memory upgrade.



The following example of Disc Usage is valuable for understanding the space available on servers or a firewall. Note that log file accumulation can fill up servers rapidly so the monitoring of disc space and perhaps alerting on low server disc space should be considered.



CIS #1.6: Address unauthorized assets

MAPPING THE CIS V7.1 Control 1 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1				**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***		
1	1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #1 Sub-Control 6 as follows:

- CSF Function: Respond
- CSF Category: Data Protect
- CSF Category Identifier: PR.DS-3
    - CSF Control: Assets are formally managed throughout removal, transfers, and disposition
- Category: 1 - Basic

Upon detection of unauthorized network assets (found via active scanning [CIS 1.1], Passive Scanning [CIS 1.2], DHCP Log file review [CIS 1.3], or noted on an asset inventory discrepancy [CIS 1.4]), the asset should be removed from the network and quarantined for analysis. Additional analysis of potential network impact(s) from the device may also require investigation in accordance with corporate information security policies and procedures.

CIS #4: Controlled Use of Administrative Privileges

Cyber Security Control #4 prescribes for the Continuous Vulnerability Assessment & Remediation requiring continuous monitoring of all active and passive network devices and remediation of inventoried network devices. CIS #4 is composed of 8 sub controls that address the provision of guidelines around performing vulnerability scans, monitoring and correlating logs, staying on top of new and emerging vulnerabilities and exposures, remediation, and establishing a process to assign risk ratings to vulnerabilities. Each of these sub controls must be implemented to fully realize the cyber security vulnerability mitigation intended by CIS #4. This paper will walk through the deployment of CIS# 4, sub control 4.1

Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

If you don't know what vulnerabilities exist on your network, you have no way to identify and mitigate potential threats and vulnerabilities that exist on your network. CIS #4 Sub control 4.1 requires an automated vulnerability scanning tool that scans against all systems on the network on a weekly or more frequent basis. The scanning tool will provide prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project). A consistent and scheduled scanning program must be deployed to satisfy CIS #4.1 sub control.

WHAT IS SCAP EXACTLY?

First, it is a protocol. SCAP is a suite of four open specifications that standardize the format and nomenclature by which software communicates information about publicly known software flaws and security configurations annotated with common identifiers and embedded in XML. Essentially this is a

means of establishing some automated "on/off" switches when checking to see if a server or desktop is compliant with the standard in question. This is practical because the output is a standardized, non-proprietary format that can be used across different organizations. Each specification is known as an SCAP component. (NIST also gives more information on SCAP v1.0 components.)

GAP OR RISK ADDRESSED

The CSF ID.RA functional categories referenced above critical to develop a baseline of risk and

vulnerabilities. This function enables the organization to understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. The CSF PR.ID functional category referenced above can be in response to the risk assessment findings. Based on those findings, security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. The CFS DE.CM functional categories referenced above tests and validates the security policies developed in the PR.ID function. This function addresses the monitoring of the information system and assets at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. The CFS RS.MI functional categories referenced above acts on security events that occur. This function addresses the activities that are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

SCANNING TOOLS

To satisfy CIS #4.1, a Security Content Automation Protocol Validated (SCAP) scanning tool should be used. NIST provides a list of products and modules that have been validated by NIST as conforming to the SCAP and its component standards. SCAP validated products and modules have completed formal testing at an NVLAP accredited laboratory and meet all requirements as defined in NIST IR 7511. There are many NIST validated tools available. The following 10 tools have been most recently validated by NIST: (See below for the link to the complete list)

1. Rapid1 - 3/29/2017
2. RedHat- 2/22/2017
3. Threat Guard- 12/13/2016
4. Spawar- 8/26/2016
5. IBM- 6/9/2016
6. Microsoft- 9/28/2015
7. Tenable- 8/25/2015
8. Qualys- 2/26/2015
9. Saint- 1/27/2015
10. BMC- 12/30/2014

There are a couple free scanners available like from Qualys however they are limited in their functionality and are usually aimed at encouraging a purchase of their complete product.

PROS AND CONS

It is always a good idea to use tools that meet industry standards and have validation from organizations such as NIST. The NIST validated tools provide the modules needed to implement and manage to CIS #4. Some of the Pros about these tools are:

- Prioritize your vulnerabilities ensuring you always fix the most dangerous issues first
- Automate the entire vulnerability management process from scanning to report distribution
- Status dashboards identifying the program's performance

Some of the Cons about these tools are:

- Can be expensive especially for multi-site/customer use
- Network scans create a lot of network traffic and can be difficult to deploy on a client's network
- In some cases, it may require a special set of skills to effectively implement these tools especially around complex networks

ANTICIPATED OUTPUT

- Automatic verification of the installation of patches
- Check lists and active validation of system security configuration settings
- Examination of systems for signs of compromise
- Report and Views of program performance

SELECTING A SCAP TOOL

Selecting a SCAP tool will require an investigation of the tools on the market, the levels of functionality desired and the investment you are willing to make. The following link has the NIST validated SCAP products listed.

https://nvd.nist.gov/scap/validated-tools

CIS #4.1: Maintain Inventory of Administrative Accounts

MAPPING THE CIS V7.1 Control 4 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges**	***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***		
4	4.1	Users	Detect	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.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 1 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-1
    - CSF Control: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
- Category: 1 - Basic

Use automated tools to inventory all administrative accounts, including domain and local accounts, to

ensure that only authorized individuals have elevated privileges.

Maintaining this list of administrative accounts is crucial to keeping track of the organization's security footprint, as each administrative account needs to be treated as a vulnerable point of ingress, especially if not used properly. Traditionally, this inventory was maintained manually; however, it is not possible to keep up with this list, especially in smaller organizations where duties are shared and not segmented. In any organization, this detection type sub-control will require a bit more resources to implement and may require an investment into an IT management platform such as ManageEngine or SolarWinds. Both software suites offer similar functions, which include centralized auditing on system configurations, including an inventory of Administrative Accounts.

It is recommended that this sub-control is implemented with 4.8 and 4.9, as all three can be implemented within the same software security platform. Some examples are provided in sub-control 4.8 and should be carefully reviewed once the other sub-controls have been implemented.

CIS #4.2: Change Default Passwords

MAPPING THE CIS V7.1 Control 4 Sub-Control 2 TO THE CYBER SECURITY FRAMEWORK

CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
			Controlled Use of Administrative Privileges	***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***		
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 2 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-1
    - CSF Control: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
- Category: 1 - Basic

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

As one of the most common-sense sub-controls, Change Default Passwords can be an excellent segue into other sub-controls. It is an excellent conversation starter, providing a base for deeper thought on the subject of organizational security. The scope of this is *everything from servers to cameras and printers.* They key here is to follow this control completely, ensuring default passwords are replaced with standards on par with *administrative level account standards.*

When reviewing the organization's current compliance with this, a more general understanding of its importance in relation to security is needed. Take the example of a common device such as a printer:

even though the printer may not inherently have control over user accounts, think of its place in

business process, including sensitive information that passes through its memory. Everything from employee data, copies of checks, product pricing, contracts, and other sensitive information passes through it at any given time. There are key feature-sets inherent to the printer's operation that when altered through an administrative login can result in organizational extradition of data to un-approved parties. Some of these features include emailing of scanned documents, saving print jobs in memory, and hosting file shares on the network. All of these functions can be manipulated by a disgruntled person, or an unknown hacker on the inside. The key takeaway here is that simply changing the default password on the printer will help *protect* the organization here.

Take the printer example and apply it to a camera or surveillance system. Think again of the how surveillance is used in business, and at its core, its function is to record/document activities for *legal reasons*. Think of that system with its default password left enabled; in what ways can it be tampered with? To name a few: deletion of video, cameras disabled, sensitive footage leaked, etc.

Continue to follow this logic and you will find similar scenarios can be played over and over again as we move from system to device in an organization's network, taking into account each device/system's place in business process Again, getting back to key takeaway, ***protect the organization through simply changing default passwords!***

CIS #4.3: Ensure the Use of Dedicated Administrative Accounts

MAPPING THE CIS V7.1 Control 4 Sub-Control 3 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges**	***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***		
4	4.3	Users	Protect	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.	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 3 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-4
    - CSF Control: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- Category: 1 - Basic

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.

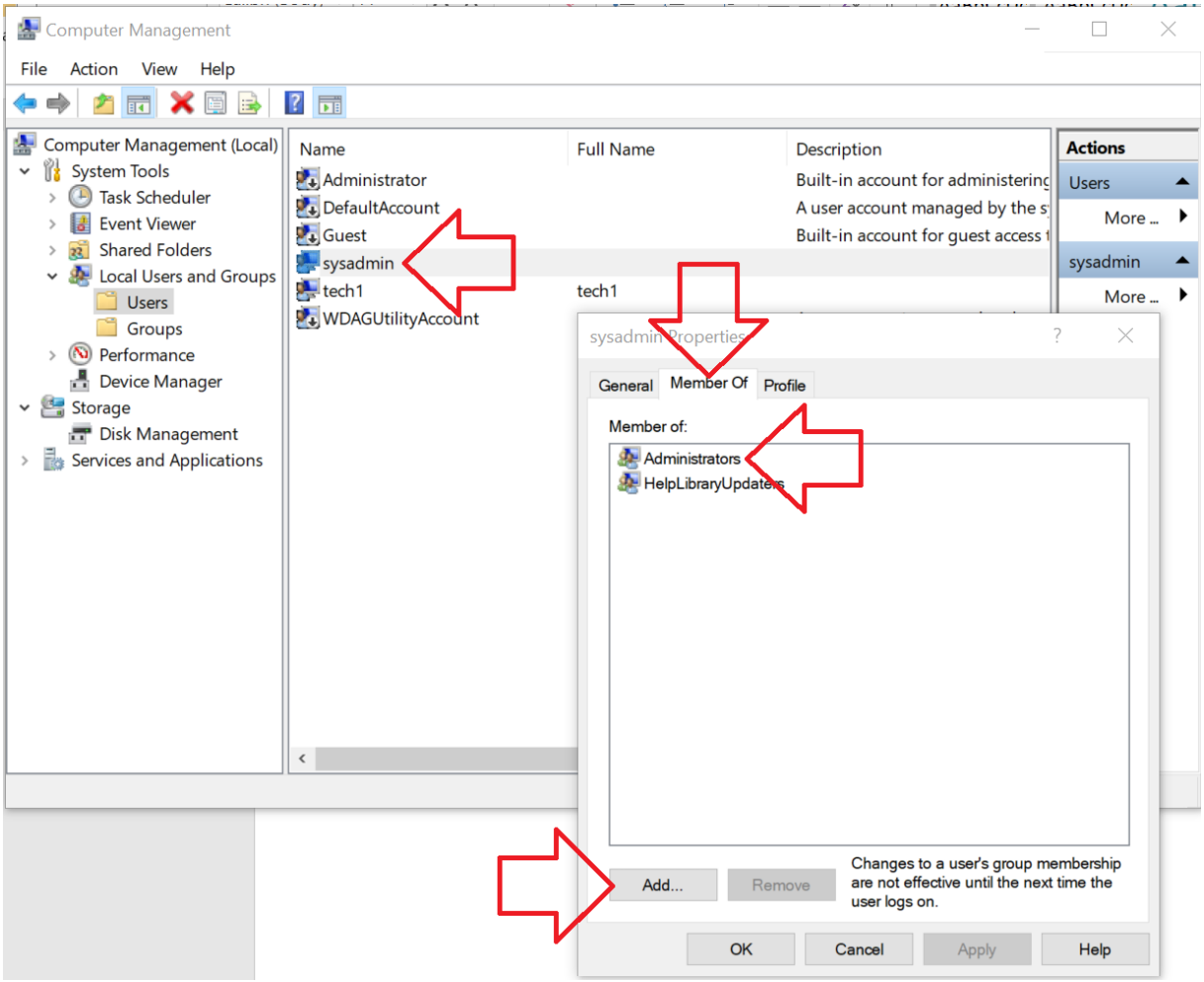
With an expanding landscape of vulnerabilities, coming into contact with a vulnerable system while concurrently using administrative privileges can result in a successful cyber breach, no clicks required. This puts everyone, even the most experienced cyber-aware persons at risk of facilitating a cyber breach. ***The answer to this is simple: your primary account should not have administrative privileges!***

In a domain environment, this is fairly straightforward. By default, when creating users, the administrator role must be added to a user. Domain admins should have a regular user on the same level as the secretary. In the event software needs to be installed or configurations changed, they can key in administrative credentials.

In a non-domain environment, such as in the field in a support scenario, a technician may need immediate access to run an update or elevated privileges to launch a programming tool. In this case, the login they are using for everyday use should not be an administrative account. Rather, as needed, when the dialog comes up asking for administrative permissions, they should key in a *local administrative* account specifically created for local admin tasks.

Have a look at the below screen grab from a Windows 10 computer, specifically in the *Computer Management* window > Local Users and Groups > Users. Out of the accounts listed, there are two accounts "tech1" and "sysadmin" created by whomever set the computer up. Tech1 was created for field work, and sysadmin was created for administrative tasks. Opening the properties dialog of sysadmin and selecting the "Member Of" tab shows this account as part of the "Administrators" group. This is a *local administrator* group, allowing full control over this particular computer, but those permissions are isolated to this computer. **If you were to open the tech1 properties dialog/Member Of, the "Administrators" should not be listed.**

The operator of this computer should only be logging in as tech1, and keying in the "sysadmin" credentials as needed when operating the computer.



In the same manner, purposely using dedicated administrative accounts applies to all systems and users with no exception where-ever possible. Taking this precaution ensures a proactive active to security, minimizing opportunities of attack.

CIS #4.4: Use Unique Passwords

MAPPING THE CIS V7.1 Control 4 Sub-Control 4 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				Controlled Use of Administrative Privileges	*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*		
4	4.4	Users	Protect	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.		

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 4 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier:
  - CSF Control: Use Unique Passwords
- Category: 1 - Basic

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.
The idea of unique passwords needs justification, and is an absolute necessity once understood the **ramifications of not using unique passwords.** Let's start with a password, only known to John Smith, with his username being johnsmith@company.com. John's password is fairly strong, with a very unique combination of characters. He uses it for his company email, and he also uses it for the payroll system, the project management system, as well as some online business websites he has signed up for. Herein lies the issue: ***John has no control over these systems.*** A single breach in one of these systems could result with an exposed password database, resulting in an exposure of all John Smith's company accounts.

John Smith's scenario is not just hypothetical; it happens every day. There are troves of breached password directories available on the internet, organized by systems and accounts for easy reference and simple "hacking". The only answer here is to use a unique password for all accounts, ensuring that when your password is discovered and logged, the fallout is contained to a single system. This approach

fits into a proactive approach to security, ensuring not any one breach results in a breach of multiple systems.

There is a drawback to this method… a unique password does not include variations of the same password. For example, B@s3B&LL and Ba$eB^1L are variations of the same password. Utilizing variations of the same password is not secure, and these variations can be guessed, or brute forced. Therefore, it is recommended to use a password generator to set unique passwords.

An example of two unique passwords from a generator: ***e3qp5K5V@4@a*** *and* ***!HsdN9#$!7K7***

In review of the unique password examples, these cannot be memorized or remembered. *How does one manage all the unique passwords?* The generally accepted password storage method is a ***password manager***. A password manager can be tied to a single individual to start, and scale to manage multiple users and thousands of passwords organization wide.

Password managers simplify management… providing access to a secure application to store all the user's account information for the various systems. Combined with multi-factor authentication, utilizing a password manager makes it simple to save, access, and generate additional passwords as needed***. The key here is to utilize multi-factor authentication in order to access the password manager, ensuring all passwords in the vault are behind an additional layer of security.*** Most password managers come with a browser extension for simple integration into web pages, but more robust managers can also be used and integrated into operating systems and application suites. When selecting a password manager, pay attention to the way the data is stored, ensuring it is a fully encrypted solution and is regularly audited.

Some examples of password managers: - Lastpass - Dashlane - 1Password - Keeper	Some examples of MFA, or Multifactor Authentication: - Yubikey - Google Authenticator - SMS Text (not secure / DO NOT USE) - Apple FaceID / Finger

CIS #4.5: Use Multifactor Authentication for All Administrative Access

MAPPING THE CIS V7.1 Control 4 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges** ***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***			
4	4.5	Users	Protect	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 5 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-7
    - CSF Control: Use Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
- Category: 1 - Basic

Use multi-factor authentication and encrypted channels for all administrative account access.

Protecting administrative access is key to protecting an organization, so putting additional layers of security such as multifactor authentication for all administrative access is a simple proactive step in reducing risk. Furthermore, all communications should be encrypted when accessing the administrative account.

In the previous sub-control regarding unique administrative passwords, multifactor authentication was touched upon, but it was not explained in detail. In summary, multifactor authentication is achieved by using two or more different types of authenticating while logging in. The first means of authentication is usually a secret, or password. The next could be a biometric, a push notification, or even a hardware key. As an example, a Yubikey USB key generates a unique encryption key every time it is plugged into a usb port, acting as a second means of authentication. In an iPhone, a finger or face can be used as a second means of authenticating in a multifactor application.

This is not to be confused with using a biometric in the absence of a password, *which is not multifactor authentication.* In other more traditional means, a text message can be generated with a one-time code. However, text messages should be avoided where-ever possible as they can be read in route to your phone. This is because a SMS text message is not encrypted, so it can be read in transit.
When reviewing authentication options for multifactor authentication, keep in mind most systems do not support all multifactor authentication options. In fact, most systems do not support more than one authentication option, the password. Because of this, a password manager and a unique password will need to be used. Compliance will then be achieved by using multifactor authentication on the password manager, ensuring the unique password is stored inside an encrypted vault, only accessible via multifactor authentication.

The second aspect to this sub-control is the use of encrypted channels. It was mentioned that a SMS text message is not encrypted, so it should not be used. Encryption works by applying a mathematical formula to data before it travels to another location, ensuring the data cannot be read unless the other side has the right “key” to decode the data. This means that when using an administrator account in a web page, the web page should have a “lock” in the corner and have a valid certificate. In a network administration scenario, this means that protocols like Telnet and other non-encrypted configuration channels should be disabled, and SSH, or Secure Shell should be used. This will ensure that administrative credentials will not be sniffed or read during the configuration session with the system.

CIS #4.6: Use Dedicated Workstations for All Administrative Tasks

MAPPING THE CIS V7.1 Control 4 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges** ***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***			
4	4.6	Users	Protect	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.		

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 6 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier:
    - CSF Control: Use Dedicated Workstations for All Administrative Tasks
- Category: 1 - Basic

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.

This sub-control is straightforward and relies on discipline as well as a bit of planning to ensure time and resources are put aside for a proactive, dedicated administrative workstation(s). Traditionally, administrative tasks were completed with administrative accounts, all on shared workstations and infrastructure. However, as breaches spread quickly, a layered approach to securing the organization is needed to ensure minimal damage.

One of the recommended ways to is to segment administrative workstations wherever possible, using them for only administrative tasks and removing internet from them. When a workstation is segmented and internet removed, the attack surface to that workstation is minimized, allowing for more secured management of the organization's infrastructure. Furthermore, as administrative tasks are the only activity on the workstation, it is less likely that the administrator's elevated privileges will be able to be used during everyday business activities like browsing the web and email. One can go as far as ensuring this administrative workstation is off any workplace domain, and all activity is one way.

This workstation(s) is initiating administrative task connections to the primary infrastructure, not the other way around. This ensures and additional layer of segmentation, minimizing risk and adding onto the layered security approach.

CIS #4.7: Limit Access to Script Tools

MAPPING THE CIS V7.1 Control 4 Sub-Control 7 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges**	***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***		
4	4.7	Users	Protect	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.	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

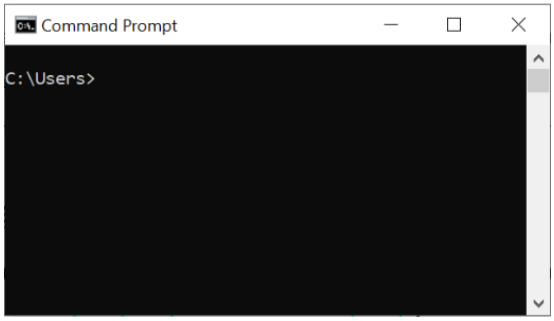
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 7 as follows:

- CSF Function: Protect
- CSF Category: Protective Technology
- CSF Category Identifier: PR.PT-3
    - CSF Control: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
- Category: 1 - Basic

Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.

This *protect* type sub-control seeks to reduce the attack surface found in an organization's fleet of workstations by reducing the number of tools hackers have available. The most common way hackers carry out attacks is via scripting tools; therefore, limiting access to scripting tools is naturally a must. From a non-technical side, scripting can be explained as inputting of pre-defined strings/sentences of text, resulting in a complete group or set of instructions for the target computer system. These strings/sentences are loaded into a CLI, or Command Line Interfaces. In example, one of the oldest scripting CLIs still in use today is CMD command prompt. In its earlier form, it was known as MSDOS, or DOS. At one time, everything that could be done on a computer system could be input into the command prompt as text data. However, CMD is gradually becoming less useful, and has largely been replaced by more advanced CLI interfaces such as PowerShell.

Years ago, much of the text data input into the DOS command line was typed in manually as needed. *This is not scripting.* Scripting was achieved in DOS through typing multiple lines of code inside text files, saving the file, then instructing the computer through an execution command to "run" the contents of the file. The computer would then read the contents of the file, and a group of processes would all be done in sequential order. This saved on time, allowing super users to process and run common tasks more quickly and efficiently.



Over time higher level graphical user interfaces such as Windows replaced CLI for most users, making systems more user friendly and visual. However, complexity increased and system administrators required access to more powerful CLI interfaces to manage ever-increasing system complexity. Scripting tools became more powerful and as a result, more dangerous. As an example, Microsoft's CLI PowerShell can be used to manage an entire organization's server and computer infrastructure through its CLI interface. It is also extensible into the Azure ecosystem (and others), allowing control over entire virtual infrastructures across the globe. An administrator can prepare hundreds of pages of command scripts in a text application like Notepad, then copy and paste them into a PowerShell window, making massive system changes in a matter of minutes. This is where the risk lies… take the same tool and put it into the hands of a hacker. Thousands of scripts are available both pre-written and well documented, able to be customized for both Administrator and hacker alike. Furthermore, PowerShell is not the only CLI that poses a risk. There are many other CLI interfaces that are simple to run and require no installation such as Putty, Python, or Netcat. Therefore, a more robust solution is needed to vet and control these software tools as a matter of necessity.

Now that the risk of script tools is understood, limiting access is a more advanced sub-control for smaller organizations to implement. It requires some understanding, expertise, and ongoing software management on behalf of the technology team. Simply disabling all scripts can potentially break certain programs and updates, so without a security software suite or a dedicated person who can implement this sub-control, there is not a simple catch-app solution. This will also require a professional level version of Microsoft Windows, as the use of AppLocker and domain policy cannot be accessed on a consumer version of Windows such as Windows Home. If your organization is running consumer versions of Windows in a non-domain environment, a large portion of this does not apply as group policy and AppLocker cannot be applied to a non-domain Windows versions. AppLocker and Group policy can be combined to limit scripts, scripting tools, and whitelist software: all of this translates to a lot of time and resources small organizations often lack. Fortunately, there is a simpler recommended solution: ***subscribe to a more robust security suite for your workstations that supports script control and ensure the use of dedicated administrative accounts (reviewed in earlier sub-control). Without limiting administrative access, legitimate scripts can still be run with elevated privileges and security suites can be disabled.***

Some examples of Security Suites with Script Blocking feature-sets:
- Malwarebytes – detects and blocks scrips when programs execute
- Norton Antivirus – detects and removes scripts from emails / attachments
- Avast Antivirus – detects and blocks scrips when programs execute

CIS #4.8: Log and Alert Access to Administrative Changes to Group Membership

MAPPING THE CIS V7.1 Control 4 Sub-Control 8 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges** ***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***			
4	4.8	Users	Detect	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 8 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-7
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 1 - Basic

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

The step of logging and alerting in the event of administrative changes to group membership means that whenever a user gains or is removed from administrative access, an audit trail / log is created, and an alert is generated. This requires a centralized logging service that stores the information for review and is intelligent enough to set up alerts based on specific log content. This service can be part of a SIEM, or security information event management, which is a classification of software for managing an organization's security footprint, or it can be a more advanced logging utility that systematically categorizes events and generates alerts / rules off the data. In either case, this sub-control represents a higher level of security awareness, a solution based *detect* type. The simplest way to implement this is within a SIEM solution, such as SolarWinds. There are many available solutions for these types of logs and alerts.

Some example SIEM Solutions: - SolarWinds Security Event Manager - AlienVault USM (AT&T Cybersecurity) - LogRythm	- ManageEngine SIEM - Splunk - McAfee Enterprise Security Manager" - IBM QRadar

CIS #4.9: Log and Alert on Unsuccessful Administrative Login

MAPPING THE CIS V7.1 Control 4 Sub-Control 9 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4				**Controlled Use of Administrative Privileges** ***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***			
4	4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #4 Sub-Control 9 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-7
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 1 - Basic

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

The step of logging and alerting in the event of unsuccessful logins to and administrative account is to test the previous sub-control of administrative changes to group membership. Please refer to that sub-control regarding SIEM solutions. This sub-control adds in the logging and alerts in the event an administrative login is unsuccessful during the login process. This *detect* type sub-control will allow an organization to quickly identify all failed attempts at administrative access to organizational systems. It does require a SIEM to identify the failed *administrative* attempt at logging in, as it needs to be able to determine group administrative membership or keep track of a list of administrative accounts.

CIS #7: Email and Web Browser Protections

CIS #7 is defined as "*Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.*"

CIS #7.1: Ensure Use of only Fully Supported Browsers and Email Clients

MAPPING THE CIS V7.1 Control 7 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.1	Applications	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 1 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Web Browsers

Web browsers and email are integral parts of conducting business in today's world. It's easy to take for granted that the tools we use every day are safe and secure. Also, many of the applications that have traditionally been installed on our PCs are now being replaced with a web browser. This presents a different set of security vulnerabilities that need to be managed.

If you do a simple search on the internet for common web browsers, you will easily find results for a couple dozen. The top few you have probably heard of and/or use. Beyond those, there are several others that you are likely not familiar with. In general, web browsers are available for download for free.

Here are some of the more common browsers available:

Google Chrome is a popular browser that is free from Google. This browser is typically highly compatible across platforms.

Mozilla Firefox is similar to Chrome; this browser is free and is also highly compatible across platforms.

Microsoft Edge was created in 2015 by Microsoft as the successor to Internet Explorer. Initially it was only available for Windows 10, but now has compatibility across most platforms.

Safari is the native browser for Apple based products. It does not support current Microsoft Windows operating systems.

Internet Explorer – although included with Windows 10, this browser has been replaced by Microsoft Edge.

When considering web browsers for your organization, beware of issues such as compatibility, updates and support, security features and longevity.

It is important to have standards concerning what web browser(s) are acceptable for use within your organization. Not all browsers are equal. Some browsers come built in with your Windows, Apple, or Linux computer, but that doesn't mean that they are the best browser for your business and uses. The browser you select should have strong security features including TLS, popup blockers, malware and phishing protection, warnings before accessing unsecure sites, automatic updates and even sandboxing of sites before going to them.

Once you have selected a preferred browser or browsers for your organization, share that information with your employees. Let them know why the choice was made to standardize on the web browser. This will assist with adoption of the web browser. It will also establish which web browser(s) employees are expected to use and will receive support on. It is also extremely important that updates are done routinely to maintain security. The browser may do automatic updates, and updates may be pushed out from your IT team as well.

Email Clients

Like web browsers, there are several email clients available for download. Typically email clients are determined based on compatibility with the email service provider. Compatibility across platforms and devices also drives standardization of applications.

Here are some of the more common email clients available:

Microsoft Outlook encompasses several legacy platforms from Microsoft including Hotmail, Live, MSN and others. Outlook has been a staple in Windows environments for many years. It is also offered as a free service outside of business as well and is compatible across multiple platforms including Apple and Android.

Google Gmail is available both for business and personal uses. Gmail rivals Outlook for user adoption and is also compatible across multiple platforms including Microsoft, Apple and Android.

Yahoo is also a commonly used service for personal email. It Is compatible across multiple platforms.

Apple Mail is native to Apple products, Mail can also bring in accounts from other services too. The program is not compatible with platforms outside of Apple, but the email account may be used with programs such as Outlook.

Mozilla Thunderbird is lesser known. This mail client is the cousin of Mozilla's Firefox and is independent of some of the other giants. Is compatible across multiple platforms.

Once you have selected your email service provider and the email client(s) for use by your organization, share that information with your employees. Let them know why the choice was made to standardize on the email provider and client. It will establish which email client employees are expected to use and will receive support on. It is also extremely important that updates are done routinely to maintain security. The email client may do automatic updates, and updates may be pushed out from your IT team as well.

Email security focuses on protecting access to the email account and the content in the account. In general, email is not protected during transit unless when using encryption services.

You will need to decide how restrictive your environment will be. Measures can be taken to prevent users from installing new applications without administrative rights. Also, periodic scans of the computers in your organization can also provide information about the internet browsers and email clients that are installed. With either approach, it is very important to ensure that updates are being done regularly and automatically when possible.

CIS #7.2: Disable Unnecessary or Unauthorized Browser or Email Client Plugins

MAPPING THE CIS V7.1 Control 7 Sub-Control 2 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

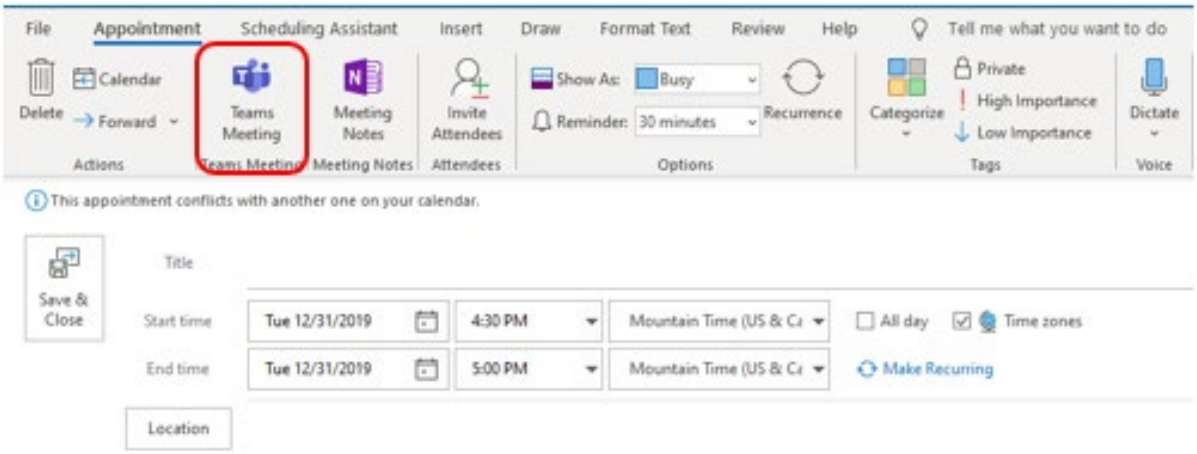
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 2 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

The next step in securing your web browsers and email clients is to control the use of plugins. Plugins can go by several names depending on the application and the technology. They are sometimes called Extensions (Google Chrome) and other times they are referred to as Add-ins (Microsoft Outlook).

"Plugins are software additions that allow for the customization of computer programs, apps, and web browsers; as well as the customization of the content offered by websites." According to lifewire.com.

New plugins often get installed with new applications. They are a tool to allow interoperability between an application and your email client as well as your web browser. For example, I have Microsoft Teams as an Add-in (Plugin) into Microsoft Outlook for scheduling of conference calls and meetings.



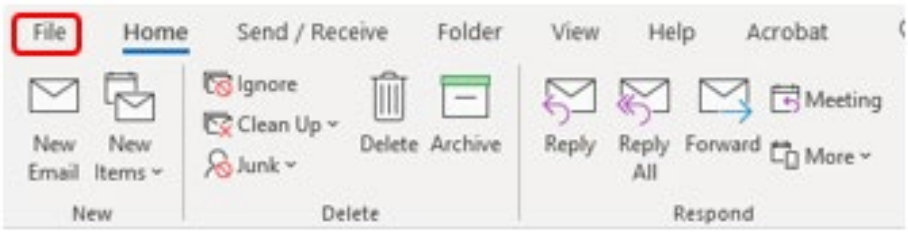
Likewise, I have Zoho Vault as an Extension (Plugin) in Google Chrome for managing my usernames and passwords securely.

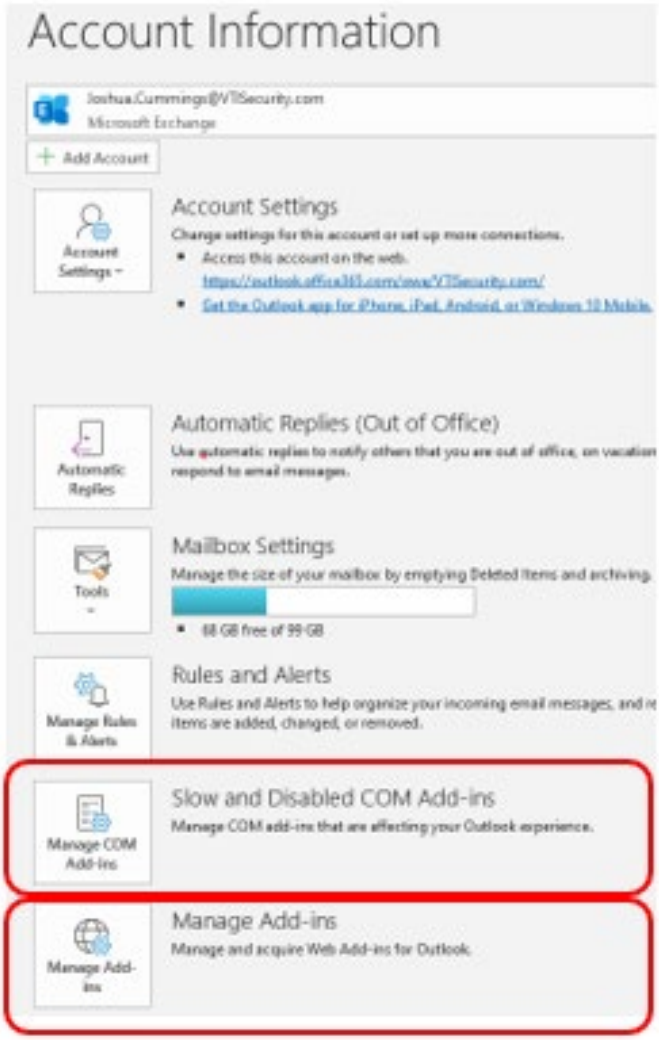
It is important to routinely review the plugins that are installed for both your email client as well as your web browser. Any plugin that is not needed or unauthorized should be uninstalled or at least disabled.

Email Client – Add-in Management

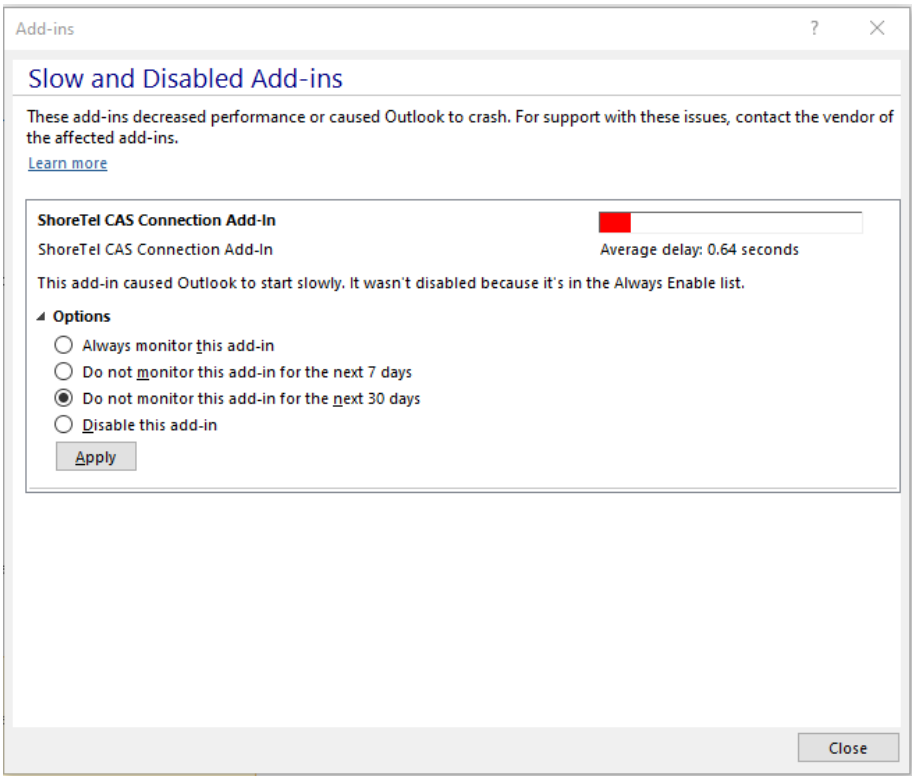
Here is an example of how to review and disable a plugin within Microsoft Outlook.

1. Within the Windows client for Outlook, select file. You will see two sections for Managing COM Add-ins (Non-Web Add-Ins) and for Managing Web Add-Ins. It is important to review both sections.



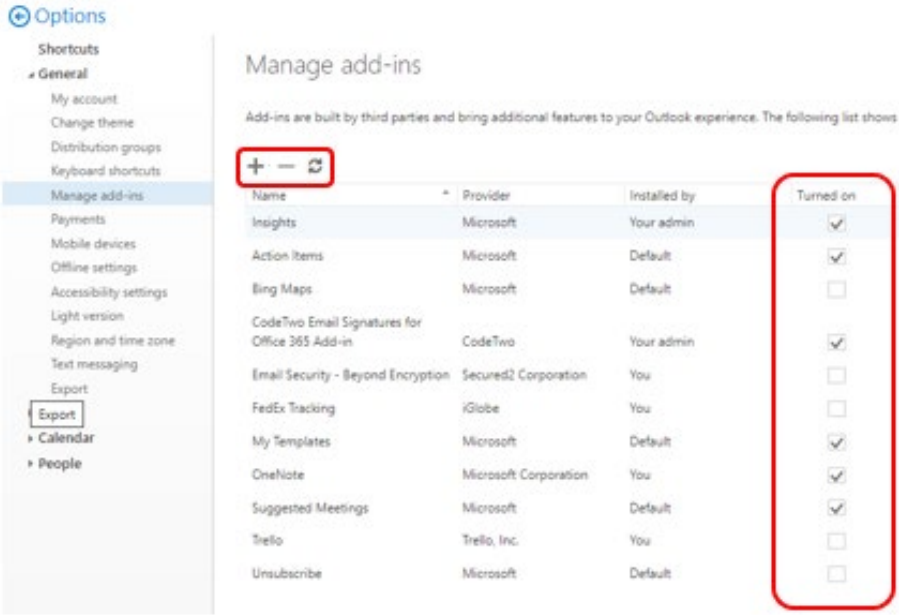


2. Select Manage COM Add-Ins. This will open a new window to review the Add-Ins.



Here you can select to “Disable this add-in” if it is not needed.

3. Likewise, you can select Manage Add-Ins to see your Web Add-Ins
4. This will open a web browser and bring you to your office 365 setting for managing Add-ins.



Here you can see what Add-ins are installed, by whom and whether they are turned on.

5. Uncheck the “Turned On” box to disable the Add-in

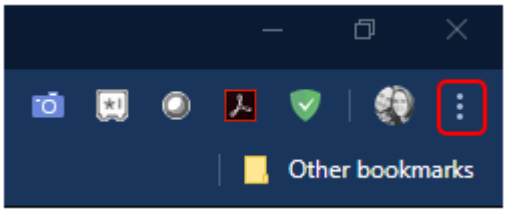
6. Highlight the Add-In and select the "-" to remove it

7. Other email clients have similar management options available

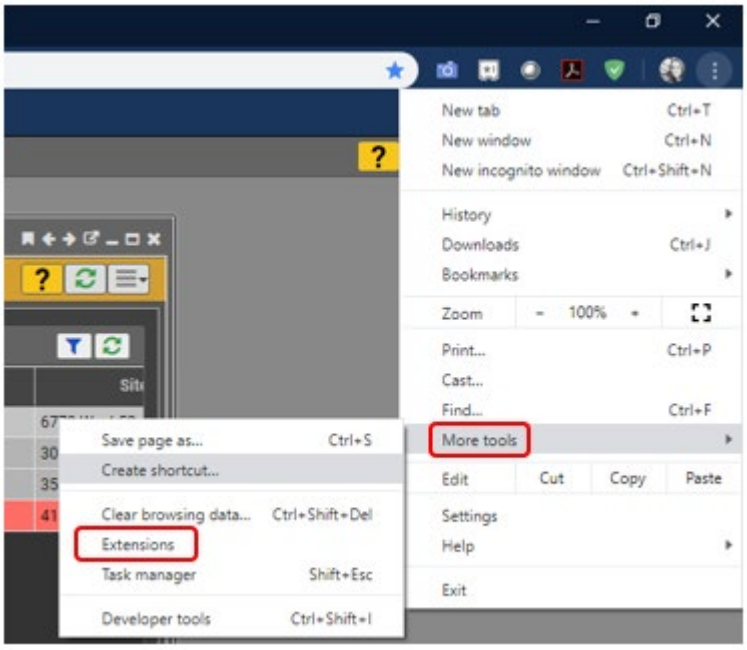
Internet Browser – Extension Management

Here is an example of how to review and disable a plugin within Google Chrome.

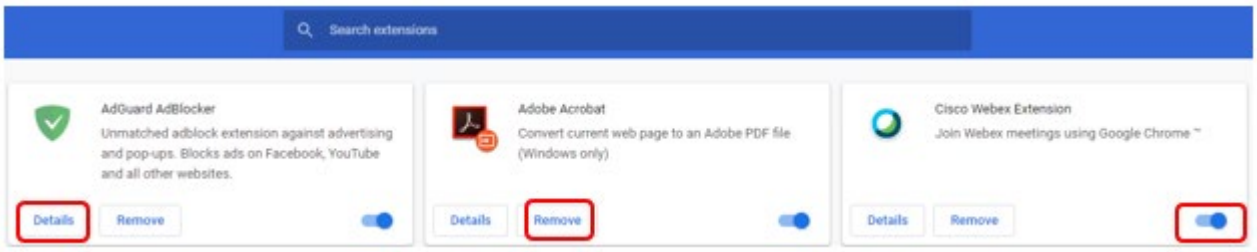
1. Within Google Chrome, select the three dots on the right-hand side of the tool bar



2. Select More Tools and then Extensions



3. This opens the Extensions management page



4. Here you can see the details of the extension, disable it with the radio button or remove it all together.

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

MAPPING THE CIS V7.1 Control 7 Sub-Control 3 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections** ***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***			
7	7.3	Applications	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 3 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

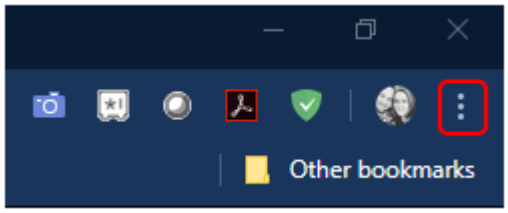
Ensure that only authorized scripting languages are allowed to run in all web browsers and email clients.

*"**Scripts** are lists of commands executed by certain programs or **scripting** engines. They are usually text documents with instructions written using a **scripting** language. They are **used** to generate Web pages and to automate computer processes." According to Techopedia.com.*

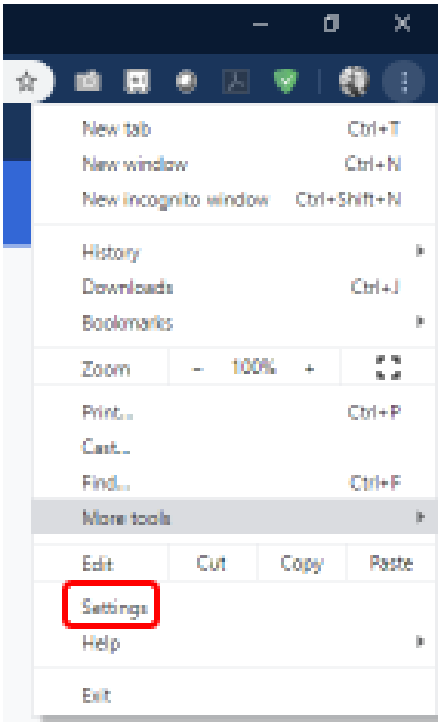
Scripting languages are less common in email clients today. Previously, they were used to execute functions within the application. Java Script is still used very commonly in web browsers. It is important to limit the use of scripting languages in your Web Browser as they can execute code to perform a task that could be used maliciously if not careful.

For this example, we will look at how to manage scripting language in Google Chrome.

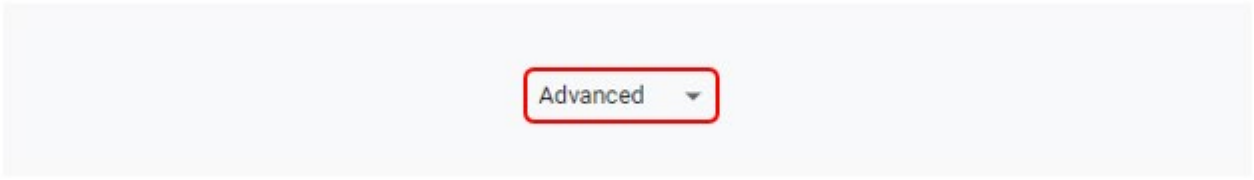
1. Within Google Chrome, select the three dots on the right-hand side of the tool bar



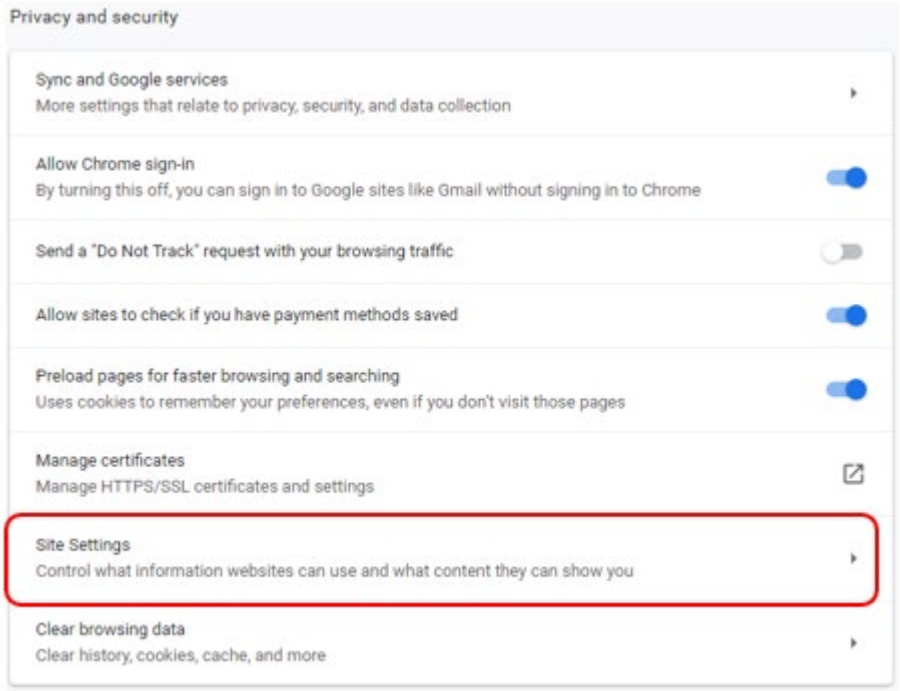
2. Choose Settings



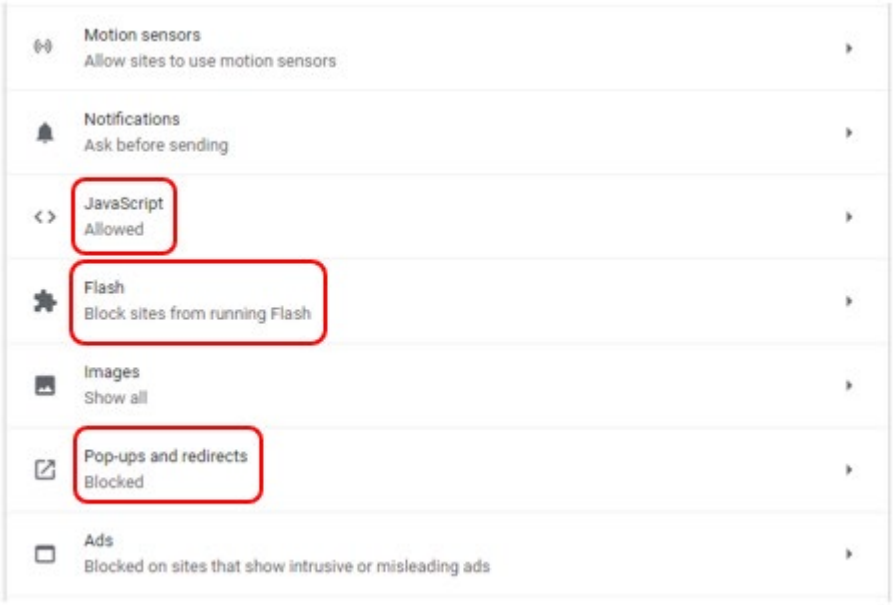
3. Then select Advanced at the bottom of the page. You may have to scroll down to see it.



4. Select Site Settings



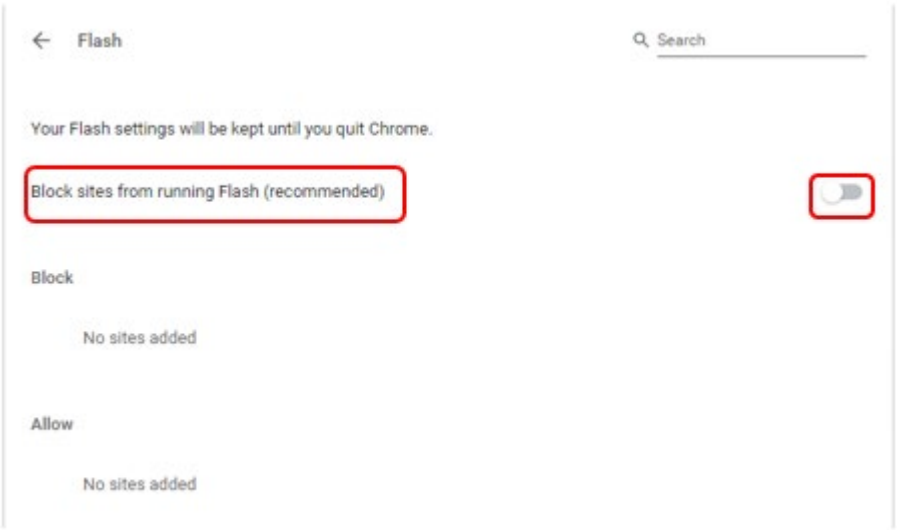
5. Then select JavaScript.



6. Here you can choose if JavaScript is allowed, as well as you can list sites that should be blocked and/or allowed.

7. JavaScript may be important for some website functionality, such as using hyperlinks to open an email.

8. Likewise, you can look at Flash and adjust settings as well. Adobe Flash is recommended to be turned off due to vulnerabilities. Web Browsers have moved away from this technology.



It is a good idea to review these setting periodically. If Adobe Flash is enabled in the browser, it is recommended that it be disabled. If JavaScript is enabled, it is recommended that sites be Allowed or Blocked. Any known malicious sites should be blocked. It is also a best practice to enable Pop-up Blocker.

CIS #7.4: Maintain and Enforce Network-Based URL Filters

MAPPING THE CIS V7.1 Control 7 Sub-Control 4 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.4	Network	Protect	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

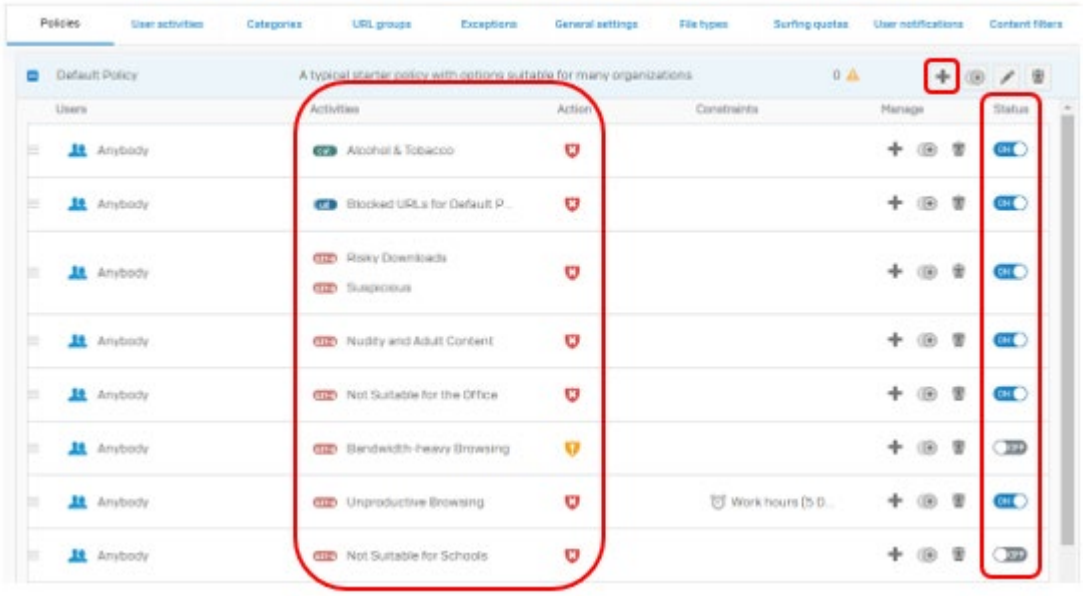
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 4 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-7
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 2 - Foundational

Throughout Sub-Controls 7.4 – 7.10 we will be referencing the functionality of a Next-Gen Firewall. These types of firewalls combine multiple functions into one appliance. Prior to the Next-Gen Firewall, a user would need multiple appliances on their network to achieve the many functions required for protecting a network. The Next-Gen Firewall includes an Intrusion Protection System (IPS), Advanced Threat Protection (ATP), Endpoint protection, Web Filtering, Sandboxing of Email and Files, Email Protection, Data Loss Protection (DLP), Virtual Private Networks (VPN) and many other features.

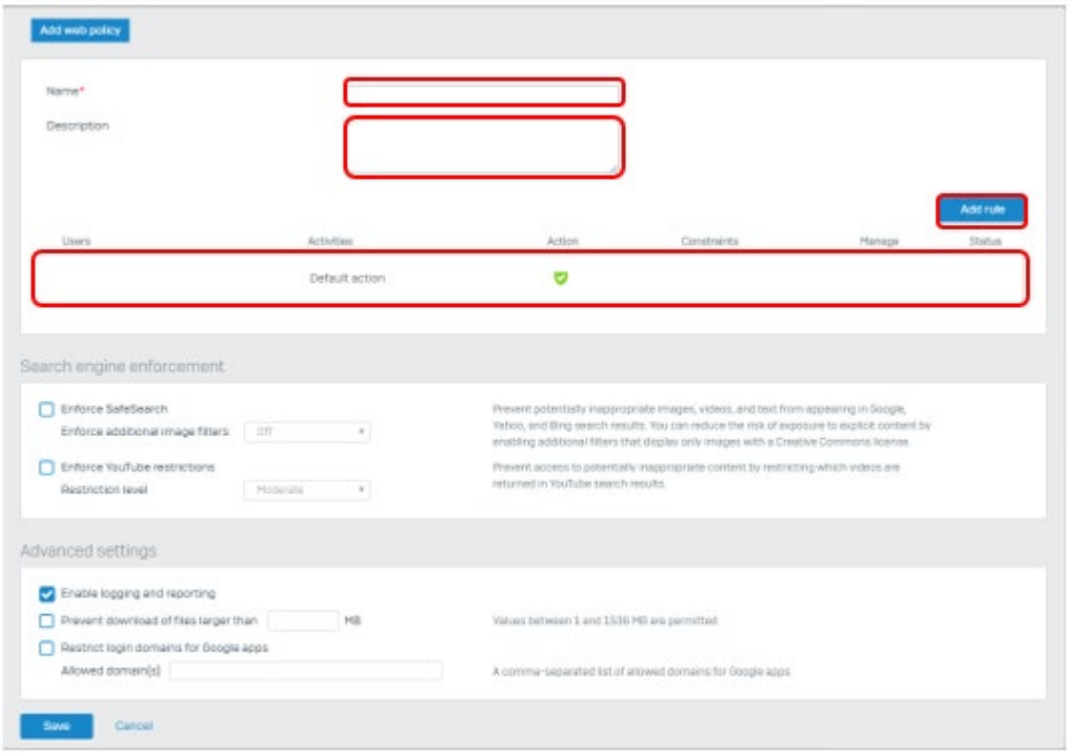
Typically, a Next-Gen Firewall will come with preconfigured policies that are best practices for IT security.

In this example, you can see that this firewall already has several policies that are included out of the box for filtering URLs and can be enabled or disabled based on your business needs.



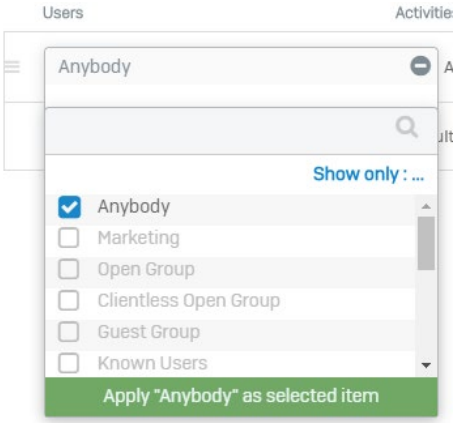
You can also create your own policy with requirements specific to your business by selecting the "+" sign above.

1. This opens a window to create a new policy.
2. Give the policy a name and description
3. Select Add Rule

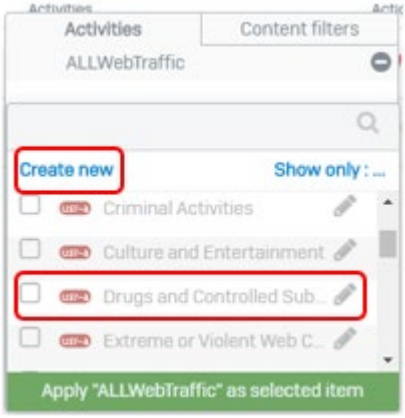


4. This creates a blank rule to configure

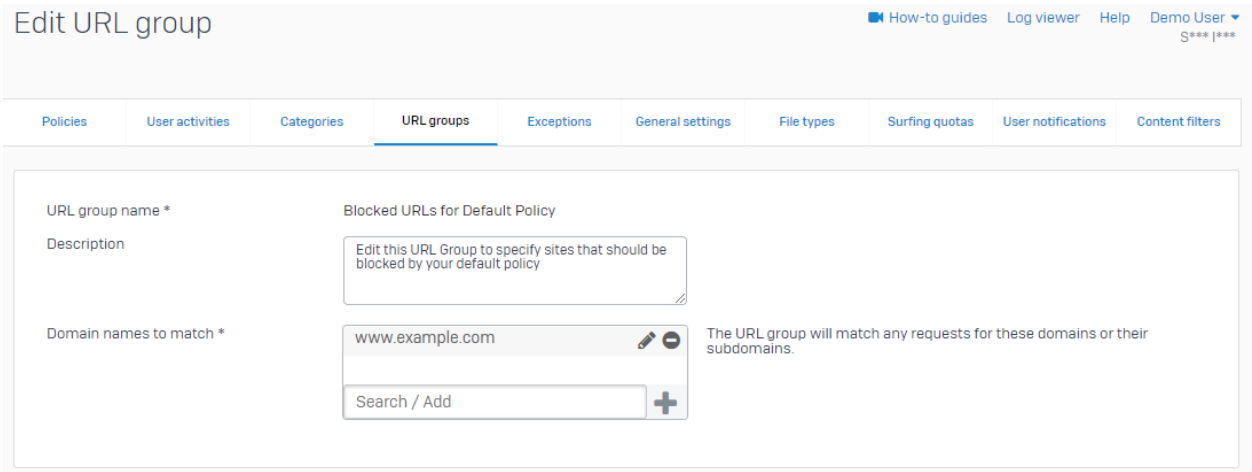
5. Choose which users it applies to using predefined or self-created user groups



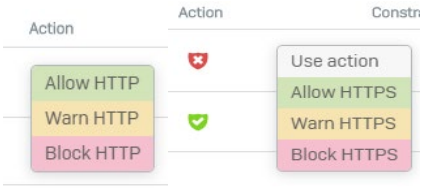
6. Choose the Activities (URL Web Traffic) that the rule should apply to. These can be selected from the predefined list of activities or you can create a new one of your own.



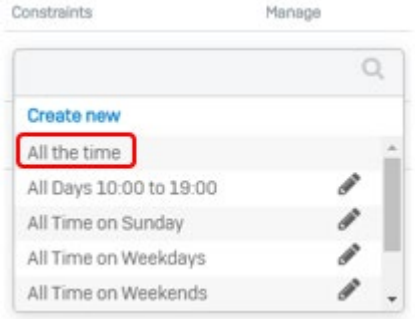
7. By selecting the pencil, you can edit the existing URL group



8. Choose whether the rule applies to HTTP and/or HTTPS traffic and whether it should allow, warn or block the traffic.



9. Then select when the rule should be active. It could run 24/7 or during specified times. Choose "create new" to setup a new time constraint.



10. Once complete, choose "save" and your rule becomes active.

CIS #7.5: Subscribe to URL-Categorization Services

MAPPING THE CIS V7.1 Control 7 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.5	Network	Protect	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.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 5 as follows:

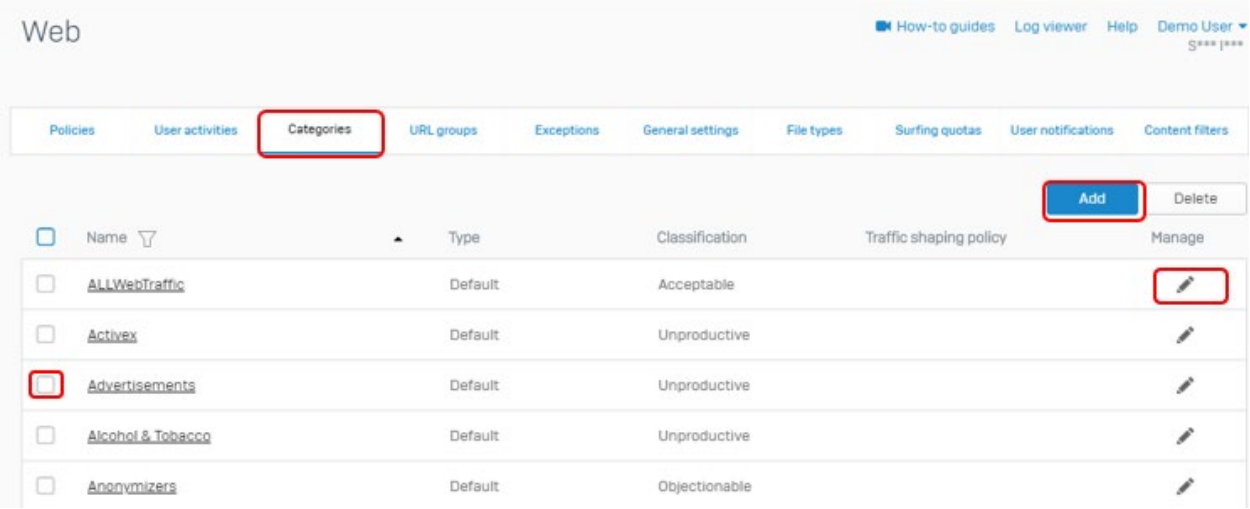
- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-7
  - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 2 - Foundational

There are millions of websites on the internet and there are new ones popping up every day. It is too much for any individual or IT group to try and keep up with. As a feature set of the Next-Gen Firewall,

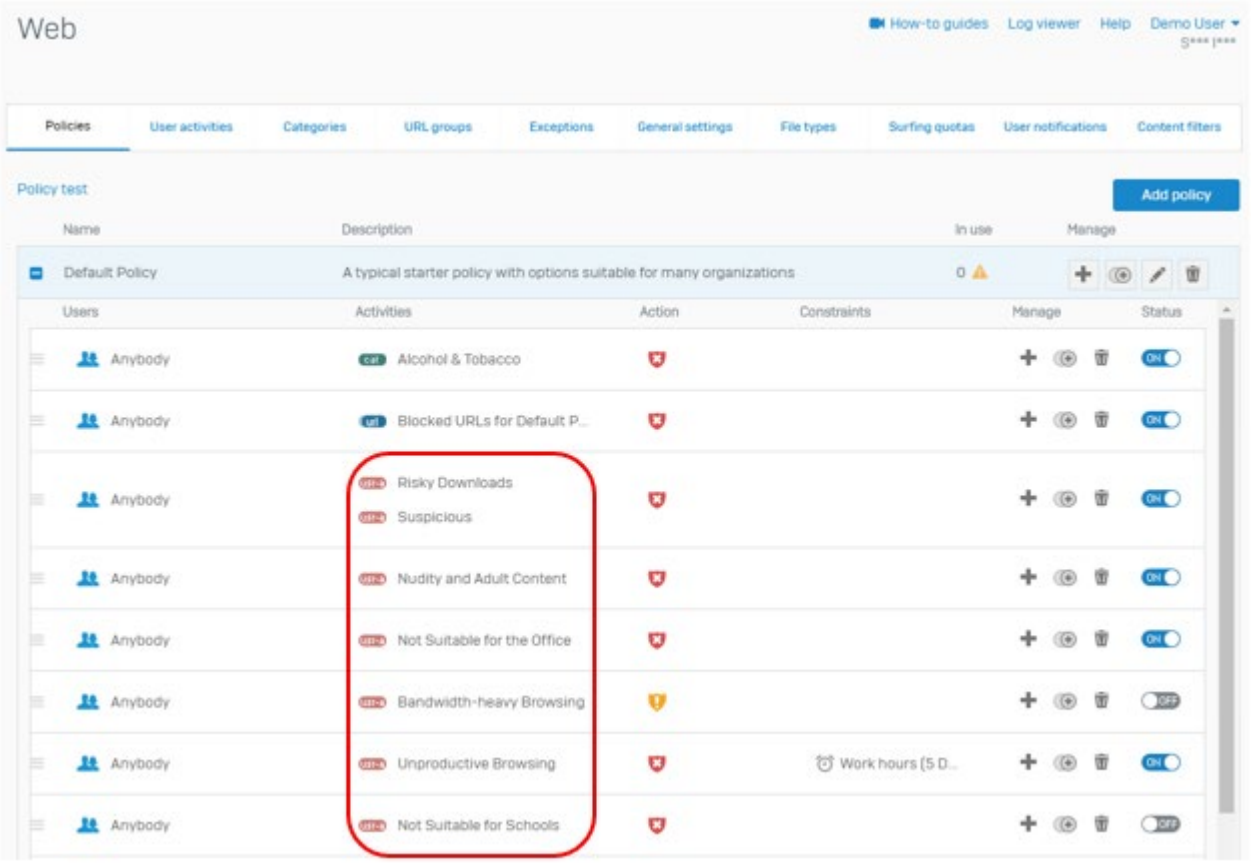
the provider will typically include URL-Categorization Services. These services should be kept up-to-date by the provider.

The service does just what the name indicates and categorizes URL's so that they can easily be used in Firewall Policies. As an additional level of security, websites that haven't been categorized can be blocked by default. This is important as it can take time to discover new websites and categorize them. During that time, a user could browse to the site and be exposed.

From within the Firewall, you can see and/or edit the categories based on your business needs. As you can see the categories are listed in the same area as the Firewall Policies.



1. Select the checkbox next to the category
2. You can use the edit (pencil icon) function to make changes to the group if needed.
3. You can also choose to add or delete a category as well.
4. From the policy, you can see the categories listed as "Activities"



CIS #7.6: Log All URL Requests

MAPPING THE CIS V7.1 Control 7 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.6	Network	Detect	Log all URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors

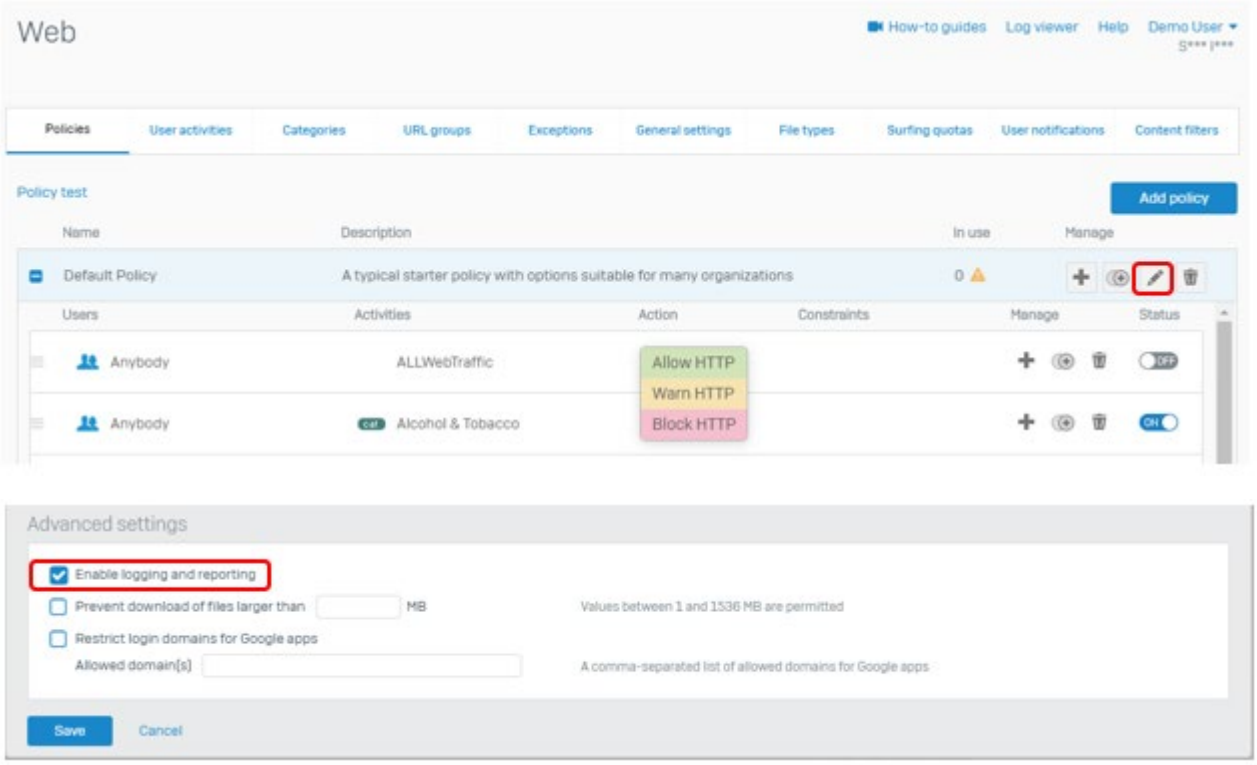
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 6 as follows:

- CSF Function: Detect
- CSF Category: Anomalies and Events
- CSF Category Identifier: DE.AE-3
    - CSF Control: Event data are aggregated and correlated from multiple sources and sensors
- Category: 2 - Foundational

It is extremely important to log activity within the firewall. Logs can be generated for various functions and requests monitored by or performed by the firewall. All URL requests should be logged by the firewall.

Ensure that URL requests are logged within your firewall policies.

1. Select the policy and choose “edit” (pencil icon)
2. Scroll through the setting and locate the option to enable logging and reporting



3. Choose “save”

CIS #7.7: Use of DNS Filtering Services

MAPPING THE CIS V7.1 Control 7 Sub-Control 7 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				Email and Web Browser Protections *Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.*			
7	7.7	Network	Protect	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.	DE.CM-1	The network is monitored to detect potential cybersecurity events
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

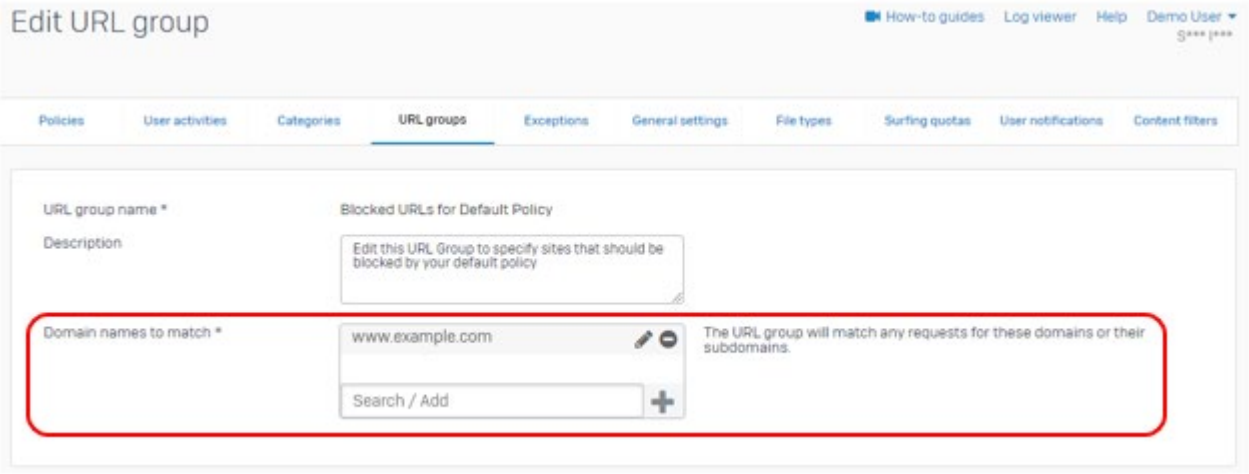
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 7 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier:
  - DE.CM-1
    - CSF Control: The network is monitored to detect potential cybersecurity events
  - DE.CM-7
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 2 - Foundational

The firewall should also have the ability to filter based on Domain Name System (DNS). DNS is used commonly to provide a reference between a web address (ex. www.google.com) and the IP address that the web address represents (172.217.2.196). Without DNS services, web browsing would have to be done via the IP address of the site.

DNS Filtering Services go hand in hand with URL Categorization Services. This is another service that the firewall can provide to help block known malicious domains. You can also block domains specific to your business needs. For example, those of a competitor or of domains that have been of issue to your organization.

1. Enable DNS Filtering options. This may be done through a radio button, checkbox, or other method within the firewall.
2. You can then navigate to the URL Group section to edit any of the URL groups
3. These are the same as the Categorization groups. Select a group and choose “edit”.
4. When editing the URL group, specify any specific domain names to match in the rule



5. These Domain names will be allowed or denied based on the firewall rule configuration.

CIS #7.8: Implement DMARC and Enable Receiver-side verification

MAPPING THE CIS V7.1 Control 7 Sub-Control 8 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.8	Network	Protect	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 Domain Keys Identified Mail(DKIM) standards.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 8 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Next-Gen Firewalls also have the ability to protect users from spoofing or phishing emails as well. They do this by implementing Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC) policy and verification.

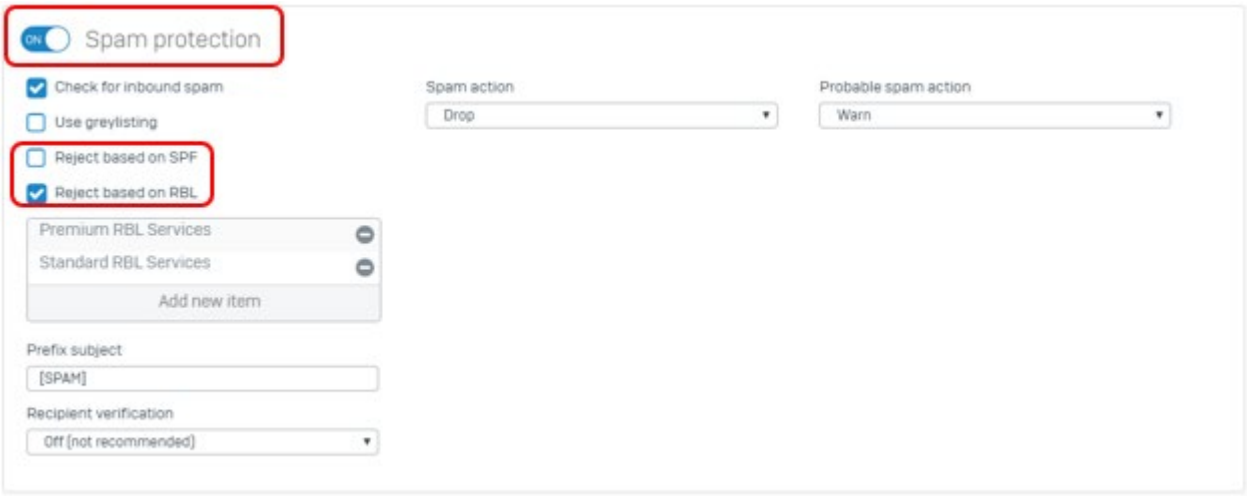
"Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of email." According to Wikipedia.com.

"Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails (email spoofing), a technique often used in phishing and email spam." According to Wikipedia.com.

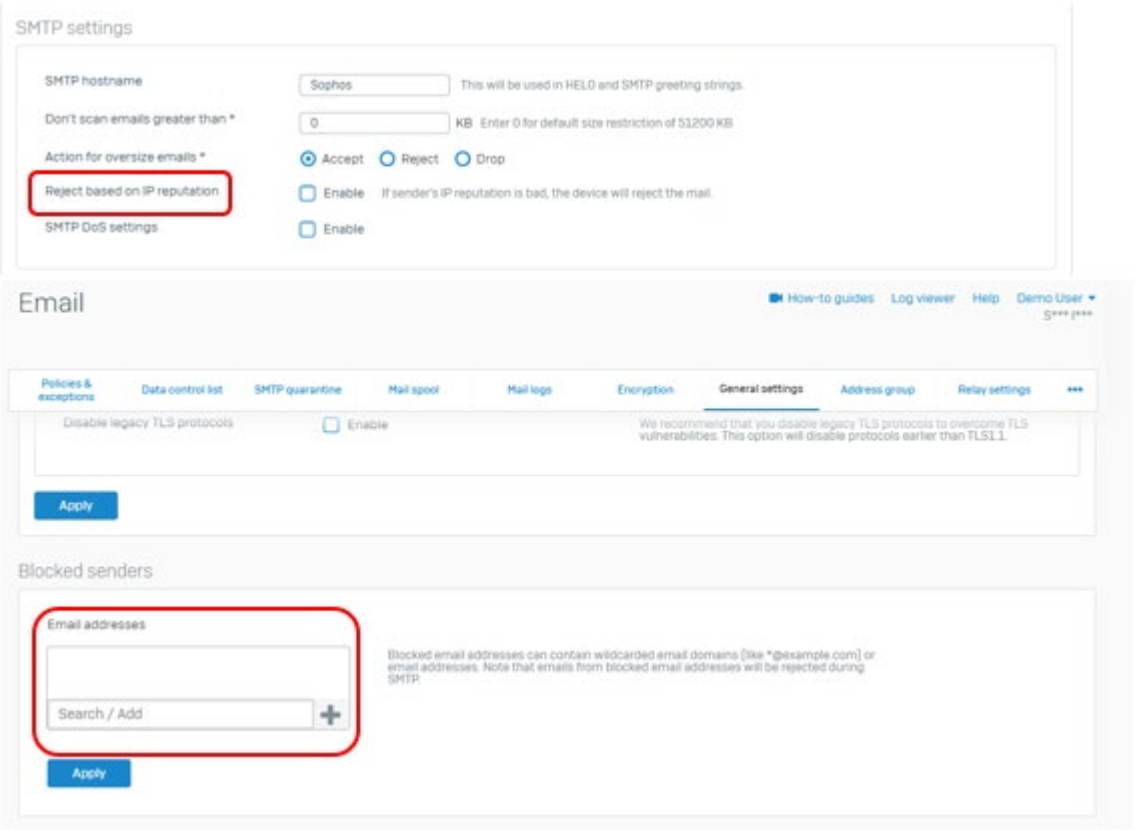
"Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing." According to Wikipedia.com.

Enabling email protection enables multiple protection methods against phishing, spam, spoofing and many other types of malicious emails. Often, it is as simple as enabling the protection. The firewall will implement SPF, DKIM and DMARC. As with all of its features, you will see ways to modify, limit, exempt and log these rules and policies so that they are tailored to your organization's needs.

Below, you can see in the interface the ability to enable Spam Protection. This tells the firewall to check all inbound email for Spam.



You can also have the firewall reject emails based on SPF and/or RBL as well as take a specific action and provide warnings. Below are additional settings for rejecting email based on an IP address, as well as rejecting specific email addresses.



CIS #7.9: Block Unnecessary File Types

MAPPING THE CIS V7.1 Control 7 Sub-Control 9 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.9	Network	Protect	Block Unnecessary File Types	Block all e-mail attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 9 as follows:

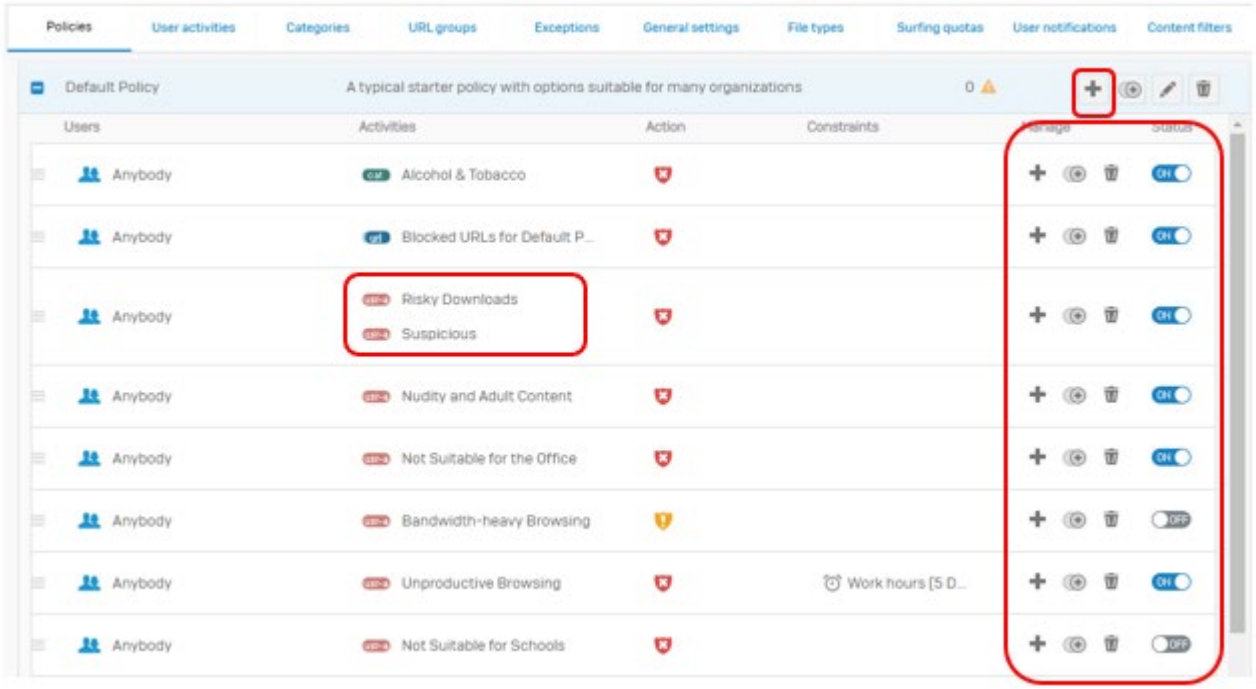
- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-7
    - CSF Control: Monitoring for unauthorized personnel, connections, devices, and software is performed
- Category: 2 - Foundational

The Next-Gen Firewall may also have the ability to restrict specific files or groups of files types from web traffic as well as from email attachments. Any files types that are unnecessary or are known to be malicious should be restricted from your network. Some files can be utilized to gain access, execute code, steal data and credentials, as well as other malicious acts.

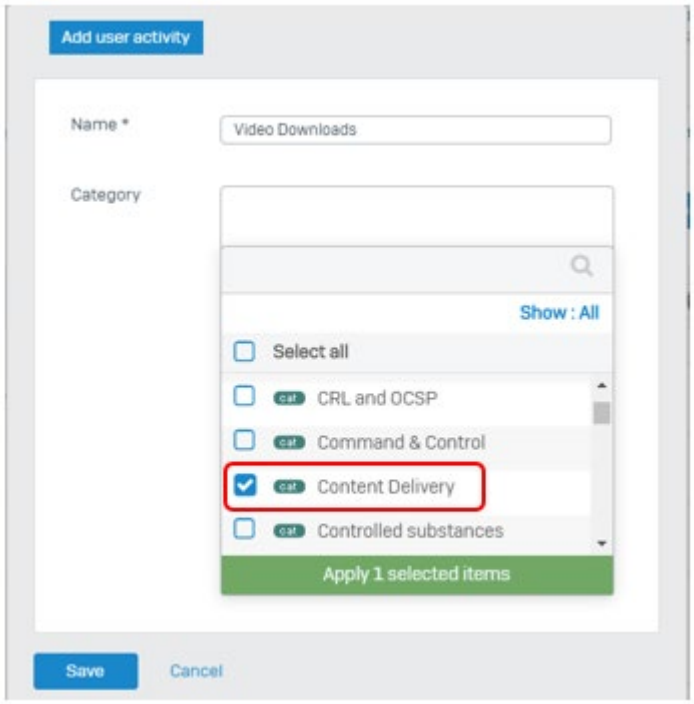
As previously reviewed in Sub-Control 7.4, the firewall will likely have predefined rules available for implementation on the network. These rules can limit the use of file types. You can also create new rules to block specific file types as well as edit the predefined rules and allow or deny file types.

The firewall shown below already has a policy in place to prevent “Risky/Suspicious Downloads”. You could use this existing policy and add or remove file types that you would like to block. The policies can be created to apply to web traffic as well as email.

For Web traffic, you can see an existing policy is in place for “Risky Downloads”



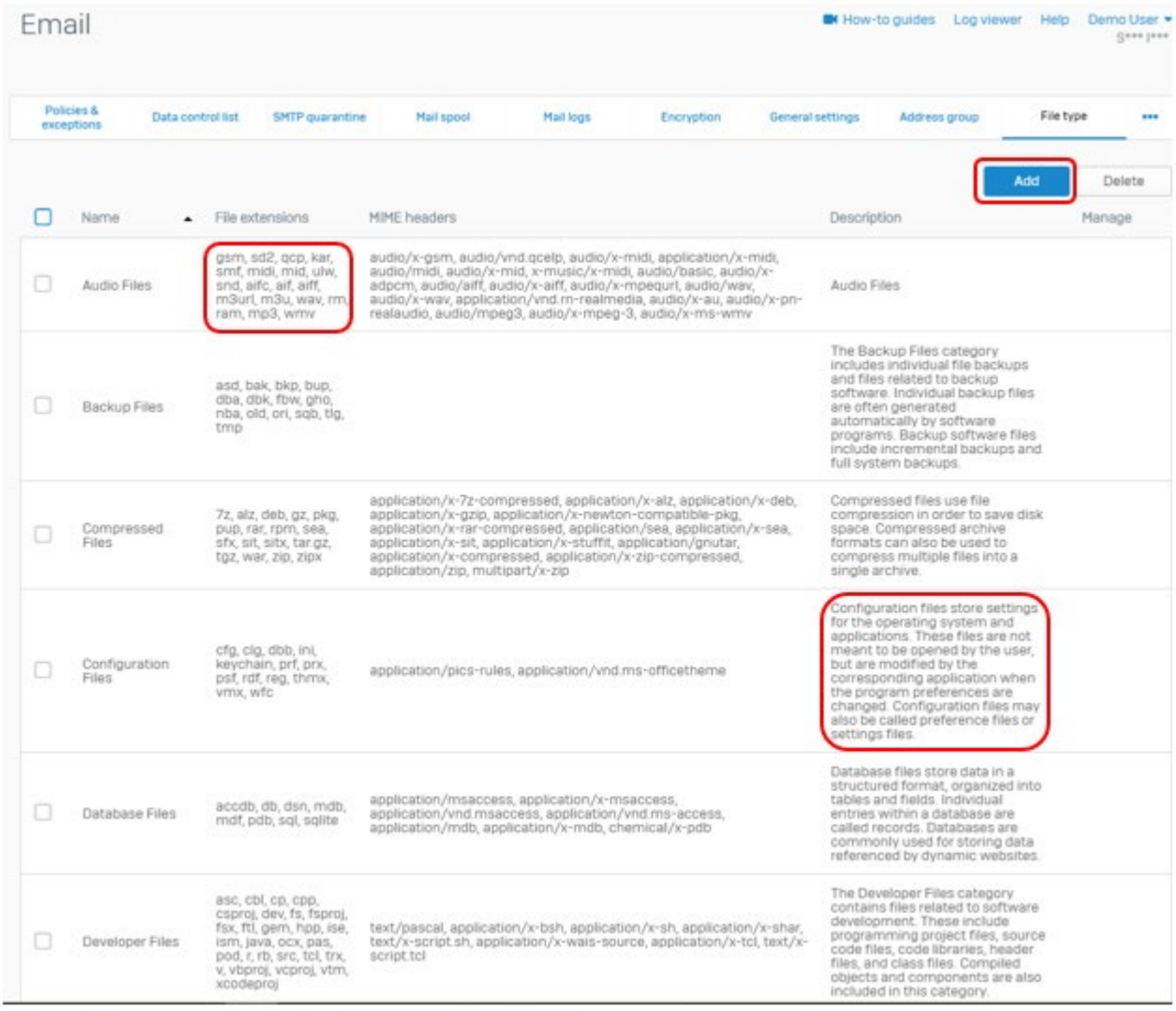
1. Highlight the policy for “Risky Downloads”
2. Select the edit function (Pencil icon)
3. Select the Type of files that you would like to restrict



4. Choose Save

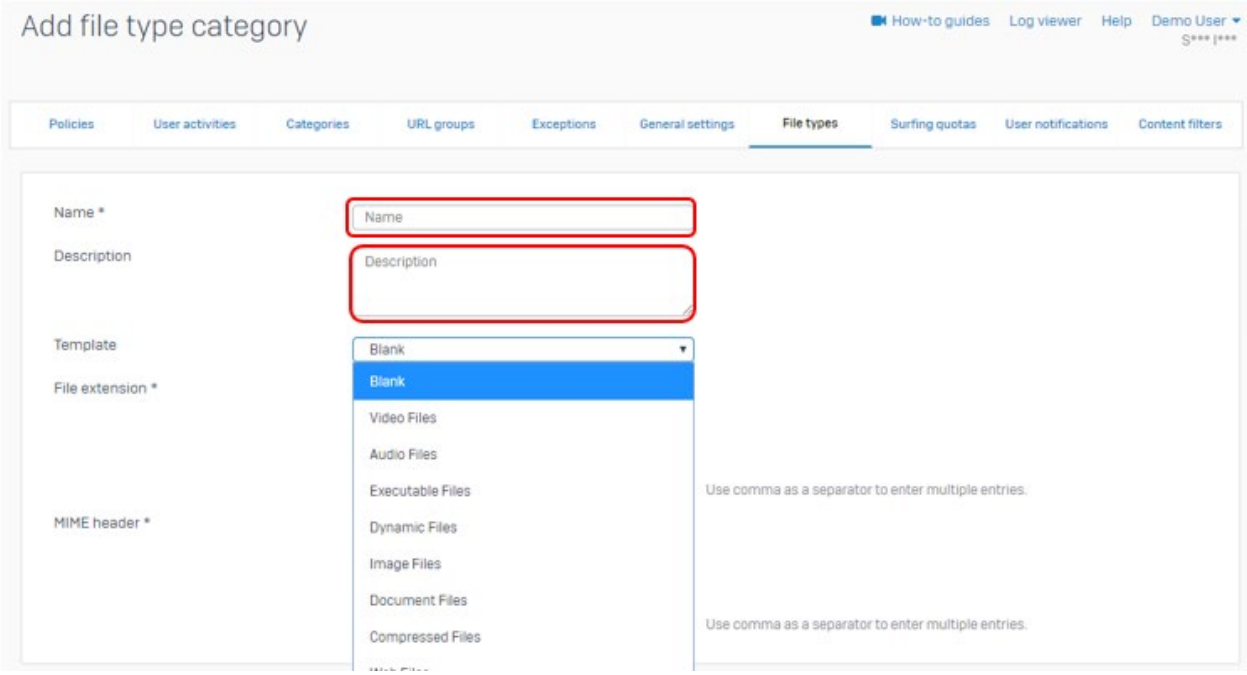
For email traffic, enable File Protection and select the file types that are to be blocked.

1. Within the configuration screen, enable “File Protection”
2. Select file types to be blocked vs allowed
   File Types are categories of files that you can allow or deny. In this firewall, you can review these types. This categorization allows for choosing all file extensions of a certain type for allowing or blocking.



If you do not see the file type that you would like to block, you can add it

1. Select “Add” from the File Type screen
2. Give it a name and description
3. Then choose the file use case from the list. This will help you capture all file types of that specified nature.



4. When finished select save

CIS #7.10: Sandbox All Email Attachments

MAPPING THE CIS V7.1 Control 7 Sub-Control 10 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7				**Email and Web Browser Protections**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***		
7	7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	DE.CM-4	Malicious code is detected

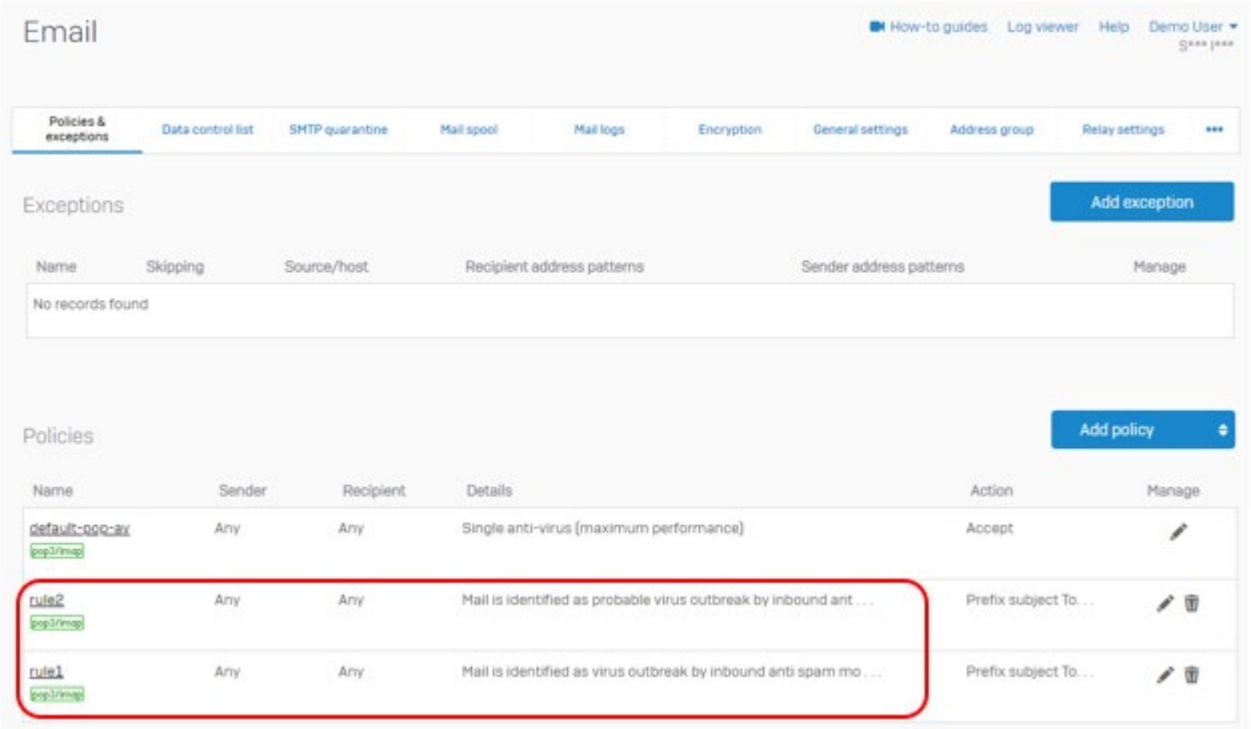
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #7 Sub-Control 10 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-4
    - CSF Control: Malicious code is detected
- Category: 2 - Foundational

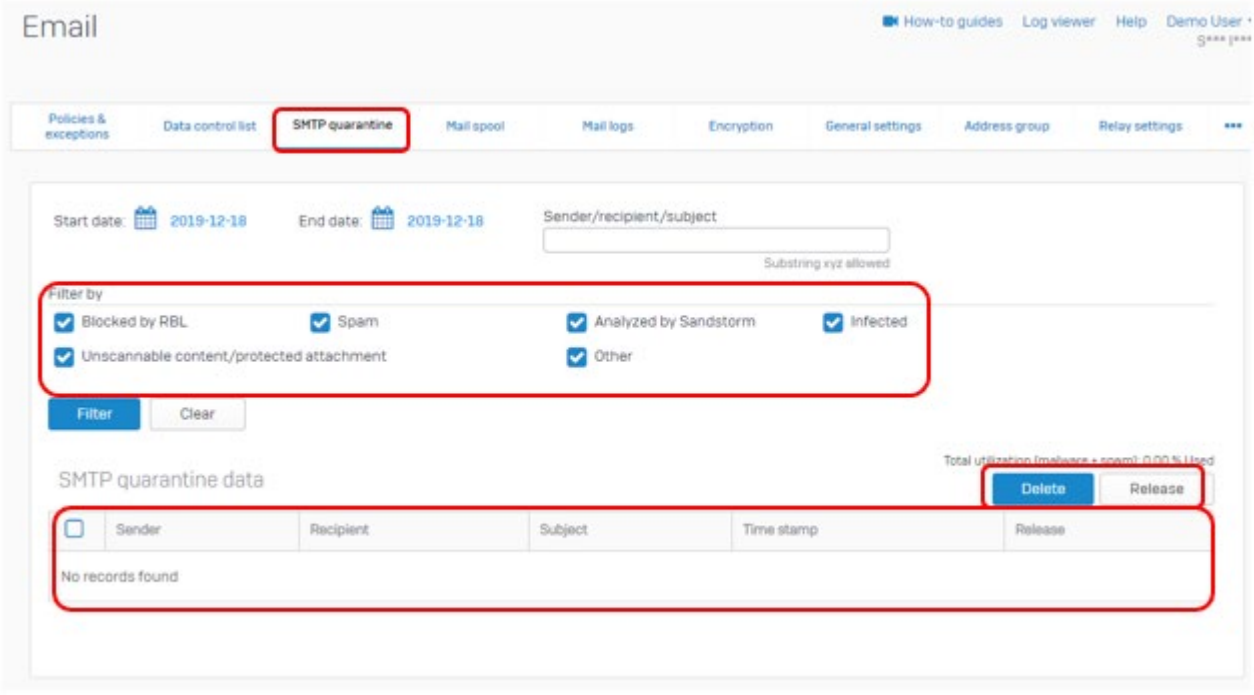
Sandboxing is the practice of isolating a file and safely executing it to see what the result is. This allows the firewall to determine if the file is malicious. The sandbox is a protected area that prevents the network from being affected by executing the file.

Enabling Sandboxing requires monitoring of the logs and results. At times, legitimate files may be quarantined because they appear to be malicious. The firewall will store these files in a quarantined area that needs to be monitored and reviewed. From there, the file can be destroyed or released if it is legitimate.

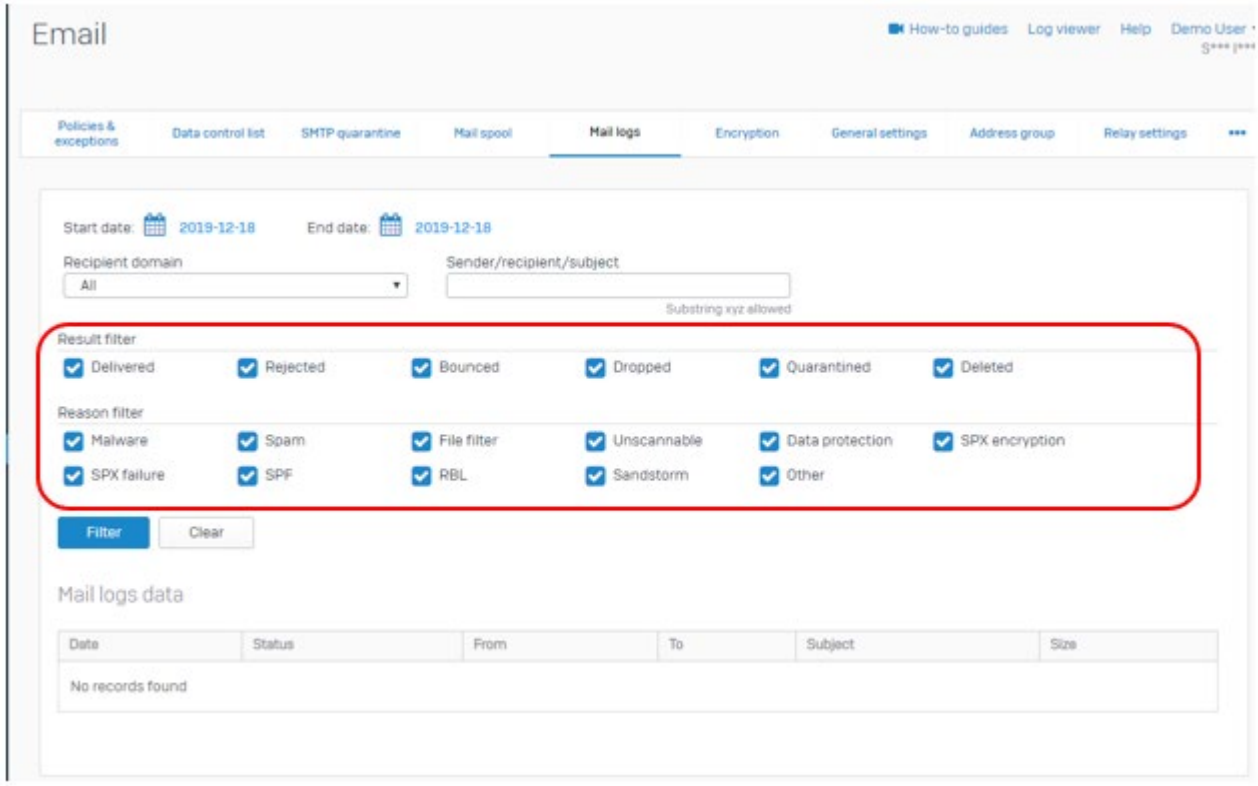
Below is an example of two rules that monitor inbound email and analyze attachments before sending them on to the user.



The results of those scans can lead to quarantined files which are logged for review below.



Likewise, the email itself may be flagged as suspicious. These emails are shown below in the Mail Logs section.



Emails logged here, can be reviewed, deleted and/or released. Above you can see the various filters that can be applied to analyze the log data. As mentioned in Sub-Control 7.6, it is very important to log information in the firewall.

Sub-Control 7.10 is the only sub-control within section 7 that is identified as only in Implementation Group 3. This is due to the requirements for resources for monitoring and maintaining the email sandbox of file types.

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

CIS #8: Malware Defenses

MAPPING THE CIS V7.1 Control #8 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
8				**Malware Defenses** ***Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.***			
8	8.1	Devices	Protect	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.	DE.CM-4	Malicious code is detected
8	8.2	Devices	Protect	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.	DE.CM-4	Malicious code is detected
8	8.3	Devices	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
8	8.4	Devices	Detect	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.	DE.CM-4	Malicious code is detected
8	8.5	Devices	Protect	Configure Devices Not To Auto-Run Content	Configure devices to not auto-run content from removable media.	PR.PT-2	Removable media is protected and its use restricted according to policy
8	8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors
8	8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	DE.AE-3 DE.CM-1	Event data are collected and correlated from multiple sources and sensors The network is monitored to detect potential cybersecurity events
8	8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors

The NIST Cyber Security Framework Version 1.1 (CSF) has 3 Mappings for CIS #8 and 4 Mappings for CIS #12. Those that are relevant to this article, but not limited to, are:

- CSF Function: Detect
- CSF Category: Anomalies and Events, Security Continuous Monitoring, Detection Processes
- CSF Category Identifier: DE.AE, DE.CM, DE.DP
- CSF Control: DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
- CSF Control: DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
- CSF Control: DE.AE-5: Incident alert thresholds are established
- CSF Control: DE.CM-1: The network is monitored to detect potential cybersecurity events
- CSF Control: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

- CSF Control: DE.CM-4: Malicious code is detected
- CSF Control: DE.DP-4: Event detection information is communicated to appropriate parties
- Category: 2 - Foundational

Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack your systems, devices, or your data. It can be fast-moving, fast-changing, and enter through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware can be designed to avoid defenses, or to attack or disable them.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like Incident Response. They must also be deployed at multiple possible points-of-attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that

all defenses are active and current on every managed

Due to the emergence of cloud computing and data farm advancement in the information and communication technology (ICT) storage space, cloud systems have increasingly become targets for attack and ransom. To combat threats, malware architecture must consider the network perimeter no longer exists as users engage networks from global positions with both trusted and untrusted personal devices to conduct business. In the end, malware defensive architecture must be flexible to consider organizational transition as physical application and infrastructure move to trusted third parties as the greatest transfer of risk management and responsibility is now underway.

TOOLS TRIED/USED/INVESTIGATED

Darktrace, BluVector, CyberadAPT

SYNOPSIS

There are many tools that fall under the IDS category that can detect intrusions and anomalies on your network. When implemented, their function is to provide constant vigilance of the infrastructure and alert and/or contain upon an incident. These threats could include fileless malware, zero-day, ransomware and brute force. When selecting a manufacturer, it is important to understand how they go about monitoring and detecting, reside in your environment, and manage the incident. Be sure to discuss connections to cloud based applications like o365.

Machine Learning (AI) has taken the industry by storm and is dynamic and fluid in nature in that it is not fixed to set parameters. It is constantly learning the environment and adjusting over time, then alerting when anomalous behavior is detected. Some tools use a more traditional method of combing through logs, packet captures, and adhering to fixed parameters; to name a few. These solutions should not be used in lieu of traditional of anti-virus and malware detection. Rather, these provide an additional layer of defense and detection.

Often, an appliance (server) software is installed on premise with sensors throughout the infrastructure. This data can be sent up to the cloud for additional triaging or remain on premise. Also, some

manufacturers offer Managed Services which include an analyst who will contact you in the event of a detection and hold routine meetings to discuss the ongoing health of the system. However, the end-user would still have visibility of system health and threat levels through a dashboard or mobile app.

HOW IT WORKS

- Appliance/software that connects to the core and monitors inbound/outbound traffic
- Creates a benchmark of normal behavior; usually 2 weeks recommended
- Analyzing packet captures from end to end
- Log collection and analysis
- Flags unusual behavior; large data transfer, suspicious external domains, activity at unusual hours, unauthorized attempts, etc.

ADVANTAGES INCLUDE

- Constant monitoring of network traffic from client to outbound
- Great tool for small and large IT teams
- Can detect unusual traffic patterns
- Record traffic patterns for later reporting
- Some offer Manage Services; live operator

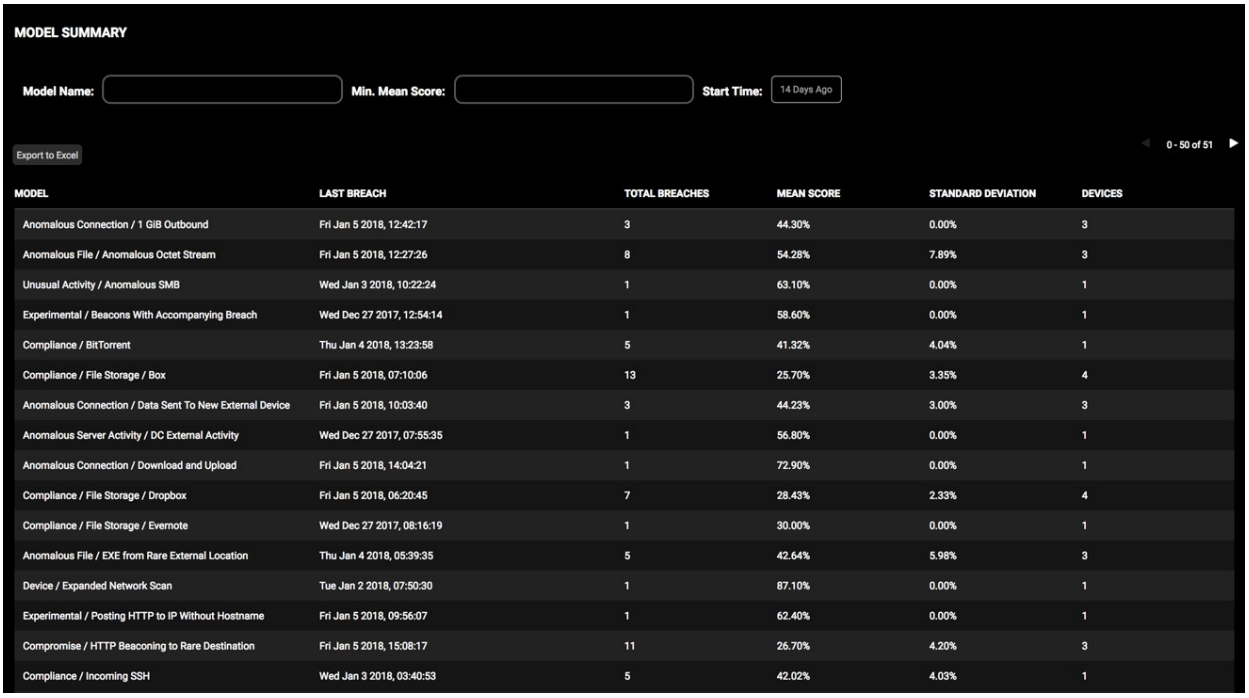
- Can detected malware sending outbound traffic
- Easy deployment of appliance within hours; no extensive training

CONS

- Expensive
- May need multiple appliances based on traffic, footprint, and topology
- Client's infrastructure topology could limit data gathering; discuss with manufacturer
- Some cannot quarantine a threat

ANTICIPATED OUTPUT

- Complete network visibility
- Traffic capture from end to end
- Easy to use interface with granular data
- Detection of anomalous behavior
- Quarantining of threat
- Robust reporting

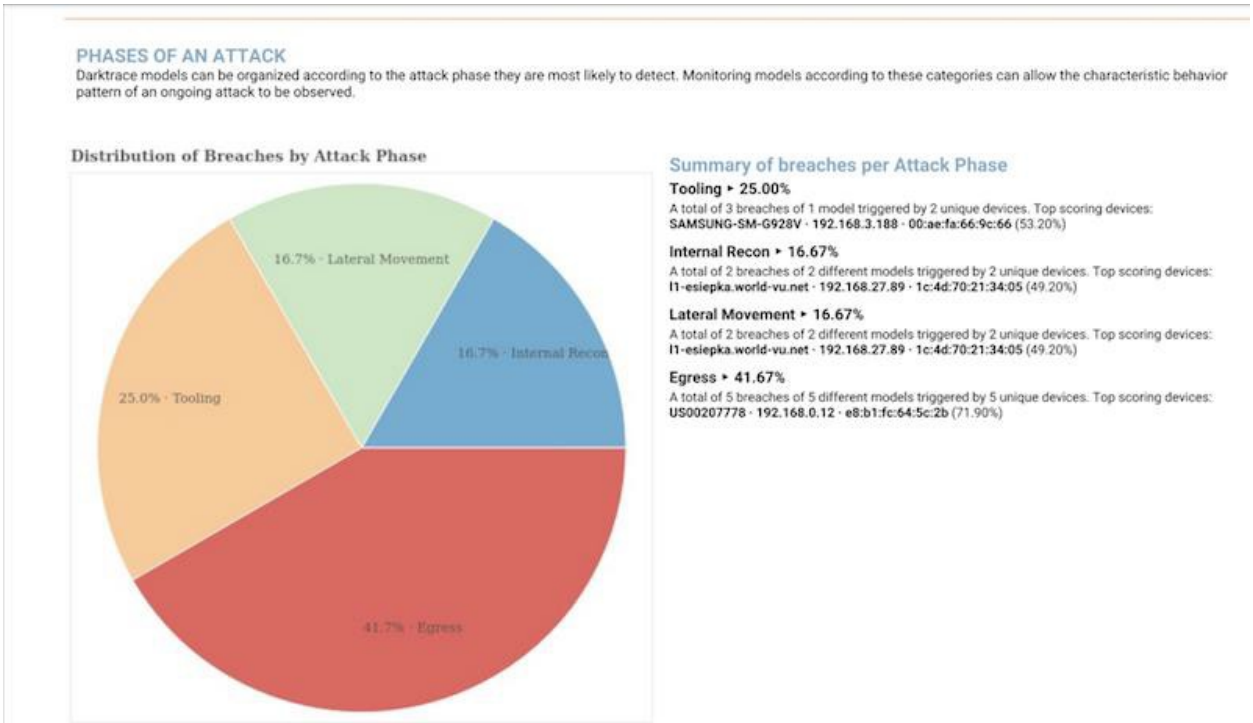


MODEL SUMMARY

Model Name: Min. Mean Score: Start Time: 14 Days Ago

Export to Excel 0 - 50 of 51

MODEL	LAST BREACH	TOTAL BREACHES	MEAN SCORE	STANDARD DEVIATION	DEVICES
Anomalous Connection / 1 GiB Outbound	Fri Jan 5 2018, 12:42:17	3	44.30%	0.00%	3
Anomalous File / Anomalous Octet Stream	Fri Jan 5 2018, 12:27:26	8	54.28%	7.89%	3
Unusual Activity / Anomalous SMB	Wed Jan 3 2018, 10:22:24	1	63.10%	0.00%	1
Experimental / Beacons With Accompanying Breach	Wed Dec 27 2017, 12:54:14	1	58.60%	0.00%	1
Compliance / BitTorrent	Thu Jan 4 2018, 13:23:58	5	41.32%	4.04%	1
Compliance / File Storage / Box	Fri Jan 5 2018, 07:10:06	13	25.70%	3.35%	4
Anomalous Connection / Data Sent To New External Device	Fri Jan 5 2018, 10:03:40	3	44.23%	3.00%	3
Anomalous Server Activity / DC External Activity	Wed Dec 27 2017, 07:55:35	1	56.80%	0.00%	1
Anomalous Connection / Download and Upload	Fri Jan 5 2018, 14:04:21	1	72.90%	0.00%	1
Compliance / File Storage / Dropbox	Fri Jan 5 2018, 06:20:45	7	28.43%	2.33%	4
Compliance / File Storage / Evernote	Wed Dec 27 2017, 08:16:19	1	30.00%	0.00%	1
Anomalous File / EXE from Rare External Location	Thu Jan 4 2018, 05:39:35	5	42.64%	5.98%	3
Device / Expanded Network Scan	Tue Jan 2 2018, 07:50:30	1	87.10%	0.00%	1
Experimental / Posting HTTP to IP Without Hostname	Fri Jan 5 2018, 09:56:07	1	62.40%	0.00%	1
Compromise / HTTP Beaconing to Rare Destination	Fri Jan 5 2018, 15:08:17	11	26.70%	4.20%	3
Compliance / Incoming SSH	Wed Jan 3 2018, 03:40:53	5	42.02%	4.03%	1



ROI

ROI is difficult to quantify so you should look at it as an insurance policy. While typically expensive, you should weigh the pro's and con's and consider the consequences of not have such a tool. Depending on the severity, data breaches can cost you millions, destroy your reputation or even bankruptcy.

FOR CONSIDERATION

- Constant network monitoring without requiring your own NOC or additional headcount
- Through Managed Services, you can leverage their experience and expertise
- Savings through reduced headcount
- Mitigate damage

CLOSING

In closing, as advanced malware and attacks become more dangerous to modern computing infrastructure, defenses required include physical, structural and best practice defenses to combat threat vectors to preserve ICT assets. With the emergence of cloud and malware defense available in the cloud, the transfer of risk can be quantified to support security and investment decisions regarding network governance, risk and risk tolerance which will be the driving force to determine a blueprint for the future.

CIS #9: Limitation and Control of Network Ports Protocols, and Services

Bad actors are in a constant state of war with all of us. Time and time again we read about malicious hacks that cause business disruption, data theft or worse. Statistically, bad actors gain access to internal networks and maintain persistence in these networks for months and quite possibly years before they are detected. How do they get access to our networks? How do they stay in our networks for so long? How do they go undetected?

The control of network traffic is one of the most effective methods that you can implement to protect your organization's infrastructure. In most cases, the cost of the firewall or UTM has already been invested in, there is a minimal cost (mainly consisting of man hours) for enhancing its operational configuration.

Changing hearts and minds and instilling a culture of Security is sometimes a very daunting proposition. Ease of use is the Achilles' Heel of the network administrator and the bad actors know it. It is easier to capitulate to end user push-back rather than implement proper security controls. IT people are fully entrenched in the Accessibility portion of the CIA Triad. They live and die by uptime. Not too long ago, a firewall was the main control used to stop traffic from the Internet into our internal networks. The controls mainly consisted of port blocking.

Fast forward to 2019 these rudimentary controls, by themselves, are no longer as effective and a different mindset is needed to combat the ever-changing threat landscape that affects our Information Security posture. The segmentation networks help reduce the east-west traffic in the network. It also gives an additional layer of network security by examining traffic to and from the server network. In addition, it is recommended that Building Automation systems, Cameras and Access Control systems reside on a segmented and fire-walled network. Traffic is controlled and monitored Malicious traffic would potentially be halted and legitimate traffic would be allowed to pass to legitimate hosts. The control of network traffic flow is vital to an organization's holistic Information Security program.

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

MAPPING THE CIS V7.1 Control #9 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9				**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.1	Devices	Identify	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.		

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #9 Sub-Control 1 as follows:

- CSF Function: Identify
- CSF Category:
- CSF Category Identifier:
    - CSF Control: Associate Active Ports, Services and Protocols to Asset Inventory
- Category: 2 - Foundational

It is imperative that all legitimate ports and protocols that are necessary for applications and services are associated with the organization's hardware and software inventory.

This process begins with CIS 1 and CIS 2. An updated and accurate inventory of all authorized hardware and software assets needs to be performed. Then, the ports and protocols for each application or service can be mapped to each individual host.

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

MAPPING THE CIS V7.1 Control #9 Sub-Control 2 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9				**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.2	Devices	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

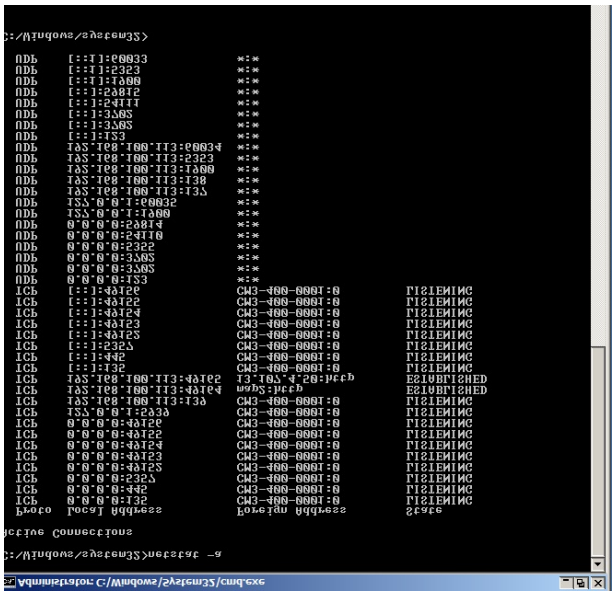
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #9 Sub-Control 2 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system. It is quite common for an installed application to open ports that are not entirely necessary for the operation of the application.

All unnecessary ports and protocols should then be disabled.

The detection of these ports and protocols can performed by using port scans and by querying the local operating system. Netstat is a common tool to determine which local ports listening for connections or are already connected to local or remote connections.



CIS #9.3: Perform Automated Port Scans Against All Key Components in the Network

MAPPING THE CIS V7.1 Control #9 Sub-Control 3 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9				**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.3	Devices	Detect	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.	DE.CM-8	Vulnerability scans are performed

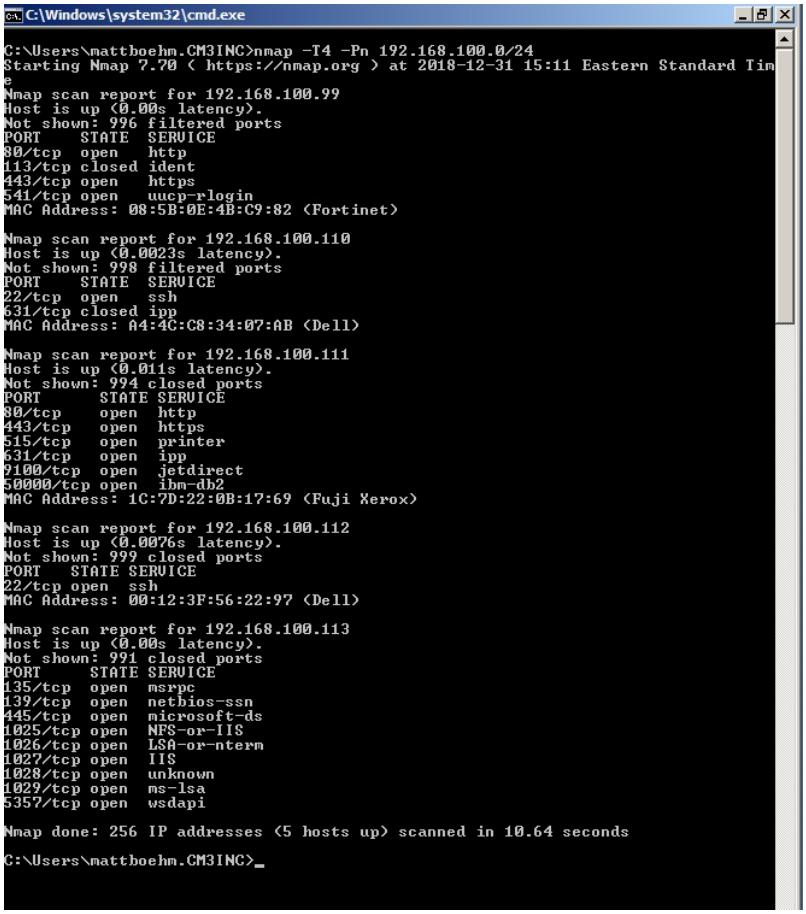
The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #9 Sub-Control 3 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-8
    - CSF Control: Vulnerability scans are performed
- Category: 2 - Foundational

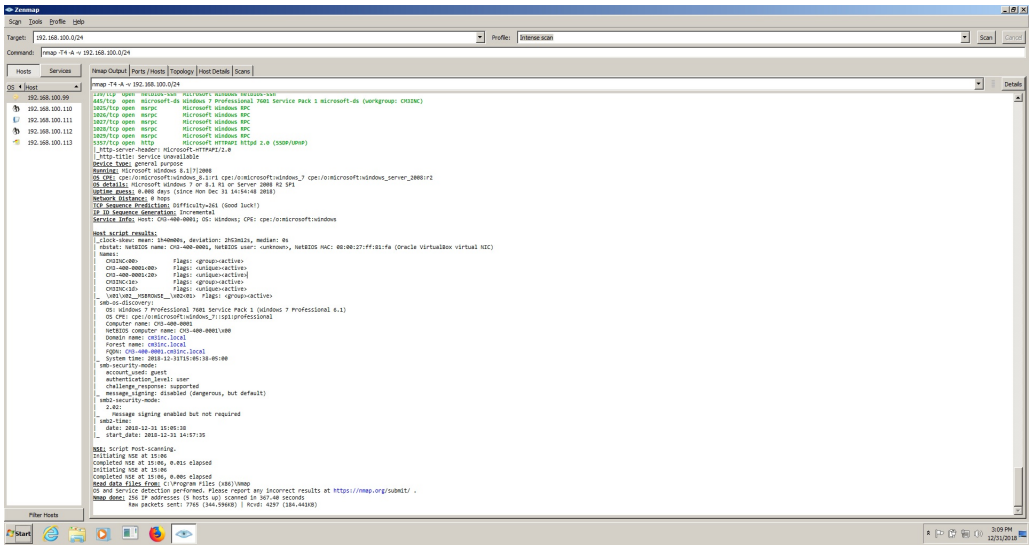
Perform automated scans of mission critical devices on your network. The information received from this scan will determine which ports are open on a particular host. Unusual ports or ports that are not assigned to the function of the device may indicated that a compromise has occurred.

Automated port scans of your internal network may alert you to the presence of an attacker on your network. It may be a tell-tale sign of an intrusion if non-standard ports are discovered. Automated port scans can be performed with open source tools such as OpenVAS. There are also many commercially available products available for a fee such as Nessus, Retina and Nexpose to name a few.

Nmap is an extremely useful and powerful tool to determine the accessibility to ports on remote systems. Nmap is available for both Windows and Linux distributions. Zenmap is a Graphical version of Nmap. It is a multi-platform application that works on Linux, Windows, Mac OS X and BSD.
This can be used for "spot checking" hosts or can be used to scan an entire network.
Below is an example of a Nmap scan for an entire small network



This is an example of the same scan using Zenmap.



CIS #9.4: Apply Host-based Firewalls or Port Filtering Tools

MAPPING THE CIS V7.1 Control #9 Sub-Control 4 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9				**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.4	Devices	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #9 Sub-Control 4 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

A host-based firewall will allow any necessary business-related traffic to and from your Workstations and Servers while blocking any traffic that is not needed.

Restrict which ports hosts on your network use to communicate with your critical business processes. This can be done through the configuration of Windows Firewall locally or by group policy or the installation of a third-party host-based firewall solution.

CIS #9.5: Implement Application Firewalls

MAPPING THE CIS V7.1 Control #9 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9				**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.5	Devices	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) systems to provide only essential capabilities

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #9 Sub-Control 5 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - CSF Control: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Place application firewalls in front of critical servers to verify and validate the traffic going to the server. This includes performing micro-segmentation between your servers and workstations in your production environment.

If your server is visible on the Internet and is critical for a business purpose it must be protected. Place the server in a DMZ, Harden the operating system, and Implement an Application Firewall to allow for Intrusion Detection and Prevention. In addition, diligently patch the operating system and ANY application components that reside on the server.

Segmenting networks helps reduce the east-west traffic in the network. It also gives and additional layer of network security by examining traffic to and from the server network. In addition, it is recommended that BAS, Camera and Access Control systems reside on a segmented and fire walled network. Traffic is controlled, monitored and malicious traffic could potentially be halted while allowing legitimate traffic to pass to legitimate intended targets.

If access to the server is not needed from the Internet, move the server to an internal network that is behind your firewall.

CIS #10: Data Recover

THIS PAPER PROVIDES AN EXAMPLE OF AN IMPLEMENTATION OF THE CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROL (CIS) #10.

CIS #10.1: Back to the Future – Data Recover Strategy

MAPPING THE CIS V7.1 Control #10 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
10				**Data Recovery Capabilities** ***The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.***			
10	10.1	Data	Protect	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.	PR.IP-4	Backups of information are conducted, maintained, and tested

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #10 Sub-Control 1 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-4
  - CSF Control: Backups of information are conducted, maintained, and tested
- Category: 2 - Foundational

Critical Security Control #10 is a foundational control that prescribes for processes and tools used to properly back up critical information with a proven methodology for timely recovery of it. CIS #10 is composed of 1 sub control that address the activities for backups of information that are conducted, maintained, and tested periodically. This sub control must be implemented to fully realize the cyber security vulnerability mitigation intended by CIS #10. This paper will walk through the essentials of CIS# 10, sub control 10.1.

BACKGROUND

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine. Data backup and recovery is critical given there can be several instances beyond an attack that requires data to be recovered. Therefore, it is critically important to have a solid data recovery capability in place tested and maintained on a regular basis.

MAPPING THE CIS #10 TO THE CYBER SECURITY FRAMEWORK

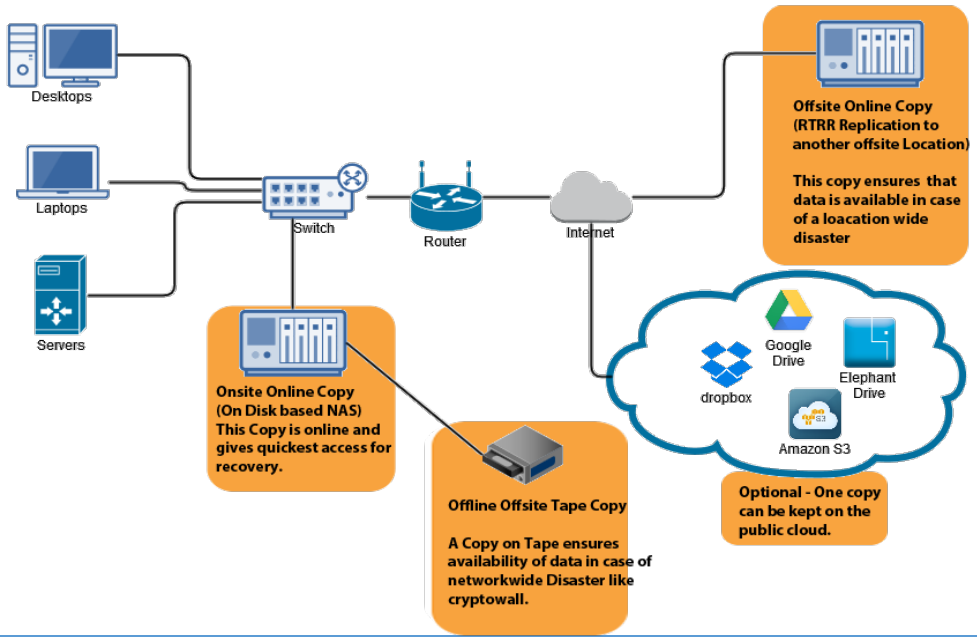
DATA RECOVER PLAN –*KEY STRATEGIC POINTS*

1. Ensure Regular Automated Backups
   a. Ensure that all system data is automatically backed up on a regular basis
2. Perform Complete System Backups
   a. Ensure that all 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.
3. Test Data on Backup Media
   a. Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
4. Protect Backups
   a. 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.
5. Ensure Backups Have At least One Non-Continuously Addressable Destination
   a. Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

PROCEDURES & TOOLS

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional. In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

TYPICAL BACKUP AND DISASTER RECOVERY MODEL



TIPS AND INDUSTRY EXPERT ADVICE

- Ensure that all system data is automatically backed up on regular basis.
- 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.
- Make sure your data is encrypted, in motion, and protected in all ways possible.
- Think quicker recovery time and not quicker backup time
- Maintain sufficient back up history
- Back up essential data AND applications
- Have off site and or online backup
- Fix broken access controls on file servers
- Always test restores of data on a scheduled basis and when any new software or hardware is implemented in the backup and recovery process
- Establish a File Organization Standard. Organization is key. Determine Which Files Need to Be Preserved. Once you have organized your files, determine which ones are important.
- Automate your backup procedures.

A good backup plan includes the whole network, not just data

"We all appreciate the importance of backing up our data, but a backup plan for the network is usually given less thought. The question is not whether your business will lose Internet connectivity, it's when. In some areas Internet connectivity can experience service disruption up to several times a month, which exposes businesses to risks of lost revenue, reduced productivity and customer experience issues. One possible solution is upgrading to a more robust wired connection, but it's expensive and still susceptible to outages and service disruption. An alternative option is to bridge the inevitable gap with wireless WAN

failover, which is quick and easy to deploy. There are few businesses that can afford to take the risk of network connections failing, so organizations need to place a priority on backing up their network." *Ken Hosac, VP of IoT strategy and business development, Cradlepoint*

Data backup should be done early, often, and not too close

"Backing up business critical data is more complex than many people realize which may be why backup and disaster recovery plans fall apart in the hour of need. World Backup Day is an important reminder of this reality, and many fall short with a few common missteps. The closer your backup is to the primary data, the more likely it is to suffer the same fate as your primary data. Additionally, performing backups as frequently as possible often falls by the wayside of priorities, but this is a very effective way to prevent data loss. Lastly, while emphasis is frequently on the recovery point of when your last backup was taken, recovery time is just as important. The bottom line is that we all need to take some time to review backup plans and find out if you need to be doing more to prevent the next data loss event lurking around the corner." *Jason Collier, co-founder, Scale Computing*

Backup systems should be scalable to keep pace with data growth

"Data has become an integral component of our personal and professional lives, from mission-critical business information to personal photos and videos, with an estimated 1.8 zettabytes of data generated per year. So, it's surprising that only four in ten companies have a fully documented disaster recovery plan in place, and 30 percent of respondents have never backed up their data. On World Backup Day, we are all reminded of the importance on implementing a disaster recovery and backup strategy that is secure, compliant and scalable to respond to challenging data protection demands. DRaaS solutions also use scalable infrastructure, allowing virtual access of assets with little or no hardware and software expenditures. Data backups are an essential aspect of any disaster recovery plan, because it's always better to be prepared before a disaster strikes." *Matt VanderZwaag, director of product development, US Signal*

Archived storage adds an extra layer of peace-of-mind

"In 2018 backup and data recovery is critical, and it's not enough for it to simply, well, back up. Evolved options like archive storage solutions can help to eliminate data loss as well as provide added layers of security from tampering, corruption and ransomware – business necessities in today's threat landscape. Archive storage can also help drive cost and performance benefits by allowing for greater long-term retention of data. A fully comprehensive data backup strategy should include business continuity, data protection and enhanced security features on top of fast and efficient storage." *Gary Watson, chief technology officer and founder, Nexsan*

**Backup systems should be top-of-mind at budget time
**

"World Backup Day is a good time to remember to not overlook backup and disaster recovery plans as you budget for your primary datacenter. All flash is becoming a commoditized market and prices are dropping so there's no need to overspend in this area. The deals are out there, but organizations will have to work harder than ever to know if they're truly getting the best deal for the long run on primary storage, which can ultimately free up funds for backup and support solutions." *Bill Miller, chief executive officer, X-IO Storage*

Digital transformation makes data backup more challenging, and critical

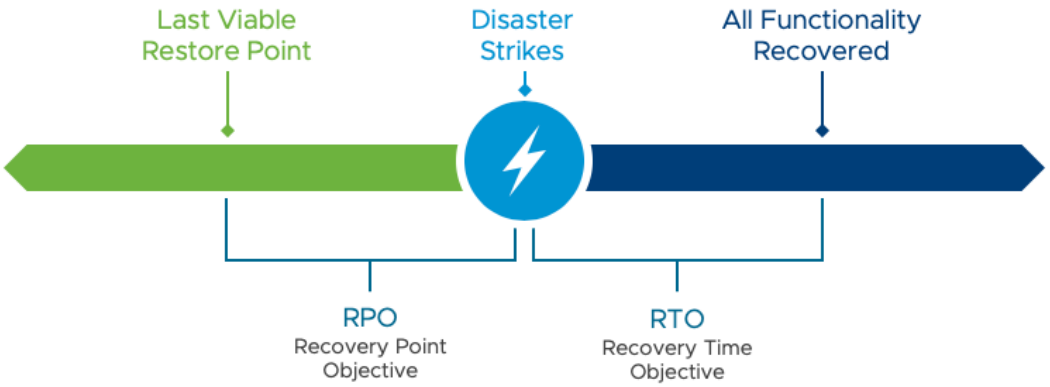
"For many, World Backup Day probably evokes thoughts of 'gold copies' stashed away in a safe place waiting to be retrieved when something goes wrong. However, this simplistic example belies the fact that solutions for these situations are often complex and painful to execute, particularly at the enterprise level as many organizations are undergoing major IT transformations. The truth is that planned and unplanned disruptions are only on the rise, sometimes because of the adoption and innovation of the latest technology. The convergence of these factors will require businesses to look outside traditional backup capabilities and develop an IT resilience strategy that's up to the many challenges of digital transformation. When these capabilities come together, businesses will have an IT resilience strategy to protect their infrastructure and reputation, and also enable innovation and transformation." *Rob Strechay, senior vice president of product, Zerto*

With backups being a screenshot of the past, it's merely impossible to know when you'll need to recover in the time of crisis. It's even more difficult to guarantee that if after a disaster hits that you'll be able to get the business back operational as expected after data is successfully recovered. In the previous section it explains the importance of backing up the whole network and not just server data. You need to know what to focus on when securing data, backing it up, and restoring it successfully to support DRP/BCP organization goals

Here's a few points to add to your considerations when implementing or improving a data recovery program

- Type of data - Organizations must fully understand and comply with GDPR (General Data Protection Regulation) and CCPA (California Consumer Policy Act) rules. You would need to ensure that the data being backed up follows state and government / country laws.

- Recovery Performance - RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are two metrics organizations consider when implementing a disaster recovery plan. Businesses need to know what their tolerance is for being 'offline'. The tolerance and legal obligations will drive the level of investment required to meet those requirements. The return on these investments can be measured through recovery time and recovery points.



- "As ransomware becomes increasingly sophisticated, successful attacks are more prevalent. To respond quickly, enterprises are adopting a holistic ransomware response strategy. The introduction of Polaris Radar to our SaaS platform has expanded upon that idea to accelerate recovery from ransomware with minimal business disruption and data loss." *Chris Wahl, chief technologist, Rubrik Blog*

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

CYBER SECURITY CONTROL #11: SECURE CONFIGURATION FOR NETWORK DEVICES, SUCH AS FIREWALLS, ROUTERS AND SWITCHES

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Factory Defaults

It is extremely important to understand that most, if not all, network devices are shipped from the factory with some default configurations. Common Default Configurations consist of:

- Default Usernames
- Passwords
- Network Configurations
- Unneeded Protocols

These default settings are usually common knowledge and can be easily found by doing an Internet Search.

If left unchanged, these default settings provide for an easy and quick method for bad actors to gain control of your network. These settings may also allow for an attacker to maintain persistence on your network undetected.

CIS# 11.1 Baseline configuration should be well documented and reviewed. Should follow Organization's Configuration Policy.

MAPPING THE CIS V7.1 Control #11 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 1 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Document all the current configurations that exist on network devices. All configuration should be required to adhere to the organization's configuration policy. All initial configurations should be reviewed and audited and any deviations from accepted policy should be documented.

A Baseline Configuration policy is usually a checklist of tasks to be performed for example:

Install all network devices in physically secure locations.
Change default passwords.
Update firmware
Use secure protocols such as SSH and TLS to manage/administer devices
Use strong encryption
Disable any unused interfaces

Synchronize time to a Network Time Protocol Server
Disable any unneeded administrative accounts
Enable password policies
Configure auditing and logging
Restrict access to authorized devices only
Disable all non-secure (deprecated) protocols such as telnet, ftp
Disable unneeded protocols. If you do not use SNMP in your environment, for example, disable it if enabled by default.

Checklist items may be added and deleted depending on your organization's requirements.

CIS# 11.2 Changes to the initial baseline configuration must follow the Organization's Change Management policy.

MAPPING THE CIS V7.1 Control #11 Sub-Control 2 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.2	Network	Identify	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.	ID.AM-3	Organizational communication and data flows are mapped

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 2 as follows:

- CSF Function: Identify
- CSF Category: Asset Management
- CSF Category Identifier: ID.AM-3
    - Organizational communication and data flows are mapped
- Category: 2 - Foundational

New configuration rules should be documented and reviewed and approved by the proper authority in accordance the organization's Change Management Policy prior to implementation.

Sometimes changes on the fly produce unintended consequences and can lead to mistakes and misconfigurations which can increase the risk of a cyber-attack.

CIS# 11.3 Use automated tools to verify and detect changes

MAPPING THE CIS V7.1 Control #11 Sub-Control 3 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.3	Network	Detect	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.	PR.IP-3	Configuration change control processes are in place
						DE.CM-8	Vulnerability scans are performed

The NIST Cyber Security Framework Version 1.1 (CSF) has 2 Mappings for CIS #11 Sub-Control 3 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-3

  - Configuration change control processes are in place
- Category: 2 - Foundational

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-8
  - Vulnerability scans are performed
- Category: 2 - Foundational

The scanning of network devices with commercial automated compliance scanning tools such as Nessus, Nexpose will detect vulnerabilities in these devices. The Greenbone Community Edition vulnerability scanner is an open source tool that can be used to detect vulnerabilities that may exist in the network environment.

All changes must adhere to the organization's Change Management Policy.

CIS# 11.4 Install the latest stable version of any security-related updates on all network devices

MAPPING THE CIS V7.1 Control #11 Sub-Control 4 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				Secure Configuration for Network Devices, such as Firewalls, Routers and Switches *Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*			
11	11.4	Network	Protect	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.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 4 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
  - A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Security-related updates, commonly known as patches are updates to device operating systems and software that mitigate or correct bugs and vulnerabilities as well as introducing new features to devices. These patches are critical to maintaining a mature security posture. Un-patched, and potentially vulnerable systems could be used by attackers to gain unauthorized access, maintain persistence and/or use these devices as pivot points to other network resources.

It is extremely important to implement a patch Management program to allow for timely and efficient installation of software and firmware updates.

Patches must test to ensure proper operation and must also comply the organization's Change Management Policy.

CIS# 11.5 Manage Devices using multi-factor authentication

MAPPING THE CIS V7.1 Control #11 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the risks) transaction (e.g., individuals' security and privacy risks and other organizational

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 5 as follows:

- CSF Function: Protect
- CSF Category: Information Protection Processes and Procedures
- CSF Category Identifier: PR.IP-1
    - A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- Category: 2 - Foundational

Multi-factor authentication is an authentication practice in which two or more methods are used to validate and authenticate users. These factors are typically:

- Something you Have
    - Hardware Token
    - Smartcard
    - Smart Phone
- Something you Know
    - Password
    - Passphrase
- Something you Are
    - Biometrics such as Fingerprint, Face, Voice, or Iris

An additional factor that is currently becoming more mainstream is Location Based Authentication.

This type of authentication would be used to control administrative and user access from different locations in different manners. For example, internal network traffic would have different controls than traffic coming in from a remote site or VPN.

The addition of Multi-factor authentication to your environment will greatly enhance your information security posture. If one of the factors is compromised, for example a stolen password, an attacker will still need an additional factor able to gain access.

CIS# 11.6 Use a dedicated machine for all administrative tasks.

MAPPING THE CIS V7.1 Control #11 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.6	Network	Protect	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.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 6 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-5
    - Network integrity is protected (e.g., network segregation, network segmentation)
- Category: 2 - Foundational

A separate workstation should be assigned to each Administrator to be used strictly for the administrative management of the network infrastructure. This workstation that should not be used for email, Internet access or any other task that is not related to the administration and configuration of network devices.

It is desirable that this system’s connection is restricted to the organization's control network(s), is only accessible locally with no remote access and does not have access to the Internet.

CIS# 11.7 Use a separate management VLAN with no connection to production networks for access to networking devices.

MAPPING THE CIS V7.1 Control #11 Sub-Control 7 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11				**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** ***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***			
11	11.7	Network	Protect	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 VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #11 Sub-Control 7 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-5
    - Network integrity is protected (e.g., network segregation, network segmentation)
- Category: 2 - Foundational

Network Devices should be configured so that the actual administration can only be performed on a "control network" that is completely segmented from the organization's production networks.
This type of network segmentation will reduce the risk of an attacker changing the configuration of your network devices.

This network should be on a Separate VLAN, that is NOT routable to the production network, and is NOT connected to the Internet.

In addition to the recommended sub-controls, Network devices must be managed and maintained periodically to ensure the proper security controls and procedures are in place.

Periodic management of network devices will assist you with discovering misconfigurations, one-off temporary configurations and mistakes that have been left uncorrected.

Ongoing management of network devices should include Traffic Flow monitoring and log auditing.

It is advisable to periodically review and refresh devices as configurations tend to become dated and less secure over time. This management plan will also allow for the update of access control rules to accommodate new access requirements. In addition, an organization will be able to mitigate new and emerging threats, to check for anomalies and discover inconsistent ruleset configurations.

CIS #12: Boundary Defense

CYBER SECURITY CONTROL #12 BOUNDARY DEFENSE

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multilayered, relying on firewalls, proxies, DMZ perimeter networks, and network based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing because of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

MAPPING THE CIS V7.1 Control #8 AND #12 TO THE CYBER SECURITY FRAMEWORK

The Cyber Security Framework (CSF) has 3 Mappings for CIS #8 and 4 Mappings for CIS #12. Those that are relevant to this article, but not limited to, are:

- CSF Function: Detect
- CSF Category: Anomalies and Events, Security Continuous Monitoring, Detection Processes
- CSF Category Identifier: DE.AE, DE.CM, DE.DP
- CSF Control: DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
- CSF Control: DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
- CSF Control: DE.AE-5: Incident alert thresholds are established
- CSF Control: DE.CM-1: The network is monitored to detect potential cybersecurity events
- CSF Control: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
- CSF Control: DE.CM-4: Malicious code is detected
- CSF Control: DE.DP-4: Event detection information is communicated to appropriate parties
- Category: 2 - Foundational

TOOLS TRIED/USED/INVESTIGATED

Darktrace, BluVector, CyberadAPT

SEE CIS #8 FOR FULL SYNOPSIS & MAPPING (PG 67)

CIS #12.6: Deploy Network-Based IDS Sensors

MAPPING THE CIS V7.1 Control #12 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
12				**Boundary Defense**			
				Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.			
12	12.6	Network	Detect	Deploy Network-Based IDS Sensors	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.	DE.CM-1	The network is monitored to detect potential cybersecurity events

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #12 Sub-Control 6 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-1
    - The network is monitored to detect potential cybersecurity events
- Category: 2 - Foundational

Intrusion detection system (IDS) software is designed to automatically alert administrators when there is an attempt by someone or something to compromise an information and communication technology (ICT) system through malicious activities or through a security policy breach.

An IDS operates by monitoring ICT activity, examining system vulnerabilities, evaluating the integrity of files and by conducting an analysis of patterns based on already known attacks. In addition, IDS technology monitors the internet to search for new emerging threats which could result in a future intrusion of an ICT system.

There are three primary components of IDS technology: (Techopedia, 2018)

- Network Intrusion Detection System (NIDS) - This performs analysis for traffic on a whole subnet and will match to attacks already known in a library of known attacks.

- Network Node Intrusion Detection System (NNIDS) - This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.

- Host Intrusion Detection System (HIDS) - This takes a “picture” of an entire system’s file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the system administrator.

Topology – IDS Technology Deployment

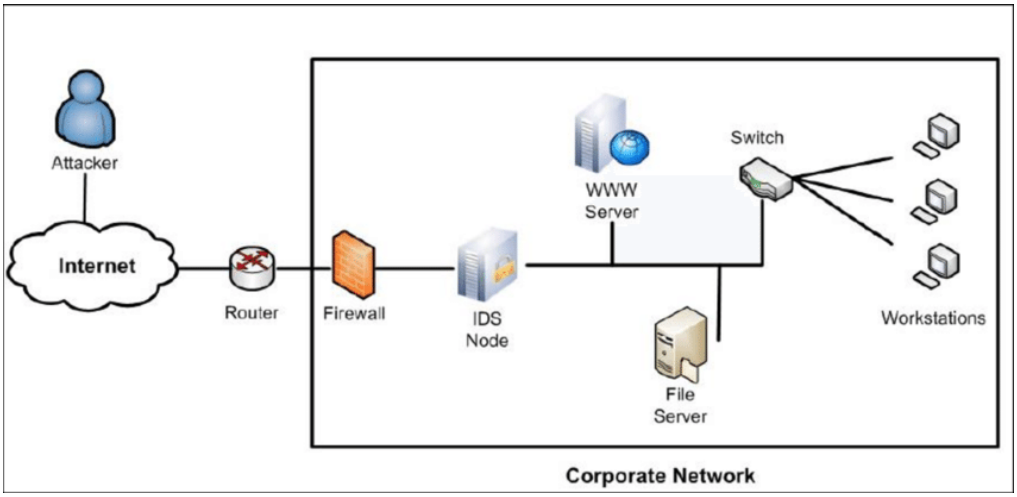


Figure 1. Placing IDS in a Network

Before deploying IDS technology, understanding network topology and network traffic is key to deployment success. Marta (2016) cites four areas to consider before deploying an IDS:

- How much traffic is expected?
- Type of traffic expected?
- Quantity of connections between network and internet?
- Complexity of network – small, medium, enterprise?

TIP - Initially deploy IDS devices with default rules. This will provide a baseline from which to work when you adjust IDS settings. Upon deployment, fine-tune the device to ensure that the alerts you see reflect actual and actionable events. As an example, you can set the event action override to drop packets with a risk rating greater than 90% because if you have too many events, it quickly becomes difficult to determine which are false positives. If you have too few, then the IDS is not doing its job and you run the risk of getting false negatives.

CIS #12.7: Deploy Network-Based Intrusion Prevention Systems

MAPPING THE CIS V7.1 Control #12 Sub-Control 7 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
12				**Boundary Defense** ***Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.***			
12	12.7	Network	Protect	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.	DE.CM-1	The network is monitored to detect potential cybersecurity events

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #12 Sub-Control 7 as follows:

- CSF Function: Detect
- CSF Category: Security Continuous Monitoring
- CSF Category Identifier: DE.CM-1
    - The network is monitored to detect potential cybersecurity events
- Category: 2 - Foundational

An intrusion prevention system (IPS) is technology that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log information, attempt to block the identified activity and report activity to an administrator for review.

Intrusion prevention systems are deployed to function as a security filter for malicious activity. IPS technology can analyze and take automated action to classify network traffic. Those actions can include alerting administrators, dropping dangerous packets, blocking traffic coming from the source address(es) of malicious activity, and restarting connections. One negative aspect of an IPS is the ability through too strict filtering which may hinder network performance. In the end, the goal of an IPS is to work in real-time identify malicious activity and notify system administrators while avoiding false positives.

Topology – IPS Technology Deployment

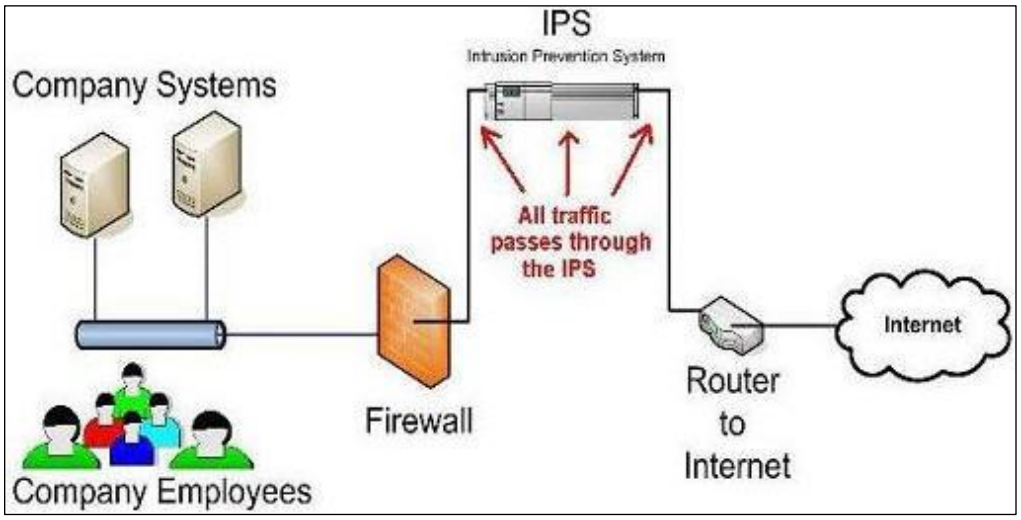


Figure 2. Placing IPS in a Normal Network

TIP – When deploying an IPS run in monitor mode until the system is properly tuned. This will result in functionality as an IDS where the system will identify potential threats but not block the flow of network traffic. In addition, keep the number of "block" mode rules to a small, finely tuned set to reduce the possibility of false positive blocks. And lastly, consider using a fail-open device to limit the effect of a device failure on your network. In the event of an IPS failure, this allows all traffic to continue uninterrupted. While it's a less-secure configuration, it keeps the network up and running.

Analysis – What is the difference between IDS and an IPS?

By Panda Security

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) deployments increase the security level of networks, monitor traffic and inspect and scan packets for suspicious data. Detection in both systems is mainly based on signatures already detected and recognized – know threats.

The main difference between IDS and IPS is the action they take when an attack is detected in its initial phase (network scanning and port scanning).

- Intrusion Detection System (IDS) technology provides the network with a level of preventive security against any suspicious activity. The IDS achieve this objective through early warnings aimed at systems administrators. However, unlike IPS, it is not designed to block attacks.
- Intrusion Prevention System (IPS) technology is a device that controls access to IT networks to protect systems from attack and abuse. It is designed to inspect attack data and take the corresponding action, blocking it as it is developing and before it succeeds.

Comparative Analysis – What is the difference between IDS, IPS and NGFW Technology?

Firewall technology is somewhat simplistic – function in a networked environment and block unauthorized traffic while permitting communication. Firewalls reside between a local network and the internet, and ultimately filters traffic that might be harmful to an ICT system.

Comparing NGFW technology to IDS and IPS platforms, Pritha (2016) draws comparison to a firewall as security personnel at the gate and IDS technologies as a security camera after the gate. A firewall can block connections, while an IDS cannot block connection, but can alert any intrusion attempts to a security administrator to act and evaluate network vulnerabilities. In comparison to IPS deployments, NGFW have greatly advanced and now combined L3/L4 packet filtering with deep packet inspection in addition to IPS technology.

To understand NGFW capabilities and evaluate against IDS and IPS technologies, Pritha (2016) identifies the **Top 9** features of NGFW technology.

1. Application Awareness – NGFW identify, allow, block or limit applications regardless of port, protocol etc. This provides visibility into unknown & proprietary application within the organization network.

2. Identity Awareness – NGFW supports identity awareness for granular control of applications by specific users, group of users and machines that the users are using.

3. **Centralized Management, Administration, Logging and Reporting -** Separate management solution is available for management, logging and reporting. This tool is also used to export firewall rules set and configuration. Centralized management provides administrator with security health dashboard to view the happenings and traffic patterns and associated risks in network in real time.

4. State-full Inspection – NGFW tracks the connections from layer 2 to layer 7 (even layer 8 due to identity awareness) in contrast with the traditions firewalls which tracks the traffic from layer to layer 4. This difference allows a lot more control and provides the organizations the ability to have very granular policies.

5. Deep-Packet Inspection - Deep packet inspection (DPI) is one of the prior features of next-generation firewall (NGFW). DPI can rapidly identify and then block Trojans, viruses, spam, intrusion attempts and any other violations of normal protocol communications.

6. Integrated IPS - In an environment where a traditional firewall is deployed, it is common to see an IDS or IPS deployed. With a NGFW technology the IPS or IDS appliance is fully integrated. It can be activated and de-activated when required. The IPS functionality itself is the same as it was with a separate appliance; the main difference is in the performance and accessibility of the information from all layers of traffic.

7. **Able to monitor SSL or other encrypted traffic – NGFW technology** can monitor SSL and HTTP tunneled traffic flows. To secure encrypted traffic, the NGFW supports all inbound and outbound SSL decryption capabilities. This helps organizations identify and prevent threats and malware in encrypted network streams.

8. **Integration with other security solutions – NGFW** is capable with integrating with other security solutions such as SIEM tools, reporting tool, two factor authentication systems etc. This enhances the overall capability of security systems of an organization.

9. **Inbuilt Antivirus and Anti-Bot solution – NGFW technologies** have an inbuilt antivirus engine and able to inspect https traffic on in real-time for infected files. These protections are available for protocols like HTTP, HTTPS, FTP, POP3, SMTP, SMB etc. They are also capable of identifying malware coming from incoming file and malwares downloaded from internet.

Why is this control important?

Even the most secured networks can be susceptible from un-trained employees who lack good cyber-hygiene. Ultimately, people are an organization's greatest weakness when it comes to protecting itself from attack. People are who install security software, schedule security patches, enforce internal policies, or receive phishing emails are at risk. Proper security awareness, or cyber-hygiene, is an organization-wide requirement. Everyone has their own responsibility to protect themselves and the company from outside attacks. Non-technical personnel must be aware of social engineering attacks and how to spot them. System administrators must be aware of vulnerabilities in their system and how to fix them. And IT-operations personnel must be aware of the security implications involving who and what is on the network.
Physical security integrators face a unique risk because of their access to larger corporations' networks. Many attackers are choosing to target vendors with the goal of gaining access to the bigger clients of said vendor. Integrators often have hundreds of end users connecting to clients' networks daily. Because of this, its crucial integrators have a proper employee training and awareness program implemented to protect both themselves and their clients from attackers.

An effective training and awareness program will consist of multiple elements:

EDUCATION

Naivety and a lack of knowledge are two of the primary reasons personnel fall victim to attacks. The education component must teach users why they are targets, how attackers target them, and the implications for both themselves and organizations if falling victim. Showing organization-wide implications is particularly important since many cybersecurity policies are viewed as "cumbersome" or
"ridiculous". An education program must show every individual person why these policies must be followed, as well as the role each person plays in protecting the organization.
-Security Software. Many high-risk actions by users such as storing password on notes or visiting dangerous websites while on an organization-provided device can be prevented by software.

- Password managers allow users to store thousands of passwords inside a digital "vault." Thus, preventing the need to write down passwords on paper. Password managers are particularly useful for integrators because often many technicians will use the same credentials to access a client's network. Instead of emailing passwords, another high-risk action, certain password managers allow users to share passwords with other users through an encrypted connection.

- Internet traffic blockers are also a very important software organizations can utilize to better protect users from visiting malicious websites.

- Email security software should be utilized by any organization, no matter the size. Email is the number one method used by attackers against a company. Email security software varies greatly by product, but a basic

one should include scanning attachments and URLs for malicious content, encryption for all emails sent and received, virus scanning, and spam protection.

TRAINING

Education combined with training is the best strategy for employees to improve their cybersecurity awareness. Employees must be given the ability to implement the cyber-hygiene education they received. Training is crucial for employees to fully retain what they have learned, and it is a necessary element of any security training and awareness program. A proper training program should:

- Be part of new employee on boarding. From Day 1, employees should be receiving cybersecurity training
- Be continuous and always evolving. New threats emerge every day, so a training program should always be changing allowing employees to be up to date.
- Involve a learning management system that is fun and engaging for existing employees.
- Put more emphasis on where employees have improved instead of where they failed. Recognition of improvement is crucial to get employees to support the organization's cybersecurity goals.
- Be tailored to each individual's role inside the organization. HR personnel will face different attacks than C-suite executives. Social engineering attacks are personalized for a specific person, so each employee must be able to recognize the types of attacks they are most likely to see.
- Involves periodic testing. Testing is important for employees to put their training to practical use. Having real-life examples to compare to will help when an employee is faced with an actual attack.

It's important to not only continually train employees, but also continually reward and recognize them for improvement. If an employee spots a phishing email, notify the whole company about their accomplishment. Showing employees first-hand how they protected the company from attack will encourage them to continually improve their cyber-awareness. Since cybersecurity is an everchanging landscape, its crucial for employees to be aware of the most recent threats and how to protect themselves. An effective training program will include new and emerging threats.
The above actions outline important and crucial elements of an effective cybersecurity awareness training program. When implementing such a program, it is very important to think of cybersecurity as both a technical and human problem. Technical solutions and protocols can only provide so much protection. Ultimately, people are the weakest link when it comes to cybersecurity. Organizations must promote good cyber-hygiene and provide employees with the education and training needed to improve their cybersecurity awareness.

CONCLUSION

With the continued advancement of threats aimed at global ICT systems, advanced training and awareness are a foundational requirement before the deployment of layers of security considering IDS, IPS and NGFW technologies. This paper concludes while IDS and IPS technology deployments have historically offered protective security programs over ICT systems, NGFW technology offers more robust options while converging technologies to manage a security technology program.

While IDS and IPS technologies in practice have and will continue to subside to NGFW technologies, NGFW deployments will in time give-way to the advancement of cloud hosted security Software as a Service (SaaS) platforms. In totality – the consensus is the deployment of IDS, IPS and NGFW technologies will recede due to the explosive expansion of cloud-hosted and security SaaS platforms. Supporting this position, Plato (2018) identifies

four possible positions that outline the projection of on-premise security technology deployments; 1) network perimeter is gone, 2) NGFW are not designed for cloud architecture, 3) cloud and SaaS providers can offer better capabilities for fractional cost, and 4) security breaches cannot necessarily be prevented from deployment of IDS, IPS or NGFW technologies.

In the end, with the vast advancement of cloud hosted SaaS technologies and the exponential growth of cloud computing the most likely future for Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Next Generation Firewalls (NGFW) – Rest in Peace…

CIS #14: Controlled Access Based on Need to Know

CIS Control 14 is defined as "The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CIS #14.1: Segment the Network Based on Sensitivity

MAPPING THE CIS V7.1 Control #14 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

14				**Controlled Access Based on the Need to Know** ***The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.***			
14	14.1	Network	Protect	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).	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #14 Sub-Control 1 as follows:

- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-5
    - Network integrity is protected (e.g., network segregation, network segmentation)
- Category: 2 - Foundational

The first step in being able to control your data is to create a security policy. You can find resources on the PSA Security website www.psasecurity.com/resources/tools. Under the Cybersecurity tools follow the link to Information Security Policy Templates. This will take you to www.sans.org/security-resources/policies where you will find templates for various security policies.

The security policy should define how to classify or label your data as well as what level of protection should be applied based on that classification. When labeling the data, the value of the data to the organization or owner must be determined. Ultimately the goal is to protect the confidentiality and integrity of the data.

The Federal Government has clearly defined labels that get applied to all their data. Those being Top Secret, Secret, Confidential, Sensitive by Unclassified and Unclassified. Each classification is based on the potential damage to National Security the information could pose in the wrong hands. For more information on these classification levels you can visit this link
https://en.wikipedia.org/wiki/Classified_information_in_the_United_States

In the private sector, there is not one standard for classifying data. Many examples exist of classification schemes. An example of a classification scheme could be Confidential, Private, Sensitive and Public. The classifications you choose should be documented in your security policy and should reflect the value of the data to your organization.

You will also want to segment your network based on your data classifications. This can be done using Virtual Local Area Networks otherwise known as VLANs. Within a network, you may have several VLANs. A VLAN is a logical grouping of network resources and access to each VLAN can be specified and controlled.

At a minimum, you will want to segment data that is public from data that is private. Your company may have a customer portal or website where data is available to the public.

This data should be segmented away from your private data on your internal network. Likewise, within your internal network, you may need to segment data further based on its classification.

All employees may need access to common data, while sensitive data such as financial information and Human Resources documents may be restricted based on an employee's role within your organization. Likewise, it is a good practice to segment the management of your data and network to a VLAN that is only accessible to employees responsible for that management.

You may also need to segment your customer's data. Customer data may be sensitive in nature. Not all employees should have access to Customer data. This access should be given based on Need to Know and valid permission to access the data. Contract requirements may dictate that you have a separate VLAN for a customer's data.

Careful planning should go into the development of your security policy, data classification and network segmentation to ensure data is protected appropriately.

CIS #14.4: Encrypt All Sensitive Information in Transit & 14.8 Encrypt Sensitive Information at Rest

MAPPING THE CIS V7.1 Control #14 Sub-Control 1 TO THE CYBER SECURITY FRAMEWORK

14				**Controlled Access Based on the Need to Know** ***The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.***			
14	14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	PR.DS-2	Data-in-transit is protected

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #14 Sub-Control 4 as follows:

- CSF Function: Protect
- CSF Category: Data Security
- CSF Category Identifier: PR.DS-2
    - Data-in-transit is protected
- Category: 2 - Foundational

Additional protection can be achieved by using encryption. Encryption uses algorithms to make the data undecipherable without the encryption key. There are several types of encryption algorithms. Some encryption types are suited for protecting email and other files in transit and others are suited for protecting files at rest.

Sensitive data must be protected while in transit. If data is not encrypted, it can be intercepted during transmission. This can affect the confidentiality of the data. If sensitive data is transmitted and intercepted, it could be used against your organization. For example, financial information that is intercepted could be used to steal from your company. Additionally, the integrity of the data could be lost. A hacker could intercept your sensitive data, alter it and send it on to the recipient changing the content before being delivered.

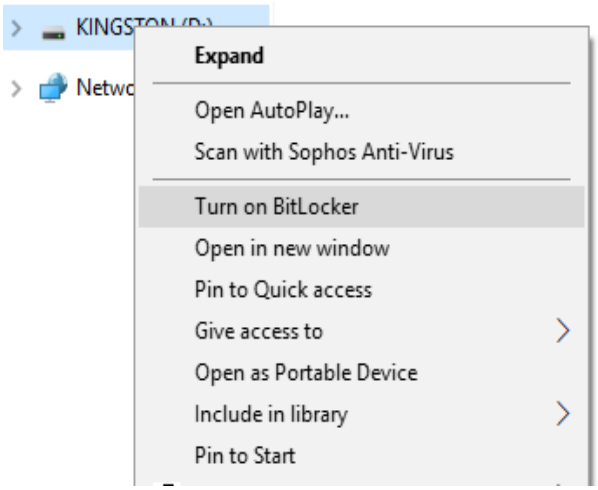
Many file share programs such as ShareFile, Dropbox, Box, Google Drive and others support password protection and encryption of files before transmission. When encrypting and sending files, you will need to send the encryption key and/or password for the intended recipient to open the file. Most email programs offer tools for sending encrypted emails. The recipient will need to utilize the same tool to receive the email. Don't send the password for your file through a standard email. Emails are transmitted in plain text and can be intercepted.

Sensitive data should also be encrypted while at rest. Think of a laptop computer. Many users store files on their laptop. These files could be sensitive data. The risk is that the laptop could be stolen, and the data could be accessed. You protect the operating system with a username and password, however the hard drive could be

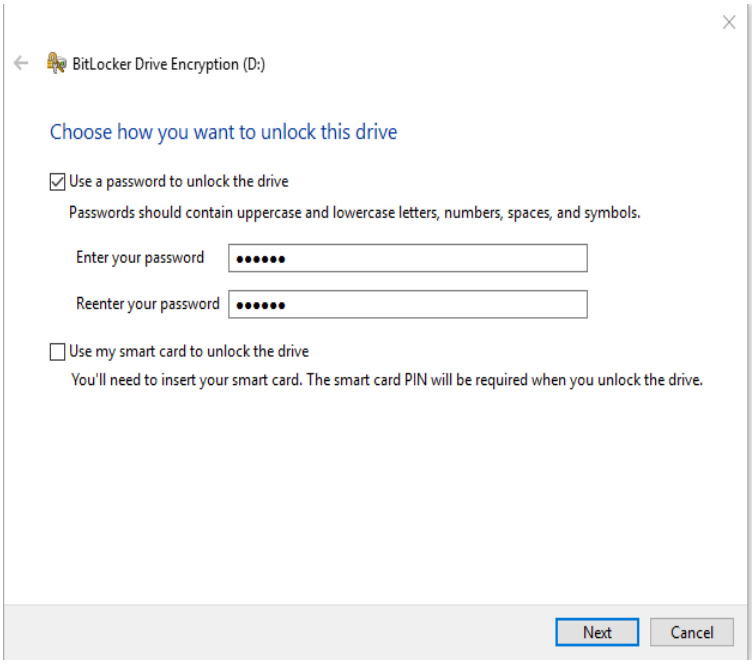
removed and accessed. There are tools available to turn a hard drive into a USB drive for access. To protect against this, the hard drive can be encrypted to protect the data. When the hard drive is encrypted, the data is not decipherable without the encryption key. Microsoft supports encryption of the hard drive or USB drive via a feature called BitLocker. Encryption can be enabled through the OS. Bitlocker can encrypt both hard drives and USB Drives.

To enable Bitlocker encryption:

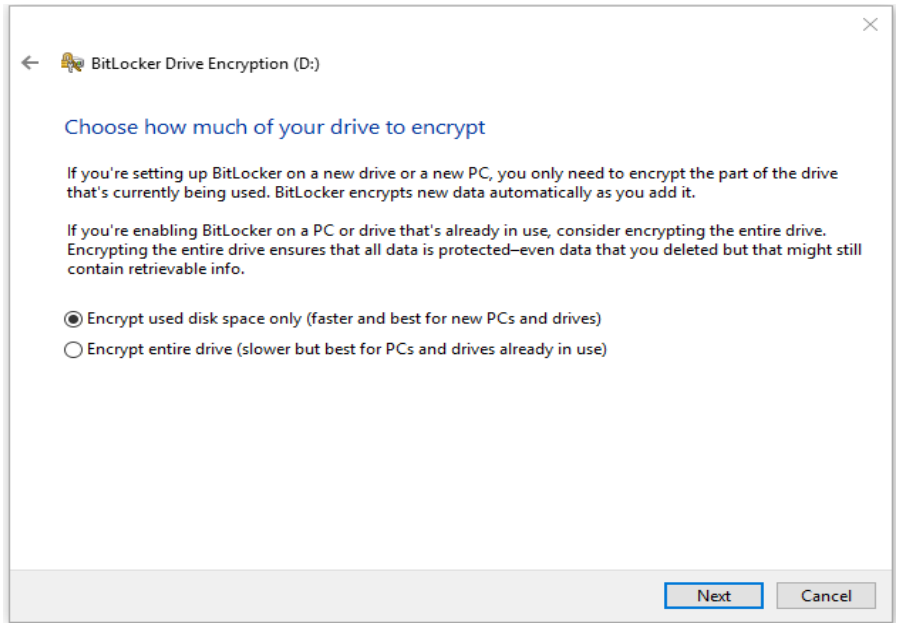
1. Locate the drive in File Explorer and right click. Choose "Turn on Bitlocker"



2. Choose to either use a password or smartcard to unlock the drive

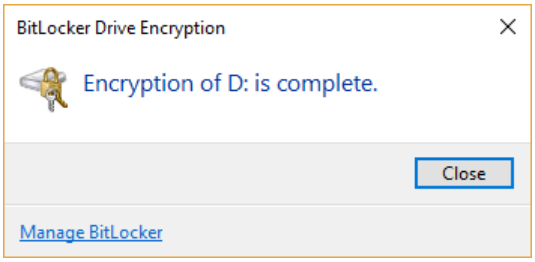


3. Save your backup recovery key in a location you can access
4. Choose whether to encrypt just the data in use or the entire drive. Windows gives you direction on which may fit best.



5. Choose the appropriate mode for encryption. Pay attention to the guidance Windows provides.

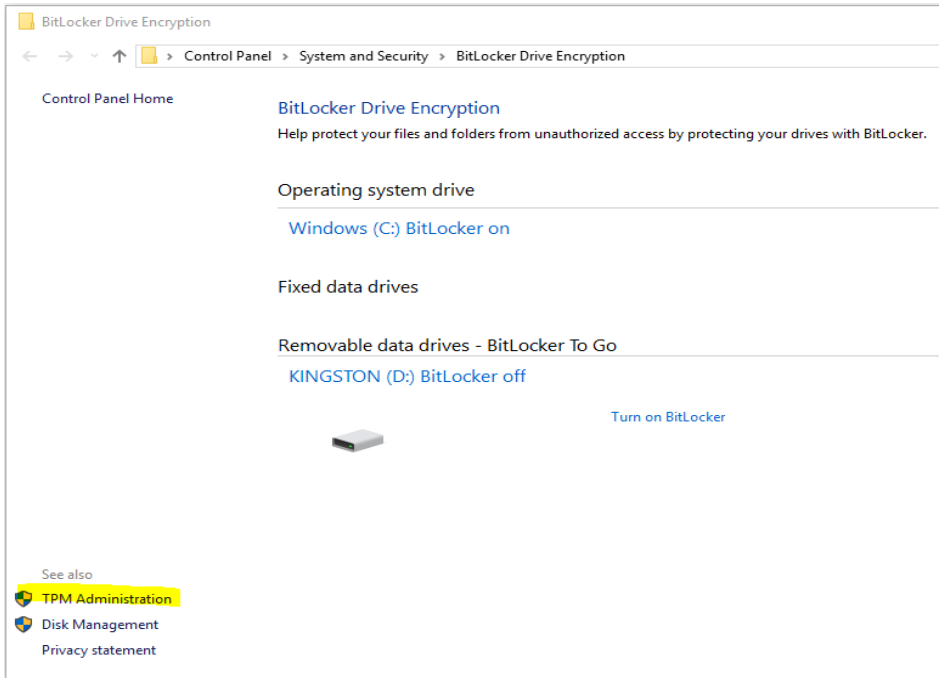
6. Select “Start Encrypting”



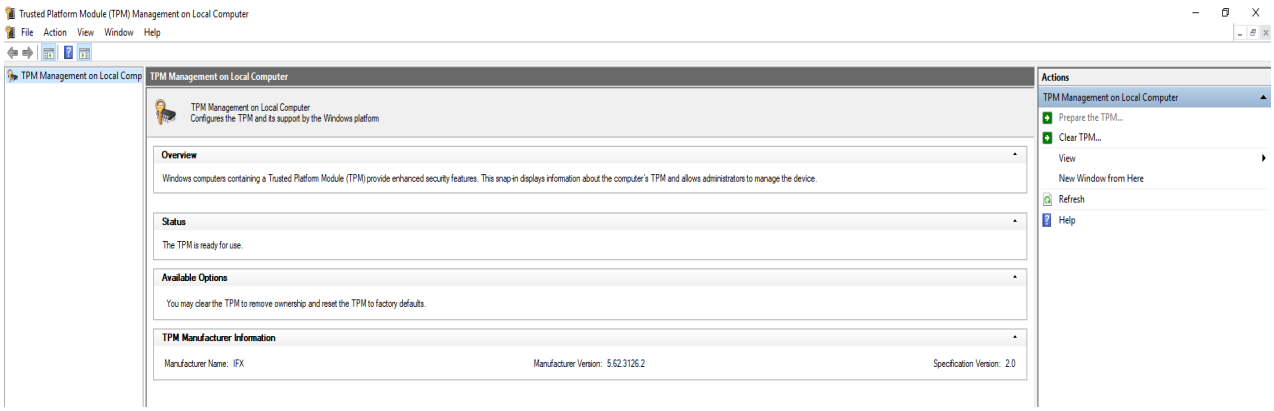
For more information on Bitlocker, visit the knowledge base by Microsoft here: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Additionally, your computer may be equipped with a TPM or Trusted Platform Module. The TPM is a piece of hardware that is incorporated into your laptop or PC. The hard drive can only be decrypted using the TPM. This ensures that if the hard drive were to be stolen, without the TPM, the data could not be accessed.

To view information about your TPM module choose TPM Administration from the Bitlocker management screen.



This will display the TPM Management screen. Here you can find general information on the TPM.



For more information on TPM, visit the knowledge base by Microsoft here: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

CIS #14.5: Utilize an Active Discovery Tool to Identify Sensitive Data

MAPPING THE CIS V7.1 Control #14 Sub-Control 5 TO THE CYBER SECURITY FRAMEWORK

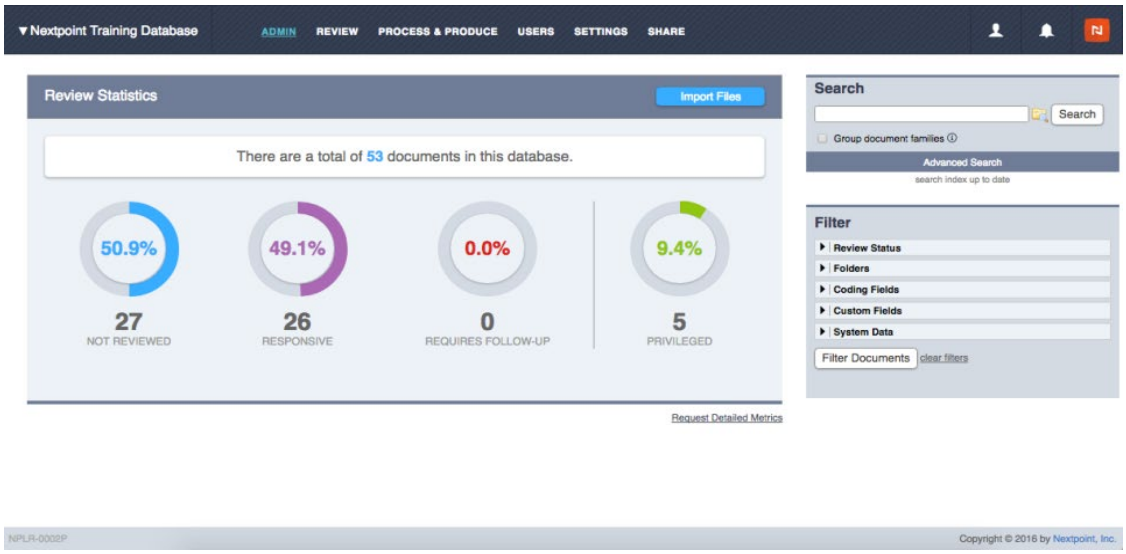
14				**Controlled Access Based on the Need to Know** ***The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.***			
14	14.5	Data	Detect	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, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.		

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #14 Sub-Control 1 as follows:

- CSF Function: Detect
- CSF Category:
- CSF Category Identifier:
    - o
- Category: 2 - Foundational

The next step is to locate and document where your sensitive data is. Data can be dispersed in various locations in your organization. It could reside on a server, a workstation or laptop, a USB drive or even in cloud storage. It is important to understand where all your sensitive information is located. This can be a daunting task. Fortunately, there are commercial eDiscovery products that can assist you in locating and documenting where your sensitive data is located. Do your due diligence when searching for an eDiscovery tool. Their feature sets and strengths will vary. Some of the common products available on the market are Logikcull, Lexbe, Nextpoint and CloudNine. Many of these products can search both on premise and cloud-based storage.

Here is an example of the user interface for Nextpoint, a web-based eDiscovery tool.



In this example, the software has been used to scan a database and provide information back on the information discovered.

Your organization likely stores, processes and transmits a large amount of data daily. Think about all the ways you interact with data daily. You may receive and transmit data for functions such as accounting, purchasing products or even processing credit card payments. You also transmit data inside and outside your organization through email, file share and cloud services.

You will need to locate and document your data before applying labels to it. The benefit of using an eDiscovery tool is ensuring that all the data is discovered and labelled. An incomplete inventory of your data can lead to inconsistent or incomplete protection of your sensitive data.

CIS #14.6: Protect Information Through Access Control Lists

MAPPING THE CIS V7.1 Control #14 Sub-Control 6 TO THE CYBER SECURITY FRAMEWORK

14				**Controlled Access Based on the Need to Know** ***The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.***			
14	14.6	Data	Protect	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.	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for CIS #14 Sub-Control 6 as follows:

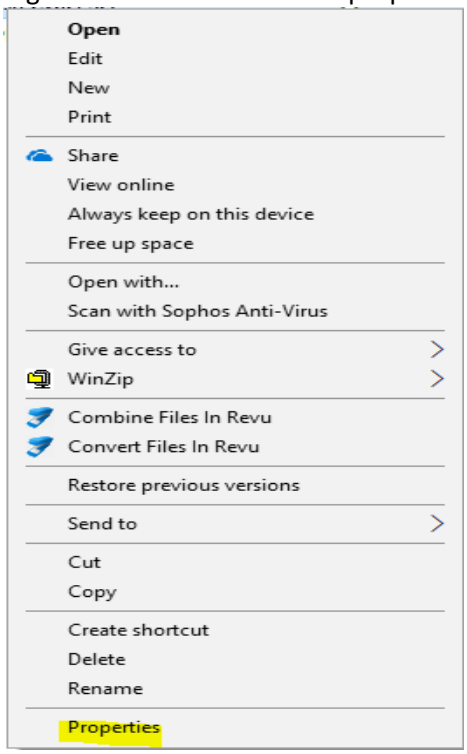
- CSF Function: Protect
- CSF Category: Identity Management and Access Control
- CSF Category Identifier: PR.AC-4
    - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- Category: 2 - Foundational

Like a card access system, information systems use access control lists. The data may be located on a server, a file system, in the cloud, an application or even a database. The access control list dictates if the user can view, create, edit and/or delete the data. The level of protection applied to the data is determined by the data owner. There are multiple types of access control systems, but they primarily fall into one of two categories: discretionary or role-based access control.

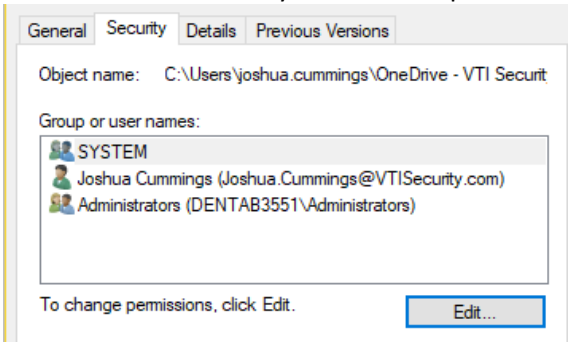
In a discretionary access control model, the owner of the data determines for each user what their permissions are to the data. This type of model can be complex and requires individual file or folder management. The most common application of this model may be the files system within an operating system such as Microsoft Windows.

You can view and/or edit the permissions of any file within Windows by doing the following steps:

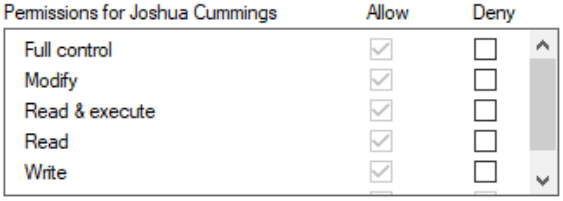
1. Right click the file and select properties



2. Then Select the Security Tab at the top and choose Edit



3. Here you can add and remove users who have access to the file. You can also set their permissions for Full Control, Modify, Read & execute, Read, Write or Special Permissions



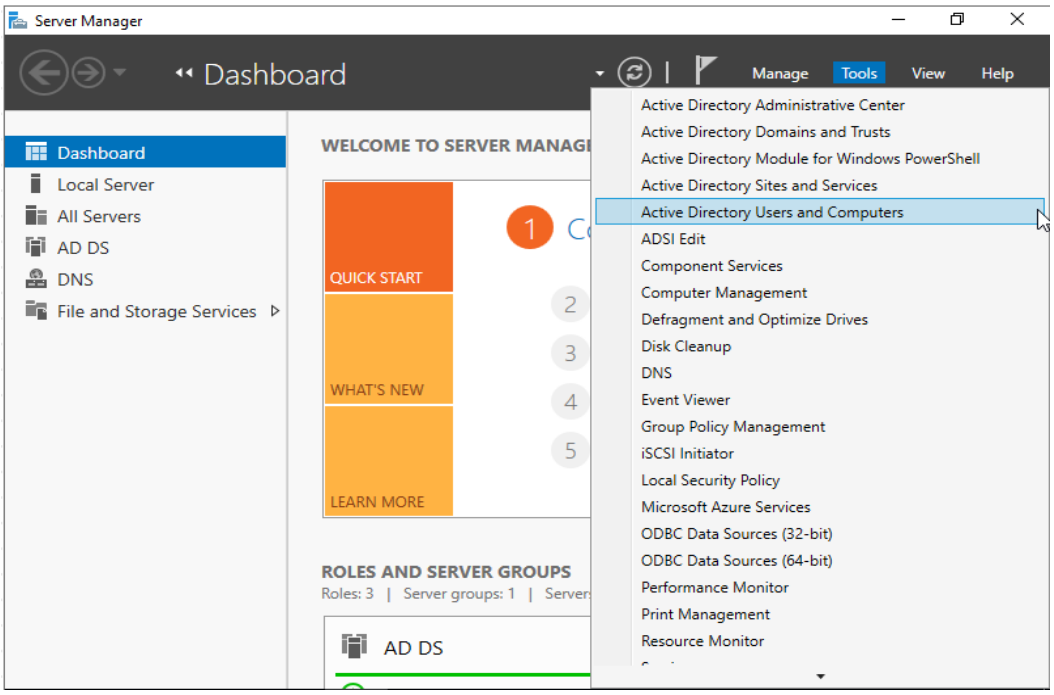
4. This can be done on a folder level as well where the permissions are pushed down to all files in the folder

In a role base access control model, users are grouped together, and the group is given permissions to data as demonstrated above. This model allows for easier management of data permissions. The permissions can be modified centrally and pushed out to the users in the group. A common example of this type of access control would be Active Directory. Above, you saw how permissions can be granted to individuals as well as groups.

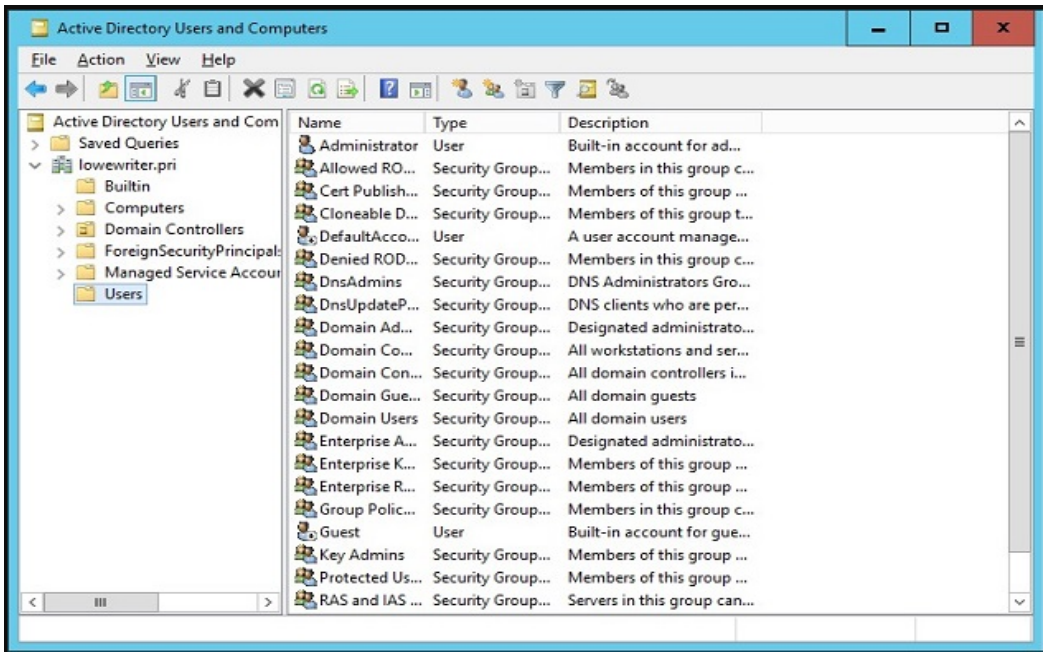
In this example, Windows allows the grouping of users. Then the group is given permissions to create, view, edit and/or delete data. Users can be added and removed from the group and permissions are changed without having to modify each file or folder. Likewise, when permissions changes are needed, the group is modified and all users in the group inherit the changes.

Follow these steps for adding groups or users to an Active Directory account.

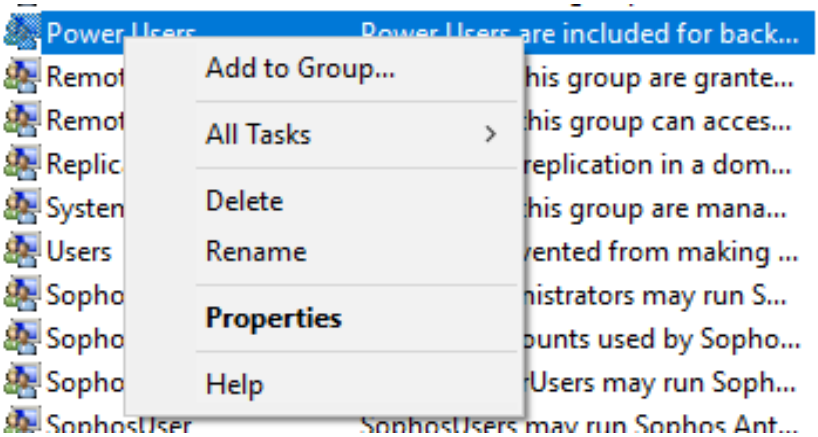
1. On the Directory Server, open Server Management and choose Tools – Active Directory Users and Computers



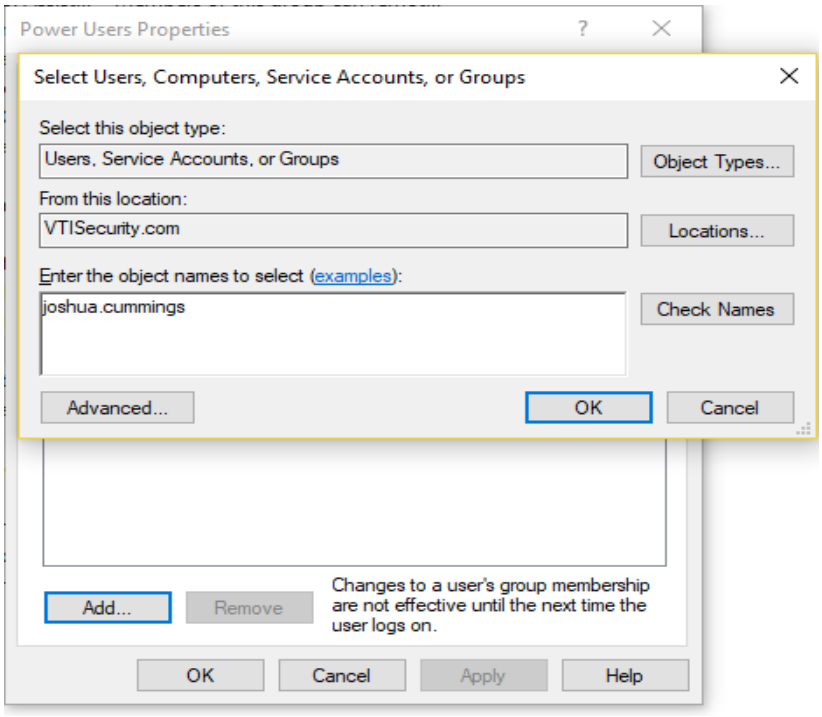
2. Select the Users folder, here you will see groups and users



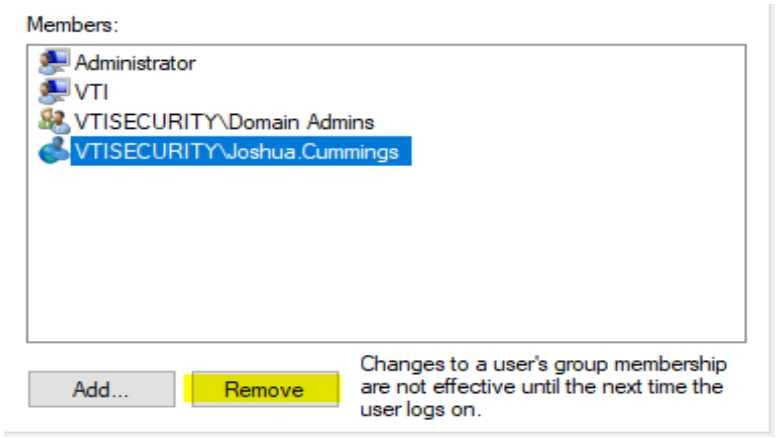
3. Right click the group you want to modify and choose properties



4. Add users by choosing add. Type in their username and choose check names



5. Remove users by highlighting the user and choosing Remove



It is very common to use a mixture of access control lists based on the type of system being used and the data being protected. As with the examples, within the Windows operating system, we see both types of models in use.

CIS #15: Wireless Access Control

Function: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

MAPPING THE CIS V7.1 Control #15 TO THE CYBER SECURITY FRAMEWORK *2

Of the Ten Sub-controls of this CIS control we are focusing our efforts on the four Sub-controls highlighted below. Sub-control 15.1 Identify has already been performed as a part of this exercise. The other three functions Map to Protect (PR) Sub-category Access Control (AC) of the CSF.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
15				**Wireless Access Control** ***The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.***			
15	15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	ID.AM-3	Organizational communication and data flows are mapped
						DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
15	15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
15	15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	PR.DS-2	Data-in-transit is protected
15	15.10	Network	Protect	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.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)

WHY IS THIS CIS CONTROL CRITICAL?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelers are infected on a regular basis through remote exploitation while on public wireless networks found in airports and cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment. *1

RISK ADDRESSED

In this environment, there is only ONE network. All the workstations, including those with financial, customer and central station data (critical data) are on the same network and router as the wireless and guest wireless WLANS. There are 43 wireless devices on this network, eleven of which are BYOD smart phones or tablets. This environment provides for extreme vulnerabilities because: 1.) There is no separation between the Wireless LANS and the Corporate Network. Anybody with access to the wireless network can find their way onto the corporate network. 2.) Eleven of the devices are BYOD and there is no control of OTHER networks that the devices might be exposed to malware on. And if exposed to malware could ultimately be transferred to the Corporate LAN by way of the WLAN(s). 3.) Since the credentials for the Guest WLAN are public and not updated regularly the entire network is exposed to any perpetrator within wireless range of the building.

INITIAL STEPS TO MITIGATE VULNERABILITIES

Performed comprehensive assessment to identify and log all wireless devices communicating on the network [CIS 15.1]. 2.) Identified the wireless devices that could communicate hardwired instead of wirelessly and deactivated the wireless connection from the devices [CIS 15.4]. 3.) Assure that Advanced AES is the encryption standard employed in the Wireless router(s) and required credentials for connection to network [CIS 15.7].

SECONDARY STEPS TO BE PERFORMED WITHIN 30 DAYS:

Create four new and totally separated (Air Gapped) networks for the environment [CIS 15.10]:

1. Network #1: Hardwired Network (Corporate LAN) used only for critical data in Rest, Transport and Use
2. Network #2: Hardwired Network (DMZ) used only for test-bed equipment and internet facing devices that can be browsed to
3. Network #3: Wireless Network for authorized wireless assets using AES protection. Typically, smart devices used only for data in transit and Use via Azure Cloud Services.
4. Network #4: Open Wireless Network for guest user wireless connections employing basic password protection

PROS & CONS:

This is a relatively simple security exerCISe that has a large and immediate security impact compared to other Controls. It can typically be deployed quickly. There really is no downside to the exerCISe sans for the temporary inconvenience to Wi-Fi system users.

TIME SPENT:

Less than one week to perform the analysis and then design and implement the solution.

EXPECTED OUTCOME:

That vulnerabilities to an open wireless network are closed. That all critical data is segregated from Wi-Fi connections used by guests and vendors. All test labs and internet facing wireless devices are on a dedicated network so that objectives can be easily met without exposing critical data to vulnerabilities. Day-to-day wireless devices (typically remote) with access to cloud service (Azure) communicate conveniently with AES encryption.

RETURN ON INVESTMENT:

Aside from people either accidentally or intentionally introducing Malware to a network, wireless networks are the most vulnerable and susceptible to attack. The ROI is immediate considering the simplicity and time spent to deploy versus the vulnerability that is mitigated.

CIS #17: Implement a Security Awareness and Training Program

MAPPING THE CIS V7.1 Control #17 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
17				**Implement a Security Awareness and Training Program** ***For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.***		
17	17.1	N/A	N/A	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.		
17	17.2	N/A	N/A	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	PR.AT-5 PR.AT-4 PR.AT-3 PR.AT-2 PR.AT-1	Physical and cybersecurity personnel understand their roles and responsibilities Senior executives understand their roles and responsibilities Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities Privileged users understand their roles and responsibilities All users are informed and trained
17	17.3	N/A	N/A	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	PR.AT-1 ID.AM-6	All users are informed and trained Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
17	17.4	N/A	N/A	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.		
17	17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	PR.AT-1	All users are informed and trained
17	17.6	N/A	N/A	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.	PR.AT-1	All users are informed and trained
17	17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	PR.AT-1	All users are informed and trained
17	17.8	N/A	N/A	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.	PR.AT-1	All users are informed and trained
17	17.9	N/A	N/A	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.	PR.AT-1	All users are informed and trained

The NIST Cyber Security Framework Version 1.1 (CSF) has 1 Mapping for the Nine CIS #17 Sub-Controls are as follows:

- CSF Function: Protect
- CSF Category: Awareness and Training
- CSF Category Identifier: PR.AT-1
  - All users and re informed and trained
- CSF Category Identifier: PR.AT-2
  - Privileged users understand their roles and responsibilities
- CSF Category Identifier: PR.AT-3
  - Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
- CSF Category Identifier: PR.AT-4
  - Senior executives understand their roles and responsibilities
- CSF Category Identifier: PR.AT-5
  - Physical and cybersecurity personnel understand their roles and responsibilities
- Category: 2 - Foundational

- CSF Function: Identify
- CSF Category: Asset Management
- CSF Category Identifier: ID.AM-6
  - Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
  - Category: 2 - Foundational

The Cyber Security Function discussed in this presentation is **Protect (PR)**

Protect – Develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services. The Protect function includes the following categories of outcomes: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Protective Technology.

The Category discussed in this presentation is **Awareness and Training (AT)**

The Sub-Category discussed in this presentation is **General users are informed and trained (PR.AT-1)**

Risk Addressed (well…only one of the many risks that need to be addressed):

The technical staff, office and warehouse staff, C-Suite and Sales Department use a variety of methodology to create, save, store and retrieve login credentials and passwords for the computers, servers, email and websites, among other services and systems, required to conduct business on a daily basis. The Technicians also use disparate methodology to access all the Ethernet appliances installed at customer sites by our company. Current methods range from sticky notes adhered to undersides of keyboards on the high-risk side of the pendulum to sophisticated online password management services on the low-risk side. Needless to say, the risk associated with an unauthorized person gaining access to our network or our customer's network via a credential improperly cared for is tremendous and the potential for loss is real.

Abstract:
The Center for Internet Security (CIS) boasts of a unified information technology (IT) society - globally. This society seeks to embrace a shared vision to safeguard private and public enterprise systems against cyber intrusions which threaten organizational information and communication technology (ICT) systems. Comprising 20 Critical Security Controls (CIS), CIS-17 addresses the need to - Implement a Security Awareness and Training Program. While CIS-17 speaks of training to mitigate human vulnerabilities and social engineering threats, the CIS-17 framework has vast considerations and seeks to identify the specific knowledge, skills and abilities required to protect ICT systems from cyber intrusions. Considering specific knowledge, skills and abilities needed to support protecting enterprise networks, necessary fundamentals include education and training in advancements of intrusion detection systems (IDS) intrusion prevention systems (IPS) and next generation firewall (NGFW) technologies. *This paper offers an overview for industry apprentice level professionals to consider before the deployment of IDS, IPS or NGFW technologies, and concludes why NGFW technology deployments may offer the primer method to defend against threats aimed at enterprise ICT systems – for now.*

Keywords: Intrusion Detection, Intrusion Prevention, Next Generation Firewall

TOOLS TRIED / USED

For immediate access to relative information browsed, go to www.psasecurity.com/resources/tools where a wealth of Cybersecurity information was available for review and download. Topics we chose were as follows:

First and most important tool – Communication:

On November 10, 2017 we held an All-Hands Company Meeting to discuss the creation, storing and sharing of login and password credentials for customer IP enabled devices. All employees attended. There was a mandate implemented to immediately cease using default login and passwords. There was a guideline introduced to create and implement credentials for:

- Field Devices
  - Change the default login (if allowed)
  - Create unique passwords for every MAC Address
- Servers and workstations
  - Change the default login (if allowed)
  - Create unique passwords for every machine
- Software
  - Change the default login
  - Create unique passwords for every software

During the meeting several publications produced by the organization Securing the Human (SANS) and CSO were printed and distributed to all employees:

- SANS – Four Steps to Staying Secure
  - You
    - Guidance on being aware of how hackers attempt to get personal and proprietary information from you through malicious actions and websites
  - Passwords
    - Guidance on the creation and storing of "Strong" passwords and passphrases
  - Updating
    - Guidance on the importance of updating all things connected to the internet so that the latest software patches and updates are in effect on computers, mobile devices, and apps
  - Backups
    - Guidance on creating a solid automatic backup regiment so that in the event the device IS hacked it can be wiped and restored
- CSO – Biggest Data Breaches of the 21ST
  - The statistics from the publication in terms of compounded cost of each breach and the number of people affected (Identity stolen) provided tremendous gravity and allowed for an open discussion about how carelessness on our part could very easily translate to a similar data breach at one of our customer sites
- Other topics discussed to underscore the potential exposure caused by breech to our site or a customer site:
  - Remediation
  - Loss of Customers
  - Business Disruption
  - Regulatory Fines
  - Legal Costs
  - Public Relations
  - Breached Customer Records
  - Direct Financial Loss

- Notification Costs
- Credit Card reissues, Identity Theft Repair, and Monitoring

- Average Cost of a breach
  - Direct Cost
  - Indirect Cost
- Odds of experiencing a Data Breach
  - 28% or 1 in 4
  - Compared to being struck by lightning 1 in 960,000
- Rolled out an immediate directive to reintroduce and use LastPass Enterprise Password Manager
  - Reviewed the operation of the application with emphasis on:
    - Automatic creation of strong and unique passwords
    - Ease of use in storing, finding and retrieving passwords
    - Password sharing capabilities and benefits through the app

PROS & CONS

Pros

- Impactful and meaningful presentation resulted in active and productive discussion
- Have increased the "active" users in LastPass from 25% to 100%
- All employees keenly aware of the mandate
- All employees understand the mandate and consequences for failing to comply
- Had a company BBQ immediately afterward so subject matter discussion could continue socially and organically

Cons

- Employees were non-productive in their typical roles for about three hours

ANTICIPATED OUTPUT

- That all employees:
  - will utilize LastPass to implement strong and unique passwords for all their devices and software and update the passwords regularly.
  - have, at minimum, a high-level understanding of the real potential for a data breach or hack.
  - are very aware of the breach/hack exposure they may mitigate, or exacerbate, through their actions and habits.

MONITORING STEPS

- LastPass Enterprise has a useful dashboard that gives you a summary of your account including: the number of users, licenses available, expiration, purchase options, security grade tiles, a snapshot of all enterprise logins over the last 7 days, and important alerts regarding features and newly added services. It is a simple snapshot to ascertain whether the technicians are using the tool or not.

- Scheduled monthly meetings with employees to review Cybersecurity controls and introduce new controls. Discuss exposures and practices.

TIME SPENT

Meeting Preparation Time	4.0 Hours
Actual Meeting	2.0 Hours
Barbequing Chicken and Beef	1.0 Hour
Monitoring	0.5 Hours weekly

ROI IF POSSIBLE TO DETERMINE

While it is difficult to quantify monetarily let's claim the ROI as Immediate. The fact that not doing anything could certainly bear a devastating financial burden considering a data breach of any size. The monthly expense to deploy the LastPass Enterprise version is inexpensive compared to the cost of the time wasted and persons diverted from their productive tasks when trying to locate one of thousands of passwords for a customer server while a tech is performing a service call and cannot log into a machine. All in, including the expense to hold regularly scheduled meetings with the employees to review such matters and to create a cybersecurity atmosphere and culture is worth every dollar invested.

CIS #19: Incident Response and Management

MAPPING THE CIS V7.1 Control #19 TO THE CYBER SECURITY FRAMEWORK

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
19				**Incident Response and Management** ***Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.***			
19	19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
19	19.2	N/A	N/A	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.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
						ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
						RS.CO-1	Personnel know their roles and order of operations when a response is needed
						DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
19	19.3	N/A	N/A	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.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
						DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
19	19.4	N/A	N/A	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.	RS.CO-2	Incidents are reported consistent with established criteria
19	19.5	N/A	N/A	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.	ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers
19	19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	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.	DE.DP-4	Event detection information is communicated
						RS.CO-4	Coordination with stakeholders occurs consistent with response plans
19	19.7	N/A	N/A	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.	PR.IP-10	Response and recovery plans are tested
19	19.8	N/A	N/A	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.	RS.AN-4	Incidents are categorized consistent with response plans

- Category: 3 - Organizational

RECOVER

THE ART AND SCIENCE OF DISASTER RECOVERY

This paper identifies variables to consider both before and following a cyber infiltration of an organizations information and communication technology (ICT) system and the measures that sum the art and science of an effective Disaster Recovery (DR) program.

BACKGROUND

Disaster Recovery (DR) encompasses business continuity tactics to move beyond either a natural or man-made event impacting an organizations information and communication technology (ICT) system. Consequently, system degradation at the hands of; social engineering, insider threats, hackers or organized criminals using the computer as an instrument in a crime is unprecedented in terms of frequency and consequence. In fact, the probability of a cyber event now greatly overshadows the probability of a natural event causing critical system interruption and has taken center stage as an organizations most distressing event impacting ICT system integrity and operability.

Considering the likelihood of a cyber event impacting an organization, on March 1, 2012, then Director of the Federal Bureau of Investigation (FBI), Robert S. Mueller, while speaking at the RSA Cyber Security Conference in San Francisco, California, perhaps best describes the prospect of a cyber-attack impacting an organization by declaring; "*I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again*" (Mueller, 2012).

In totality, small, medium and enterprise ICT systems will most likely at some point be impacted by a cyber-event with little to no warning. While consequences can be cataclysmic for an organization, a tested and proven DR plan can provide the strategic framework to overcome system interruptions and recovery time. The goals - greatly reduce ICT system recovery time and promote organizational resiliency by imploring industry best-practices to return operability of ICT systems.

DISASTER RECOVERY PLAN – *THE STRATEGY*

There are several positions to consider for organizations seeking to increase awareness and a manageable framework to disaster recovery which have been widely accepted thought industry. Such a framework of options and variables noted in this paper can be built upon by IT professionals as they determine what best serves their organization based on pre-determined priorities.

1. **Identify Threats and Actions to Confront Cyber Threats**

   More than ever open source cyber intelligence can be used for the good of corporate ICT system preservation. Considering open source white papers, industry studies to chat rooms, technology professionals have access to identify both emerging threats in addition to best-practices to pursue through a risk-based approach – directing energy and resources to the most probable and high-risk threats. In the end, you cannot protect or defend against every single threat and or pursue a strategy of information/intelligence overload. Instead, place attention on threats that are probable to imminent based on intelligence and industry indicators.

2. **Perform a Business Impact Analysis (BIA)**

   Each ICT system that can be impacted by a potential cyber interruption should be put through a Business Impact Analysis (BIA). Identify the axis of the following: financial, life/safety, regulatory, legal/contractual and reputation that have a quantifiable financial, legal or brand impact. Strategy and direction of resources can pursue either the Risk Informed Decision- Making Strategy or a Minimization of Risk Subject to Budgetary Constraints Theory as outlined below.

   a. Risk Informed Decision-Making Strategy – This theory estimates risk among all assets threatened by an event. This model ranks assets from highest to lowest order and invests in funding highest priority assets first. While allocating funds to highest risk assets first; consequently, subsequent assets may not receive funding since the model promotes expenditures on high-risk/reward assets until funds are depleted.

   b. Minimization of Risk Subject to Budgetary Constraints Theory – This model proposes instead of ranking assets according to risk; optimally allocate resources across all assets so the sum of risk is reduced to a minimum. This theory seeks to reduce risk across a collection of assets in an attempt to give the best possible return-on-investment (ROI). This model proposes allocation of limited funds to return the greatest benefit for the amount invested. It also removes subjective positions out of the equation because cost effective spending is supported through the ROI performance model. Return-on-investment (ROI) informed prevention strategy reduces vulnerability across a collection of assets so the total aggregate risk is minimized.

TIP - BIA establish priorities through a risk and asset dedication strategy. No need to start from scratch to get your BIA in motion, utilize industry promoted tools to determine risk, the business impact and recovery strategy. Any effort to identify the consequences of a cyber intrusion and the business impact can greatly reduce overall organizational loss.

3. **Identify Key Personnel and Stakeholders**

   Recovery plans should dictate the actions of people through Standard Operating Procedures (SOP) in the Disaster Recovery (DR) process. When there is a framework of the DR process both efficiency and recovery actions and expectations become more of a science than art. By identifying the critical people charged to respond or notify of an ICT degradation event, effective communication both internal and external to the organization can improve recovery and eliminate wasteful steps. To note, false steps and miss-starts can impact legal, financial, and regulatory consequences, however, key stakeholder action and communication during DR can limit such consequences.

TIP – Flow charts in SOP's dictating communication trails offer an impactful and efficient communication framework on notification protocols during the recovery process. Structured and effective communication is key…

4. **Updates to DR Plans Following Lessons Learned**

   DR Plans and a response framework should not be static and should continue to mature since personnel, technology and threats will never be constant. Recovery plans are built on assumptions and variables; therefore, each lesson learned should produce steps, processes and technology considerations that will reduce downtime during future events. There will always be another opportunity to test insertions of lessons learned during the next ICT system disruption and disaster recover (DR) event.

TIP – Lessons learned may impact creative thinking and plans inserted in a SOP that have failed or delayed system recovery. Promote the insertion of new ideas in the DR plan, and do not pursue harsh actions against those who provided a failed strategy. Learn from the mistakes and move beyond mistakes in new promoted actions and processes. There will always be a future cyber event to redeem poor decisions and plans pursued during a past cyber event.

5. **Prioritization**

   Through a risk-based approach, priorities must drive the DR process and strategy. Considering threats to the organization whether operationally, legally or financially, organizational leadership should drive the strategy of priorities and are the ultimate stakeholder in the process. Since not every risk can be mitigated to its lowest denominator, areas that can be most consequential to an organization such as the preservation of customer information, proprietary or trade craft secrets usually are at the top of the priority list.

TIP – Goodrich & Tamassia (2011) note the parameters of information security and system preservation is defined by the acronym of CIA – Confidentiality, Integrity and Availability. Considering the CIA triad, recovery plans and framework should be constructed on the strategy of; preservation of confidential information, maintaining integrity of ICT systems, and speed of recovery for availability of ICT system information and resources.

6. Drills & Exercises

Table-Top exercises offer the most impactful and cost-effective measure to create a checklist of procedures to follow during a disaster (Bolch, 2009). From table-top exercises, a host of playbook options to gauge response and the value of SOP steps that outline response efforts and responsibilities of those who will be tasked to act during the DR event can be outlined. Most importantly, a DR table-top exercise can assist with plan addendums to written SOP's in addition to the determination of resources required, training and the acquisition of hardware and software services that facilitate a speedier DR reality.

TIP – Bolch (2009) identifies a table-top exercise is beneficial not only before an event occurs, but after every DR or Business Continuity update that can help identify gaps or overlaps in the DR planning strategy. Due to the threats of cyber intrusions and the low cost of hosting table-top exercises, failure to hold this strategy in an IT organizations arsenal may be considered negligence.

7. Cloud Options and Disaster Recovery as a Service (DRaaS)

Risk management of an Information and Communication Technology (ICT) system and the moving of ICT services to cloud offerings is an area that has diverse opinions among industry leaders. While there is controversy regarding cloud hosted ICT systems versus traditional and on-site system management, below depicts the variables of cloud offerings such as; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) management options. If engaging in cloud information system management, each model can have a critical impact on disaster recovery since each platform pushes elements of ICT systems to a third party or a trusted cloud partner.

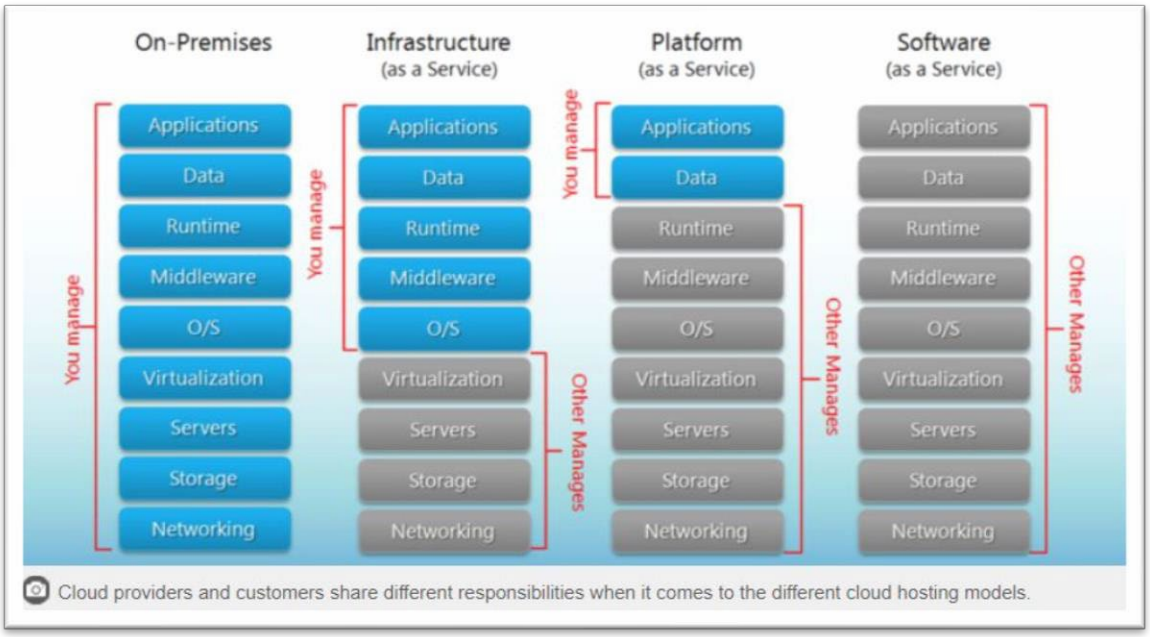


Figure 1. Cloud Offering Options (Stamey, 2007)

For the apprentice who is attempting to determine risk between traditional on-premise hosting compared to cloud hosting options, Stamey (2007) identifies the entertaining difference between; IaaS, PaaS, SaaS, and Pizza as a Service to compare what others manage when we dine out in comparison to dinning at home.

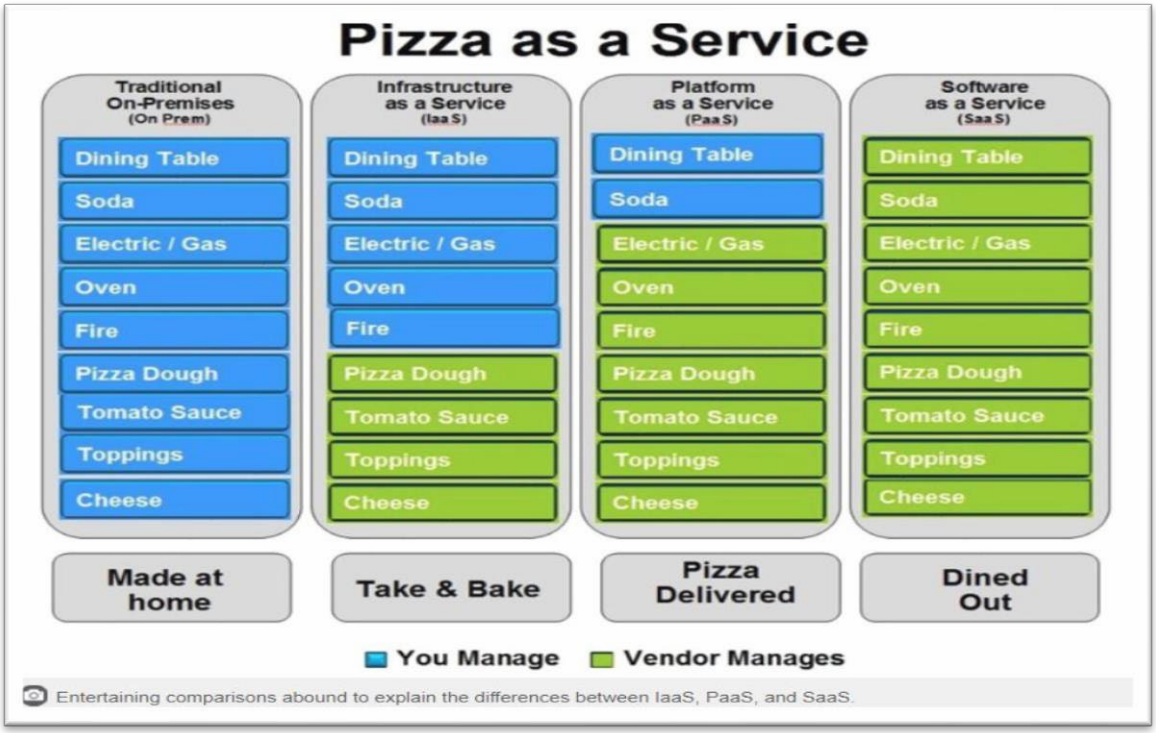


Figure 2. Pizza as a Service to compare cloud computing and dining out (Stamey, 2007)

There is an enormous shift of risk when information system resource and data management are moved to cloud operators and has helped give rise to Disaster Recovery as a Service (DRaaS) as a risk-based option. On-demand hosting and services providers have made DR more efficient, more economical, and shifts risk from internal ICT system stakeholders to organizations who continue to promote the "cloud" option as the best opportunity for managing ICT system resources. In turn, the move may reduce internal organization risk during the DR process and shift risk to hosting partners who may be better prepared and equipped to overcome cyber-attacks aimed at an organizations ICT system.

In conclusion, there are reasonable steps organizations can take to preserve ICT systems from a cyber intrusion, in addition to impactful and strategic measures to pursue in a DR program. The paper is not all inclusive, but instead offers several actions to pursue for the experienced and apprentice to the DR strategy and process. As highlighted in this paper, small, medium and enterprise ICT systems will most likely at some point be impacted by a cyber-event which will occur with little to no warning. The consequence of such will be determined by the reasonable and responsible measures to prepare for consequential infiltrations aimed at an ICT system, and leadership's preparedness and response to such events. Above all, ICT system professionals and organizational leaders need to deploy strategic measures to preserve the integrity of an organization and avoid the label of "negligence" as such a stigma may not be recoverable in terms of brand and legal consequences.

Flaws in software can leave your information systems vulnerable to attacks. Information about bugs in popular commercial and open-source software is available to everyone. Attackers exploit them once they are known, so keeping up with patch releases is essential to security. It would be my recommendation to use the following three phases. These phases were created with CCTV, Access Control, and Intrusion systems in mind.

Engineering Phase (prior to the sale) - During this phase of discovery any know vulnerabilities should be searched out via a variety of ways. One being the manufacture's site, in some cases manufactures post known issues with products along with any firmware updates or patches to the application to resolve these issues. Review sites and customer testimonials are good way to gage any issues flaws with an application. Changing of know ports from command to uncommand in the application. Establishing a company and organizational standard that separates the software or hardware your is selling and the added steps you're taking to protect it. Knowing your product and a strong competency of the product goes a long way into the Management part this control.

Deployment- Things to keep in mind when it comes to deployment is vulnerable of the application, the source doesn't matter. When dealing with applications from outside sources, whether commercial or free**, the most important consideration is to stay with a supported version and apply all security patches** in a timely manner. *This doesn't necessarily mean having the latest version!* When available, using the long-term support (LTS) version of an application can be less disruptive than updating to each new version. However, regular bug fixes and security patches still need to be applied quickly, and you should have an upgrade plan ready when the newer version is released. There's pressure to get the code working on time, which sometimes results in security considerations being pushed to the background. **It's harder to go back and catch every vulnerability than it is to stick with security-oriented development practices** that minimize the chances of exploitable bugs. This should be kept in mind, knowing you as the integrator should have a plan A, B, C and D on how you will overcome these challenges. In the constant race to zero cost by manufacture it will ultimately increase the exposure and liability of the integrator.

Post deployment- A previously undiscovered bug can turn into an active threat without warning. Zero-day exploits take advantage of these to steal vast amounts of data or gain control of computers. Criminals or malicious attackers will have information about these vulnerabilities before you do. Having a compressive way to respond to these attacks is key to any security organizations. These are some ways you as the professional can start the discussion internally:

- **Join communities:** Your company is not the only one that experiences incidents. Consider joining the Information Sharing and Analysis Center for your industry and following organizations such as US-CERT.
- **Managed detection and response:** Managed detection and response services provide 24/7 detection and response in your environment and can be a great fit for organizations that don't have the staffing, budget, or time to fully support incident response activities internally. Check out this evaluation brief, "How to Choose a Managed Detection and Response Provider," for some helpful questions to ask when deciding on a provider.
- **Incident response retainer:** Incident response retainers offer customers the ability to rapidly engage skilled personnel to perform a forensic investigation in the event of a suspected compromise or the real deal. These retainers are often an annual expense you either use or lose, so

ensure your pick allows you to move from being reactive to proactive and reallocate your hours toward penetration testing or tabletop exercises, like we do here at Rapid7.

- **Cyber-insurance:** For many companies, cyber-insurance is a “check the box” control. When purchasing cyber-insurance, it is important to understand what is and isn’t covered as part of your plan. For example, many insurance policies will be nullified if you are not properly managing your logging infrastructure. It is also important to realize that cyber-insurance is not a replacement for implementing security controls. Do your research before purchasing a cyber-insurance policy and be sure your legal team weighs in, too.

CYBERSECURITY KEY TERMS

Active interception - normally refers to placing a computer between a sender and receiver and an effort to capture and possibly modify information

Ad filtering - ways of blocking and filtering out unwanted advertisements pop-up blockers and content filters are considered to be at filtering methods

Adware - type of spyware that pops up advertisements based on what it has learned about you

Application whitelisting - a method of restricting users to specific applications

Attack vector - the path or means by which an attacker gains access to a computer

Back doors - used in computer programs to bypass a normal authentication and other security mechanisms in place

Bluejacking - the sending of unsolicited messages to Bluetooth enabled devices such as mobile phones and tablets

Bluesnarfing - the unauthorized access of information from a wireless device through a Bluetooth connection

Botnet - a group of compromised computers used to distribute malware across the internet the members are usually zombies

Business Impact Analysis (BIA) – a systematic process aimed at predicting and evaluating the potential impact and loss of critical business operations as a result of disaster, accident or emergency

C and C (Command and Control) – A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. ... C&C servers also serve as the headquarters for compromised machines in a botnet

CIA Traid – Confidentiality, Integrity, and Availability (CIA)is a model designed to guide strategy and policy governance over the security of information systems within an organization. Confidentiality aims at a set of rules that limits access to information, integrity is the assurance information is trustworthy and accurate, and availability is a guarantee system resources will be available upon request by authorized users

Content filters - individual computer programs that block external files that use JavaScript or images from loading into the browser

DMZ – A physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network such as the Internet.

DNS (Domain Name System) – The Internet's system for converting alphabetic names into numeric IP addresses. For example, when a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name.

Easter egg - a platonic extra added to an OS where application as a sort of joke the harmless cousin of the logic bomb

Firewall - A part of a computer system or network that is designed to block unauthorized access while permitting outward communication

Grayware - a general term used to describe applications that are behaving improperly but without serious consequences often describes types of spyware

Hardware security module - a physical device that deals with the encryption of authentication processes digital signings and payment processes

Host based intrusion detection system – a type of system loaded on an individual computer and analyzes and monitors what happens inside that computer

Information & Communication Technology (ICT) – the infrastructure, network components, applications and information systems that enable modern networking and computing

Logic bomb – code that has, in some way, been inserted into software it is meant to initiate some type of malicious function if specific criteria are met

Malware – software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent

Mobile device management - is centralized software solution that allows for the control configuration of mobile devices

Open mail relay – also known as an SMTP open relay, enables anyone on the internet to send an email through an SMTP server

Personal firewall - an application that protects an individual computer from unwanted internet traffic it does so by way of rules and policies

Phishing – The fraudulent practice of sending emails appearing to be from reputable entities in order to trick or entice individuals to reveal information, such as usernames, passwords and/or other personally identifiable information.

Pivot Point – A hacked computer that is used to route the traffic from a to and from an attacker and other networks that are not directly accessible by an attacker.

Pop-up blocker - an application or add onto a web browser the blocks pop-up windows that you see contain advertisements

Privilege escalation - the act of exploding a bug or design flaw in a software or firmware application to gain access to resources that normally would have been protected from an application or user

Ransomware - a type of malware that restricts access to a computer system and Demands a ransom be paid

Risk-Based Security (RBS) – security model that attempts to deliver the most effective security in the most efficient manner by steering resources and assets to the highest areas of security risk and vulnerability

Rootkit - a type of software design to gain administrator level control over a computer system without being detected

Social Engineering Attacks – the psychological manipulation of organizational employees to attain confidential information for the purposes of fraud, gathering information or systems access. This type of activity aims at using human interaction in an attempt to trick employees to break organizational security procedures to gain access to buildings, systems, or organizational

Spam - the abuse of electronic messaging systems such as email broadcast media and instant messaging

Spyware - a type of malicious software either downloaded unwittingly from a website or installed along with some other third-party software

Storage segmentation - a clear separation of organizational and personal information applications and other content

Threat Vector - the method of threat uses to gain access to a target computer

Time bomb - a Trojan set off on a certain date

Trojan Horse - an application that appears to perform desired functions but is actually performing malicious functions behind the scenes

Typosquatting - a method used by attackers that takes advantage of user's typos when accessing websites. Instead of the expected website the user ends up at a website with a similar name but often malicious content

UTM – Unified threat management, commonly abbreviated as UTM, is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network.

Virus - code that runs on a computer without the user's knowledge it infects the computer when the code is accessed and executed

Worm - code that runs on a computer without the user's knowledge a worm self-replicates whereas a virus does not

Zombie - an individual compromised computer in a botnet

REFERENCES:

Bolch, M. (2009). *Using a tabletop exercise for disaster recovery planning.* TechTarget. Retrieved from http://searchdisasterrecovery.techtarget.com/tip/Using-a-tabletop-exerCISe-for-disaster-recovery-planning

Center for Internet Security (2018). *Implement a security awareness and training program.* Retrieved from https://www.CISecurity.org/controls/implement-a-security-awareness-and-training-program/

Cloudnine Realtime (2018). *Utilize an active discover tool to identify sensitive data*. Retrieved from https://www.cloudninerealtime.com/

DeMuro, J., & Turner, B. (2020). *Best email clients of 2020: free and paid apps and software*. Techradar. Retrieved from https://www.techradar.com/best/best-email-clients

Draicchio, C. (2018, August 13). *Incedent response and management strategy*. Retrieved from: https://blog.rapid7.com/2018/08/13/CIS-critical-security-control-19-steps-for-crafting-an-efficient-incident-response-and-management-strategy/

George, A. (2019, July 1). *What are plugins and how do they work.* Lifewire. Retrieved from https://www.lifewire.com/what-are-plugins-4582189

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to computer security*. Boston: Pearson.

Intrusion Detection System (IDS). *Techopedia*. Retrieved from https://www.techopedia.com/definition/3988/intrusion-detection-system-ids

Intrusion Prevention System (IPS). *Techopedia*. Retrieved from https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips

Logikcull (2018). *Utilize an active discovery tool to identify sensitive data*. Retrieved from https://www.logikcull.com/

Lynch, P. (2018, October 8). *Anchor technologies*. Retrieved from https://www.anchortechnologies.com

Marshall, C. (2020, February 13). *The best browser: the fastest, safest, most fun way to get online*. Techradar. Retrieved from https://www.techradar.com/best/browser

Marta. (2016). *Tips for implementing Your IDS/IPS*. Retrieved from https://community.spiceworks.com/networking/articles/2471-tips-for-implementing-your-ids-ips

Martin, J. A. (2017). *7 things your IT disaster recovery plan should cover*. *CSO*. Retrieved from https://www.csoonline.com/article/3209653/disaster-recovery/7-things-your-it-disaster-recovery-plan-should-cover.html

Microsoft.com (2018). *Encrypt all sensitive information*. Retrieved from https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

Microsoft.com (2018). *Encrypt all sensitive information at rest*. Retrieved from https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Mueller, R. S. (2012). *Robert s. mueller speech*. *RSA security conference*. Retrieved from https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Nextpoint (2018). *Utilize an active discovery tool to identify sensitive data*. Retrieved from https://www.nextpoint.com

Panda Security (2019). *What is the difference between an IDS and an IPS*. Retrieved from https://www.pandasecurity.com/usa/support/card?id=31463

Pirc, J. (2017). *The evolution of intrusion detection/prevention: then, now and the future*. Retrieved from https://www.secureworks.com/blog/the-evolution-of-intrusion-detection-prevention

Plato, A. (2018). *The NGFW is dead*. Retrieved from https://www.anitian.com/the-ngfw-is-dead/

Pritha, M. (2016). *9 top features to look for in next generation firewall (NGFW)*. Cisco. Retrieved from http://www.CISoplatform.com/profiles/blogs/9-top-features-to-look-for-in-next-generation-firewall

Prowse, D.L. (2015). *CompTIA security SY0-401* (3rd ed.) Indianapolis, IN: Pearson.

Shirgahi, H. (2016). *Placing IDS in a normal network*. Research Gate. Retrieved from https://www.researchgate.net/figure/placing-IDS-in-a-normal-network_fig3_311312293

PSA Security Network (2018). *Create a security policy*. Retrieved from www.psasecurity.com/resources/tools

Sans. (2018). *Create a security policy*. Retrieved from www.sans.org/security-resources/policies

Scripts. Techopedia. Retrieved from https://www.techopedia.com/definition/10324/scripts

Sophos. (n.d.). Retrieved from https://www.sophos.com/en-us.aspx

Stamey, L. (2007). IaaS vs. *PaaS vs. SaaS cloud models*. Hosting Advice.com. Retrieved from http://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/

Wikipedia. (2018). *Classified information in the united states*. Retrieved from https://en.wikipedia.org/wiki/Classified_information_in_the_United_Stateshttps://en.wikipedia.org/wiki/Classified_information_in_the_United_States

Wikipedia. (2020). *DMARC.* Retrieved from https://en.wikipedia.org/wiki/DMARC

MEET THE CONTRIBUTORS

Chair
Gary Hoffner

PSLA Security
Vice President

Matthew Boehm

CM3 Building Solutions, Inc.
Information Security Analyst

Daniel Brooks

Tech Systems, Inc.
IT Support Specialist

Tyrone Chambliss

Northland Controls
Program Manager

Josh Cummings

VTI Security
Director,
Engineering Services

Daniel Dollinger

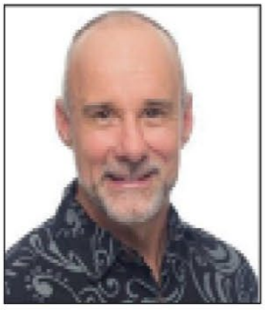
Casco Systems, Inc
Director of Application Engineering and IT

Henry Hoyne

Northland Controls
CTO

Johnny Johnson

Securitronics
Service Coordinator



Andrew Lanning

Integrated Security Technologies
Co-Founder

Scott Schmidt

Aronson Security Group
VP of Technology

Paul Schmick

Alliance Security
Vice President,
Security Technology