

RISK ASSESSMENT

August 2021



ABC COMPANY TECHNICAL REPORT

Technical report of Risk
Assessment performed by
Ascend Technologies for ABC
Company on August 27, 2021.

RISK ASSESSMENT

ABC COMPANY

Overview

Ascend Technologies was contracted by ABC Company to perform a Risk Assessment. The goal of a Risk Assessment is to determine the status of an organization's information security posture and highlight gaps that may expose the organization to unnecessary risk. This document provides an overview of the findings from the assessment and recommendations for addressing risks identified through the assessment process.

Approach

Ascend Technologies' risk assessment approach is what separates us from our competition. There are many firms that can perform automated penetration testing and generate a report – or go through a checklist to determine “compliance with best practices”. But Ascend Technologies has developed an assessment methodology based on the Center for Internet Security (CIS) Controls that provides increased business value in the following key ways: Our findings are custom written for your organization. Anyone can run some automated tools and identify vulnerabilities, but our strength lies in being able to manually verify those detected issues and then communicate them in terms of potential business impact along with sensible recommendations for correcting the discovered security weaknesses. In other words, we'll help you to understand what each particular risk really means to your organization and exactly how someone could go about exploiting that vulnerability.

We educate our client throughout the process. In our view, it would be a great disservice to do an assessment, deliver a report with findings and recommendations and then walk away. We prefer to work as partners with our clients, helping them to understand the many information security challenges and compliance requirements being faced and to develop an appropriate and cost-effective approach for dealing with those challenges.

Our extensive work in harmonizing standards and best practices and then integrating them into our assessment method ensures that your organization is prepared to meet not just today's information security requirements, but tomorrow's as well.

Ascend Technologies' approach is consultative and educational. We will help you identify which information security requirements and guidelines may apply to your organization. We can translate these lengthy texts into plain English, in terms of what it means to your business and what, if anything needs to be done.

Contents

OVERVIEW	1
APPROACH	1
TWENTY CRITICAL SECURITY CONTROLS COMPLIANCE	5
CIS CONTROLS FRAMEWORK	5
Critical Control 1: Inventory of Authorized and Unauthorized Devices	5
1. Inventory of Authorized and Unauthorized Devices	5
Control 1 Overview.....	5
Control 1 Results.....	6
Critical Control 2: Inventory and Control of Software Assets.....	8
2. Inventory of Authorized and Unauthorized Software.....	8
Control 2 Overview.....	8
Control 2 Results.....	8
Critical Control 3: Continuous Vulnerability Management	11
3. Continuous Vulnerability Assessment and Remediation.....	11
Control 3 Overview.....	11
Control 3 Results.....	11
Critical Control 4: Controlled Use of Administrative Privileges	13
4. Controlled Use of Administrative Privileges.....	13
Control 4 Overview.....	13
Control 4 Results.....	13
Critical Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	16
1. Secure Configurations for Hardware/Software	16
Control 5 Overview.....	16
Control 5 Results.....	16
Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	18
Control 6 Overview.....	18
Control 6 Results.....	18
Critical Control 7: Email and Web Browser Protections	20
2. Email and Web Browser Protections	20
Control 7 Overview.....	20
Control 7 Results.....	20
Critical Control 8: Malware Defenses	23
8. Malware Defenses	23
Control 8 Overview.....	23
Control 8 Results.....	23
Critical Control 9: Limitation and Control of Ports, Protocols, and Services	25
9. Limitation & Control of Ports.....	25
Control 9 Overview.....	25

Control 9 Results.....	25
Critical Control 10: Data Recovery Capability	27
10. Data Recovery	27
Control 10 Overview.....	27
Control 10 Results.....	27
Critical Control 11: Secure Configurations for Network Devices	29
11. Secure Configurations for Network Devices	29
Control 11 Overview.....	29
Control 11 Results.....	29
Critical Control 12: Boundary Defense	32
12. Boundary Defense	32
Control 12 Overview.....	32
Control 12 Results.....	32
Critical Control 13: Data Protection	36
13. Data Protection	36
Control 13 Overview.....	36
Control 13 Results.....	36
Critical Control 14: Controlled Access Based on the Need to Know	39
14. Controlled Access based on Need to Know.....	39
Control 14 Overview.....	39
Control 14 Results.....	39
Critical Control 15: Wireless Access Control	42
15. Wireless Device Control	42
Control 15 Overview.....	42
Control 15 Results.....	42
Critical Control 16: Account Monitoring and Control.....	45
16. Account Monitoring and Control	45
Control 16 Overview.....	45
Control 16 Results.....	45
Critical Control 17: Security Skills Assessment and Training	48
17. Security Skills Assessment and Training	48
Control 17 Overview.....	48
Control 17 Results.....	48
Critical Control 18: Application Software Security	51
18. Application Software Security	51
Control 18 Overview.....	51
Control 18 Results.....	51
Critical Control 19: Incident Response and Management	54
19. Incident Response Capability	54
Control 19 Overview.....	54
Control 19 Results.....	54
Critical Control 20: Penetration Tests and Red Team Exercises	56

20. Penetration Tests and Red Team Exercises.....	56
Control 20 Overview.....	56
Control 20 Results.....	56
Critical Controls Overall Score	59
CRITICAL CONTROLS OVERALL SCORE	59
Vulnerability Assessment.....	60
VULNERABILITY ASSESSMENT	60
Summary of Results	60
RECOMMENDATIONS	61
CONCLUSIONS	61

CIS Controls Framework

The CIS Controls have been developed through a Consortium of government and private entities. Members of the Consortium include NSA, US Cert, DoD, the Department of Energy Nuclear Laboratories, Department of State, plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.

Ascend Technologies believes that the implementation of these controls can help organizations reduce risk most effectively across the board. The controls also cover a majority of the IT requirements in most regulations including PCI, HIPAA and FDIC/FFIEC regulations.

Ascend Technologies has taken these controls and integrated them with our Rapid Risk Assessment methodology. We have added a scoring system based on the “quick-wins” associated with the defined security controls. Using our scoring system Ascend Technologies can provide organizations with an overview of their compliance with the Twenty Critical Security controls. An overview of ABC Company’s compliance is outlined below.

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Score: 5 of 24

Control 1 Overview

Many criminal groups and nation-states deploy systems that continuously scan address spaces of target organizations, waiting for new and unprotected systems to be attached to the network. The attackers also look for laptops that are not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates until the following day. Attackers from anywhere in the world may quickly find and exploit such systems that are accessible via the Internet. Furthermore, even for internal network systems, attackers who have already gained internal access may hunt for and compromise additional improperly secured internal computer systems. Some attackers use the local nighttime window to install backdoors on the systems before they are hardened.

Additionally, attackers frequently look for experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization. Such experimental systems tend not to have as thorough security hardening or defensive measures as other systems on the network. Although these test systems do not typically hold sensitive data, they offer an attacker an avenue into the organization and a launching point for deeper penetration.

As new technology continues to come out, many employees bring personal devices into work and connect them to the network. These devices could already be compromised and be used to infect internal resources. Attackers are also increasing the use of pivot points, compromising one system and using that as an anchor point to break into other systems that might not be directly visible to them.

Control 1 Results

METRIC 1: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). This metric covers the use of active tools that scan through IPv4 or IPv6 network address ranges.

RESULT 1: [MSP] uses a combination of [Tool X] and [Tool Y] for asset inventory of workstations and servers on ABC Company's network. [Tool X] is an agentless tool while [Tool Y] uses an agent. There is not currently any asset inventory of network devices.

Result 1 Score: 2 of 3

METRIC 2: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). This metric covers the use of passive tools that identify hosts based on analyzing their traffic.

RESULT 2: No passive asset inventory tools are currently configured or utilized. It is recommended to use a passive asset inventory discovery tool that can automatically detect devices on the network and update the asset inventory. Passive asset inventory discovery tools continuously monitor traffic on the local network to identify new assets. Tools like Automate, Lansweeper, Service Desk Plus, and SCCM have automated passive asset inventory discovery components to them.

Result 2 Score: 0 of 3

METRIC 3: If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging and use this information to improve the asset inventory and help detect unknown systems.

RESULT 3: DHCP server logging is enabled by default but is not used to help improve the asset inventory. Reviewing DHCP server logs can help identify new assets to add to the asset inventory in case one might be missed by automated tools.

Result 3 Score: 1 of 3

METRIC 4: 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.

RESULT 4: ABC Company does not currently have an up-to-date inventory of all technology assets with the potential to store or process information. Having an up-to-date asset inventory is critical to ensuring all devices are accounted for and have the proper security measures applied.

Result 4 Score: 0 of 3

METRIC 5 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.

RESULT 5: The asset inventory includes network address, hardware address, and machine name but does not include asset owner or department for each asset. Including this additional information can make it easy to track the owner of a device and where the device is situationally on the network.

Result 5 Score: 2 of 3

METRIC 6 Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.

RESULT 6: ABC Company does not currently have a method for detecting unauthorized assets on the network. A tool like Qualys can help approve assets in the network and identify unauthorized assets. When an unauthorized asset is detected, it is important to remove it in a timely fashion.

Result 6 Score: 0 of 3

METRIC 7 Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.

RESULT 7: Network Access Control (NAC) has not been deployed in the network. When deploying NAC it is important to use a certificate based NAC solution to ensure maximum effectiveness.

Result 7 Score: 0 of 3

METRIC 8 Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

RESULT 8: ABC Company does not have a NAC solution deployed.

Result 8 Score: 0 of 3

Critical Control 1 Overall Score: 5 of 24

Critical Control 2: Inventory and Control of Software Assets

Score: 14 of 30

Control 2 Overview

Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Without the ability to inventory and control which programs are installed and allowed to run on their machines, enterprises make their systems more vulnerable. Such poorly controlled machines are more likely to be either running software that is unneeded for business purposes, introducing potential security flaws, or running malware introduced by a computer attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Control 2 Results

METRIC 1 : Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

RESULT 1 : **An up-to-date list of authorized software is not currently maintained. Tools like Automate, Qualys Cloud Agents, or Manage Engine can identify software installed on devices. This can be used to help compile a list of approved software. A formal list of authorized software should be compiled and regularly updated to ensure only approved software is installed on devices in the network. Unauthorized software or software that is not on the approved list should be uninstalled from systems to mitigate potential vulnerabilities. Deviations from the standard list of approved software should be documented as an exception with a valid business need along with the person or group that approved the exception.**

Metric 1 Score: 0 of 3

METRIC 2 : Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

RESULT 2: While an authorized software inventory is not currently maintained, ABC Company uses [Tool Z] to deploy software and collect information about software installed on each device. All software in the inventory system is supported by the software vendor.

Metric 2 Score: 2 of 3

METRIC 3: Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

RESULT 3: ABC Company uses [Tool Z] to collect and maintain an inventory of software used throughout the organization.

Metric 3 Score: 3 of 3

METRIC 4: The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

RESULT 4: [Tool Z] is able to track the name, version, publisher, install date, etc. for all software used by the organization.

Metric 4 Score: 3 of 3

METRIC 5: The software inventory system should be tied into the hardware asset inventory, so all devices and associated software are tracked from a single location.

RESULT 5: [Tool Z] ties the hardware asset inventory to the software inventory, so they are able to see what software is installed on a particular device.

Metric 5 Score: 3 of 3

METRIC 6: Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

RESULT 6: ABC Company does not maintain a list of authorized software. Users do not have local admin privileges so software must be installed by IT administrators. As attackers and malware become more sophisticated, it is possible that a malicious entity can potentially escalate privileges and install unauthorized software on devices. This is why an inventory of authorized software is essential and should be regularly reviewed. Once a list of authorized software has been compiled, regularly review the list and ensure that any unauthorized software is removed from devices.

Metric 6 Score: 0 of 3

METRIC 7: Utilize application whitelisting technology on all assets to ensure that only authorized software executes, and all unauthorized software is blocked from executing on assets.

RESULT 7: There is currently no application whitelisting technology deployed in the network. Microsoft or Apple's AppLocker is an example of an application whitelisting technology that can be used to ensure only authorized software can execute on machines.

Metric 7 Score: 0 of 3

METRIC 8: The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.

RESULT 8: When deploying an application whitelisting technology, ensure that only authorized software libraries are allowed to load.

Metric 8 Score: 0 of 3

METRIC 9: The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.

RESULT 9: AppLocker can ensure that only digitally signed scripts are allowed to run, however, this can be difficult to implement and enforce. It is important to identify any unsigned scripts that may need to execute on given systems in the network and formally document those exclusions to the policy.

Metric 9 Score: 0 of 3

METRIC 10: Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

RESULT 10: ABC Company has some network segmentation in place. There is currently no software that is being utilized within the organization that would incur a higher risk for other devices in the network.

Metric 10 Score: 3 of 3

Critical Control 2 Overall Score: 14 of 30

Critical Control 3: Continuous Vulnerability Management

Score: 6 of 21

Control 3 Overview

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised.

Control 3 Results

METRIC 1: Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

RESULT 1: Vulnerability scanning is not being conducted at this time. It is extremely important to conduct vulnerability scans of the entire environment to identify vulnerabilities that can be used by hackers or malware to compromise systems in the network. This should be conducted on a weekly or more frequent basis. Any high or critical level severity vulnerabilities should be remediated ASAP. Tools like Qualys, Nessus, or Nexpose are examples of SCAP-compliant vulnerability scanners that can be leveraged to identify vulnerabilities in the organization.

Metric 1 Score: 0 of 3

METRIC 2: Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

RESULT 2: Ensure that vulnerability scans use authentication to perform a more thorough scan for vulnerabilities on host systems.

Metric 2 Score: 0 of 3

METRIC 3: Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.

RESULT 3: When performing authenticated vulnerability scans, use a dedicated account that is not used for any other administrative purposes.

Metric 3 Score: 0 of 3

METRIC 4: Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

RESULT 4: ABC Company uses a combination of [Tool Y] and [Tool Z] for patching. Servers and workstations are running the most recent security updates.

Metric 4 Score: 3 of 3

METRIC 5: Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

RESULT 5: [Tool Y] and [Tool Z] are used to update third party software on devices.

Metric 5 Score: 3 of 3

METRIC 6: Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

RESULT 6: Vulnerability scans are not completed on the entire environment. Once a vulnerability management program has been implemented, compare the results of vulnerability scans to ensure vulnerabilities are being remediated in a timely manner.

Metric 6 Score: 0 of 3

METRIC 7: Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

RESULT 7: Most vulnerability scanning tools, like Qualys or Nessus, utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. Severity four or five level vulnerabilities should be prioritized first and remediated in a very timely fashion.

Metric 7 Score: 0 of 3

Critical Control 3 Overall Score: 6 of 21

Critical Control 4: Controlled Use of Administrative Privileges

Score: 9 of 27

Control 4 Overview

The misuse of administrator privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user, running as a privileged user, is fooled into opening a malicious e-mail attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote-control software to find administrator passwords and other sensitive data. Similar attacks occur with e-mail. An administrator inadvertently opens an e-mail that contains an infected attachment, and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges. One of the most common of these attacks involves the domain administration privileges in large Windows environments, giving the attacker significant control over large numbers of machines and access to the data they contain.

Control 4 Results

METRIC 1: Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

RESULT 1: Automated tools are not utilized to inventory all administrative accounts. All users have local admin privileges on their systems. It is critically important to restrict access to administrative privileges on all systems. Only authorized personnel should have administrative privileges. Allowing all users to have administrative privileges significantly increases the risk to the organization. Tools like Netwrix and ADAuditPlus or various SIEM solutions can inventory administrative accounts. It is important to continuously review findings and alerts to ensure only authorized individuals have elevated privileges.

Metric 1 Score: 0 of 3

METRIC 2: Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

RESULT 2: Default passwords are changed to strong secure passwords. Workstations are set with a 12-character password with complexity enforced and network equipment uses 16-character passwords that are randomized and also use complexity.

Metric 2 Score: 3 of 3

METRIC 3: 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.

RESULT 3: [MSP], ABC Company's managed services provider (MSP), is the only ones with domain admin accounts. These accounts are only used for administrative purposes.

Metric 3 Score: 3 of 3

METRIC 4: 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.

RESULT 4: All accounts use passwords that are unique to that system.

Metric 4 Score: 3 of 3

METRIC 5: Use multi-factor authentication and encrypted channels for all administrative account access.

RESULT 5: ABC Company is currently in the process of implementing multi-factor authentication. Multi-factor authentication should be deployed to all systems that have administrative account access.

Metric 5 Score: 0 of 3

METRIC 6: 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.

RESULT 6: Administrators do not currently use a dedicated machine, like a jump box, for all administrative tasks or tasks that require administrative access. The RMM tool is used to login to machines they need access to. It is recommended to use a dedicated machine that is isolated from the network when performing administrative tasks to provide maximum protection to devices on the network. This device should not have access to the internet or email.

Metric 6 Score: 0 of 3

METRIC 7: Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.

RESULT 7: There are not currently any measures in place to restrict access to scripting tools. Microsoft or Apple's AppLocker can help to restrict access to scripting tools once deployed in the network.

Metric 7 Score: 0 of 3

METRIC 8: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

RESULT 8: No alerts are generated when a system is added to or removed from a group with administrative privileges. This can be achieved using a SIEM solution.

Metric 8 Score: 0 of 3

METRIC 9: Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

RESULT 9: Alerts are not generated on unsuccessful logins to an administrative account. This can also be accomplished using a SIEM solution.

Metric 9 Score: 0 of 3

Critical Control 4 Overall Score: 9 of 27

Critical Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Score: 6 of 15

Control 5 Overview

On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way it was delivered from manufacturers and resellers, thereby making it immediately vulnerable to exploitation. Default configurations are often geared to ease-of-deployment and ease-of-use and not security, leaving extraneous services that are exploitable in their default state. Attackers attempt to exploit both network-accessible services and browsing client software using such techniques.

Defenses against these automated exploits include procuring computer and network components with the secure configurations already implemented, deploying such preconfigured hardened systems, updating these configurations on a regular basis, and tracking them in a configuration management system.

Control 5 Results

METRIC 1: Maintain documented, standard security configuration standards for all authorized operating systems and software.

RESULT 1: [MSP] maintains their own standard security configuration for operating systems in ABC Company's network.

Metric 1 Score: 3 of 3

METRIC 2: Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

RESULT 2: Standard images are not currently used to deploy new machines but are configured in accordance with their standard security configuration. Images should be built using secure configurations and security software installed. All devices should be reimaged using this standard image to ensure all devices in the network are properly secured.

Metric 2 Score: 1 of 3

METRIC 3: Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

RESULT 3: Master images are not currently used. Once they are, they should be stored securely on servers with integrity checking tools to ensure only authorized changes are made.

Metric 3 Score: 0 of 3

METRIC 4: Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

RESULT 4: Active Directory Group Policy is used on servers as they are Windows based systems. System configuration management tools are not fully in use to automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals on workstations. [Tool Z] may be able to do this for workstations in the network.

Metric 4 Score: 1 of 3

METRIC 5: Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

RESULT 5: [Tool X] is used to monitor configurations of network equipment and alerts to any changes that are made. This should be done for workstations and servers as well. Tools like OSSEC can help to enforce this on workstations and servers.

Metric 5 Score: 1 of 3

Critical Control 5 Overall Score: 6 of 15

Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

Score: 11 of 24

Control 6 Overview

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damage done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

Control 6 Results

METRIC 1: Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

RESULT 1: ABC Company currently only uses one synchronized time source. A minimum of three synchronized time sources should be utilized to ensure all time information on logs are consistent.

Metric 1 Score: 1 of 3

METRIC 2: Ensure that local logging has been enabled on all systems and networking devices.

RESULT 2: Local logging is enabled on all systems.

Metric 2 Score: 3 of 3

METRIC 3: Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

RESULT 3: Local logs include detailed information such as event source, date, user, timestamp, etc.

Metric 3 Score: 3 of 3

METRIC 4: Ensure that all systems that store logs have adequate storage space for the logs generated.

RESULT 4: All systems have adequate storage space for logs.

Metric 4 Score: 3 of 3

METRIC 5: Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

RESULT 5: Network logs are stored in the FortiManager. Workstation and server logs are not sent to a centralized logging device. Logs from all devices in the network should be sent to a central log management system to allow for better log retention and protection from corruption.

Metric 5 Score: 1 of 3

METRIC 6: Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

RESULT 6: Logs are not currently being sent to a SIEM or log analytic tool. All logs should be sent to a SIEM to allow for better analysis and visibility into network activity.

Metric 6 Score: 0 of 3

METRIC 7: On a regular basis, review logs to identify anomalies or abnormal events.

RESULT 7: ABC Company does not currently review logs on a consistent basis. Log review should be conducted on a regular basis to identify anomalies or abnormal events in the network.

Metric 7 Score: 0 of 3

METRIC 8: On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

RESULT 8: A SIEM solution has not been deployed at this time. Once a SIEM solution has been deployed, it should be tuned frequently to better identify actionable events and decrease event noise.

Metric 8 Score: 0 of 3

Critical Control 6 Overall Score: 11 of 24

Critical Control 7: Email and Web Browser Protections

Score: 13 of 30

Control 7 Overview

Many controls in this document are effective but can be circumvented in networks that are poorly designed. Without carefully planned and properly implemented email servers, attackers can bypass security controls and spoof the identity of anyone in the organization. Attackers frequently take advantage of poorly secured email servers to mask their identity and gain credibility in phishing attacks. Additionally, web browsers that are not consistently updated are vulnerable to a variety of client-side attacks that take advantage of the web browser.

Web browsers and email clients are very common points of entry and attack because of their high technical complexity and flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.

Control 7 Results

METRIC 1: 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.

RESULT 1: ABC Company uses only fully supported web browsers and email clients like Chrome, Safari, Firefox, etc.

Metric 1 Score: 3 of 3

METRIC 2: Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

RESULT 2: Users are unable to install any other browsers. All browsers and email clients used in the organization are authorized and fully supported.

Metric 2 Score: 3 of 3

METRIC 3: Ensure that only authorized scripting languages are able to run in all web browsers and email clients.

RESULT 3: JavaScript is not locked down and ActiveX is not supported on Mac. Administrators should restrict the ability to use scripting languages (like ActiveX and JavaScript) in web browsers and email clients unless there is a valid business reason. If it has been determined that a user has a valid business need for such scripting languages, a dedicated browser should be utilized with these languages enabled and allow browsing to only those specific websites that require those scripting languages with that browser.

Metric 3 Score: 1 of 3

METRIC 4: 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.

RESULT 4: Network-based URL filtering is not currently in place at this time. This is primarily due to issues with network speed that are working on being resolved. Once troubleshooting has completed and the issue has been resolved, URL filters will go back to being in place again. The FortiGates they have in the network fully support this. This should be implemented quickly within the environment to limit access to websites not approved by the organization. The FortiGates along with the FortiClient have the capability to restrict access to sites even when devices are off network.

Metric 4 Score: 1 of 3

METRIC 5: 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.

RESULT 5: The FortiGate has an active subscription to URL categorization services. Uncategorized websites are not being blocked at this time but should be once issues with network speed have been resolved.

Metric 5 Score: 1 of 3

METRIC 6: Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

RESULT 6: URL requests are not logged on devices on network due to issues with network speed. These requests are not logged on mobile devices that are off network either. It is recommended to retain logs for at least a year and mobile devices adhere to the same URL filtering profiles while on the network.

Metric 6 Score: 0 of 3

METRIC 7: Use DNS filtering services to help block access to known malicious domains.

RESULT 7: DNS filtering services are not currently being utilized. DNS filtering services are designed to help block access to known malicious domains. The FortiGates have this capability.

Metric 7 Score: 0 of 3

METRIC 8: To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification,

starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

RESULT 8: ABC Company has implemented SPF but not DMARC or DKIM. It is recommended to implement DMARC and DKIM to provide additional email security.

Metric 8 Score: 1 of 3

METRIC 9: Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

RESULT 9: ABC Company uses Office 365 and specific types of e-mail attachments are blocked by default.

Metric 9 Score: 3 of 3

METRIC 10: Use sandboxing to analyze and block inbound email attachments with malicious behavior.

RESULT 10: ABC Company does not currently utilize a mail filtering solution that has a sandboxing component. It is recommended to utilize a sandbox to provide an additional layer of security for potentially malicious email attachments and links.

Metric 10 Score: 0 of 3

Critical Control 7 Overall Score: 13 of 30

Critical Control 8: Malware Defenses

Score: 24 of 24

Control 8 Overview

Malicious software is an integral and dangerous aspect of Internet threats, targeting end users and organizations via web browsing, e-mail attachments, mobile devices, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. Modern malware aims to avoid signature-based and behavioral detection and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block its execution.

Control 8 Results

METRIC 1: Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

RESULT 1: ABC Company uses SentinelOne for anti-malware protection and is centrally managed.

Metric 1 Score: 3 of 3

METRIC 2: Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

RESULT 2: Agents are set to automatically update.

Metric 2 Score: 3 of 3

METRIC 3: 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.

RESULT 3: DEP and ASLR are enabled by default on modern operating systems.

Metric 3 Score: 3 of 3

METRIC 4: Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

RESULT 4: SentinelOne will scan content on removable media for malicious software when inserted or connected.

Metric 4 Score: 3 of 3

METRIC 5: Configure devices to not auto-run content from removable media.

RESULT 5: Devices are not allowed to auto-run content from removable media.

Metric 5 Score: 3 of 3

METRIC 6: Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.

RESULT 6: Administrators receive alerts on malware detection events.

Metric 6 Score: 3 of 3

METRIC 7: Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.

RESULT 7: SentinelOne does DNS queries to look for hostnames associated with known malicious domains.

Metric 7 Score: 3 of 3

METRIC 8: Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

RESULT 8: Command-line audit logging for command shells is enabled through Sentinel One and CLI commands are blocked with the exception of certain ones.

Metric 8 Score: 3 of 3

Critical Control 8 Overall Score: 24 of 24

Critical Control 9: Limitation and Control of Ports, Protocols, and Services**Score:** 4 of 15**Control 9 Overview**

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

Control 9 Results

METRIC 1 Associate active ports, services, and protocols to the hardware assets in the asset inventory.

RESULT 1: ABC Company has not associated active ports, services, and protocols to hardware assets on servers or workstations. This should be done for all devices in the network. Limiting access to services, ports, and protocols on the standard image using the Windows Firewall can help to implement this across the entire environment.

Metric 1 Score: 0 of 3

METRIC 2: Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

RESULT 2: The ports, protocols, and services open on servers and workstations should be labeled to associate them with a piece of software installed on the device. This can be accomplished in an asset inventory tool and enforced with Windows Firewall for Windows devices or iptables in UNIX devices.

Metric 2 Score: 0 of 3

METRIC 3: Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

RESULT 3: Automated port scans are not being performed. Several tools exist that can conduct automated port scans and generate an alert if an unauthorized port is detected.

Metric 3 Score: 0 of 3

METRIC 4: 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.

RESULT 4: Sentinel One acts as a host-based firewall but does not have a default-deny rule.

Metric 4 Score: 1 of 3

METRIC 5: 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.

RESULT 5: FortiGate firewalls are in place on the network and protect critical servers located in the DMZ.

Metric 5 Score: 3 of 3

Critical Control 9 Overall Score: 4 of 15

Critical Control 10: Data Recovery Capability

Score: 12 of 15

Control 10 Overview

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 attackers' presence on the machine.

Control 10 Results

METRIC 1: Ensure that all system data is automatically backed up on regular basis.

RESULT 1: ABC Company's devices are backed up using Veam. Incremental backups are performed every hour, full backups on Sunday mornings, and differential backups are on Wednesday.

Metric 1 Score: 3 of 3

METRIC 2: 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.

RESULT 2: All of the organizations key systems are backed up as a complete system.

Metric 2 Score: 3 of 3

METRIC 3: Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

RESULT 3: Data restoration is not performed on a regular basis. Data restoration should be performed on a quarterly or more frequent basis on all key systems to validate the integrity of backups. This process should be tracked and documented.

Metric 3 Score: 0 of 3

METRIC 4: 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.

RESULT 4: All backups are encrypted, both in transit and at rest, and physically secured.

Metric 4 Score: 3 of 3

METRIC 5: Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

RESULT 5: All backups have a location that is not continuously addressable.

Metric 5 Score: 3 of 3

Critical Control 10 Overall Score: 12 of 15

Critical Control 11: Secure Configurations for Network Devices

Score: 13 of 21

Control 11 Overview

Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, as the exceptions are deployed, and as those exceptions are left in place when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to gain access to target networks, redirect traffic on a network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

Control 11 Results

METRIC 1: Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.

RESULT 1: [MSP] manages the configuration for ABC Company's network equipment and uses their own hardening guidelines based on industry best practices. These configurations are monitored by [Tool X] and alerts are generated when changes occur. Any changes or requests would come in the form of a ticket or email to [MSP] staff.

Metric 1 Score: 3 of 3

METRIC 2: All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.

RESULT 2: Changes to network configurations are documented. The FortiManager helps to identify the user making the change along with the specific changes that were made to the system.

Metric 2 Score: 3 of 3

METRIC 3: Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.

RESULT 3: [Tool X] is used to detect and alert on changes to network configurations.

Metric 3 Score: 3 of 3

METRIC 4: Manage network devices using two-factor authentication and encrypted sessions.

RESULT 4: Network devices are managed using encrypted sessions, but two-factor authentication is not enabled. It is important to use two-factor authentication to login to network devices to provide an additional level of security.

Metric 4 Score: 1 of 3

METRIC 5: Install the latest stable version of any security-related updates on all network devices.

RESULT 5: The latest stable version of firmware is currently installed on all network devices. When new firmware is released, [MSP] checks the release notes to identify bug fixes and security updates the new firmware will apply and consider any known issues with the new firmware.

Metric 5 Score: 3 of 3

METRIC 6: Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

RESULT 6: A dedicated machine is not utilized for all administrative tasks. It is recommended to use a dedicated machine that is isolated from the network when performing administrative tasks to provide maximum protection to devices on the network.

Metric 6 Score: 0 of 3

METRIC 7: 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.

RESULT 7: The network has some network segmentation, however, there is not a dedicated VLAN where management of network infrastructure is performed. Ideally the network should have an admin or a management VLAN where all network infrastructure is managed. Only administrators should be allowed onto this network segment and firewall rules should be in place to only allow ports needed to perform administration of devices in the network.

Metric 7 Score: 0 of 3

Critical Control 11 Overall Score: 0 of 21

Critical Control 12: Boundary Defense

Score: 8 of 36

Control 12 Overview

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 multi-layered, 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 as a result 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. Even with 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.

Control 12 Results

METRIC 1: Maintain an up-to-date inventory of all of the organization's network boundaries.

RESULT 1: An up-to-date inventory of the organization's network boundaries is currently maintained. It is important to have a well-documented inventory of network boundaries for all network segments. It is highly recommended that all ports open on external network boundaries are included in the documentation as well as ports open between VLANs on the internal network.

Metric 1 Score: 2 of 3

METRIC 2: Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

RESULT 2: Regular scans are not performed outside of each trusted network boundary. Network scanning tools and/or vulnerability scanning tools such as Qualys, Nessus, and Nexpose can help detect unauthorized connections accessible across trusted network boundaries. Results from scans should be compared to existing documentation of open ports between network boundaries.

Documentation should be updated to reflect ports added or removed from access between network boundaries.

Metric 2 Score: 0 of 3

METRIC 3: Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.

RESULT 3: Communications to known malicious IP addresses or unused (bogon) IP addresses are not restricted at this time due to troubleshooting network speed issues.

Metric 3 Score: 0 of 3

METRIC 4: Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

RESULT 4: Ports are not currently locked down between all network boundaries. Currently the only traffic limited is between the internal network and DMZ. Only ports with a specific business need should be opened on inbound and outbound network traffic. This includes LAN to WAN policies. If unsure of what ports truly need to be open, perform an analysis on network traffic over the course of a month and tie specific protocols being used between network boundaries to applications in use by the organization. If specific protocols cannot be tied to a specific business process or application, they should be restricted.

Metric 4 Score: 1 of 3

METRIC 5: Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

RESULT 5: Full packet captures are not collected at all of the network boundaries. Network Detection and Response (NDR) tools like ProtectWise or MixMode can help provide much more visibility into traffic passing between network boundaries by taking full packet captures of network activity.

Metric 5 Score: 0 of 3

METRIC 6: 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.

RESULT 6: The FortiGate acts as an IDS.

Metric 6 Score: 3 of 3

METRIC 7: Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

RESULT 7: Intrusion Prevention System (IPS) functionality of the FortiGate is not enabled at this time for troubleshooting purposes. It is important to enable this functionality again as quickly as possible to prevent potential issues in the network. IPS sensors are important to help prevent attacks and intrusion attempts at network boundaries.

Metric 7 Score: 1 of 3

METRIC 8: Enable the collection of NetFlow and logging data on all network boundary devices.

RESULT 8: There is currently no collection of NetFlow and logging data on network boundary devices. By enabling NetFlow and analyzing flow data, administrators can build a picture of network traffic flow and identify where traffic is coming from and going to along with how much traffic is being generated.

Metric 8 Score: 0 of 3

METRIC 9: Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.

RESULT 9: Network traffic does not pass through an authenticated application layer proxy.

Metric 9 Score: 0 of 3

METRIC 10: Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.

RESULT 10: ABC Company does not currently do SSL inspection on encrypted traffic. Many modern next generation firewalls have the capability to perform SSL inspection. This should be implemented to help identify potentially malicious activity on the network including data exfiltration.

Metric 10 Score: 0 of 3

METRIC 11: Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.

RESULT 11: Multi-factor authentication is not required for remote login access at this time but is encrypted through the use of an SSL-VPN. Requiring multi-factor authentication for remote access can help significantly increase security of the network.

Metric 11 Score: 1 of 3

METRIC 12: Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

RESULT 12: Devices remotely connecting to the network are not scanned to ensure adherence to the organization's security policies such as having anti-virus installed with up-to-date definitions, latest security patches are installed, etc. The FortiGate can enforce these types of controls.

Metric 12 Score: 0 of 3

Critical Control 12 Overall Score: 8 of 36

Critical Control 13: Data Protection

Score: 3 of 27

Control 13 Overview

In recent years, attackers have exfiltrated more than 20 terabytes of often sensitive data from DoD and defense industrial base organizations (e.g., contractors doing business with the DoD), as well as civilian government organizations. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet in most cases, the victims were not aware that significant amounts of sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data is leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

Data loss prevention refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

Control 13 Results

METRIC 1: Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.

RESULT 1: ABC Company does not currently have an inventory of all sensitive information stored in the network. To properly protect data in the network, an inventory of all sensitive information needs to be maintained. Tools like Spirion, Varonis, STEALTHbits, or Netwrix Auditor can be used to help identify sensitive information on the network.

Metric 1 Score: 0 of 3

METRIC 2: Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

RESULT 2: Any sensitive information or systems containing sensitive information that are not regularly access should be disconnected from the network, isolated, or turned off until needed.

Metric 2 Score: 0 of 3

METRIC 3: Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

RESULT 3: ABC Company does not have an automated tool to look for unauthorized transfers of sensitive information. A Data Loss Prevention (DLP) tool should be deployed to identify and prevent sensitive information from leaving the network.

Metric 3 Score: 0 of 3

METRIC 4: Only allow access to authorized cloud storage or email providers.

RESULT 4: Access to cloud storage or email providers is not restricted. To minimize the risk of data exfiltration, access to cloud storage and email providers such as Dropbox, Yahoo mail, Gmail, Pastebin, etc. should be restricted. Only individuals or specific groups with a valid business reason should be allowed to access only approved cloud storage and email providers. Allowing access to personal email providers like Gmail from business resources significantly increases the risk of network compromise as well given the lack of corporate network security controls in place like email filtering and sandboxing.

Metric 4 Score: 0 of 3

METRIC 5: Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

RESULT 5: ABC Company does not currently have a method to detect the unauthorized use of encryption. This can be implemented by utilizing a solution that can perform deep packet inspection and scanning the traffic with a data loss prevention (DLP) tool.

Metric 5 Score: 0 of 3

METRIC 6: Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.

RESULT 6: File vault is partially deployed to laptops in the organization and alerts every 30 days for devices that are not enabled so they can remediate.

Metric 6 Score: 3 of 3

METRIC 7: If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.

RESULT 7: ABC Company does not restrict the use of USB storage devices. Cylance and Sophos are examples of companies that provide device control tools that will restrict the types of USBs that can be plugged into computers within the organization.

Metric 7 Score: 0 of 3

METRIC 8: Configure systems not to write data to external removable media, if there is no business need for supporting such devices.

RESULT 8: Systems are not currently configured to prevent writing data to external removable media. Only specific devices that have been identified as having a business need to write data to removable media should be allowed. All other devices should be configured to prevent writing data to removable media.

Metric 8 Score: 0 of 3

METRIC 9: If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

RESULT 9: Data written to USB storage devices is not encrypted. Sophos offers a tool that can automatically encrypt data being written to USB devices.

Metric 9 Score: 0 of 3

<i>Critical Control 13 Overall Score: 3 of 27</i>
--

Critical Control 14: Controlled Access Based on the Need to Know

Score: 13 of 27

Control 14 Overview

Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks. In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance. In several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data.

Control 14 Results

METRIC 1: 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).

RESULT 1: The network is segmented but not based on the label or classification level of the information stored on the network. The first step is to identify all of the sensitive information stored in the network. Next, classify the data (i.e., confidential, secret, top-secret, etc.), determine who needs access to the data, and create VLANs based on the sensitivity of the information being stored.

Metric 1 Score: 1 of 3

METRIC 2: Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.

RESULT 2: Firewall filters are currently in place between the internal network and the DMZ. Administrators should regularly revisit what devices and users should have access between VLANs as well as the ports and protocols that are allowed to each VLAN.

Metric 2 Score: 3 of 3

METRIC 3: Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.

RESULT 3: Private VLANs or micro segmentation has not been implemented to limit workstation to workstation communication. It is highly recommended to implement private VLANs, micro segmentation, or otherwise restrict the ability for devices on the same subnet to communicate with each other to prevent lateral movement.

Metric 3 Score: 0 of 3

METRIC 4: Encrypt all sensitive information in transit.

RESULT 4: Sensitive information is encrypted in transit.

Metric 4 Score: 3 of 3

METRIC 5: Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.

RESULT 5: ABC Company does not currently have an automated tool to identify sensitive information on the network. Tools like Varonis, STEALTHbits, or Netwrix Auditor can be used to help identify sensitive information on the network.

Metric 5 Score: 0 of 3

METRIC 6: 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.

RESULT 6: Access to information on the network is protected through the use of access control lists (ACLs).

Metric 6 Score: 3 of 3

METRIC 7: Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.

RESULT 7: ABC Company does not use an automated tool such as host based DLP. It is recommended to implement a Data Loss Prevention (DLP) tool to track what happens with sensitive data and protect against data theft.

Metric 7 Score: 0 of 3

METRIC 8: Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

RESULT 8: Sensitive information is encrypted at rest.

Metric 8 Score: 3 of 3

METRIC 9: Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

RESULT 9: ABC Company does not have SIEM or FIM deployed at this time. It is recommended to use both FIM and SIEM to monitor access to sensitive data or changes to sensitive data.

Metric 9 Score: 0 of 3

Critical Control 14 Overall Score: 13 of 27

Critical Control 15: Wireless Access Control

Score: 18 of 30

Control 15 Overview

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from nearby parking lots, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as backdoors when they are reconnected to the network of a target organization. Still 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.

Control 15 Results

METRIC 1: Maintain an inventory of authorized wireless access points connected to the wired network.

RESULT 1: ABC Company does currently maintain an inventory of all authorized wireless access points connected to the network.

Metric 1 Score: 3 of 3

METRIC 2: Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.

RESULT 2: Vulnerability scanning tools are not configured to detect or alert on unauthorized wireless access points connected to the wired network. Many firewalls or wireless access controllers have rogue access point (AP) detection capabilities that can prevent and alert to unauthorized wireless access points from connecting to the network.

Metric 2 Score: 0 of 3

METRIC 3: Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.

RESULT 3: The Ubiquiti access points utilized contain a built-in wireless intrusion detection system to detect and alert on unauthorized access points connected to the network. Detecting unauthorized wireless access points is very important to protecting devices using wireless in the network.

Metric 3 Score: 3 of 3

METRIC 4: Disable wireless access on devices that do not have a business purpose for wireless access.

RESULT 4: All devices in the network have a business purpose for wireless access.

Metric 4 Score: 3 of 3

METRIC 5: Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

RESULT 5: Wireless access on devices has not been configured to connect only to authorized wireless networks. This can be configured through group policy to ensure that devices only connect to trusted networks.

Metric 5 Score: 0 of 3

METRIC 6: Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.

RESULT 6: Peer-to-peer wireless network capabilities has not been disabled on wireless clients.

Metric 6 Score: 0 of 3

METRIC 7: Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

RESULT 7: The wireless network currently uses AES to encrypt wireless data in transit.

Metric 7 Score: 3 of 3

METRIC 8: Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.

RESULT 8: EAP/TLS is utilized but multi-factor authentication is not a requirement. Requiring multi-factor authentication to connect to the wireless network can help protect against malicious users that may somehow know the password to connect to the wireless network but do not have a valid multi-factor token.

Metric 8 Score: 2 of 3

METRIC 9: Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.

RESULT 9: Wireless peripheral access is not disabled but is generally necessary for all devices.

Metric 9 Score: 2 of 3

METRIC 10: 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.

RESULT 10: ABC Company has a guest network for guest users or employee's personal devices to connect to that is separate from the corporate network. Employees are not allowed to connect their personal devices to the corporate network by policy, but no tools are in place to enforce this.

Metric 10 Score: 2 of 3

Critical Control 15 Overall Score: 18 of 30

Critical Control 16: Account Monitoring and Control

Score: 22 of 39

Control 16 Overview

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

Control 16 Results

METRIC 1: Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.

RESULT 1: ABC Company maintains an inventory of all authentication systems used by the company.

Metric 1 Score: 3 of 3

METRIC 2: Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

RESULT 2: Account access is primarily configured through Active Directory.

Metric 2 Score: 3 of 3

METRIC 3: Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

RESULT 3: Multi-factor authentication (MFA) is not required for all user accounts but is in the process of being implemented. MFA should be enabled for all user accounts especially for externally facing systems like Outlook Web Access (OWA), VPN, and all cloud-based applications. Attackers are leveraging credential harvester attacks (attacks designed to steal an individual's username and password) more frequently as it is easier for them to bypass security controls that may be in place. Having multi-factor authentication enabled protects user accounts from being compromised in the event they fall victim to a credential harvester attack.

Metric 3 Score: 1 of 3

METRIC 4: Encrypt or hash with a salt all authentication credentials when stored.

RESULT 4: Credentials are encrypted or hashed.

Metric 4 Score: 3 of 3

METRIC 5: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

RESULT 5: Credentials are transmitted through the network using encrypted channels such as SSH, HTTPS, etc.

Metric 5 Score: 3 of 3

METRIC 6: Maintain an inventory of all accounts organized by authentication system.

RESULT 6: ABC Company maintains an inventory of all accounts through Active Directory.

Metric 6 Score: 3 of 3

METRIC 7: Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

RESULT 7: There is currently not an automated process for revoking system access once an employee has been terminated. It is recommended to use a tool such as CyberArk or Secret Server to help automate the process of revoking system access upon termination.

Metric 7 Score: 0 of 3

METRIC 8: Disable any account that cannot be associated with a business process or business owner.

RESULT 8: There is no official review process to check for accounts that cannot be associated with a business process or owner. This review process is important to establish to be able to identify any accounts that are no longer needed.

Metric 8 Score: 0 of 3

METRIC 9: Automatically disable dormant accounts after a set period of inactivity.

RESULT 9: Dormant accounts are not automatically disabled after a set period of inactivity. This can be configured through Active Directory and should be implemented to prevent abuse of inactive accounts.

Metric 9 Score: 0 of 3

METRIC 10: Ensure that all accounts have an expiration date that is monitored and enforced.

RESULT 10: Accounts do not have an expiration date that is monitored and enforced. Expiration dates should be used when creating accounts especially for temporary accounts like those given to contractors. This can easily be setup and enforced through Active Directory.

Metric 10 Score: 0 of 3

METRIC 11: Automatically lock workstation sessions after a standard period of inactivity.

RESULT 11: Workstations are locked automatically after a set period of inactivity.

Metric 11 Score: 3 of 3

METRIC 12: Monitor attempts to access deactivated accounts through audit logging.

RESULT 12: Attempts to access deactivated accounts are monitored.

Metric 12 Score: 3 of 3

METRIC 13: Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

RESULT 13: Alerts are not generated when users deviate from normal login behavior. A SIEM solution can also generate alarms for this type of behavior.

Metric 13 Score: 0 of 3

Critical Control 16 Overall Score: 22 of 39

Critical Control 17: Security Skills Assessment and Training

Score: 6 of 27

Control 17 Overview

- ❑ End users are fooled via social engineering scams in which they are tricked into providing passwords, opening attachments, loading software from untrusted sites, or visiting malicious web sites.
- ❑ System administrators are also fooled in the same manner as normal users but are also tested when attackers attempt to trick the administrator into setting up unauthorized accounts.
- ❑ Security operators and analysts are tested with new and innovative attacks introduced on a continual basis.
- ❑ Application programmers are tested by criminals who find and exploit the vulnerabilities in the code that they write.
- ❑ To a lesser degree, system owners are tested when they are asked to invest in cyber security but are unaware of the devastating impact a compromise and data exfiltration or alteration would have on their mission.

Any organization that hopes to be ready to find and respond to attacks effectively owes it to its employees and contractors to find the gaps in its knowledge and provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved and can also help determine proper allocation of limited resources to improve security practices.

Training is also closely tied to policy and awareness. Policies tell people what to do, training provides them the skills to do it, and awareness changes behaviors so that people follow the policy. Training should be mapped against the skills required to perform a given job. If after training, users are still not following the policy, that policy should be augmented with awareness.

Control 17 Results

METRIC 1: 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.

RESULT 1: ABC Company undergoes simulated phishing exercises every few weeks. This helps with skills gap analysis for all workforce members. This is important to help establish a baseline so that training efforts can focus on addressing these gaps.

Metric 1 Score: 3 of 3

METRIC 2: Deliver training to address the skills gap identified to positively impact workforce members' security behavior.

RESULT 2: Training is provided to users that fail a simulated phishing exercise.

Metric 2 Score: 3 of 3

METRIC 3: Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

RESULT 3: ABC Company does not have a security awareness program established. It is extremely important to develop one and ensure all users go through training during onboarding and on an annual or more frequent basis at a minimum.

Metric 3 Score: 0 of 3

METRIC 4: Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.

RESULT 4: Once a security awareness program has been established, make sure that it is updated on an annual or more frequent basis.

Metric 4 Score: 0 of 3

METRIC 5: Train workforce members on the importance of enabling and utilizing secure authentication.

RESULT 5: Part of the security awareness training should include reinforcing the importance of utilizing secure authentication.

Metric 5 Score: 0 of 3

METRIC 6: Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.

RESULT 6: As part of the yearly training, users should be trained on how to identify different forms of social engineering attacks.

Metric 6 Score: 0 of 3

METRIC 7: Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.

RESULT 7: All workforce personnel should be trained to identify and properly store, transfer, archive, and destroy sensitive information.

Metric 7 Score: 0 of 3

METRIC 8: 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.

RESULT 8: Workforce personnel should be trained to be aware of causes for unintentional data exposures.

Metric 8 Score: 0 of 3

METRIC 9: Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

RESULT 9: Employees should be trained on how to identify the most common indicators of an incident and how to properly report the incident.

Metric 9 Score: 0 of 3

Critical Control 17 Overall Score: 6 of 27

Critical Control 18: Application Software Security

Score: 15 of 33

Control 18 Overview

Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years. Application software that does not properly check the size of user input, fails to sanitize user input by filtering out unneeded but potentially malicious character sequences, or does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

To avoid such attacks, both internally developed and third-party application software must be carefully tested to find security flaws. For third-party application software, enterprises should verify that vendors have conducted detailed security testing of their products. For in-house developed applications, enterprises must conduct such testing themselves or engage an outside firm to conduct it.

Control 18 Results

METRIC 1: Establish secure coding practices appropriate to the programming language and development environment being used.

RESULT 1: ABC Company uses secure coding practices and follows best practices.

Metric 1 Score: 3 of 3

METRIC 2: For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

RESULT 2: Explicit error checking is performed to the best of their ability. It is important to incorporate explicit error checking into every phase of the software development lifecycle (SDLC) and documented. This ensures errors are caught during each phase of the SDLC making it easier to find and fix problems before moving onto the next phase which can make remediation of issues more difficult.

Metric 2 Score: 2 of 3

METRIC 3: Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.

RESULT 3: ABC Company currently verifies that all software versions acquired from outside the organization is still supported by the developer or appropriately hardened based on developer security recommendations.

Metric 3 Score: 3 of 3

METRIC 4: Only use up-to-date and trusted third-party components for the software developed by the organization.

RESULT 4: ABC Company selects validated 3rd party components that have an owned or open-source track record or ones that provide distinct advantages where a user base is small but growing with an active support process.

Metric 4 Score: 3 of 3

METRIC 5: Use only standardized and extensively reviewed encryption algorithms.

RESULT 5: Secure standardized encryption algorithms are not typically utilized. Organizations should utilize SHA256 and/or AES encryption algorithms and avoid the use of DES, 3DES, and CBC.

Metric 5 Score: 0 of 3

METRIC 6: Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

RESULT 6: Developers do not currently receive training in writing secure code for their specific development environment. It is highly recommended to send developers to formal trainings in person or online to continue education in secure code training. This helps to ensure developers stay up to date with the latest threats and how to prevent them through secure coding practices. SANS, Veracode, or Cybrary offer training in this area.

Metric 6 Score: 0 of 3

METRIC 7: Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

RESULT 7: ABC Company does not use a static or dynamic analysis tool to verify secure coding practices are being adhered to. Using a combination of a web application scanning tool like Qualys along with a tool like Veracode can help identify vulnerabilities and provide recommendations on how to fix them.

Metric 7 Score: 0 of 3

METRIC 8: Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.

RESULT 8: There is a process for this internally but currently no process to accept and address reports of software vulnerabilities externally. A process needs to be developed to address vulnerabilities when identified internally through vulnerability scans or if identified by an external entity. This should

include a method for who to contact when a vulnerability has been identified, method to validate the vulnerability, and how to remediate the vulnerability once validated.

Metric 8 Score: 1 of 3

METRIC 9: Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.

RESULT 9: ABC Company has separate environments for dev, staging, and production.

Metric 9 Score: 3 of 3

METRIC 10: Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

RESULT 10: Web applications are not protected by a web application firewall (WAF). While many next-generation firewalls can protect against web-based attacks, they must share resources with other feature sets and are not dedicated to only detecting and preventing OWASP Top 10 attacks. Qualys WAF and Fortinet's FortiWeb are examples of web application firewalls that can be used to protect web applications.

Metric 10 Score: 0 of 3

METRIC 11: For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

RESULT 11: Standard hardening configuration templates are not utilized. Systems that are part of critical business processes are not tested.

Metric 11 Score: 0 of 3

Critical Control 18 Overall Score: 15 of 33

Critical Control 19: Incident Response and Management

Score: 0 of 24

Control 19 Overview

Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response plans in place. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.

Control 19 Results

METRIC 1: Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.

RESULT 1: The incident response plan does not define roles of personnel or phases of the incident handling process. Incident response plans should be detailed so that all personnel involved in supporting the incident handling process can understand their role and what is expected in each phase of the process.

Metric 1 Score: 0 of 3

METRIC 2: Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.

RESULT 2: Job titles and duties should be defined for all personnel on the team that are expected to take part in the incident handling process.

Metric 2 Score: 0 of 3

METRIC 3: Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.

RESULT 3: Management personnel should be defined in the incident response plan that will support the incident handling process and what their roles are in the process.

Metric 3 Score: 0 of 3

METRIC 4: 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.

RESULT 4: Nothing is specifically defined in the policy for time requirements to notify system administrators of anomalous events. This should be clearly defined in the policy and require the employee's signatures to ensure they understand the policy.

Metric 4 Score: 0 of 3

METRIC 5: 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.

RESULT 5: There is no formal list of third-party contact information to be used in the event of an incident. A list of contact information should be maintained so anyone involved in the incident handling process knows who to contact in the event of an incident.

Metric 5 Score: 0 of 3

METRIC 6: 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.

RESULT 6: Information regarding who to contact to report anomalous events should be communicated in policies and routine employee awareness activities.

Metric 6 Score: 0 of 3

METRIC 7: 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.

RESULT 7: Routine incident response exercises and scenarios should be conducted so employees involved in the incident handling process are ready in the event of an incident.

Metric 7 Score: 0 of 3

METRIC 8: 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.

RESULT 8: ABC Company should identify potential threats to the organization and create a scoring and prioritization schema to address these threats.

Metric 8 Score: 0 of 3

<i>Critical Control 19 Overall Score: 0 of 24</i>
--

Critical Control 20: Penetration Tests and Red Team Exercises

Score: 0 of 24

Control 20 Overview

Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they often burrow deep into target systems and broadly expand the number of machines over which they have control. Most organizations do not exercise their defenses, so they are uncertain about their capabilities and unprepared for identifying and responding to attack.

Penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization and exploiting them to determine what kind of access an attacker can gain. Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment. Vulnerability assessments focus on identifying potential vulnerabilities, while penetration testing goes deeper with controlled attempts at exploiting vulnerabilities, approaching target systems as an attacker would. The result provides deeper insight into the business risks of various vulnerabilities by showing whether and how an attacker can compromise machines, pivot to other systems inside a target organization, and gain access to sensitive information.

Red team exercises go further than penetration testing. Red team exercises have the goals of improved readiness of the organization, better training for defensive practitioners, and inspection of current performance levels. Independent red teams can provide valuable and objective insights about the existence of vulnerabilities and about the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

Control 20 Results

METRIC 1: Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.

RESULT 1: Penetration tests are not currently being performed. It is important to conduct penetration tests of the environment on an annual or more frequent basis to identify and confirm potential vulnerabilities and threats to the environment. Penetration tests should include all web applications hosted by the organization, internal and external penetration tests, and tests of the wireless network.

Metric 1 Score: 0 of 3

METRIC 2: Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

RESULT 2: It is highly important to conduct penetration tests on the internal network as well as the external network. Internal network penetration testing can identify threats posed by malicious insiders or the extent of damage that can be done by a threat actor (TA) once they have successfully compromised the network.

Metric 2 Score: 0 of 3

METRIC 3: Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

RESULT 3: Red team exercises are not being conducted at this time. Once a few penetration tests have been conducted in the environment and vulnerabilities have been effectively remediated, it is recommended to schedule a red team exercise to test the full organizational readiness against specific threats to the organization.

Metric 3 Score: 0 of 3

METRIC 4: Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.

RESULT 4: Penetration tests do not look for the presence of unprotected system information and artifacts in the network. When looking for a penetration testing provider, it is important to make sure they are testing for the presence of unprotected system information and artifacts that may be on the network.

Metric 4 Score: 0 of 3

METRIC 5: Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

RESULT 5: If necessary, create a test environment that includes copies of production systems that would otherwise be excluded from testing due to the potential for system instability, limited resources, etc.

Metric 5 Score: 0 of 3

METRIC 6: Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

RESULT 6: Vulnerability scanning should be used in addition to other penetration testing tools and methodologies.

Metric 6 Score: 0 of 3

METRIC 7: Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

RESULT 7: Penetration tests and Red Team exercise results should be delivered using open, machine-readable standards like XML.

Metric 7 Score: 0 of 3

METRIC 8: Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes and are removed or restored to normal function after testing is over.

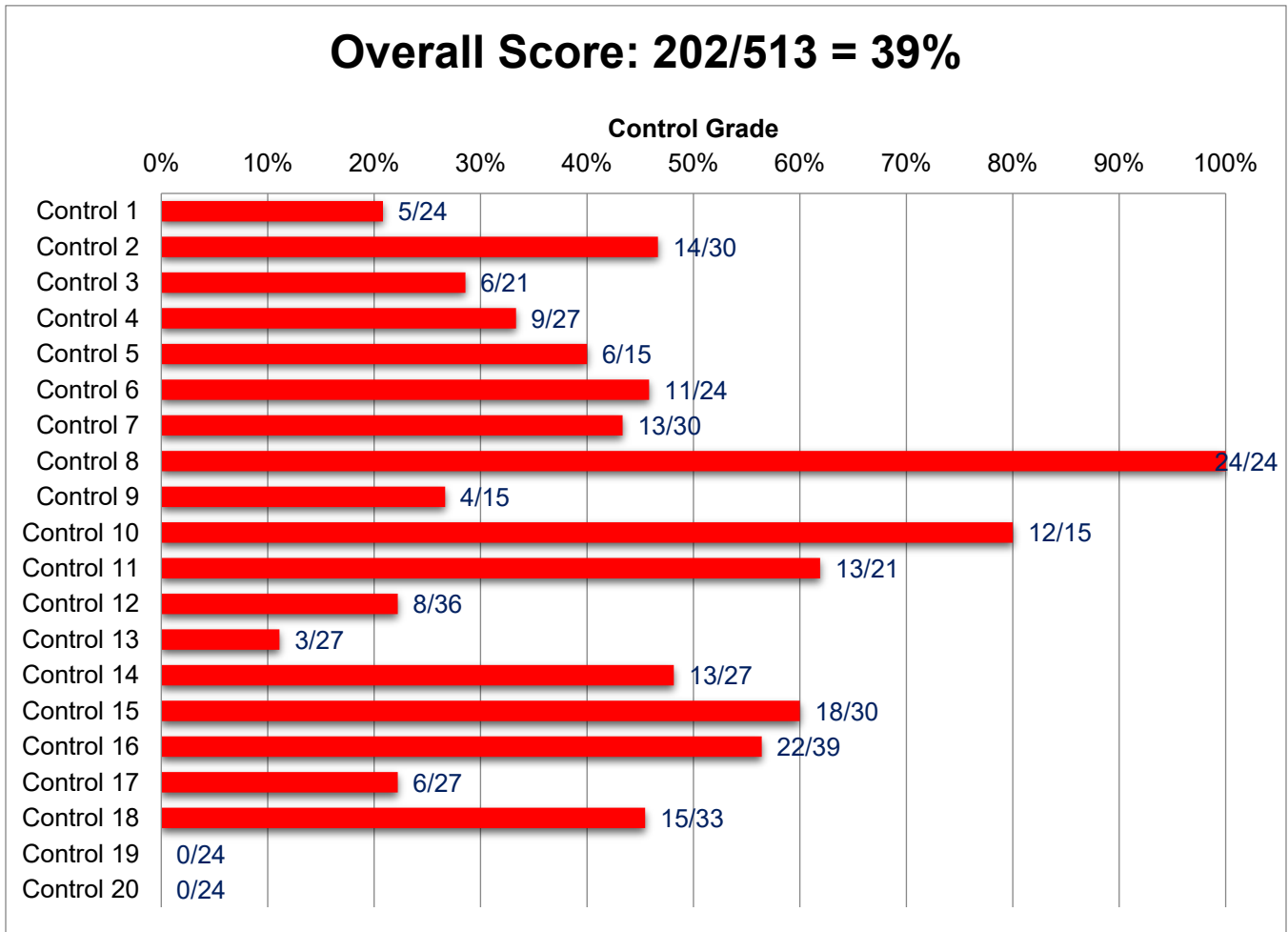
RESULT 8: If an account is ever created for white-box penetration tests, it is important to ensure it is properly controlled and monitored to ensure it is only used for legitimate and approved purposes. Once the test is over, ensure the account is properly removed from the system.

Metric 8 Score: 0 of 3

<i>Critical Control 20 Overall Score: 0 of 24</i>
--

Critical Controls Overall Score

OVERALL SCORE: 202 of 513, **39%**



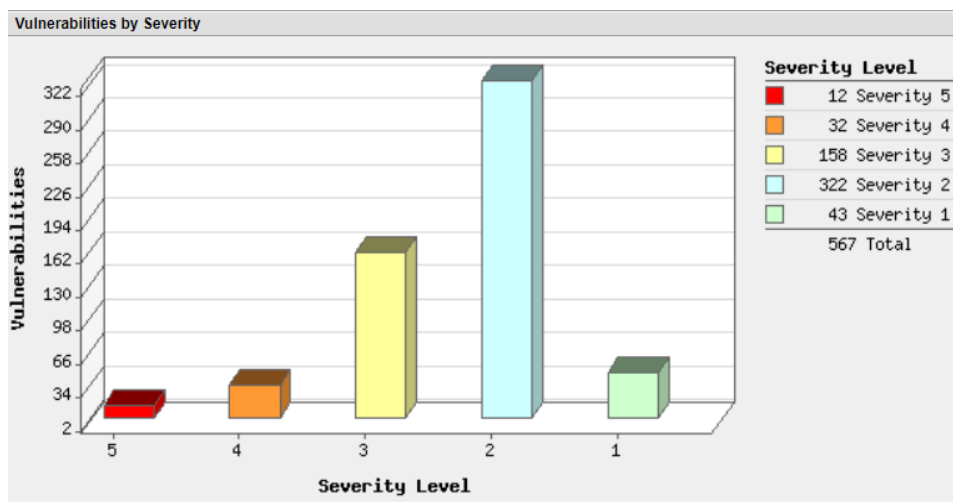
Vulnerability Assessment

Ascend Technologies performed a vulnerability scan of ABC Company's internal and external networks using Qualys. A full vulnerability report is included as an addendum to this document.

A vulnerability scan is used to identify assets on the network at risk to compromise due to insecure configuration or missing updates. Scanning is used to determine only vulnerabilities or potential vulnerabilities on systems by accessing listening services and analyzing responses to queries in order to determine vulnerability status.






Summary of Results

Vulnerabilities are classified on a scale of 1 to 5. With 5 being the most critical and 1 being innocuous. Our scanning identified 12 confirmed severity 5 vulnerabilities, and 32 confirmed severity 4 vulnerabilities. Severity 4 and 5 vulnerabilities should be addressed immediately as they generally indicate remotely exploitable vulnerabilities that an attack could use to gain control of a device. The illustration below represents a summary of the overall vulnerability status of ABC Company's internal and external networks.



Of the 567 vulnerabilities identified, 12 are severity 5, the most serious and easily exploitable. 32 severity 4 vulnerabilities were discovered on ABC Company's networks. Though not as severe as level 5 vulnerabilities, level 4 are considered critical and can provide attackers full access to information stored on the network host. A vulnerability is a design flaw or misconfiguration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vendors release periodic patches to fix software design flaws. It is important to implement these patches soon after they are released.

Below is a detailed explanation of the vulnerability security levels:

Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

The majority of discovered vulnerabilities fall under the general remote services category. These vulnerabilities can be remediated with a combination of vulnerability and patch management software. It is important to implement both vulnerability and patch management solutions to automate the discovery and tracking of vulnerable systems, and then in turn, mitigate the vulnerabilities by deploying patches to affected systems.

5 Biggest Categories	
Category	Confirmed
General remote services	341
Information gathering	19
TCP/IP	19
Web server	21
CGI	17
Total	417

Recommendations

There are a large number of security related items, both positive and negative, outlined in this document. We fully suggest reading the entirety of the document to help in developing your own strategic security plan. Below are some high-level suggestions that we recommend for addressing the most critical risks in the ABC Company environment.

1. Remediate all the vulnerabilities on your systems immediately. The most significant vulnerabilities are the EternalBlue and BlueKeep vulnerabilities which allows an attacker or malware to easily compromise the device.
2. From the list of assets, perform a routine (weekly) full authenticated vulnerability scan of the network.
 - a. Create a policy to remediate and follow up all vulnerabilities found in a timely manner.
 - b. Perform a full port scan to verify that only needed ports are open on critical assets.
3. Create an authorized software list.
 - a. Use this list to audit assets and remove or block any unauthorized software.
 - b. Review acceptable use policies and update if necessary.
4. Develop a formal written document of policies and procedures for the following (some of these may already be included in other recommendations): Acceptable Software and Installation Policy, OS deployment, Disaster Recover Policy, Employee Separation and Incident Response. The Incident Response policy in particular needs to be very detailed so that all members involved in the incident handling process understand their role and what steps need to be taken in the event of an emergency.
5. Change how new and reimage assets are deployed.
 - a. Each asset should have a baseline image installed that contains the updated OS and third-party applications. These images should be stored securely with integrity checking of the image to alert on potential unauthorized modification.
 - b. Initial deployment of servers, workstations and laptops should be completed in an isolated network environment where all required system patching, and hardening can be completed prior to deployment in the full internal environment.
 - c. Golden images should be hardened according to an established guideline such as those released by NIST, NSA, Defense Information Systems Agency (DISA), Center for Internet Security (CIS), and others.
6. Implement a file integrity monitor on all critical assets in order to alert on changes to important files on these assets.
7. Tighten controls on information leaving the organization.

- a. Lock down egress traffic on the firewall. Determine what ports need to be open and only allow those ports. Default deny all other ports.
 - b. Implement Data Leak Prevention filtering on all traffic.
 - c. Block or greatly curtail the use of Dropbox, Google Drive, Apple iCloud and external email such as Yahoo and Hotmail.
 - d. Create a strategy to monitor logs for large file transfers or unauthorized encrypted traffic.
 - e. Disable the use of USB drives where possible. Require that all data on USB drives be encrypted.
8. Training.
- a. Implement a security awareness program with all employees to make sure they are aware of security issues and are cognizant that sensitive information must be dealt with in a secure manner.
 - b. Ensure developers receive formal secure code training.
9. Implement a central logging server where all server and network asset logs are stored.
10. Implement a SIEM solution that covers the entire corporate network.
11. Removal of EOL/unsupported Operating Systems. This includes network equipment such as firewalls and switches. If removal is not possible, segment and isolated the asset from the rest of the environment.
12. Run a disaster recovery drill on assets in the DMZ and Corporate networks and update the DR guide accordingly.
13. Schedule an internal and external penetration test for the entire network and web applications.
14. Implement network access controls (NAC) on all ports in the building. When implementing a NAC solution, utilize one with a certificate-based solution. This may involve replacing phones and/or printers that can work with this solution to avoid the need for excluding devices from this control which drastically reduces the effectiveness of NAC.

Conclusions

Ascend Technologies interviewed key members of ABC Company's staff and reviewed the documentation provided in order to gain an understanding of the network as it relates to the CIS Critical Security Controls. ABC Company has a few security gaps in the network that should be addressed immediately. It is important to follow the items outlined in the recommendations section to enhance the overall security posture. The most critical security components to implement are vulnerability management, SIEM, development of an Incident Response Plan (IRP), and security awareness training.

A key piece of security that is not currently being met is the establishment of a vulnerability management program. Patching alone will not fix third party components that require updating and it will certainly not address any security misconfigurations. Utilizing a vulnerability scanner such as Qualys will help to identify these misconfigurations or missing updates. Since IT and security rapidly change and new exploits are identified every day, it is highly recommended to scan for vulnerabilities on a weekly or more frequent basis. Simply scanning for vulnerabilities is not enough, however. These results must be reviewed, and any high or critical vulnerabilities must be remediated within 48 hours as these are the biggest threats to the organization that can easily be taken advantage of.

Centralized logging and a SIEM solution are also vital components to network security. When an attacker breaks into an organization, they will do everything they can to cover their tracks which includes deleting or manipulating logs. Having logs sent to a centralized logging server with limited read only access would help to prevent an attacker from altering logs. A SIEM solution helps to correlate log events from multiple sources and alert on suspicious activity. While an event log from one source might not raise suspicion, a combination of event logs from multiple sources that relate to a single event can illustrate a larger picture of what is happening within the network. LogRhythm and EventTracker are examples of SIEM solutions that can piece together logs from multiple sources, use its built-in intelligence to correlate the events, and trigger an alarm when a suspicious event is occurring. Some SIEM solutions, like EventTracker, even have the ability to add additional security features such as file integrity monitoring (FIM) which can provide more visibility into the network and enhance the overall security of the organization.

In addition to security tools and architecture, documentation plays a key role in guiding staff members on what to do in certain scenarios. Incident Response Plans are vital to supporting an organization's effectiveness at responding to threats in the event of a breach. This document should address what is defined as an incident, who to contact in the event of a breach, what to document and steps to take to preserve forensics artifacts, etc. How quickly an organization responds to a breach and the steps taken once an incident has been identified can have a drastic impact on how quickly a threat can be contained and remediated. Incident Response Plan templates are freely available online. SANS and CIS in particular have templates and guides on what to include in the plan.

The biggest threat to any environment's network is the end user. One very important critical control that should be established immediately is a security awareness program. This program should include quizzes to measure the effectiveness of the training they are receiving. Users should also be tested through a variety of social engineering tactics. Implementation of a security awareness program would be relatively easy and inexpensive to do and will significantly enhance the security of the network.

While the overall score may seem relatively low at this time, it is important to keep in mind that this document serves as a security roadmap and many items can quickly and easily be implemented to increase the overall score in a short amount of time. It is helpful to continue to routinely perform risk assessments to gauge progress over time and determine next steps on the security roadmap. By

focusing on core policies and technologies as described in the recommendations section of this document; ABC Company can significantly increase their overall security posture within a moderate period of time.