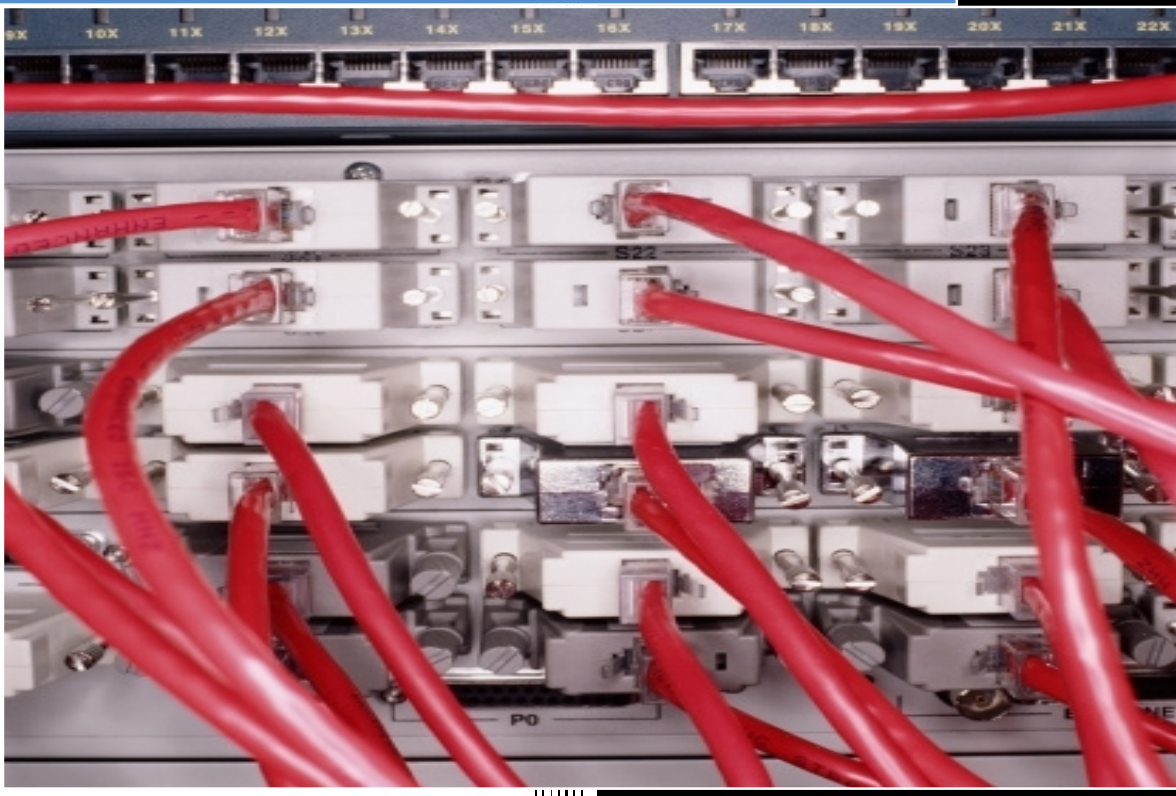
CATALYST
TECHNOLOGY GROUP
Innovating how IT is delivered.sm

Cyber Risk Assessment

Cyber Risk Analysis Report



Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

Table of Contents

Cyber Risk Analysis Report Overview

The Cyber Risk Analysis Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Cyber Risk Score and a high-level overview of the health and security of the network.

The report details the scan tasks undertaken to discover security issues. In addition to the overall Cyber Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security, Exchange, SQL Server) and compliance assessments (HIPAA and PCI) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Cyber Risk Discovery Tasks

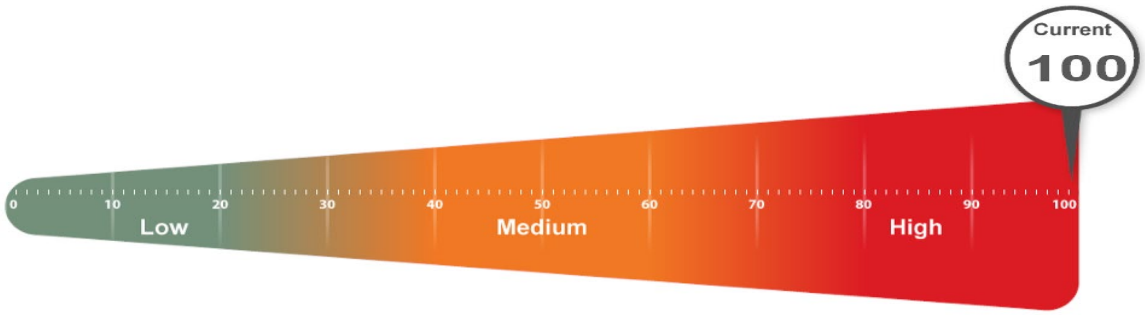
The following discovery tasks were performed.

	Task	Description
Network		
☐	Detect Domain Controllers	Identifies domain controllers and online status.
☐	FSMO Role Analysis	Enumerates FSMO roles at the site.
☐	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
☐	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
☐	Detect Local Mail Servers	Detects mail server(s) on the network.
☐	Detect Time Servers	Detects server(s) on the network.
☐	Discover Network Shares	Discovers the network shares by server.
☐	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
☐	Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
☐	Web Server Discovery and Identification	Lists the web servers and type.
☐	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
☐	Internet Access and Speed Test	Tests Internet access and performance.
☐	SQL Server Analysis	Lists the SQL Servers and associated database(s).
☐	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
☐	Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk.
☐	Missing Security Updates	Uses MBSA to identify computers missing security updates.
☐	System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
☐	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.
Security		
☐	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
☐	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
☐	Detect User Controls	Determines if controls are in place for user web browsing.
☐	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
☐	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.

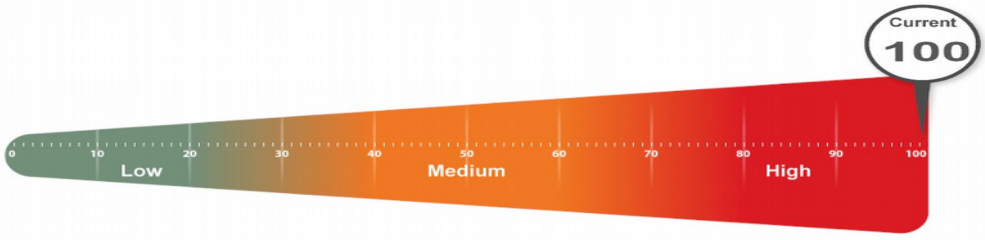
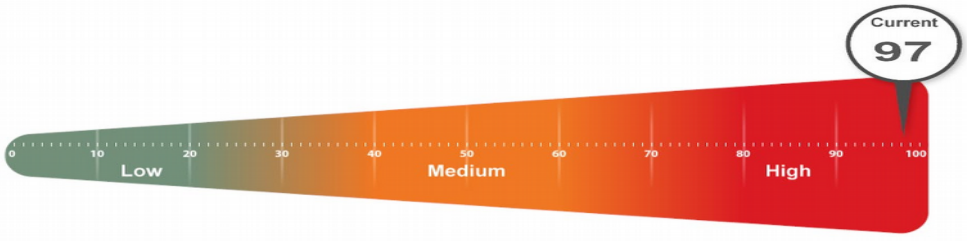
	Task	Description
☐	Network Share Permissions	Documents access to file system shares.
☐	Domain Security Policy	Documents domain computer and domain controller security policies.
☐	Local Security Policy	Documents and assesses consistency of local security policies.

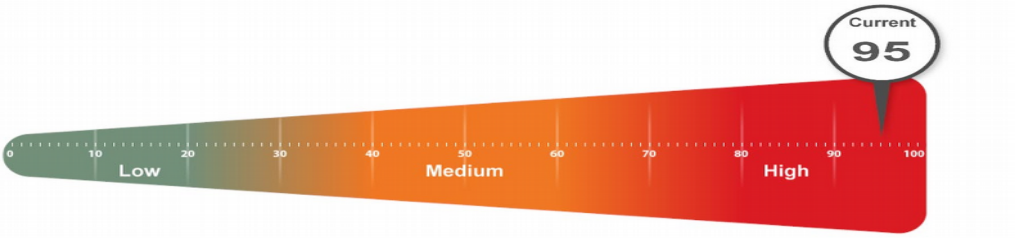
Cyber Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



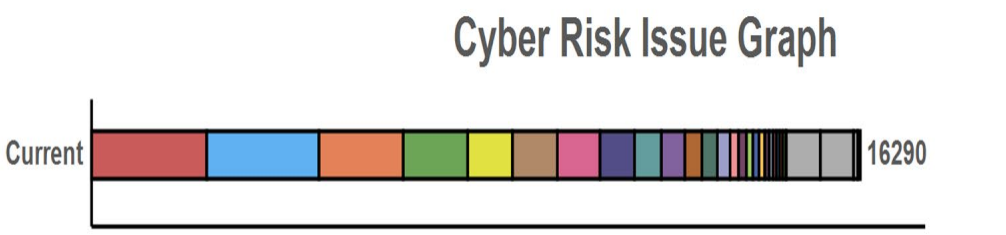
Several critical issues were identified. Identified issues should be investigated and addressed according to the Cyber Risk Analysis Report.

Module	Risk Score
Cyber Liability	
Network	

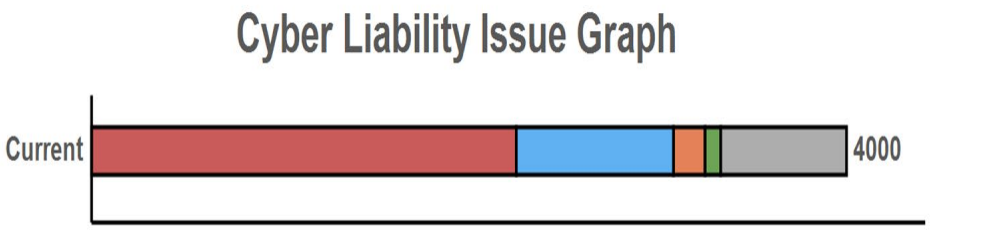
Module	Risk Score
Security	

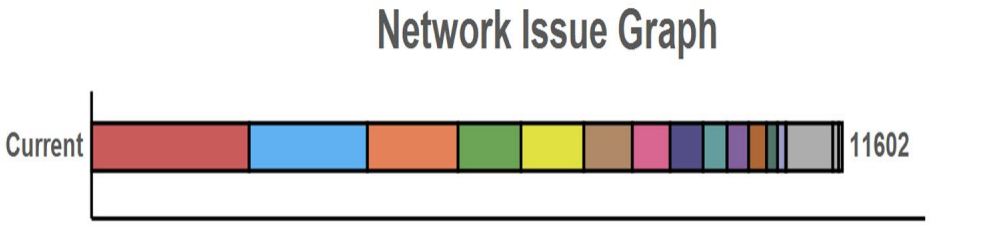
Cyber Risk Issue Graph

This section contains a summary of issues detected during the Cyber Risk Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)





Cyber Risk Issue Summary

Cyber Liability Issue Summary

	Verified incorrect response: Missing updated anti-virus (100 pts each)
2700	***Current Score:*** 100 pts x 27 = 2700: 67.5%
	Issue: You indicated that anti-virus is installed and updated on computer systems in the network; however, some computers were detected as not having updated anti-virus.
	Recommendation: Modify your response on your insurance application or install and update anti-virus on indicated computers.

	Verified incorrect response: high risk external vulnerabilities detected (100 pts each)
1000	***Current Score:*** 100 pts x 10 = 1000: 25%
	Issue: You indicated that systems in your Internet/DMZ environment are secure; however, an external vulnerability scan found issues with CVSS scores greater than 4 indicating a high risk.
	Recommendation: Modify your response on your insurance application or secure systems in your Internet/DMZ environment.

	Verified incorrect response: Terminated users with enabled accounts found (100 pts each)
200	***Current Score:*** 100 pts x 2 = 200: 5%
	Issue: You indicated that the company has established processes to ensure proper account management, including terminating computer access when an employee leaves the company. Users that were marked as terminated were found with enabled accounts.
	Recommendation: Disable all accounts from terminated users.

	Verified incorrect response: high risk internal vulnerabilities detected (100 pts each)
100	***Current Score:*** 100 pts x 1 = 100: 2.5%
	Issue: You indicated that systems in your internal environment are secure; however, some high-risk vulnerabilities were found.
	Recommendation: Modify your response on your insurance application or address all high-risk internal vulnerabilities as indicated in the Cyber Risk Management Plan.

	Verified incorrect response: Unsupported Operating Systems found ~~*(100 pts each)*~~
0	***Current Score:*** ~~100 pts x 10 = 800: 0%~~
	Issue: You indicated that the company does not use software or hardware that has been officially retired; however, some computers with Operating Systems considered “end-of-life”.
	Recommendation: ~~Modify your response on your insurance application or discontinue use or upgrade systems with unsupported Operating Systems.~~
	Exception Explanation: See Security Exception Worksheet

Network Issue Summary

	Anti-virus not installed (94 pts each)
2632	***Current Score:*** 94 pts x 28 = 2632: 22.69%
	Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend ensuring that anti-virus is deployed to all possible endpoints.

	Anti-spyware not installed (94 pts each)
1974	***Current Score:*** 94 pts x 21 = 1974: 17.01%
	Issue: Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.

	Inactive computers (15 pts each)
1515	***Current Score:*** 15 pts x 101 = 1515: 13.06%
	Issue: Computers have not checked in during the past 30 days
	Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, or powered on.

	User password set to never expire (30 pts each)
1050	***Current Score:*** 30 pts x 35 = 1050: 9.05%
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

	Significantly high number of Domain Administrators (35 pts each)
1050	***Current Score:*** 35 pts x 30 = 1050: 9.05%
	Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
	Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

	Anti-spyware not up to date (90 pts each)

810	***Current Score:*** 90 pts x 9 = 810: 6.98%
	Issue: Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.
	Recommendation: Ensure anti-spyware definitions are up to date on specified computers.

	Anti-virus not up to date (90 pts each)
630	***Current Score:*** 90 pts x 7 = 630: 5.43%
	Issue: Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.
	Recommendation: Ensure anti-virus definitions are up to date on specified computers.

	Anti-spyware not turned on (92 pts each)
552	***Current Score:*** 92 pts x 6 = 552: 4.76%
	Issue: We were unable to determine if anti-spyware software is enabled and running on some computers.
	Recommendation: Determine if anti-spyware is enabled properly.

	Operating system in Extended Support (20 pts each)
400	***Current Score:*** 20 pts x 20 = 400: 3.45%
	Issue: Computers are using an operating system that is in Extended Supported. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.
	Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

	Excessive security patches missing on computers (90 pts each)
360	***Current Score:*** 90 pts x 4 = 360: 3.1%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Lots is defined as missing four or more patches.
	Recommendation: Address patching on computers missing 4+ security patches.

	User has not logged on to domain in 30 days (13 pts each)
299	***Current Score:*** 13 pts x 23 = 299: 2.58%
	Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

	Anti-virus not turned on (92 pts each)

184	***Current Score:*** 92 pts x 2 = 184: 1.59%
	Issue: We were unable to determine if anti-virus software is enabled and running on some computers.
	Recommendation: Determine if anti-virus is enabled properly.

	Potential disk space issue (68 pts each)
136	***Current Score:*** 68 pts x 2 = 136: 1.17%
	Issue: 2 computers were found with significantly low free disk space.
	Recommendation: Free or add additional disk space for the specified drives.

	Un-populated organization units (10 pts each)
10	***Current Score:*** 10 pts x 1 = 10: 0.09%
	Issue: Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.
	Recommendation: Remove or populate empty organizational units.

	Unsupported operating systems ~~*(97 pts each)*~~
0	***Current Score:*** ~~97 pts x 10 = 776: 0%~~
	Issue: found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.
	Recommendation: ~~Upgrade or replace computers with operating systems that are no longer supported.~~
	Exception Explanation: See Security Exception Worksheet

	Potential password strength risks ~~*(100 pts each)*~~
0	***Current Score:*** ~~100 pts x 2 = 100: 0%~~
	Issue: Local account passwords on 2 accounts were found to be potentially weak. Inadequate or weak passwords on local accounts can allow a hacker to compromise the system. It can also lead to the spread of malicious software that can cause business and productivity affecting issues.
	Recommendation: ~~We recommend placing adequate password strength requirements in place and remediating the immediate password issues on the identified systems.~~
	Exception Explanation: See Compensating Control Worksheet

	Insecure listening ports ~~*(10 pts each)*~~
0	***Current Score:*** ~~10 pts x 7 = 60: 0%~~
	Issue: Computers are using potentially insecure protocols.
	Recommendation: ~~There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security.~~

Exception Explanation: See Security Exception Worksheet

Security Issue Summary

	Password complexity not enabled (75 pts each)
150	***Current Score:*** 75 pts x 2 = 150: 21.8%
	Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
	Recommendation: Enable password complexity to assure domain account passwords are secure.

	Automatic screen lock not turned on (72 pts each)
144	***Current Score:*** 72 pts x 2 = 144: 20.93%
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Critical External Vulnerabilities Detected (95 pts each)
95	***Current Score:*** 95 pts x 1 = 95: 13.81%
	Issue: Critical external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

	Account lockout disabled (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77: 11.19%
	Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
	Recommendation: Enable account lockout for all users.

	Passwords less than 8 characters allowed (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 10.9%
	Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.
	Recommendation: Enable enforcement of password length to more than 8 characters.

	Medium External Vulnerabilities Detected (75 pts each)

75	***Current Score:*** 75 pts x 1 = 75: 10.9%
	Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

	Password history not remembered for at least six passwords (72 pts each)
72	***Current Score:*** 72 pts x 1 = 72: 10.47%
	Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.
	Recommendation: Increase password history to remember at least six passwords.

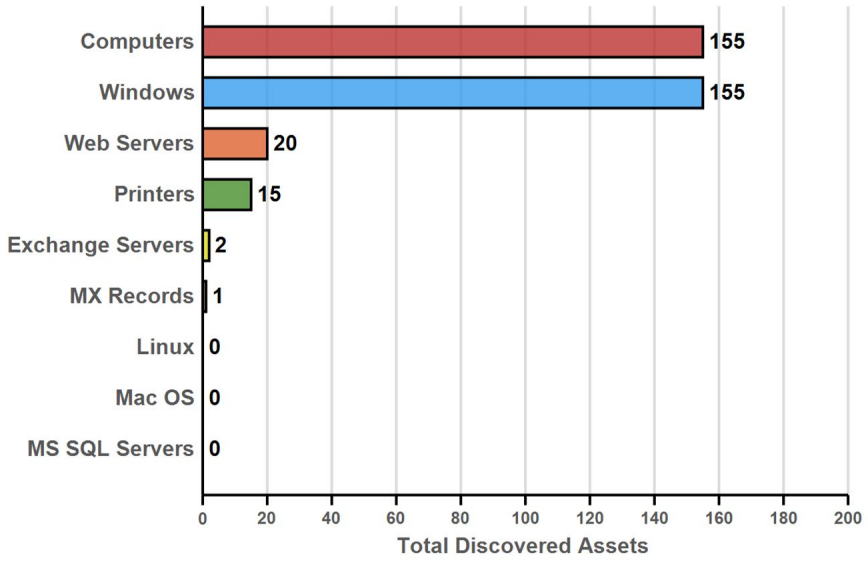
	Open or insecure WiFi protocols available ~~*(50 pts each)*~~
0	***Current Score:*** ~~50 pts x 1 = 0: 0%~~
	Issue: Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.
	Recommendation: ~~Ensure company's WiFi is secure and discourage the use of any open WiFi connections.~~
	Exception Explanation: See Compensating Control Worksheet

Internet Speed Test Results

Download Speed: **50.10 Mb/s**

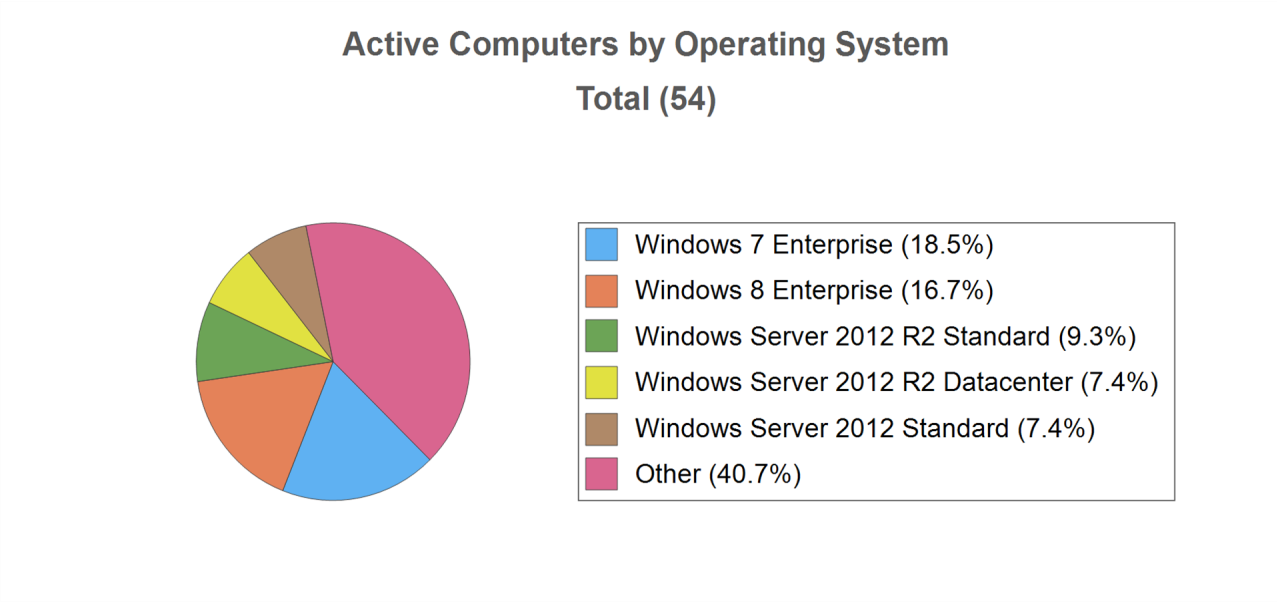
Upload Speed: **22.02 Mb/s**

Asset Summary: Total Discovered Assets



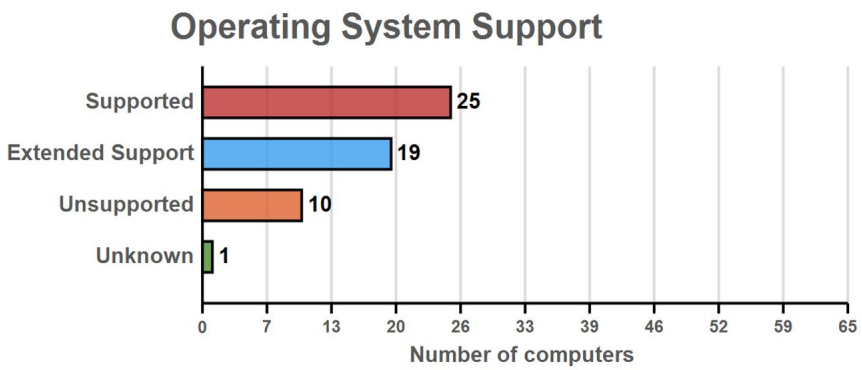
Asset Summary: Active Computers

Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.



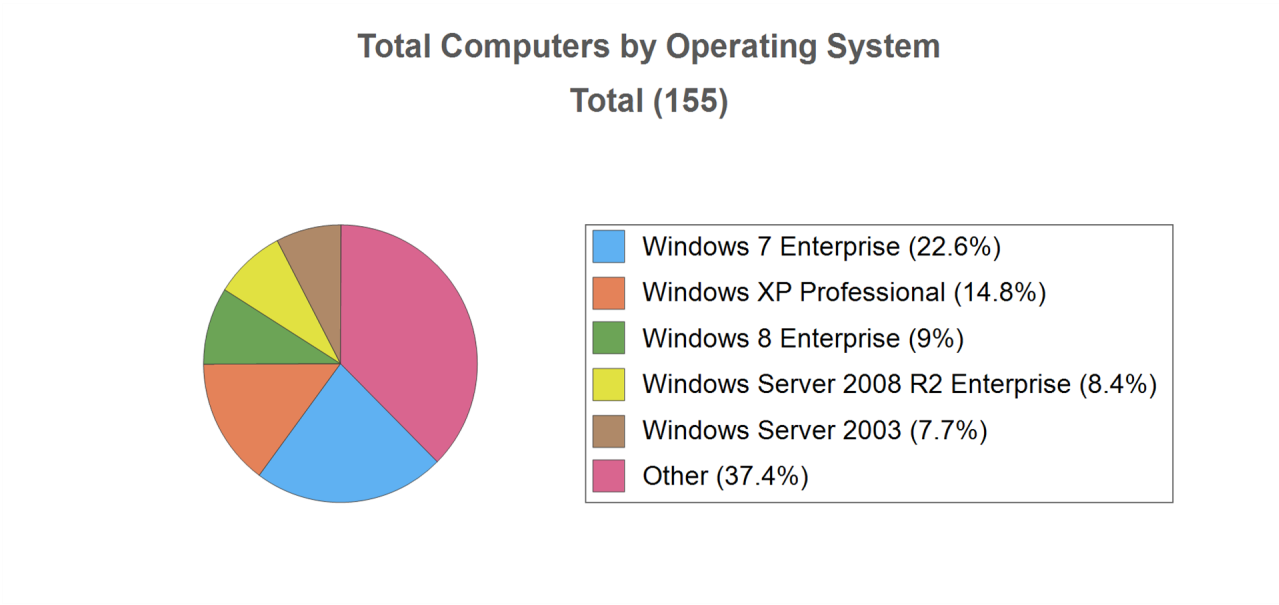
Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	10	18.5%
Windows 8 Enterprise	9	16.7%
Windows Server 2012 R2 Standard	5	9.3%
Windows Server 2012 R2 Datacenter	4	7.4%
Windows Server 2012 Standard	4	7.4%
Total - Top Five	**32**	**59.3%**
Other		
Windows 2000 Server	3	5.6%
Windows 8.1 Enterprise	3	5.6%
Windows Server 2003	3	5.6%
Windows 7 Professional	2	3.7%
Windows 8.1 Pro	2	3.7%
Windows Server 2003 R2	2	3.7%
Hyper-V Server 2012	1	1.9%
Windows 2000	1	1.9%
Windows 8 Pro	1	1.9%
Windows Server 2008 R2 Datacenter	1	1.9%
Windows Server 2008 R2 Enterprise	1	1.9%

Operating System	Total	Percent
Windows Server 2012 Datacenter	1	1.9%
Windows Vista (TM) Business	1	1.9%
Total - Other	**22**	**40.7%**
Overall Total	**54**	**100%**



Asset Summary: All Computers

The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a domain environment).

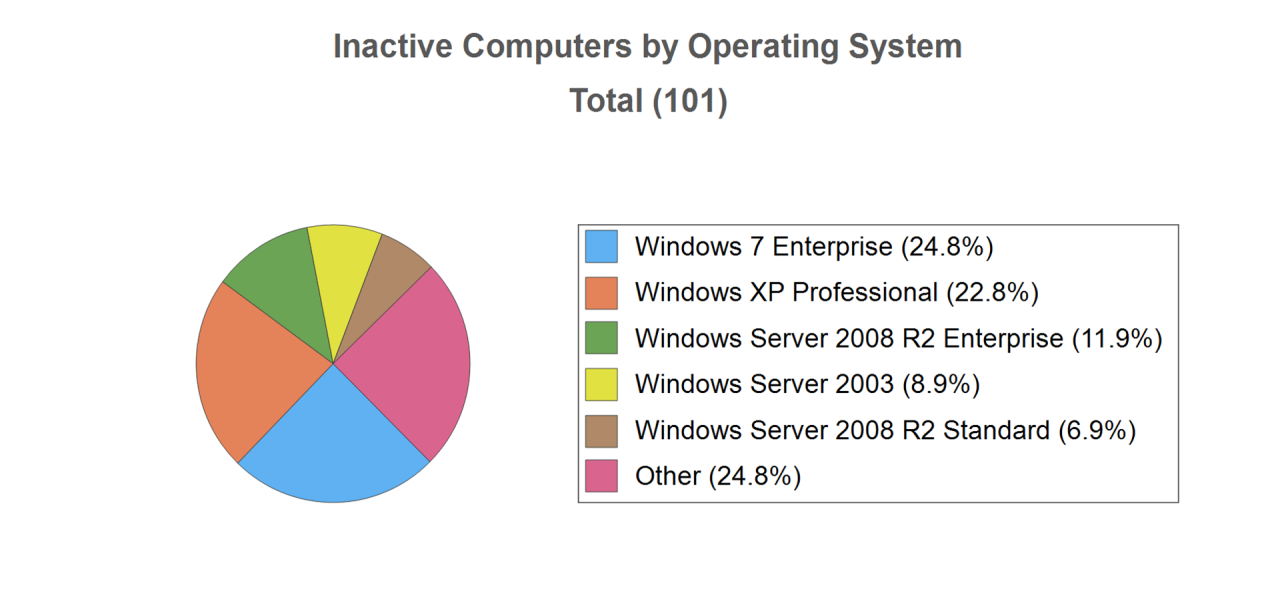


Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	35	22.6%
Windows XP Professional	23	14.8%
Windows 8 Enterprise	14	9%
Windows Server 2008 R2 Enterprise	13	8.4%
Windows Server 2003	12	7.7%
Total - Top Five	**97**	**62.6%**
Other		
Windows Server 2008 R2 Standard	7	4.5%
Windows Server 2012 Standard	7	4.5%
Windows 2000 Server	5	3.2%
Windows Server 2012 R2 Datacenter	5	3.2%
Windows Server 2012 R2 Standard	5	3.2%
Windows 7 Professional	4	2.6%
Windows 7 Ultimate	4	2.6%
Unidentified OS	3	1.9%
Windows 8.1 Enterprise	3	1.9%
Windows 8.1 Pro	2	1.3%
Windows Server 2003 R2	2	1.3%

Operating System	Total	Percent
Windows Server 2012 Datacenter	2	1.3%
Hyper-V Server 2012	1	0.6%
Windows 2000	1	0.6%
Windows 8 Consumer Preview	1	0.6%
Windows 8 Pro	1	0.6%
Windows Server 2008 Enterprise	1	0.6%
Windows Server 2008 R2 Datacenter	1	0.6%
Windows Server 2008 Standard	1	0.6%
Windows Vista (TM) Business	1	0.6%
Windows Vista Ultimate	1	0.6%
Total - Other	**58**	**37.4%**
Overall Total	**155**	**100%**

Asset Summary: Inactive Computers

Inactive computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

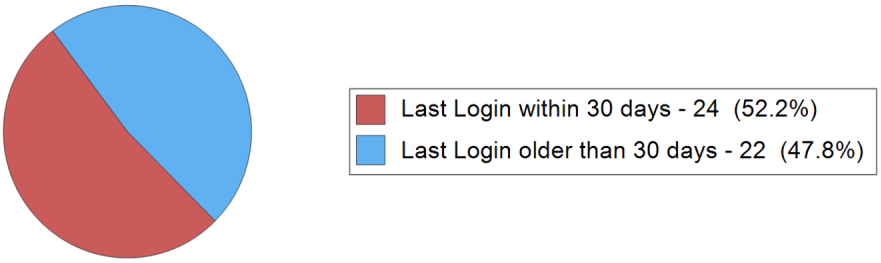


Operating System	Total	Percent
Top Five		
Windows 7 Enterprise	25	24.8%
Windows XP Professional	23	22.8%
Windows Server 2008 R2 Enterprise	12	11.9%
Windows Server 2003	9	8.9%
Windows Server 2008 R2 Standard	7	6.9%
Total - Top Five	**76**	**75.2%**
Other		
Windows 8 Enterprise	5	5%
Windows 7 Ultimate	4	4%
Unidentified OS	3	3%
Windows Server 2012 Standard	3	3%
Windows 2000 Server	2	2%
Windows 7 Professional	2	2%
Windows 8 Consumer Preview	1	1%
Windows Server 2008 Enterprise	1	1%
Windows Server 2008 Standard	1	1%
Windows Server 2012 Datacenter	1	1%
Windows Server 2012 R2 Datacenter	1	1%

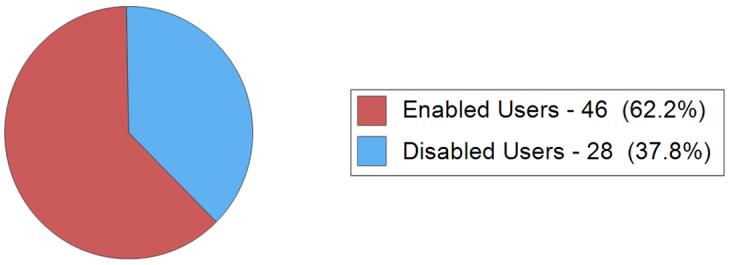
Operating System	Total	Percent
Windows Vista Ultimate	1	1%
Total - Other	**25**	**24.8%**
Overall Total	**101**	**100%**

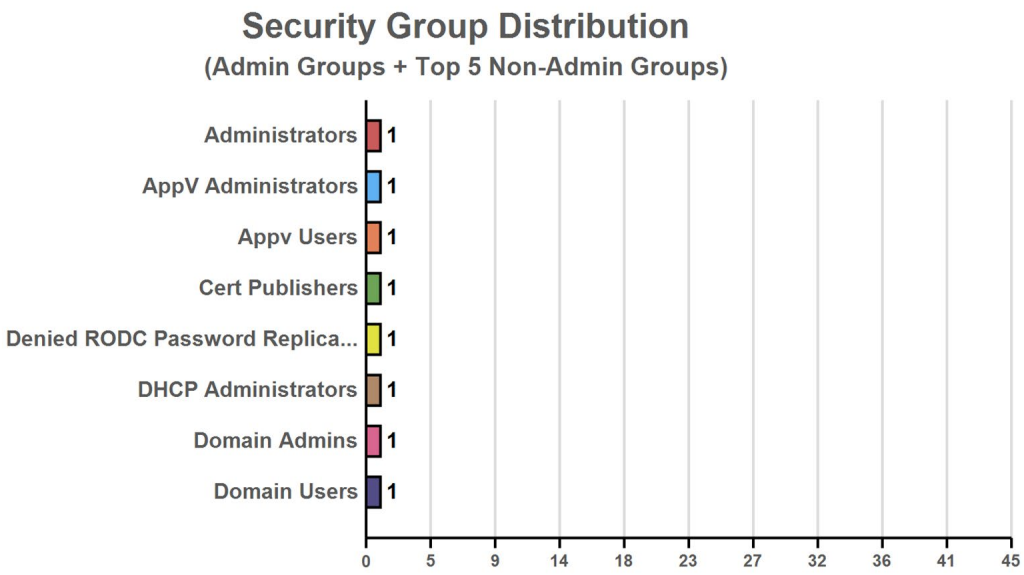
Asset Summary: Users

Users Logged in

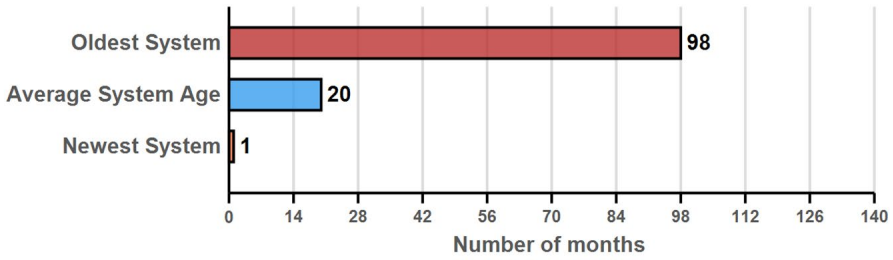


Total Users

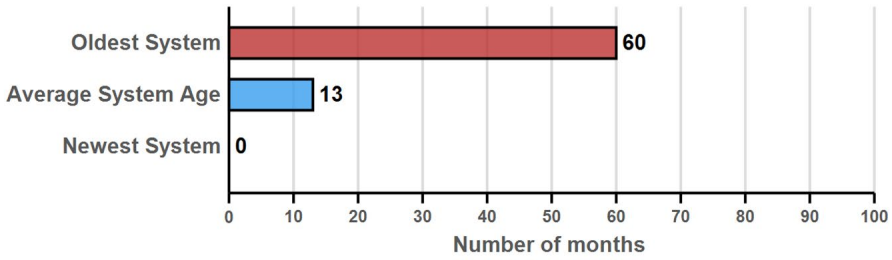



Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Administrators
1
AppV Administrators
1
Appv Users
1
Cert Publishers
1
Denied RODC Password Replica...
1
DHCP Administrators
1
Domain Admins
1
Domain Users
1
0
5
9
14
18
23
27
32
36
41
45

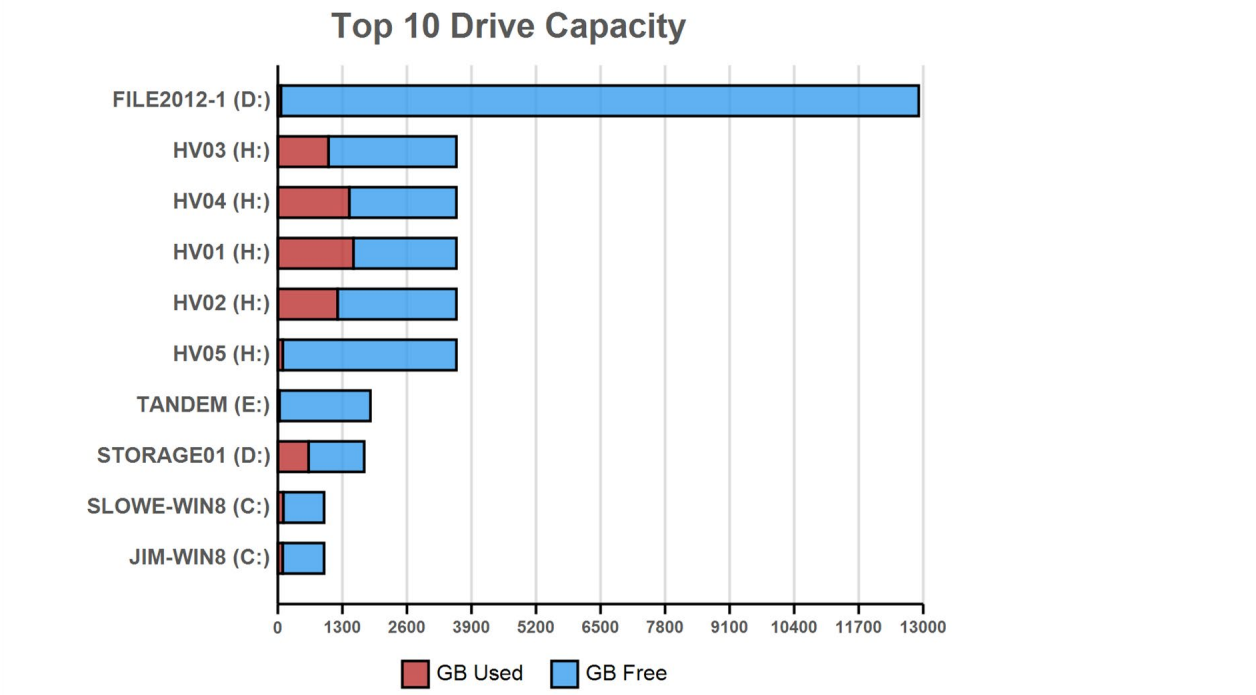
Server Aging

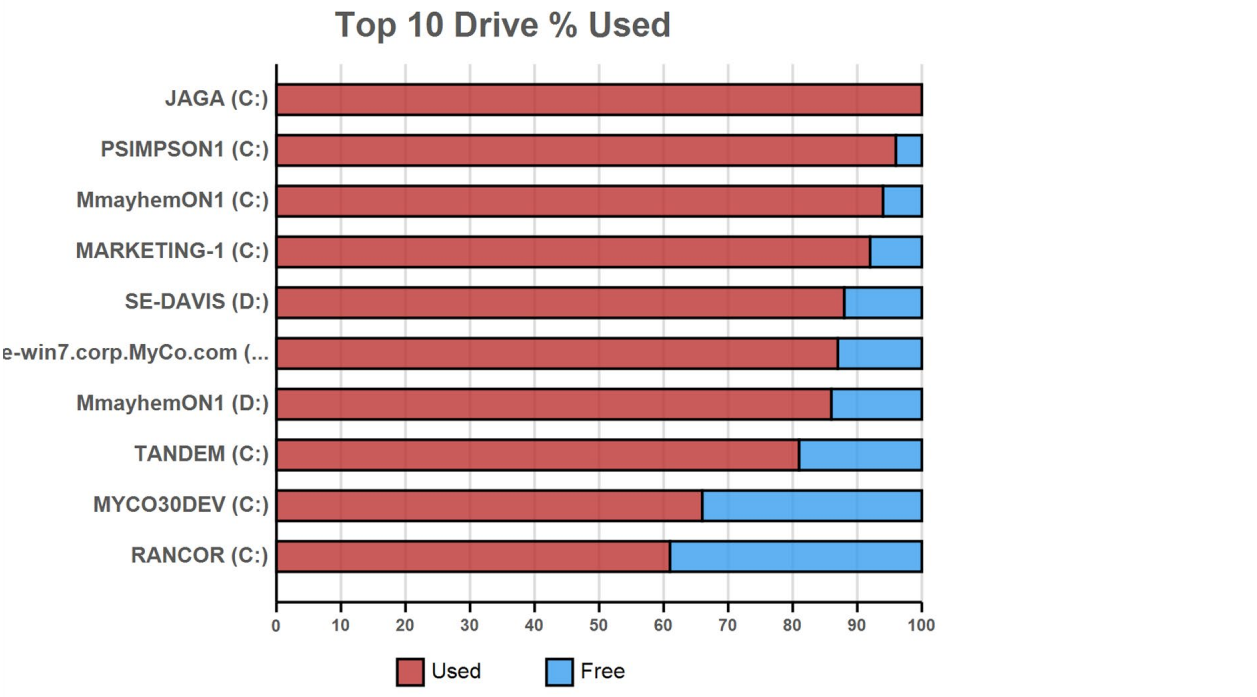


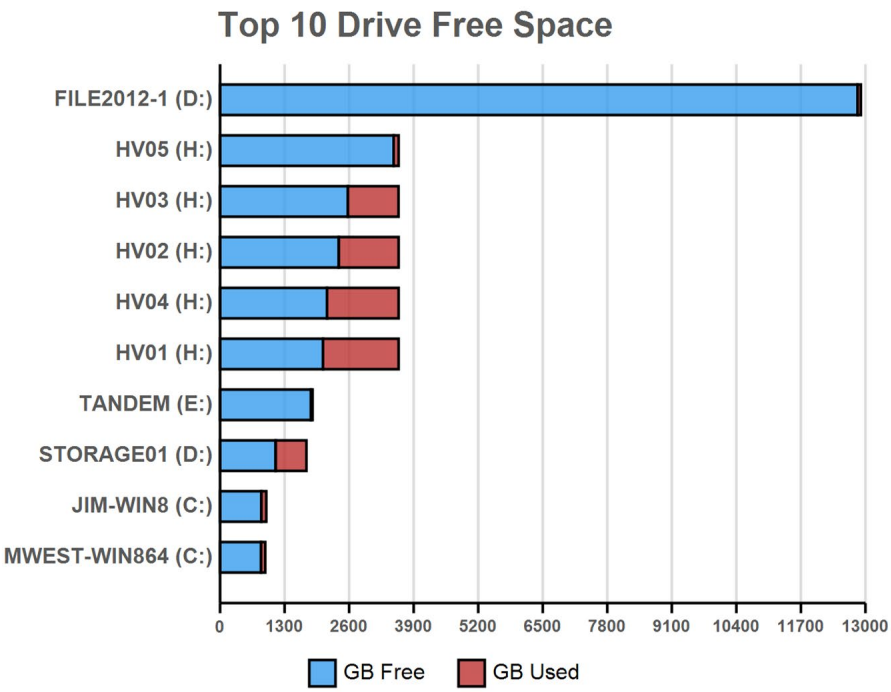
Workstation Aging



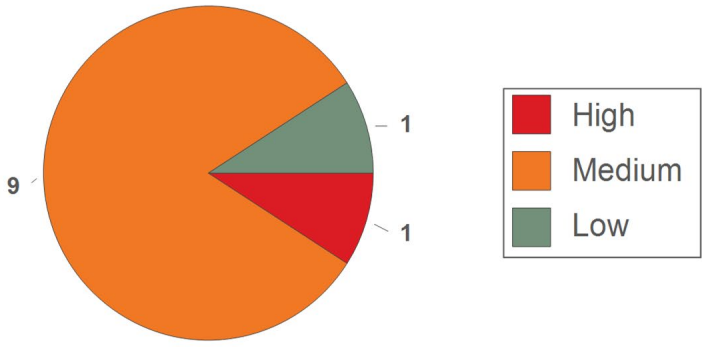
Asset Summary: Storage





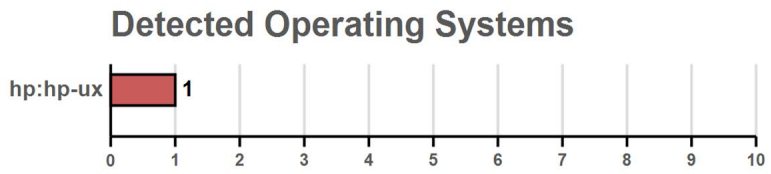

Top 10 Drive Free Space
FILE2012-1 (D:)
HV05 (H:)
HV03 (H:)
HV02 (H:)
HV04 (H:)
HV01 (H:)
TANDEM (E:)
STORAGE01 (D:)
JIM-WIN8 (C:)
MWEST-WIN864 (C:)
0
1300
2600
3900
5200
6500
7800
9100
10400
11700
13000
GB Free
GB Used

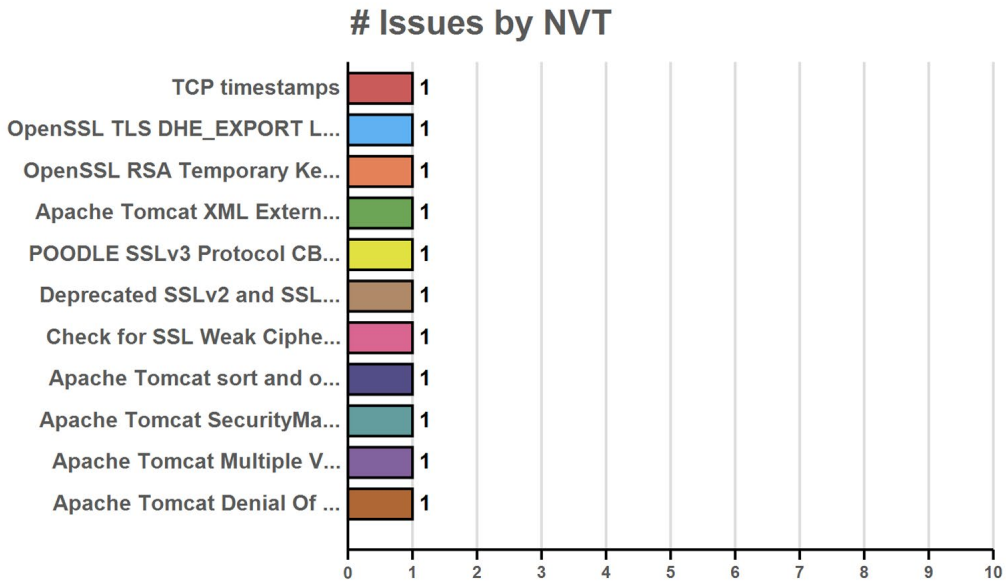
External Vulnerabilities



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
208.32.211.104	2	1	9	1	0	7.8
Total: 1	2	1	9	1	0	7.8





Issue	Count
TCP timestamps	1
OpenSSL TLS DHE_EXPORT LogJam Man in the Middle Security Bypass Vulnerability	1
OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)	1
Apache Tomcat XML External Entity Information Disclosure Vulnerability	1
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	1
Deprecated SSLv2 and SSLv3 Protocol Detection	1
Check for SSL Weak Ciphers	1
Apache Tomcat sort and orderBy Parameters Cross Site Scripting Vulnerabilities	1
Apache Tomcat SecurityManager Security Bypass Vulnerability -June15 (Linux)	1
Apache Tomcat Multiple Vulnerabilities-01 (Nov14)	1
Apache Tomcat Denial Of Service Vulnerability -June15 (Linux)	1

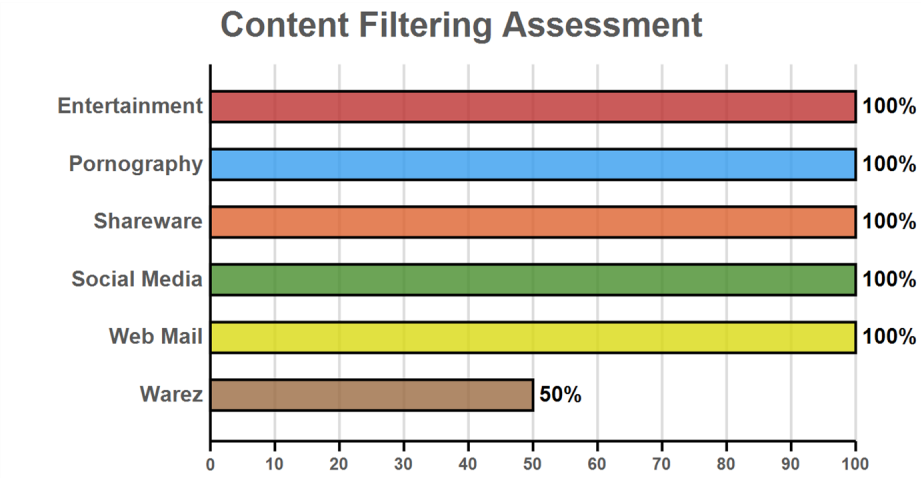
Internal Vulnerabilities

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
Total: 0	0	0	0	0	0	0.0

Unrestricted Web Content



Local Security Policy Consistency