Vulnerability Assessment and Risk Analysis

Contents

1 Executive Summary 7
2 Previous Information Security Assessments 7
3 Assessment Methodology 7
4 Assessment Findings – Vulnerabilities and Recommendations 8
4.1 Overview: Risk Totals by Rating 8
4.2 Scoring 8
4.2.1 Risk Rating Legend 8
4.3 Identified Vulnerabilities 9
4.3.1 [CRITICAL] OpenSSL CCS Security Bypass Vulnerability 9
4.3.2 [CRITICAL] Apache Tomcat Manager Common Administrative Credentials 9
4.3.3 [CRITICAL] Microsoft XML Parser (MSXML) and XML Core Services Unsupported 9
4.3.4 [CRITICAL] Oracle Java Insecure Version 10
4.3.5 [CRITICAL] McAfee Antivirus Detection 10
4.3.6 [CRITICAL] Unsupported Operating System Detection 10
4.3.7 [CRITICAL] Adobe Reader Insecure Version 10
4.3.8 [CRITICAL] HP System Management Homepage Insecure Version 11
4.3.9 [CRITICAL] Missing Critical OS Security Patches/Updates 11
4.3.10 [CRITICAL] SSL 3.0 Information Disclosure Vulnerability (POODLE) 11
4.3.11 [CRITICAL] Bash Remote Code Execution (Shellshock) 11
4.3.12 [HIGH] High Number of User Accounts Members of Domain Admins Group 12
4.3.13 [HIGH] Active Directory Account Cleanup 12
4.3.14 [HIGH] Active Directory Non-Expiring Passwords 12
4.3.15 [HIGH] Unencrypted Telnet Server 13
4.3.16 [HIGH] Web Server Transmits Cleartext Credentials 13
4.3.17 [HIGH] Permissions on Shared Folder \shares\sharedrive\ 13
4.3.18 [HIGH] “Everyone” Permission on Shared Folder \\vm-srv13\shares\ 14
4.3.19 [HIGH] “Everyone” Permission on Shared Folder \\corex\importexport\ 14
4.3.20 [HIGH] “Everyone” Permission on Shared Folder \\corex\importexport2\ 14
4.3.21 [HIGH] “Everyone” Permission on Shared Folder \\sql01\webbackup\ 15
4.3.22 [HIGH] “Everyone” Permission on Shared Folder \\sqldb\webbackup\ 15
4.3.23 [HIGH] “Everyone” Permission on Shared Folder \\core\pdpfiles\ 15
4.3.24 [HIGH] “Everyone” Permission on Shared Folder \\data\reports\ 16

4.3.25 [HIGH] “Everyone” Permission on Shared Folder \\rcd\1\ 16
4.3.26 [HIGH] “Everyone” Permission on Shared Folder \\rcd\primaryrecordings\ 16
4.3.27 [HIGH] “Everyone” Permission on Shared Folder \\web01\apps\ 17
4.3.28 [HIGH] “Everyone” Permission on Shared Folder \\web01\documents\ 17
4.3.29 [HIGH] “Everyone” Permission on Shared Folder \\rcd\primaryrecordings2\ 17
4.3.30 [HIGH] Corporate Antivirus Compliance 18
4.3.31 [HIGH] Data-at-Rest Encryption for PII or Sensitive Data 18
4.3.32 [HIGH] Portable Devices Missing Disk Encryption 18
4.3.33 [HIGH] P2P Applications Detected on Network 19
4.3.34 [HIGH] Microsoft Windows Guest Account Belongs to a Group 19
4.3.35 [HIGH] Vulnerability in Group Policy 19
4.3.36 [HIGH] Insecure Library Loading Could Allow Remote Code Execution 20
4.3.37 [HIGH] Windows Unquoted Service Path Enumeration 20
4.3.38 [HIGH] Insecure Windows Service Permissions 20
4.3.39 [HIGH] SizerOne ActiveX Control AddTab Method Remote Buffer Overflow 21
4.3.40 [HIGH] Missing Important OS Security Patches/Updates 21
4.3.41 [HIGH] Apache HTTP Server Insecure Version 21
4.3.42 [HIGH] Adobe Flash Insecure Version 21
4.3.43 [HIGH] Wireshark Insecure Version 22
4.3.44 [HIGH] VMware vSphere Insecure Version 22
4.3.45 [HIGH] Unencrypted Traffic Over WAN Connections 22
4.3.46 [HIGH] Main Office Demark Security 23
4.3.47 [HIGH] Main Office Server Room HVAC 23
4.3.48 [HIGH] OpenSSH MaxAuthTries Bypass 23
4.3.49 [MEDIUM] “Everyone” Permissions on Shared Folder \shares\apps\ 24
4.3.50 [MEDIUM] Generic User Account Member of “Administrators” Group 24
4.3.51 [MEDIUM] Generic User Account Member of “VPN Users” Group 24
4.3.52 [MEDIUM] Review Group Policy Settings 25
4.3.53 [MEDIUM] SSL/TLS EXPORT_RSA 512-bit Cipher Suites Supported (FREAK) 25
4.3.54 [MEDIUM] Transport Layer Security (TLS) Protocol Vulnerability (CRIME) 25
4.3.55 [MEDIUM] Dell OpenManage Server Administrator XSS Vulnerability 26
4.3.56 [MEDIUM] SSL/TLS Diffie-Hellman Modulus 1024 Bits (Logjam) 26
4.3.57 [MEDIUM] SSL/TLS EXPORT_DHE 512-bit Export Cipher Suites Supported (Logjam) 26

4.3.58 [MEDIUM] ESXi 5.1 Third-Party Libraries Multiple Vulnerabilities (BEAST) 27
4.3.59 [MEDIUM] Apache Tomcat Multiple Vulnerabilities (FREAK) 27
4.3.60 [MEDIUM] SNMP Agent Default Community Names 27
4.3.61 [MEDIUM] SNMP 'GETBULK' Reflection DDoS 27
4.3.62 [MEDIUM] SSL RC4 Cipher Suites Supported 28
4.3.63 [MEDIUM] SSL Version 2 and 3 Protocol Detection 28
4.3.64 [MEDIUM] Web Application Potentially Vulnerable to Clickjacking 28
4.3.65 [MEDIUM] HTTP TRACE / TRACK Methods Allowed 29
4.3.66 [MEDIUM] SSL/TLS Renegotiation Handshakes Plaintext Data Injection 29
4.3.67 [MEDIUM] Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness 29
4.3.68 [MEDIUM] Terminal Services Encryption Level is Set to Medium 30
4.3.69 [MEDIUM] SMB Signing Disabled 30
4.3.70 [MEDIUM] SSL Certificate Signed Using Weak Hashing Algorithm 30
4.3.71 [MEDIUM] SSL Low or Medium Strength Cipher Suites Supported 30
4.3.72 [MEDIUM] Windows SMB NULL Session Authentication 31
4.3.73 [MEDIUM] Windows LM / NTLMv1 Authentication Enabled 31
4.3.74 [MEDIUM] Dropbear SSH Server Insecure Version 31
4.3.75 [MEDIUM] User Cyber-Security Training 32
4.3.76 [LOW] Winlogon Cached Password Weakness 32
4.3.77 [LOW] Active Directory Computer Cleanup 32
4.3.78 [LOW] Active Directory Structure Cleanup 32
4.3.79 [LOW] Ethernet Driver Frame Padding Information Disclosure (Etherleak) 33
4.3.80 [LOW] DHCP Server Detection 33
4.3.81 [LOW] VMware ESXi NTP monlist Command Enabled 33
4.3.82 [LOW] Microsoft Windows LAN Manager SNMP LanMan Services Disclosure 34
4.3.83 [LOW] SSH Weak MAC Algorithms Enabled 34
4.3.84 [LOW] SSH Server CBC Mode Ciphers Enabled 34
4.3.85 [LOW] DNS Server Cache Snooping Remote Information Disclosure 34
4.3.86 [LOW] Network daemons not managed by the package system 35
4.3.87 [LOW] Web Filtering 35
4.3.88 [LOW] SSL Certificate Chain Contains RSA Keys Less Than 2048 bits 35
5 Remediation Intelligence – At a Glance 36
5.1 Line-of-Business Software 36

5.2 Misconfigurations and Oversights 36
5.3 Missing Software and Firmware Updates 36
6 Conclusions 37
Appendix A – References 38
Appendix B – Physical Environment Assessment Detail 39
Scoring Legend: 39
Appendix C – Employee Security Awareness Training Program 41
Key Benefits 41
Program Management 41
Cost 41
Appendix D – Remediation Level of Effort (LOE) 42
Table 1: Critical-Severity Vulnerability Remediation 42
Table 2: High-Severity Vulnerability Remediation 42
Table 3: Medium-Severity Vulnerability Remediation 43
Table 4: Low-Severity Vulnerability Remediation 44
Table 5: Estimated Remediation Totals 45
Appendix E – Sample Document for Risk Remediation Plan 46
Appendix F – Detailed Scan Output from Network Detective 47
14 Reports, 1343 Pages 47
1. Share Permission Report 47
2. Login Failures by Computer Report 47
3. User Behavior Analysis Report 47
4. Asset Detail Report 47
5. Outbound Security Report 48
6. Security Policy Assessment 48
7. Client Risk Report 48
8. Security Risk Report 48
9. External Network Vulnerabilities Summary Report 48
10. External Vulnerability Scan Detail Report 48
11. External Vulnerability Scan Detail by Issue Report 48
12. Windows XP Migration Readiness Report 48
13. Site Diagram 48
14. Full Detail Report 48

Appendix G – Detailed Scan Output from Nessus 49
4 Reports, 14,671 Pages 49
1. Advanced Scan 49
2. Credentialed Patch Audit 49
3. Windows Malware Scan 49
4. Host Discovery 49
Appendix H – Detailed Output from the Fortinet Cyber Threat Assessment 50
1 Report, 10 Pages 50
1. Security and Threat Prevention 50
2. User Productivity 50
3. Network Utilization 50

1 Executive Summary

Istonish is pleased for the opportunity to present this vulnerability assessment and cyber security risk analysis to the organization. Conducted by Istonish, this report provides identification of risk, analysis, reporting, remediation recommendations, and end user training management. Istonish began a period of data collection on Monday, January 25th 2016 and concluded the collection on Wednesday, February 3rd. During this period a combination of in-person site surveys and automated vulnerability scans were used to gather data on the organization's information technology environment.

After all vulnerability and risk data was collected, Istonish used the following several weeks to analyze, document, translate, and compile the data into a usable guide of information contained in this report. This report aims to display a holistic view of the organization's cyber security posture. In this document you'll find a detailed description of each vulnerability or risk, why each identified vulnerability is important (and just how important it is), as well as actionable remediation steps for each item.

Istonish is thankful for the opportunity to conduct and present this assessment to the organization. With Istonish's insight into the environment and into the security controls in place, Istonish can be a valuable ally to assist in the overall remediation of these vulnerabilities as well as the management oversight of such projects.

2 Previous Information Security Assessments

Previous to this assessment, the organization had not conducted a full vulnerability and risk analysis that Istonish is aware of.

3 Assessment Methodology

1. **Computing Environment and Access Control**
    a. Account permissions and memberships
    b. Basic systems aging and asset management
    c. User behavior analysis
2. **Network Vulnerability Scanning**
    a. Expose weaknesses and misconfigurations
    b. Identify missing patches and updates
    c. Malware scans on systems
3. **Physical Security Evaluation**
    a. Physical access to systems
    b. Workstation encryption
    c. Human-level security
4. **End-User Training**
    a. User awareness and understanding

Several common, industry-standard tools and services were used to collect and evaluate this data from the target environment. Output from each tool was analyzed for vulnerabilities and then documented in this report:

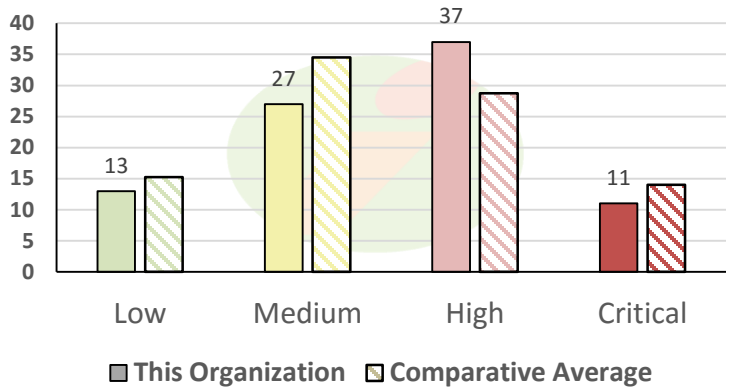
- Nessus Professional version 6.4.3.20035
- RapidFire Tools Network Detective version 3.0.1001
- Fortinet Cyber Threat Assessment Program

4 Assessment Findings – Vulnerabilities and Recommendations

This section outlines the findings discovered as a result of the security assessment.

4.1 Overview: Risk Totals by Rating

Istonish has discovered a total of eighty-eight (88) notable vulnerabilities within the environment. The following graph shows the vulnerabilities found by Istonish as detailed in this assessment, as well as a comparative average that Istonish has compiled from similar environments:



4.2 Scoring

Istonish has developed a rating methodology based loosely on those published by the National Institute of Standards and Technology in Special Publication 800-30. Below are brief descriptions of the measurements Istonish used to determine the overall risk rating that has been assigned to each threat:

Likelihood of Occurrence: An estimate of how likely the vulnerability is to be exploited over the next 12 months.

Very Likely= probable chance of occurrence
Likely= possible but improbable chance of occurrence
Not Likely= very low or insignificant chance of occurrence

Threat Impact: An estimated level of impact to the organization in the event that the listed vulnerability were to be exploited.

High= catastrophic impact on the organization; major systems outage or loss of critical data
Medium= significant impact on the organization; some impact or degradation to systems or data
Low= insignificant impact on the organization; no measurable impact to systems or data

Using the above categories, Istonish calculates and scores each vulnerability with a level of risk on a scale of Low, Medium, High, or Critical.

4.2.1 Risk Rating Legend		Threat Impact		
		Low	Medium	High
Likelihood of Occurrence	Not Likely	Low	Medium	Medium
	Likely	Medium	High	High
	Very Likely	Medium	High	Critical

4.3 Identified Vulnerabilities

Below is the list of vulnerabilities that were found or discovered in the customer environment. Each vulnerability, along with the calculated score, includes a brief overview of the vulnerability, any risk controls that are in place today, as well as suggested remediation steps to reduce the organization's risk as it pertains to the individual vulnerability.

4.3.1 [CRITICAL] OpenSSL CCS Security Bypass Vulnerability

One or more hosts facing the public internet were found to be vulnerable to an OpenSSL issue which does not properly restrict processing of ChangeCipherSpec messages. This allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information via a crafted TLS handshake (CVE-2014-0224).

Devices Affected: LAT-NSA250M (high availability pair)

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	2

Recommendation: Vulnerable appliances should be updated to the latest firmware versions as soon as possible. Dell KB article SW11605 says that the SonicWALL NSA-series firewalls are not affected by this vulnerability, however other information sources claim that this is only true for firmware versions 5.9.0.6-3o and higher.

4.3.2 [CRITICAL] Apache Tomcat Manager Common Administrative Credentials

The vulnerability scanning tool was able to gain access to the Manager web application for one or more Tomcat servers using a known set of credentials. A remote attacker can exploit this issue to install a malicious application on the affected server and run arbitrary code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix). Worms are known to propagate this way.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	2

Recommendation: Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

4.3.3 [CRITICAL] Microsoft XML Parser (MSXML) and XML Core Services Unsupported

One or more hosts were found to contain one or more unsupported versions of the Microsoft XML Parser (MSXML) or XML Core Services. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	5

Recommendation: Upgrade the software packages responsible for the unsupported DLL versions.

4.3.4 [CRITICAL] Oracle Java Insecure Version

One or more hosts were found to be running a vulnerable version of the popular Java software. Security vulnerabilities are frequently discovered and published with this software and are addressed by new versions/releases.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	3

Recommendation: Update to the latest version of Java.

4.3.5 [CRITICAL] McAfee Antivirus Detection

One or more hosts were found to be running a vulnerable version of McAfee VirusScan Enterprise (VSE) antivirus software. These vulnerabilities can result in a denial of service or an unauthorized escalation of user privileges.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	16

Recommendation: Update to the latest version of VSE.

4.3.6 [CRITICAL] Unsupported Operating System Detection

One or more hosts were found to be running an Operating System (OS) that is no longer supported by manufacturer security updates.

Detected Unsupported Versions: Microsoft Windows Server 2003; VMware ESX/ESXi 4.1.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	11

Recommendation: Upgrade the host to a supported OS or plan for the decommission of the host.

4.3.7 [CRITICAL] Adobe Reader Insecure Version

One or more hosts were found to be running a vulnerable version of the popular Adobe Reader software. Security vulnerabilities are frequently discovered and published with this software and are addressed by new versions/releases.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	1

Recommendation: Update to the latest version of Reader.

4.3.8 [CRITICAL] HP System Management Homepage Insecure Version

One or more hosts were found to be running a vulnerable version of the HP System Management Homepage software for server management. The reported version(s) are out-of-date and may contain known security flaws including cross-site scripting (XSS), buffer overflow, and Denial of Service (DoS) vulnerabilities.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	4

Recommendation: Update to the latest version of HP System Management Homepage.

4.3.9 [CRITICAL] Missing Critical OS Security Patches/Updates

One or more hosts were found to be missing Operating System (OS) security updates and patches identified by the vendor as “Critical” importance. This category of updates resolves issues which otherwise could allow exploitation of the system without any interaction from users.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	1

Recommendation: Patch the identified systems immediately.

4.3.10 [CRITICAL] SSL 3.0 Information Disclosure Vulnerability (POODLE)

One or more hosts were found to be missing one of the workarounds referenced in the Microsoft Security Advisory 3009008. SSL 3.0 uses nondeterministic CBC padding, which allows a man-in-the-middle attacker to decrypt portions of encrypted traffic using a 'padding oracle' attack. This is also known as the 'POODLE' issue.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	12

Recommendation: Apply either the Internet Explorer settings or client registry key workarounds, along with the server registry key workaround suggested by Microsoft in the advisory.

4.3.11 [CRITICAL] Bash Remote Code Execution (Shellshock)

One or more hosts were found to be running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configuration of the system, an attacker could remotely execute arbitrary code.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	High	Critical	1

Recommendation: Update Bash to a secure version.

4.3.12 [HIGH] High Number of User Accounts Members of Domain Admins Group

A high number of user accounts were found to be members of the "Domain Admins" domain security group. As members of this group, these accounts are granted administrative rights on the Active Directory domain. This configuration creates an increased risk of data loss due to the privilege and access level generally given to these users.

Member Users: admservice; administrator

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	4

Recommendation: Evaluate the business need for listed users to be members of this security group. Privileges for service accounts or vendor accounts can generally be configured in ways which do not require Domain Admin membership.

4.3.13 [HIGH] Active Directory Account Cleanup

183 active (enabled) user accounts were found that have not logged in for 30 days. This could allow unauthorized users to access the domain using these credentials.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	N/A

Recommendation: Disable or remove user accounts for users that have not logged in for 30 days. Review account termination process for gaps that may allow user accounts, particularly for former employees, to remain enabled.

4.3.14 [HIGH] Active Directory Non-Expiring Passwords

185 active (enabled) user accounts were found that have passwords set to never expire. Passwords set to never expire are more susceptible to brute-force cracking, and are also typically not changed on a regular basis.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	Medium	High	N/A

Recommendation: Review account policy and determine if changes should be made to disallow this setting on user accounts. For service accounts, ensure that coordinated password changes take place on a regular basis to reduce the security risk caused by enabling this setting. Regularly audit accounts which have this setting enabled to ensure compliance with policy.

4.3.15 [HIGH] Unencrypted Telnet Server

One or more hosts were found to be running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	4

Recommendation: Disable the Telnet service and use SSH instead.

4.3.16 [HIGH] Web Server Transmits Cleartext Credentials

One or more web pages use either Basic Authentication or contain several HTML form fields containing an input of type 'password' which transmits information to the web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	14

Recommendation: Make sure that every sensitive form transmits content over HTTPS.

4.3.17 [HIGH] Permissions on Shared Folder \shares\sharedrive\

36 explicitly-named users and groups have access to this shared folder. This high number of explicit entries creates opportunity for mismanagement, difficulty of tracking, and potential for conflicts or oversight. These problems are evidenced on this shared folder by the high number (15) of user accounts who were given access permissions in the past, but whose accounts no longer exist (shown by users represented with the account SID rather than a username). Subfolders with broken inheritance further complicate issues, and there is significant potential for data loss through unauthorized access, or by a worm/virus.

Hosted on Servers: vm-srv11; vm-srv20

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	Medium	High	2

Recommendation: Reduce the scope of access for this shared folder. Due to the size and use of this folder, this will likely require significant planning and restructuring of the folder hierarchy to achieve a useful and secure outcome.

4.3.18 [HIGH] "Everyone" Permission on Shared Folder \\vm-srv13\shares\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: vm-srv13

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.19 [HIGH] "Everyone" Permission on Shared Folder \\corex\importexport\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: corex

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.20 [HIGH] "Everyone" Permission on Shared Folder \\corex\importexport2\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: corex

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.21 [HIGH] "Everyone" Permission on Shared Folder \\sql01\webbackup\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: sql01

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.22 [HIGH] "Everyone" Permission on Shared Folder \\sqldb\webbackup\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: sqldb

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.23 [HIGH] "Everyone" Permission on Shared Folder \\core\pdpfiles\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: core

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.24 [HIGH] "Everyone" Permission on Shared Folder \\data\reports\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: data

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.25 [HIGH] "Everyone" Permission on Shared Folder \\rcd\1\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: rcd

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.26 [HIGH] "Everyone" Permission on Shared Folder \\rcd\primaryrecordings\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: rcd

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.27 [HIGH] "Everyone" Permission on Shared Folder \\web01\apps\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: web01

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.28 [HIGH] "Everyone" Permission on Shared Folder \\web01\documents\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: web01

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.29 [HIGH] "Everyone" Permission on Shared Folder \\rcd\primaryrecordings2\

The user group "Everyone" has both full Share and full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: rcd

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.30 [HIGH] Corporate Antivirus Compliance

Workstation and server scans revealed that not all organizatonal systems may be compliant with the corporate antivirus policy. These systems were identified by asset scans as not having neither AVD or McAfee VirusScan Enterprise installed, but may be using unmanaged software such as Windows Defender.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	Medium	High	24

Recommendation: Enforce compliance to centrally-managed antivirus software using technical controls, policy, or both.

4.3.31 [HIGH] Data-at-Rest Encryption for PII or Sensitive Data

Sensitive data, including PII (Personally Identifiable Information) and corporate financial data, is not stored (at rest) in an encrypted format. Security policy should be evaluated to determine whether or not this should be stored in an encrypted format, taking into account any organizational contracts that may contain requirements for this to be done.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	Unknown

Recommendation: Conduct a feasibility analysis to determine if and how data-at-rest can be stored in an encrypted format. For example, databases may use database-level encryption and file shares may use disk- or volume-level encryption. Implement these security mechanisms while ensuring that recovery keys are also stored securely.

4.3.32 [HIGH] Portable Devices Missing Disk Encryption

Scans were unable to detect a specific number of portable workstations (laptops and tablets) missing disk encryption, however it is known that a significant number of devices in the environment are not encrypted.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	Unknown

Recommendation: Mandate disk encryption with policy and choose a product that will help to manage and enforce the policy. Disk encryption should be setup as part of a standard system build or image to help enforce the deployment on all portable workstations.

4.3.33 [HIGH] P2P Applications Detected on Network

Fortinet's Cyber Threat Assessment found communications from BitComet using the internet connection at the main office. Though files did not appear to be actively shared or received during the assessment period, this shows that these applications are not blocked on the network. P2P applications pose a risk of data loss through the inadvertent sharing of files and also allow viruses to infiltrate the network when attached to downloaded files or programs that users believe to be legitimate.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Very Likely	Medium	High	Unknown

Recommendation: Block P2P applications such as BitComet/BitTorrent at all border gateways using Application Control or Intrusion Prevention systems.

4.3.34 [HIGH] Microsoft Windows Guest Account Belongs to a Group

A vulnerability was discovered in which the 'Guest' user belongs to groups other than 'Guests' (RID 546) or 'Domain Guests' (RID 514). Guest users should not have any additional privileges.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	22

Recommendation: Remove the Guest account from the Domain Users security group within Active Directory.

4.3.35 [HIGH] Vulnerability in Group Policy

One or more hosts are affected by a remote code execution vulnerability due to how the Group Policy service manages policy data when a domain-joined system connects to a domain controller. An attacker, using a controlled network, can exploit this to gain complete control of the host.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	22

Recommendation: Install Operating System (OS) patches as detailed in MS15-011. In addition to the patch(es), the GPO setting "Hardened UNC Paths" needs to be enabled.

4.3.36 [HIGH] Insecure Library Loading Could Allow Remote Code Execution

One or more hosts are missing Microsoft KB2264107 or an associated registry change, which provides a mechanism for mitigating binary planting or DLL preloading attacks.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	17

Recommendation: Install Microsoft KB2264107 and coordinate with application teams to use in conjunction with the 'CWDIllegalInDllSearch' registry setting as described in Microsoft's KB article. These protections could be applied in a way that breaks functionality in existing applications and may require significant testing.

4.3.37 [HIGH] Windows Unquoted Service Path Enumeration

One or more hosts are running at least one service installed that uses an unquoted service path, which contains at least one whitespace. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	4

Recommendation: Ensure that any services that contain a space in the path enclose the path in quotes.

4.3.38 [HIGH] Insecure Windows Service Permissions

One or more hosts are running at least one Windows service executable with insecure permissions. Services configured to use an executable with weak permissions are vulnerable to privilege escalation attacks.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Ensure the groups "Everyone," "Users," "Domain Users" and "Authenticated Users" do not have permissions to modify or write service executables. Additionally, ensure these groups do not have Full Control permission to any directories that contain service executables.

4.3.39 [HIGH] SizerOne ActiveX Control AddTab Method Remote Buffer Overflow

The SizerOne ActiveX control is installed on one or more hosts. It is included with ComponentOne Studio Enterprise as well as other applications such as TSC2 Help Desk and SAP GUI. The installed version of the control is affected by a heap-based buffer overflow vulnerability that can be triggered by adding tabs with very long captions via the control's 'AddTab()' method. If a remote attacker can trick a user on the affected host into viewing a specially crafted HTML document, this issue could be leveraged to execute arbitrary code on the affected host subject to the user's privileges.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Update to version 8.0.20081.142 of c1sizer.ocx or 7.10 PL of sizerone.ocx.

4.3.40 [HIGH] Missing Important OS Security Patches/Updates

One or more hosts were found to be missing Operating System (OS) security updates and patches identified by the vendor as “Important.” This category of updates resolves issues which otherwise could allow exploitation of the system if users disregard warnings or prompts.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	20

Recommendation: Patch the identified systems as soon as possible.

4.3.41 [HIGH] Apache HTTP Server Insecure Version

One or more hosts were found to be running a vulnerable version of the popular Apache HTTP server software (httpd). Security vulnerabilities are frequently discovered and published with this software and are addressed by new versions/releases.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	2

Recommendation: Update to the latest version of Apache.

4.3.42 [HIGH] Adobe Flash Insecure Version

One or more hosts were found to be running a vulnerable version of the popular Adobe Flash software. Security vulnerabilities are frequently discovered and published with this software and are addressed by new versions/releases.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Update to the latest version of Flash.

4.3.43 [HIGH] Wireshark Insecure Version

One or more hosts were found to be running a vulnerable version of the Wireshark packet capture software. These vulnerabilities can result in a denial of service, or possibly arbitrary code execution. A remote attacker can exploit these issues by tricking a user into opening a maliciously crafted capture file.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	2

Recommendation: Update to the latest version of Wireshark.

4.3.44 [HIGH] VMware vSphere Insecure Version

One or more hosts were found to be running a vulnerable version of the vSphere hypervisor management software. These vulnerabilities can result in memory corruption or a connection to a spoofed vCenter server.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	1

Recommendation: Patch vSphere as able or determine an alternate upgrade path.

4.3.45 [HIGH] Unencrypted Traffic Over WAN Connections

The organization uses several private-line or point-to-point WAN connections as part of its network topology. Because these links are private it is generally considered acceptable to have unencrypted traffic traversing this links, however the possibility still exists for the Service Provider or unknown other listening hosts in the route to intercept unencrypted traffic.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	N/A

Recommendation: Consider site-to-site encryption for the links between the organization's main office and the colocation data centers.

4.3.46 [HIGH] Main Office Demark Security

Security at the main office demark is essentially non-existent. The room is protected by a key lock, however it seems that access is generally readily-available and not monitored. In addition, the main demark is also an electrical closet and therefore a large number of people work in this room. Ambient temperature in this room is very warm and could contribute to frequent equipment failures, which could impact the WAN services provided to the organization.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	High	High	N/A

Recommendation: The organization should recommend security and HVAC changes to building management but is ultimately dependent on them for any improvements.

4.3.47 [HIGH] Main Office Server Room HVAC

The server room at the main office is cooled by a wall-mounted A/C unit. This A/C unit is not on backup power, so cooling will not function during power outages and, depending on the duration of the outage, could create a high-temperature condition for equipment in the server room. Additionally, this A/C unit uses a water line that runs right above one of the equipment racks. A leak in this line or with the unit itself could cause significant damage to computer equipment and possible downtime to office users or call center agents.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	N/A

Recommendation: The organization should evaluate changes to the power for this HVAC unit or implement very strict processes for mitigation of potential issues.

4.3.48 [HIGH] OpenSSH MaxAuthTries Bypass

The remote SSH server is affected by a security bypass vulnerability due to a flaw in the keyboard-interactive authentication mechanisms. A remote attacker can exploit this resulting in the ability to conduct a brute-force attack or cause a Denial of Service (DoS) condition.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Medium	High	2

Recommendation: Disable SSH on the affected hosts. Because OpenSSH is included with the VMware ESXi hypervisor running on these systems, OpenSSH cannot be updated on its own. At the time of writing the current version of ESXi still contains a vulnerable version of OpenSSH.

4.3.49 [MEDIUM] "Everyone" Permissions on Shared Folder \shares\apps\

The user group "Everyone" has full NTFS permissions to this shared folder. This effectively gives all users, including anonymous and unauthenticated users, read and write access to the folder and inheriting subfolders. This could be an avenue for worms to propagate on the network or for unauthorized employees to access sensitive data.

Hosted on Servers: vm-srv11; vm-srv20

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	2

Recommendation: Reduce the scope of access for this shared folder. At a minimum access to the folder should be given only to the user group "Authenticated Users," however this should be scoped down further to allow access on an as-needed basis.

4.3.50 [MEDIUM] Generic User Account Member of "Administrators" Group

One or more generic user accounts are members of the "Administrators" domain security group, which grants administrative control of the domain to unnamed users. This configuration can result in the mismanagement of domain systems through the inability to track changes to a specific user and poses a security risk because of the tendency to share generic passwords in a manner which are less secure and changed less frequently than named user accounts.

Member Users: user01; user02.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	N/A

Recommendation: Evaluate the business need to have these generic accounts with elevated permission and access levels.

4.3.51 [MEDIUM] Generic User Account Member of "VPN Users" Group

One or more generic user accounts are members of the "VPN Users" domain security group, which grants remote access to the Local Area Network (LAN) to unnamed users. This configuration creates risk by granting full network access to unnamed, remote users.

Member Users: wfhuser01

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Low	Medium	N/A

Recommendation: Evaluate the business need to have these generic accounts allowed to access the secure LAN remotely.

4.3.52 [MEDIUM] Review Group Policy Settings

Multiple user policies in AD Group Policy are not configured to best-practice settings.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	N/A

Recommendation: Review and implement the following settings as they relate to corporate Security Policy:

- (Password Policy) Choose to increase minimum length from 7 to 8 characters
- (Security Options) Choose to rename local administrator account to “istadmin”
- (Security Options) Change LDAP server signing requirements to Require Signature
- (Security Options) Choose to not display last user name

4.3.53 [MEDIUM] SSL/TLS EXPORT_RSA 512-bit Cipher Suites Supported (FREAK)

One or more network hosts support EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204).

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	3

Recommendation: Reconfigure the service to remove support for EXPORT_RSA cipher suites.

4.3.54 [MEDIUM] Transport Layer Security (TLS) Protocol Vulnerability (CRIME)

One or more network hosts have one of two configurations that are known to be required for the CRIME attack:

1. SSL / TLS compression is enabled.
2. TLS advertises the SPDY protocol earlier than version 4.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	4

Recommendation: Disable compression and / or the SPDY service.

4.3.55 [MEDIUM] Dell OpenManage Server Administrator XSS Vulnerability

The version of Dell OpenManage Server Administrator hosted on one or more hosts has a cross-site scripting (XSS) vulnerability. Making a specially crafted request for omalogin.html can result in client-side script injection. An attacker could exploit this by tricking a user into requesting a maliciously crafted URL.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	4

Recommendation: Upgrade Dell OpenManage Server Administrator to version 6.5, 7.0, or 7.1 and apply the appropriate patch referenced in US-CERT VU#558132.

4.3.56 [MEDIUM] SSL/TLS Diffie-Hellman Modulus 1024 Bits (Logjam)

One or more hosts allow SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	3

Recommendation: Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

4.3.57 [MEDIUM] SSL/TLS EXPORT_DHE 512-bit Export Cipher Suites Supported (Logjam)

One or more hosts support EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	3

Recommendation: Reconfigure the service to remove support for EXPORT_DHE cipher suites.

4.3.58 [MEDIUM] ESXi 5.1 Third-Party Libraries Multiple Vulnerabilities (BEAST)

One or more hosts are running VMware ESXi version 5.1 prior to build 2323236. Versions prior to this build are affected by several vulnerabilities found in bundled third-party libraries.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	2

Recommendation: Update host(s) to VMware ESXi 5.1 Update 3 (build 2323236).

4.3.59 [MEDIUM] Apache Tomcat Multiple Vulnerabilities (FREAK)

Apache Tomcat on one or more network hosts are reporting version numbers that are affected by multiple vulnerabilities.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	1

Recommendation: Upgrade to Apache Tomcat version 7.0.60 or later.

4.3.60 [MEDIUM] SNMP Agent Default Community Names

One or more network hosts are using default community strings for the Simple Network Management Protocol (SNMP).

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Low	Medium	3

Recommendation: Disable SNMP if not needed, or change the community strings to non-default values.

4.3.61 [MEDIUM] SNMP 'GETBULK' Reflection DDoS

One or more network hosts are responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this Simple Network Management Protocol (SNMP) server to conduct a reflected distributed denial of service attack on an arbitrary remote host.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	3

Recommendation: Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

4.3.62 [MEDIUM] SSL RC4 Cipher Suites Supported

One or more hosts support the use of RC4 in one or more cipher suites. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to decrypt the packets.

Detected Vulnerable Port(s): 443/tcp; 636/tcp; 1311/tcp; 1433/tcp; 2188/tcp; 2381/tcp; 3269/tcp; 3389/tcp; 5061/tcp.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	26

Recommendation: Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

4.3.63 [MEDIUM] SSL Version 2 and 3 Protocol Detection

One or more hosts accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Detected Vulnerable Port(s): 443/tcp; 636/tcp; 1311/tcp; 1433/tcp; 2381/tcp; 3269/tcp.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	15

Recommendation: Consult the application's documentation to disable SSL 2.0 and 3.0. Some affected devices may have embedded servers that do not allow direct modifications; alternative solutions for these devices should be researched, such as vendor firmware updates.

4.3.64 [MEDIUM] Web Application Potentially Vulnerable to Clickjacking

One or more hosts does not set an X-Frame-Options response header in all content responses. This could potentially expose the site to a clickjacking or UI Redress attack wherein an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

Detected Vulnerable Port(s): 80/tcp; 90/tcp; 91/tcp; 92/tcp; 443/tcp; 1311/tcp; 8080/tcp; 8085/tcp; 8180/tcp; 9880/tcp.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	23

Recommendation: Return the X-Frame-Options HTTP header with the page's response. Some affected devices may have embedded servers that do not allow direct modifications; alternative solutions for these devices should be researched, such as vendor firmware updates.

4.3.65 [MEDIUM] HTTP TRACE / TRACK Methods Allowed

One or more web servers support the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Detected Vulnerable Port(s): 90/tcp; 91/tcp; 92/tcp; 443/tcp.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	2

Recommendation: Disable these methods. Refer to the plugin output for more information.

4.3.66 [MEDIUM] SSL/TLS Renegotiation Handshakes Plaintext Data Injection

One or more hosts encrypt traffic using SSL/TLS but allows a client to insecurely renegotiate the connection after the initial handshake. This configuration could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same client and merges them at the application layer.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	5

Recommendation: Investigate the ability to use stronger encryption algorithms than SSLv3 and TLSv1.

4.3.67 [MEDIUM] Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

One or more hosts are vulnerable to a man-in-the-middle (MiTM) attack of the Remote Desktop Protocol (RDP). The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	12

Recommendation: Force the use of SSL as a transport layer for this service if supported, and/or select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

4.3.68 [MEDIUM] Terminal Services Encryption Level is Set to Medium

One or more hosts are not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. The RDP encryption level of Medium(2) or lower is not FIPS-140 compliant.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	12

Recommendation: Change RDP encryption level to either High(3) or FIPS Compliant(4).

4.3.69 [MEDIUM] SMB Signing Disabled

One of more hosts do not require signing on the hosted SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	10

Recommendation: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always).'

4.3.70 [MEDIUM] SSL Certificate Signed Using Weak Hashing Algorithm

One or more hosts use an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	8

Recommendation: Reissue certificates using a strong hashing algorithm.

4.3.71 [MEDIUM] SSL Low or Medium Strength Cipher Suites Supported

One or more hosts support the use of SSL ciphers that offer either low or medium strength encryption, which we currently regard as those with key lengths less than 112 bits.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	9

Recommendation: Reconfigure the affected application, if possible, to avoid use of low or medium strength ciphers.

4.3.72 [MEDIUM] Windows SMB NULL Session Authentication

It is possible on one or more hosts to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the hosts.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Low	Medium	10

Recommendation: Implement the following registry key settings:

1. *HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous* to 1
2. *HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess* to 1
3. Remove BROWSER from *HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes*

Reboot once the registry changes are complete.

4.3.73 [MEDIUM] Windows LM / NTLMv1 Authentication Enabled

One or more hosts are configured to attempt LM and/or NTLMv1 for outbound authentication. These protocols use weak encryption. A remote attacker who is able to read LM or NTLMv1 challenge and response packets could exploit this to get a user's LM or NTLM hash, which would allow an attacker to authenticate as that user.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	High	Medium	7

Recommendation: Change the LmCompatibilityLevel setting to 3 or higher.

4.3.74 [MEDIUM] Dropbear SSH Server Insecure Version

One or more hosts are running an out-of-date version of Dropbear SSH Server. This out-of-date version may have security flaws that allow user enumeration or Denial of Service (DoS) vulnerabilities.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Medium	Medium	1

Recommendation: Because Dropbear is included with the VMware ESXi hypervisor running on this system, Dropbear cannot be updated on its own. VMware ESXi must be updated to at least v5.0 to address this vulnerability.

4.3.75 [MEDIUM] User Cyber-Security Training

No training program appears to be in place at the organization. With a large employee base of non-technical users, this creates a knowledge gap in which users may be more prone to falling victim to things like phishing emails, malicious attachments, and social engineering.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Likely	Low	Medium	N/A

Recommendation: Begin a security training and awareness program for user education. This program should be applicable to all employees for general security training with computers, data, and the internet in general.

4.3.76 [LOW] Winlogon Cached Password Weakness

One or more hosts locally caches the passwords of the domain users when they log in, in order to continue to allow the users to log in in the case of the failure of the PDC (Primary Domain Controller).

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	21

Recommendation: Set the registry key *HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount* to 0.

4.3.77 [LOW] Active Directory Computer Cleanup

Two-hundred fifty-nine (259) inactive computer objects were found in Active Directory.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	N/A

Recommendation: Determine whether or not these computers should remain in or be removed from Active Directory.

4.3.78 [LOW] Active Directory Structure Cleanup

Ten (10) empty Organizational Units (OU's) were found in Active Directory.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	N/A

Recommendation: Empty OU's should be removed to prevent accidental misconfiguration or unintentional application of Group Policy Objects to computers and/or users.

4.3.79 [LOW] Ethernet Driver Frame Padding Information Disclosure (Etherleak)

One or more hosts use a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card. Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Follow organizational security policy for standard system configuration, and use packages supplied by the operating system vendor whenever possible.

4.3.80 [LOW] DHCP Server Detection

One or more hosts responded as a DHCP server on the network. DHCP address leases include information about the network including locations of routers, DNS servers, domain names, and more.

This item is not necessarily a vulnerability, but a possible reconnaissance vector for attackers to learn more about the local network topology.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	2

Recommendation: Limit access to DHCP addressing to only necessary network subnets, and remove any unnecessary DHCP Options that are provided to clients to minimize the information that could be inadvertently disclosed to an attacker.

4.3.81 [LOW] VMware ESXi NTP monlist Command Enabled

The version of ntpd on one or more hosts has the 'monlist' command enabled. This command returns a list of recent hosts that have connected to the service. As such, it can be used for network reconnaissance or, along with a spoofed source IP, a Distributed Denial of Service (DDoS) attack.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Apply ESXi patch ESX410-201404402-SG or update the ESXi server to a newer version that is not affected by this vulnerability.

4.3.82 [LOW] Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

One or more hosts disclose a list of LanMan services on the host in response to a remote Simple Network Management Protocol (SNMP) request with the OID 1.3.6.1.4.1.77.1.2.3.1.1. An attacker may use this information to gain more knowledge about the target host(s).

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	3

Recommendation: Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

4.3.83 [LOW] SSH Weak MAC Algorithms Enabled

The SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	9

Recommendation: Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

4.3.84 [LOW] SSH Server CBC Mode Ciphers Enabled

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	9

Recommendation: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

4.3.85 [LOW] DNS Server Cache Snooping Remote Information Disclosure

Affected DNS servers respond to queries for third-party domains that do not have the recursion bit set. This may allow an attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Review DNS architecture for possible mitigation of this risk.

4.3.86 [LOW] Network daemons not managed by the package system

Some daemon processes on one or more network hosts are associated with programs that have been installed manually. System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Follow organizational security policy for standard system configuration, and use packages supplied by the operating system vendor whenever possible.

4.3.87 [LOW] Web Filtering

Web access does not appear to be filtered by appropriate categories or ratings. This allows users to access websites that are potentially illegal or cause loss to worker productivity.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Review corporate Acceptable Use and Security policies for web access and implement technology controls as necessary to control or monitor web usage.

4.3.88 [LOW] SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

At least one of the X.509 certificates sent by the affected host(s) have a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1st 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1st 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1st 2014. Root certificates with RSA keys less than 2048 bits will not be listed as affected here if they were issued prior to December 31st 2010 as the standard considers them exempt.

Likelihood of Occurrence	Threat Impact	Calculated Risk Rating	Devices Affected
Not Likely	Low	Low	1

Recommendation: Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

5 Remediation Intelligence – At a Glance

The assessment team has noted several interesting facts about remediating the issues discovered in the environment.

5.1 Line-of-Business Software

Decommissioning the old phone platform and associated system would resolve nineteen (19) vulnerabilities listed in this document:

- Five (5) Critical
- Four (4) High
- Ten (10) Medium

Decommissioning both the old phone system and new phone system as part of the organization's ongoing upgrade initiative would resolve a total of forty-two (42) vulnerabilities listed in this document:

- Eight (8) Critical
- Eighteen (18) High
- Fourteen (14) Medium
- Two (2) Low

5.2 Misconfigurations and Oversights

A total of thirty (30) discovered vulnerabilities appear to be present due to misconfigurations or configuration oversights by users:

- Two (2) Critical
- Twenty-one (21) High
- Five (5) Medium
- Two (2) Low

These misconfigurations may have taken place at the initial install/setup of the hardware of software, or may be an ongoing oversight with system administration; this varies on a case-by-case basis.

5.3 Missing Software and Firmware Updates

A total of twenty (20) discovered vulnerabilities appear to be present due to an overwhelming amount of missing software updates (including those for Microsoft Windows as well as other products):

- Nine (9) Critical
- Six (6) High
- Four (4) Medium
- One (1) Low

Because some of the out-of-date software may have been provided or maintained by a vendor as a system component, these software packages may not have been known or it may not have been feasible to update each of them individually.

6 Conclusions

In conclusion, the organization's environment has multiple issues identified as "Critical" which need to be addressed immediately. These 'Critical' issues pose a direct threat to the security of organizational data and should be prioritized for remediation. While the number of total vulnerabilities identified in this analysis (88) is a large number, Istonish believes the majority of these to be easily remediated with some planning, testing, and upgrades to existing security technologies. Further detail on these issues can be found in the reports listed in Appendices B, F, G, and H of this document. A list of approximate Level of Efforts (LOE's) can also be found in Appendix D.

The organization's strength within its IT Department is the dedication, loyalty, and knowledge that the existing IT staff contribute to the organization. Istonish recommends that this team focus on some of the pressing issues detailed in this document, such as:

- Preventing malware from entering the network, particularly through user downloads and phishing email URL's
- Mitigation of well-known vulnerabilities, such as 'Heartbleed' and 'POODLE'
- The upkeep of systems including consistent patching of both Microsoft products and 3rd-party applications

Istonish is thankful for this opportunity to help support the organization with ongoing quality service to its customers. Overall, the results of this Vulnerability Assessment matched Istonish's expectations where the organization will have a 'Bell Curve' of discovered vulnerabilities – a higher number of "Medium" and "High" issues, with lower numbers of "Low" and "Critical" issues. With background knowledge gained from this assessment Istonish is available as a resource to the organization, if desired, to begin working through this issue list as a project and to prioritize risk mitigation.

Appendix A – References

National Institute of Standards and Technology. (2013, July 22). *NIST Computer Security Publications - NIST Special Publications (SPs).* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/PubsSPs.html

Appendix B – Physical Environment Assessment Detail

This table is used by Istonish personnel during the physical walk-through of the customer site to assess the physical security of the environment. Each line item is scored as **Pass**, **Fail**, or **N/A**. These results are interpreted as direct inputs to the discovered vulnerabilities listed in this document.

Scoring Legend:

Pass: ✓ Fail: ✗ N/A: N/A

Measurement	Result	Comment
Servers and network infrastructure are powered by multiple electrical circuits.	✓	
Servers and network infrastructure are connected to surge-protected power strips or PDU's.	✓	
Mission-critical equipment is connected to battery backup power (UPS).	✓	
UPS is not indicating a low-battery or battery-failure condition.	✓	
UPS is not indicating or does not appear to be overloaded.	✓	
Plumbing is not running above or near server or network infrastructure equipment.	✗	Plumbing present in office ceiling and A/C drain line.
Rooms housing servers and network infrastructure are climate-controlled.	✗	Office demark is extremely hot and not controlled.
Rooms housing servers and network infrastructure are protected by fire detection and suppression.	✓	
Rooms housing servers and network infrastructure do not have exterior windows.	✓	
Rooms housing servers and network infrastructure are on upper floors or do not appear to be susceptible to flooding.	✓	
Raceway or conduit is used for network cabling that is not run inside of walls or in ceilings.	✓	
Rooms housing servers and network infrastructure are not shared with 3rd-party organizations, or the equipment in a shared space is appropriately secured from 3rd-party access or tampering.	✗	Office demark is shared with other building tenants.
Rooms housing servers and network infrastructure are not used for non-IT storage.	✗	Non-IT storage present in network closet
User access to computer rooms is controlled by key or badge.	✓	
User access to phone room or demark controlled by key or badge.	✓	
A list is available and kept current of users who have keys or badge access to computer rooms and/or demarks.	✓	
Employee wearable ID badges distributed and used.	✗	Entry badges are not used as identification.
Keyed doors to restricted areas (such as file rooms) are kept locked.	✓	
Burglary alarm system for windows and doors is present and used after working hours.	N/A	Personnel onsite 24/7.

Guests or visitors are required to sign in and out when entering office areas.	✓	
Guests or visitors are escorted at all times in non-public office areas.	✓	
Security cameras are in use and record to a storage medium.	✓	
Non-public Wi-Fi is protected with at least WPA2 encryption; WPA is not presented as an option.	✓	
Public Wi-Fi is segregated from the internal LAN.	✓	
Rogue wireless access points are not present; broadcasting SSID's are known and/or accounted for.	✓	
Wireless access points are enclosed in locked housings or are otherwise unable to be tampered with.	✓	
Network ports in public areas are disconnected, disabled, or are non-trunking ports connected to a segregated VLAN or network.	✓	
Unmanaged Layer-2 switches are not present, or are known and accounted for.	✓	
BPDU guard or other port security is enabled on distribution switches to prevent the use of unmanaged Layer-2 switches.	✓	
Users are prompted for authentication before being able to access servers or network infrastructure equipment locally, such as via console cable or crash cart.	✓	
User workstations are kept locked when unattended.	✗	Workstations frequently found unlocked.
Employees challenge users not wearing ID badges.	N/A	
User account passwords are not visible near the workspace (such as on a sticky note).	✓	
Privacy filters are used on computer monitors near public areas where PII may be used (such as reception).	N/A	
Users print PII data with a print code, print PII data to a designated printer in a secure location, or do not print PII data at all.	✓	
Hard drives, flash media, optical discs, and magnetic drives/cartridges are securely erased or destroyed when non-functional or retired.	✓	
Stored media is marked appropriately as spare or for erasure/destruction.	✓	
Backup media rotated offsite or written to cloud storage.	✓	
Offsite backup media is encrypted.	✗	Not encrypted but kept in secure storage areas.
Offsite backup location is secured with the same access controls as the production environment, or with an archival service such as Iron Mountain.	✓	

Appendix C – Employee Security Awareness Training Program

If desired, Istonish is able to provide access to online Cyber Security Awareness training through the SANS Securing the Human program. This product is a set of educational videos and assessments that focus on cybersecurity awareness both at work and at home. Istonish has successfully deployed and managed this program in other environments and is a great option for training in any work place.

Key Benefits

- ✓ Covers the basics about being safe and secure:
  - Email safety
  - Strong passwords
  - Safely using social media
  - Website browsing
  - Computer security
  - Mobile device security
- ✓ Ability to provide training in large group settings
- ✓ Ability to send out training to individuals
- ✓ Assessments for measuring knowledge retention
  - Explanation-based learning with wrong answers explained
- ✓ Completion tracking
  - Ability to track and email completion/non-completion
- ✓ Modular and customizable
  - Adjust curriculum to fit organizational needs

Program Management

As part of this training package, Istonish will manage the administration, distribution, tracking, and follow-up using the tools provided with the training. Istonish's management services will also include:

1. A deployment schedule, estimated timeline, and training completion due date.
   - These dates can be established once the product is purchased.
2. Optionally, an Istonish representative can be onsite for an all-staff meeting to explain the process.
   - Intro to the program
   - What to expect and see from Istonish
   - Overall goals and objectives

Cost

Istonish will provide resources to configure, oversee, and track the completion of training courses. Due to the various environments and options for this training program, Istonish will work with the customer to scope this project and provide a customized hours and cost estimate for the program management. Additionally, the licensing cost for this training program is $3750 per year for the first 500 users.

Appendix D – Remediation Level of Effort (LOE)

Tables in this section detail an estimated Level Of Effort (LOE) for resolution of the discovered vulnerabilities listed in this document. Labor hours and non-labor costs are estimates only; if Istonish is contracted for remediation activities then further analysis will be performed to generate a more precise LOE.

Table 1: Critical-Severity Vulnerability Remediation

Remediation Task		Estimated Labor Hours	Estimated Non-Labor Costs
SonicWALL NSA Firmware Update		8 hours	N/A
Apache Tomcat Manager Admin Credentials Fix		8 hours	$0 *
Software packages update for unsupported DLL versions		8 hours	$0 *
Update to latest Java version		2 hours	$0 *
Update to latest McAfee VSE version		4 hours	$0
Update to latest Adobe Reader version		0.25 hours	$0
Update to latest HP System Management Homepage version		2 hours	$0
Install Operating System patches and updates		20 hours	$0
Implement vendor fixes for 'POODLE' vulnerability		4 hours	$0
Update Bash to mitigate 'Shellshock' vulnerability		1 hour	$0 *

** may require vendor Professional Services; feasibility and cost TBD.*

Table 2: High-Severity Vulnerability Remediation

Remediation Task		Estimated Labor Hours	Estimated Non-Labor Costs
Reduce number of users in 'Domain Admins' group		20 hours	$0
AD cleanup for enabled user accounts		10 hours	$0
Review and audit accounts using non-expiring passwords		16 hours	$0
Disable telnet servers, replace with SSH		40 hours	$0
Reconfigure web servers to use HTTPS or other secure authentication mechanism		24 hours	$0 *
Restrict permissions on primary file share (ShareDrive)		80 hours	$0
Restrict permissions on multiple shared folders		6 hours	$0 *
Enforce corporate antivirus requirements and regularly audit compliance		24 hours	$0
Feasibility analysis for data-at-rest encryption		40 hours	$30,000

Implement portable device disk encryption		80 hours	$0
Prevent P2P applications from communicating to the internet		1 hour	$0
Remove “Guest” account from ‘Domain Users’ group		0.1 hours	$0
Implement vendor fixes for Group Policy vulnerability		4 hours	$0
Implement vendor fix for binary planting vulnerability		10 hours	$0 *
Ensure that any services that contain a space in the path enclose the path in quotes		2 hours	$0 *
Restrict permissions on service executable files		1 hour	$0 *
Update to latest SizerOne version		5 hours	$0 *
Install Operating System patches and updates		30 hours	$0
Update to latest Apache HTTP server version		4 hours	$0 *
Update to latest Adobe Flash version		2 hours	$0
Update to latest Wireshark version		1 hour	$0
Update to latest vSphere version		1 hour	$0
Consider Encryption over point-to-point WAN links		60 hours	$12,000
Recommend changes to main office building demark		4 hours	$0
Risk mitigation for main office server room A/C unit		4 hours	$4000
Disable SSH on VMware ESXi hosts		0.5 hours	$0

** may require vendor Professional Services; feasibility and cost TBD.*

Table 3: Medium-Severity Vulnerability Remediation

Remediation Task		Estimated Labor Hours	Estimated Non-Labor Costs
Restrict permissions on file repository (Apps)		4 hours	$0
Generic users Domain Admins		12 hours	$0
Generic users VPN Users		4 hours	$0
Review Group Policy settings		4 hours	$0
Remove support for EXPORT_RSA cipher suites		4 hours	$0 *
Reconfigure hosts to mitigate ‘CRIME’ vulnerability		3 hours	$0 *
Update to latest Dell OpenManage Server Administrator version		10 hours	$0
Use a unique Diffie-Hellman moduli of 2048 bits or greater		3 hours	$0 *

Remove support for EXPORT_DHE cipher suites		4 hours	$0 *
Install latest patches for VMware ESXi 5.1		6 hours	$0
Update to latest Apache Tomcat version		3 hours	$0 *
Disable SNMP or change default community names		1 hour	$0
Discontinue use of RC4 ciphers		6 hours	$0 *
Implement vendor fixes for disabling SSL v2.0 and v3.0		8 hours	$0
Configure web servers to set an X-Frame-Options response header in all content responses		12 hours	$0 *
Disable the HTTP TRACE and TRACK methods on web servers		3 hours	$0 *
Use stronger encryption algorithms than SSLv3 and TLSv1		10 hours	$0
Use SSL or enforce Network Level Authentication for RDP		20 hours	$0
Change RDP Encryption level to High or FIPS-Compliant		4 hours	$0
Enable SMB signing using Group Policy		4 hours	$0
Reissue certificates using a strong hashing algorithm		4 hours	$0
Avoid use of Low- or Medium-strength ciphers		4 hours	$0
Implement vendor fix for SMB NULL session vulnerability		6 hours	$0
Change the LmCompatibilityLevel setting to 3 or higher		2 hours	$0
Update VMware ESXi to mitigate Dropbear SSH vulnerability		5 hours	$0
Implement cyber security awareness and training program		30 hours	$3500

** may require vendor Professional Services; feasibility and cost TBD.*

Table 4: Low-Severity Vulnerability Remediation

Remediation Task		Estimated Labor Hours	Estimated Non-Labor Costs
Implement vendor fix for cached-logon vulnerability		8 hours	$0
Computer object cleanup in Active Directory		6 hours	$0
OU and Container hierarchy cleanup in Active Directory		6 hours	$0
Use packages supplied by the Operating System vendor whenever possible		3 hours	$0
Review DHCP Options to minimize information disclosure		1 hour	$0

Update VMware ESXI to mitigate NTP 'monlist' vulnerability		5 hours	$0
Disable or filter SNMP to mitigate a LanMan services disclosure vulnerability		1 hour	$0
Disable MD5 and 96-bit MAC algorithms		4 hours	$0 *
Disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption		4 hours	$0 *
Review DNS architecture to minimize information disclosure		4 hours	$0
Implement web filtering to block access to unwanted categories of websites.		4 hours	$0
Replace certificates in certificate chains which have less than 2048-bit key lengths		3 hours	$0

** may require vendor Professional Services; feasibility and cost TBD.*

Table 5: Estimated Remediation Totals

Severity Type	Estimated Labor Hours	Estimated Non-Labor Costs
Critical	57.25 hours	$0
High	469.6 hours	$46,000
Medium	176 hours	$3500
Low	49 hours	$0
TOTAL:	**751.85 hours**	**$49,500 ***

** additional vendor Professional Services may be required; cost TBD.*

Appendix E – Sample Document for Risk Remediation Plan

This document provides an example outline to be used to track and implement remediation activities in conjunction with the organization's Change Management protocol. If Istonish is contracted for remediation activities then Istonish will provide a similar document for each remediation task outlined in Appendix D of this document.

Risk Remediation Plan
July 31, 2015

Date Risk Reported:
June 1, 2015

Risk Summary:
Several Windows servers are missing security updates and/or service packs.

Responsible Business Units:
Information Services

Affected Business Units:
Entire organization

Affected Systems:
WebServer01 (192.168.0.1)

Organizational Impact:
Server hosting the website will be offline for approximately 10 minutes while the server is rebooted following installation of necessary patches.

Date and Time of Remediation:
August 9, 2015 10:00pm-12:00am

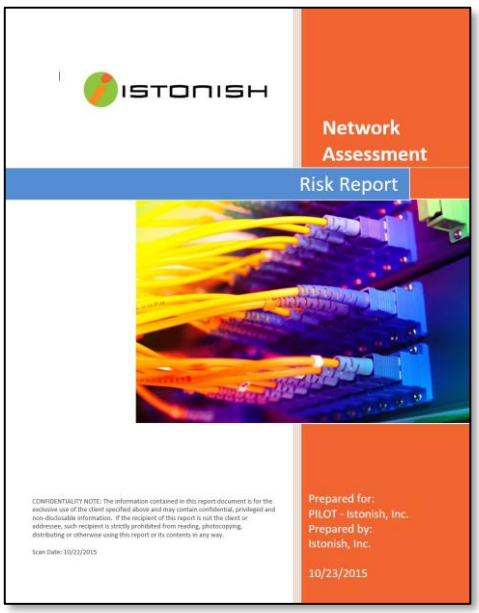
Remediation Procedure:

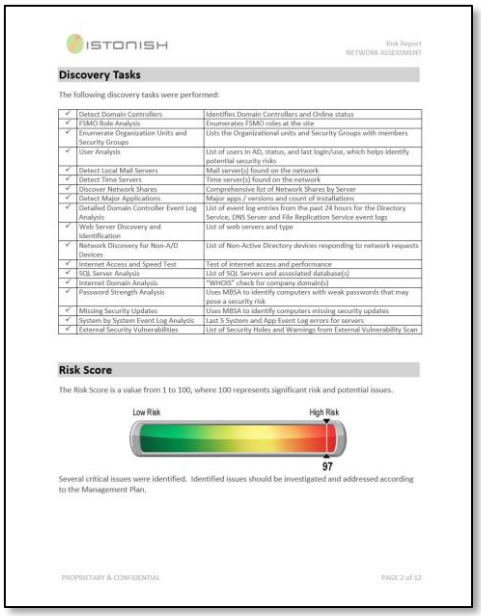
1. Run a full backup job on WebServer01 using Symantec Backup Exec.
2. Install Microsoft Windows patch to address security bulletin MS13-050 (KB2839894).
    i. Estimated duration of work: 30 minutes.
3. Reboot WebServer01 to complete patch installation
4. Verify that patch has been applied and that the system is functioning correctly.

Back-Out Plan:
In the event that the listed system(s) do not function properly after the remediation steps have been put into place, the Windows patch will be removed from the system. If the patch cannot be removed or does not resolve the issue, the server will be restored from the latest full backup. Information Services will troubleshoot the patch installation in a lab environment and reschedule the maintenance after the issue has been resolved.

Appendix F – Detailed Scan Output from Network Detective

The reports generated from the Network Detective Tool contain detailed information about systems on the network and within Active Directory. Information generated from this tool helps Istonish to analyze the environment for user roles and memberships, file share permissions, user behavior analysis, disk encryption, and detail about computer assets on the network. Reports are available for download Here.





14 Reports, 1343 Pages

Network Detective generates multiple reports the cover a variety of topics about the environment:

1. **Share Permission Report**
   260 pages in length – The Share Permission Reports outlines the user and group permissions that are configured on each shared folder. This provides visibility to see who has permissions to access what data.

2. **Login Failures by Computer Report**
   132 pages in length – This reports shows failed logon attempts on each computer. By analyzing this report it can be seen which computers are under attack or have tried to be accessed by unauthorized users.

3. **User Behavior Analysis Report**
   33 pages in length – The User Behavior Analysis Report shows which accounts have logged on to which computers. This helps to determine whether or not users are accessing systems that they should not be, and can also help to identify viral traffic using user accounts.

4. **Asset Detail Report**
   104 pages in length – This report contains a basic asset inventory of all systems discovered on the network. It contains data such as hardware specifications, install date, available disk space, software installed, and much more asset data for each system.

5. **Outbound Security Report**
   6 pages in length – The Outbound Security Report tests for website filtering. The automated scan tests whether or not it is able to access commonly-forbidden categories of websites and reports the results.

6. **Security Policy Assessment**
   20 pages in length – This report details the technical controls that were discovered which enforce common security policy, such as password strength requirements and lockout periods.

7. **Client Risk Report**
   11 pages in lenth – The Client Risk Report scores each workstation's or server's individual level of risk on a scale from 1 to 100. This score is computer by a number of listed factors, such as the presence of antivirus, operating system version, and the role of the system on the network.

8. **Security Risk Report**
   7 pages in length – This report analyzes information found during the network scans and scores the organization on a general level of risk on a scale from 1 to 100.

9. **External Network Vulnerabilities Summary Report**
   2 pages in length – The External Network Vulnerabilities Summary Report provides a high-level overview of the risks that were identified while scanning the organization from the public internet. This report presents a risk score and recommended remediation solution for each risk.

10. **External Vulnerability Scan Detail Report**
    21 pages in length – Sorted by public IP address, this report reveals the vulnerabilities that were discovered while scanning the outside public IP addresses of the organization.

11. **External Vulnerability Scan Detail by Issue Report**
    5 pages in length – Sorted by unique issue, this report reveals the vulnerabilities that were discovered while scanning the outside public IP addresses of the organization.

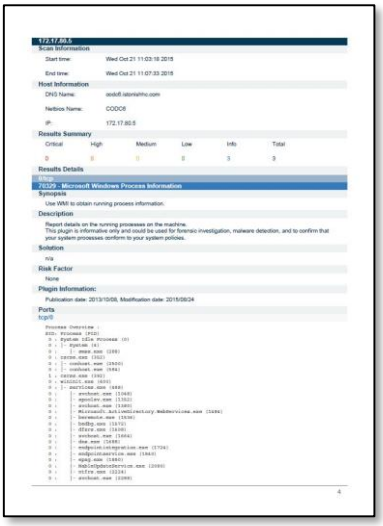
12. **Windows XP Migration Readiness Report**
    6 pages in length – For organizations that are still working through the migration of computers from Windows XP to a newer Operating System, the Windows XP Migration Readiness Report provides an analysis of the Windows XP systems on the network and shows whether or not they are ready to upgrade.

13. **Site Diagram**
    26 pages in length – The Site Diagram shows the organizational structure of the Active Directory forest. It also sorts the systems by Operating System and shows a count of either Severe or Potential Risks as well as missing updates for each individual machine.

14. **Full Detail Report**
    710 pages in length – The Full Detail report provides a deep-dive view into the computing environment. This report is chalked full of information regarding servers, computers, users, printers, and policies configured for the organization.

Appendix G – Detailed Scan Output from Nessus

Nessus Professional is an industry-standard vulnerability scanning tool. Nessus contains a large database of known application vulnerabilities and streamlines the assessment process by automatically scanning networks for these weaknesses. Istonish analysts review Nessus' findings and correlate vulnerabilities in order to provide a business-relevant view of the tool's findings. Reports for each Nessus scan are available for download Here.



4 Reports, 14,671 Pages

Each Nessus report reflects an individual 'scan' of the network – each scan looks for specific sets of vulnerabilities.

1. **Advanced Scan**

   3904 pages in length – Vulnerabilities sorted by plugin.
   8565 pages in length – Vulnerabilities sorted by host.
   The Advanced Scan report shows the results of the most comprehensive scan conducted with Nessus. This scan looks for thousands of vulnerabilities on a wide variety of devices, and also finds systems missing patches and updates.

2. **Credentialed Patch Audit**

   2058 pages in length – This report analyzes each host in detail to find missing updates. Device credentials are used to connect to each host and verify exactly which patches and application versions are missing from each individual host.

3. **Windows Malware Scan**

   87 pages in length – The Windows Malware Scan report displays results of a Nessus-run scan for viruses and other malware on each host in the scan. The results detailed in this report should be used as either confirmation or exposure of the organization's anti-malware software effectiveness.

4. **Host Discovery**

   57 pages in length – This report is a simple scan of hosts that are responding on the orgnaization's network. This informational report can be analyzed to determine the number of alive (online) hosts on each network segment.

Appendix H – Detailed Output from the Fortinet Cyber Threat Assessment

Fortinet's Cyber Threat Assessment Program (CTAP) provides high-level insight into your organization's use of a sampled internet connection. The report that Fortinet generates shows what is coming in and going out from your internet connection, including viruses and threats from the internet and also user productivity, web usage, and high-risk applications being used on the network. Istonish reviews and analyzes this report for risks and also to measure the effectiveness of any intrustion prevention technologies in place on the network firewall. The report is available for download Here.

1 Report, 10 Pages

Threats from the web and user productivity are detailed within a single report from Fortinet.

1. **Security and Threat Prevention**
   Fortinet's industry-leading threat detection technologies analyze the data coming in and out of your internet connection for security issues and live threats. Because the monitoring appliance is typically deployed behind the organization's existing firewall, any threats that are found here should be remediated immediately.

2. **User Productivity**
   How are users communicating on the internet? Fortinet's application analysis determines what programs users are running, what websites they're frequently visiting, and if any Peer-to-Peer (P2P) clients are being used. This information can help adminsitrators determine whether technologies such as web filtering should be put in place or should be more strictly enforced.

3. **Network Utilization**
   Firewall statistics such as CPU utilization and memory usage help organizations understand the performance requirements of their network, based on real activity from users. This information can help administrators troubleshoot speed issues on the network and can aide in capacity planning.

Have Istonish prepare your assessment today!

303.771.1765

5500 Greenwood Plaza Blvd., Suite 200

Greenwood Village, CO 80111

www.istonish.com | info@istonish.com