CATALYST TECHNOLOGY GROUP

Innovating how IT is delivered.℠

26-Sep-2019

CYBER RISK ASSESSMENT

CYBER RISK CHANGE SUMMARY REPORT

My Client's Company

Prepared by: YourIT Company

Scan Date: 26-Sep-2019

Table of Contents

1 - Discovery Tasks

	Task	Description
☐	Detect Domain Controllers	Identifies domain controllers and online status.
☐	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
☐	Detect Local Accounts	Detects local accounts on computer endpoints.
☐	Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
☐	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
☐	Missing Security Updates.	Identifies computers missing security updates.
☐	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

2 - Assessment Summary

Domain	Previous	Current	Change
Domain Controllers	2	2	0
Number of Organizational Units	11	11	0

Users	Previous	Current	Change
# Enabled	32	32	0
Last Login within 30 days	9	10	+1
Last Login older than 30 days	23	22	-1
# Disabled	2	2	0
Last Login within 30 days	0	0	0
Last Login older than 30 days	2	2	0

Local Accounts	Previous	Current	Change
# Enabled	58	56	-2
Last Login within 30 days	29	29	0
Last Login older than 30 days	29	27	-2
# Disabled	111	109	-2
Last Login within 30 days	15	15	0
Last Login older than 30 days	96	94	-2

Active Directory Computers	Previous	Current	Change
Total Computers	35	35	0
Last Login within 30 days	35	35	0
Last Login older than 30 days	0	0	0
Windows 10 Enterprise	15	15	0
Windows 10 Enterprise 2015 LTSB	1	1	0
Windows 10 Enterprise N	1	1	0
Windows 10 Pro	2	2	0

Active Directory Computers	Previous	Current	Change
Windows 7 Professional	2	2	0
Windows 8.1 Pro	4	4	0
Windows Server 2012 R2 Standard	2	2	0
Windows Server 2012 Standard Evaluation	1	1	0
Windows Server 2016 Standard	7	7	0

Non-A/D Computers	Previous	Current	Change
Total Computers	1	1	0
Last Login within 30 days	0	0	0
Last Login older than 30 days	1	1	0

Miscellaneous	Previous	Current	Change
Non-A/D Systems	24	23	-1
External Network Security (High Risk)	0	0	0
External Network Security (Medium Risk)	1	1	0

3 - myclientsnetwork.com

3.1 - Domain Controllers

There is 2 domain controllers:

No Change

3.2 - Users

34 total users

No Change

3.3 - Computers in Domain

No Change

4 - Non A/D Devices

No Change

5 - Patch Summary

This section contains the patching status of computers determined through the Microsoft Baseline Security Analyzer and Windows Update. MBSA gathers data through a remote scan and looks primarily for Security Updates. Windows Update checks the local computer for all non-hidden updates. Missing updates in both areas are highlighted in red. Security and critical updates are bolded.

Windows Updates

IP Address	Computer Name	Issue	Result	Assessment
176.16.1.14	APPSVR01	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.142	BDR01	Drivers, Windows Server 2016 and Later Servicing Drivers	Failed (non-critical)	6 updates are missing.
		Updates, Windows Server 2016	Failed (non-critical)	2 updates are missing.
176.16.1.12	DCCTLR01	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.13	DCCTLR02	Definition Updates, Windows Defender	Failed (non-critical)	2 updates are missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.116	**DSKPC-09UPSPO**	Security Updates	Failed (non-critical)	1 security update is missing.
		Security Updates, Windows 10, version 1903 and later	**Failed (critical)**	**2 security updates are missing.**
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.124	DSKPC-191IJQL	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.104	DSKPC-4PF2ICP	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.24	DSKPC-534MS45	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.22	DSKPC-85BJGJT	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.119	DSKPC-BDJFFLG	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.19	DSKPC-F0M1O27	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.106	DSKPC-F6CKERQ	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.

IP Address	Computer Name	Issue	Result	Assessment
176.16.1.100	DSKPC-HN95P9Q	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.146	DSKPC-LIFRCFU	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.144	DSKPC-MA551PF	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.120	DSKPC-MJOD0L9	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.112	DSKPC-RB3LBP3	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
176.16.1.20	DSKPC-U1K3NAF	Definition Updates, Windows Defender	Failed (non-critical)	2 updates are missing.
		Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.15	EXCHSVR01	Definition Updates, MS Security Essentials	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2012 R2	Failed (non-critical)	2 updates are missing.
176.16.1.16	FSVR01	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2016	Failed (non-critical)	1 update is missing.
176.16.1.17	SQLSVR01	Updates, Windows Server 2012 R2	Failed (non-critical)	2 updates are missing.
176.16.1.21	SQLSVR02	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Feature Packs, Silverlight	Failed (non-critical)	1 update is missing.
		Microsoft SQL Server 2016, Service Packs	Failed (non-critical)	1 update is missing.
176.16.1.102	WRKSTN10-1	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.108	WRKSTN10-2	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.113	WRKSTN10-3	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.114	WRKSTN10-4	Updates, Windows 10, version 1903 and later	Failed (non-critical)	1 update is missing.
176.16.1.111	**WRKSTN7-1**	no issues	Passed	No updates missing.

IP Address	Computer Name	Issue	Result	Assessment
176.16.1.115	**WRKSTN7-2**	**Security Updates, Windows 7**	**Failed (critical)**	**1 security update is missing.**
176.16.1.105	WRKSTN8-1	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 8.1	Failed (non-critical)	2 updates are missing.
176.16.1.103	WRKSTN8-2	Updates, Windows 8.1	Failed (non-critical)	2 updates are missing.
176.16.1.107	WRKSTN8-3	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 8.1	Failed (non-critical)	2 updates are missing.
176.16.1.110	WRKSTN8-4	Definition Updates, Windows Defender	Failed (non-critical)	1 update is missing.
		Updates, Windows 8.1	Failed (non-critical)	2 updates are missing.
176.16.1.122	WS2012SVR	Feature Packs, Windows Server 2012	Failed (non-critical)	1 update is missing.
		Updates, Windows Server 2012	Failed (non-critical)	2 updates are missing.

6 - External Security Vulnerabilities

This section contains an overview of external vulnerabilities detected during the scan, with items in red indicating a risk.

External IP Address	Risk	High Risk	Medium Risk	Low Risk	Port and Protocol
97.72.92.49 (97-72-92-49-static.atl.earthlinkbusiness.net)	Medium	0	1	0	**21/tcp (ftp)**, **22/tcp**, **21/tcp**, **23/tcp**

7 - Local Accounts

165 total local accounts

Change Status	Local Account	Display Name	Enabled	Last Login
Deleted	HVSVR1\administrator		enabled	**07-Nov-2017 7:21:21 PM**
Deleted	HVSVR1\dbuser	DB Local Admin	enabled	**17-Dec-2018 8:51:46 AM**
Deleted	HVSVR1\defaultaccount		disabled	
Deleted	HVSVR1\guest		disabled	