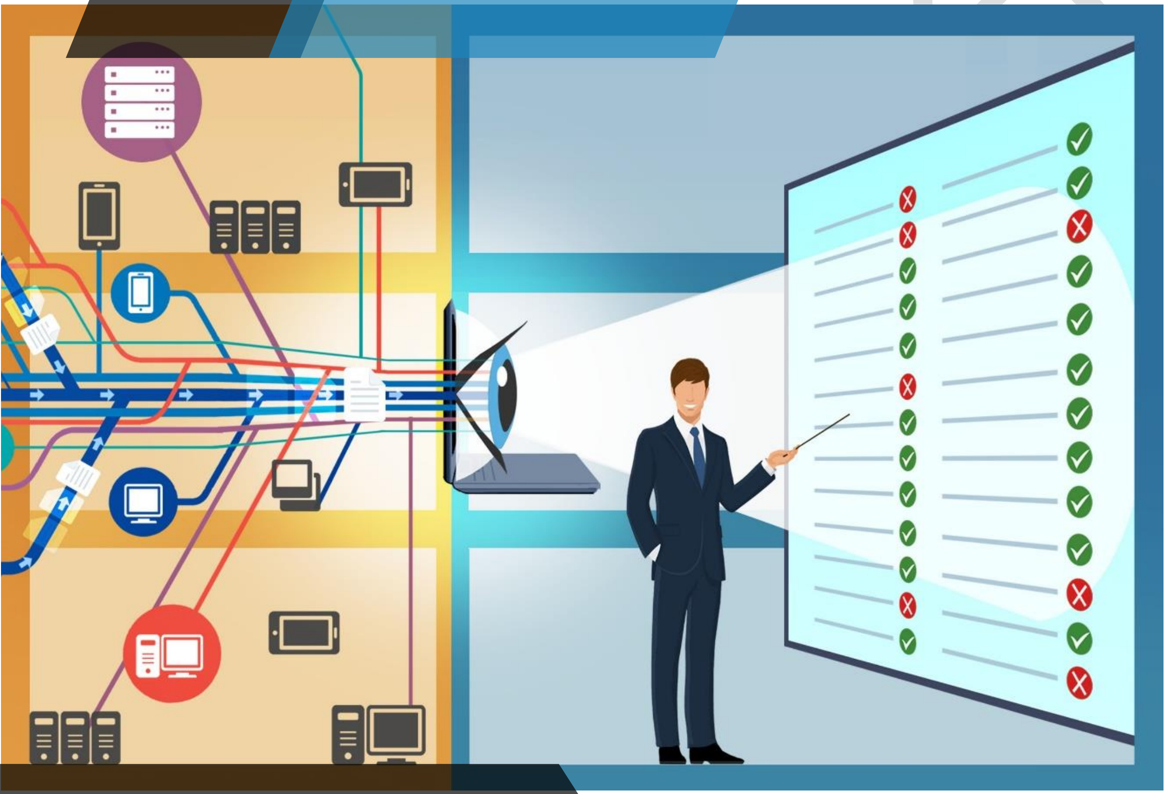
CSAT



Cybersecurity Report

Contoso

This document is strictly private, confidential and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party.

Contents

1 Management Summary

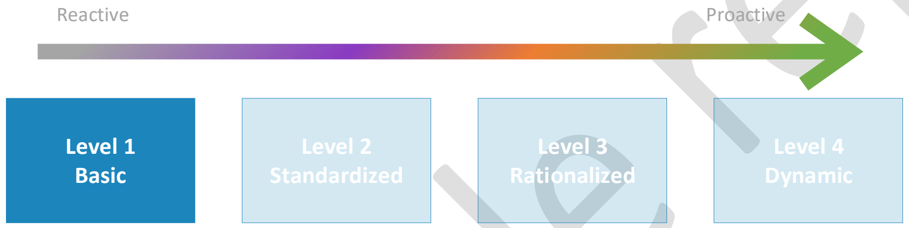
This Cybersecurity Report is the result of a Cybersecurity assessment that was executed for **Contoso** by **QS solutions** in **July 2019**.

This Cybersecurity Assessment Report is intended to provide an overall review of **Contoso**'s cybersecurity program and practices. **Contoso**'s cybersecurity maturity was measured through a questionnaire and by an automated scan of security related data. The report is not meant to be a detailed control review or a security audit.

The result of this assessment is an action plan with security improvement initiatives that will help **Contoso** to improve its overall cybersecurity position.

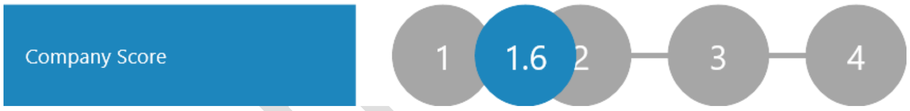
1.1 Company Rating

After reviewing the CIS Controls™ (v7) questionnaire, described in detail later, the assessment of **Contoso**'s cybersecurity program and practices shows a global maturity rating of: **Basic (1)** based on the lowest maturity score to a questionnaire answer.



The average score is also calculated and can be used to track progress in future security scans:

Company Score



While **Contoso**'s size, industry, regulatory environment, and other risk factors might influence the final recommendations associated with this global rating, at a high level given the current state of cybersecurity related threats and risks, **Contoso**'s cybersecurity position has the following implications:

- The programmatic aspects are reactive rather than mostly proactive.
- The security risks facing the organization are generally understood although not in a managed way.
- The organization is generally aware of the security threats it faces but not from a programmatic method.

- The governance of the cybersecurity program is structured but not fully integrated with other governance areas.
- The operational aspects of the cybersecurity program are not consistent or quantitatively managed and automated.
- The organization's employees are unaware of today's cybersecurity threats and related training around security and privacy awareness is missing.

1.2 Organizational Recommendation

Organizations should be proactive in avoiding cybersecurity risks and related cyberthreats by establishing policies and procedures around cybersecurity and IT infrastructure protection. A proactive approach opposed to reactive mitigation is highly recommended as a point of improvement for the organization.

Risk Management is another key element to implement for **Contoso**, which is mandatory to take the appropriate steps to identify, protect, detect and respond to the risks and secure the organization and IT environment. Proper Risk Management is a top-level strategic issue and demands executive leadership participation as the key stakeholder in the process.

As the most common threats are directly related to end-users because of phishing emails, malware, data theft or loss, a mandatory security training program for all employees should be adopted. The program should be sponsored by the executive management team of the organization to create a good foundation for awareness throughout the entire organization on security threats.

2 Action Plan to improve Cyber Security

2.1 Urgent priority Actions

These are the Urgent priority Actions identified in the Assessment and detailed below in this report. We recommend that the following items are assessed and acted on as the first priority:

Priority	Action	Associated Software Products
Urgent		
2. Inventory and Control of Software Assets	• Embed a discovery tool for software asset management.	• Software Asset Management (SAM) tooling • System Center Configuration Manager (SCCM) • Azure Security Center • Cloud App Security • Microsoft Defender ATP
3. Continuous Vulnerability Management	• Implement vulnerability scan software. Scan for vulnerabilities regularly, especially on systems contain sensitive information.	• System Center Configuration Manager (SCCM) • Microsoft Defender ATP • Azure Security Center • Cloud App Security
3. Continuous Vulnerability Management	• Implement a patch management process and tooling. Gain insights on the patch status of all systems	• System Center Configuration Manager (SCCM) • Windows Server Update Services (WSUS) • Intune • Azure Security Center
4. Controlled Use of Administrative Privileges	• Setup personal admin accounts and enable multi-factor authentication for all external administrative access.	• Azure AD Privileged Identity Management (PIM) • Privileged Access Management (PAM) • Azure Multi-Factor Authentication
8. Malware Defenses	• Enable the default tools for antivirus, anti-malware and DEP on the organization's systems.	• Microsoft Cloud App Security (CAS) • Microsoft Defender ATP
13. Data Protection	• Enable encryption on the organization's main data sources.	• BitLocker • System Center Configuration Manager • Intune
16. Account Monitoring and Control	• Define a standard password policy definition for all the applications and infrastructure services. Start implementing MFA on all systems, increase password length if MFA is not yet available	• Azure Multi-Factor Authentication (MFA) • Conditional Access
AD.2. Data Governance	• Define a labeling and classification policy and implement it.	• Azure Information Protection Scanner • Data Loss Prevention • Azure Information Protection P2

2.2 Quick wins

With the actions below, security improvements are visible, have direct benefits for Contoso and can be quickly deployed in the organization. Overview of the advised actions and products:

Priority	Action	Associated Software Products
Quick Wins		
Separate Wi-Fi Guest network from the corporate network	• Physically separate the wireless network from the organization's boundaries. Assign a separate internet connection/VLAN to the guest wireless network.	
(Azure) Active Directory accounts	• Review accounts with risky UAC details (see chapter 4.1.1) and remove these AD settings • Disable old/unused accounts. • Implement Multi Factor Authentication (MFA) for all user accounts. • Review External users	• Azure MFA
Administrators	• Review administrator accounts and clean up old/unused accounts	• Azure Privileged Identity Management (PIM)
Password policy	• Enhance the password policy (see chapter 4.1.4)	• Azure MFA
Operating systems	• Migrate the (almost) end-of-life operating systems	•
Windows updates	• Roll out the available security patches on all endpoints.	•
Antivirus	• Update the out of date antivirus definitions and enable antivirus on all endpoints	•
Firewalls	• Enable the firewalls on all endpoints	•
Data Encryption	• Enable BitLocker on all endpoints, starting with mobile devices	• BitLocker

3 Cybersecurity Findings and Recommendations

More important than the single, all-up Organization Rating, are the specific ratings associated with each of the CIS Controls™ (v7) controls and the controls taken from the ISO/IEC 27001 framework. Each rating projecting the current state has an implication, particularly when compared to where <Customer>'s cybersecurity program and practices should be in a future state.

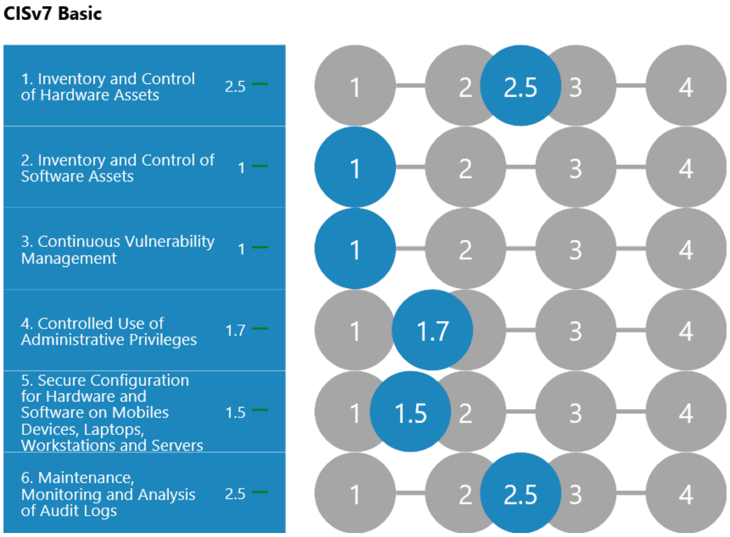
3.1 Basic CIS Controls

The Basic CIS Controls are related to inventory, scoping and control of the IT environment to its full extend. The six (6) Basic CIS Controls and their objective(s) are:

Topic	Objective
1. Inventory and Control of Hardware Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring and Analysis of Audit logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

3.1.1 Basic CIS Controls - Organizational Rating

The assessment has taken a measurement based on the above objectives of the Basic CIS Controls and projected these to <Customer>'s current position on each of the Basic CIS Controls, resulting in a rating of:



3.1.2 Basic CIS Controls - Findings and Recommendations

The detailed findings below are associated with each of the six (6) Basic CIS controls, and lead to the following recommendations for **<Customer>**:

Urgent				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
2. Inventory and Control of Software Assets	Are Discovery tools implemented to identify all software applications throughout the organization's infrastructure?	Basic (1) Not implemented	Embed a discovery tool for software asset management.	Software Asset Management (SAM) tooling, System Center Configuration Manager (SCCM), Azure Security Center, Cloud App Security, Microsoft Defender ATP
3. Continuous Vulnerability Management	Are Discovery tools implemented to identify any software vulnerabilities on systems within the infrastructure of the organization?	Basic (1) Not implemented	Implement vulnerability scan software. Scan for vulnerabilities regularly, especially on systems contain sensitive information.	System Center Configuration Manager (SCCM), Microsoft Defender ATP, Azure Security Center, Cloud App Security
3. Continuous Vulnerability Management	Has an automated patch management solution been implemented to continuously update all of the organization's systems?	Basic (1) Not implemented	Implement a patch management process and tooling. Gain insights on the patch status of all systems	System Center Configuration Manager (SCCM), Windows Server Update Services (WSUS), Intune, Azure Security Center
4. Controlled Use of Administrative Privileges	Does every administrator have a dedicated personal admin account, separated from their normal user account? The organization implemented multi-factor authentication (MFA) for all administrative access. Just in Time Access rules are applied to limit the default permissions.	Basic (1) Not implemented	Setup personal admin accounts and enable multi-factor authentication for all external administrative access.	Azure AD Privileged Identity Management (PIM), Privileged Access Management (PAM), Azure Multi-Factor Authentication
4. Controlled Use of Administrative Privileges	Does the organization have an entitlement review process to validate that each person with administrative privileges on servers, desktops, and laptops is authorized by a senior executive on a repeating schedule?	Basic (1) No process in place	Implement an entitlement and approval review process with Azure AD PIM Access Reviews for all accounts with administrative privileges, to regularly check these. Clean up old unused accounts.	Azure Privileged Identity Management (PIM), Azure AD Access Review

Urgent				
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	Are Discovery tools implemented to identify any misconfigured security settings on all of the organization's systems within the infrastructure?	Basic (1) Not implemented	Implement a configuration management tool, to check all systems for a minimal set of security settings	System Center Configuration Manager, Microsoft Defender ATP, Azure Security Center, Cloud App Security, Intune

High				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
1. Inventory and Control of Hardware Assets	Are Discovery tools (active and passive) implemented to identify all devices attached to the organization's infrastructure?	Standardized (2) Implemented with a limited scope	Extend the scope of the discovery tool(s) to the entire IT infrastructure.	System Center Configuration Manager (SCCM), Network discovery solution
2. Inventory and Control of Software Assets	Are Software whitelisting tools implemented that only allow authorized software programs to be executed on all of the organization's systems?	Basic (1) Not implemented	Configure whitelisting to restrict the usage of unwanted and malicious software.	System Center Configuration Manager (SCCM), Microsoft AppLocker, Windows Defender Application Control, Azure Security Center, Cloud App Security
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	Does the organization have an implemented secure hardening baseline for all new systems, disabling old NTLM and SMB and more security registry keys?	Standardized (2) Implemented for some key systems (like Webservers, DMZ servers)	Define a secure hardening baseline for all (types of) systems, to lock down all systems by default.	Azure VM's, Azure CIS hardened images, Intune, System Center Configuration Manager (SCCM)
6. Maintenance, Monitoring and Analysis of Audit Logs	Have all devices and servers, including Domain Controllers, firewalls, network-based IPS, and inbound and outbound proxies, been implemented and configured to verbosely log all traffic (both allowed and blocked) and failed login attempts?	Standardized (2) Implemented on some network devices	Point the logging configuration of all devices to the central logging platform. Use Azure Sentinel, to aggregate data from all sources, including users, applications, servers, and devices running on-premises or in any cloud.	Azure Sentinel, Azure Security Center, Azure Advanced Threat Protection (ATP), Advanced Threat Analytics (ATA), Microsoft Cloud App Security

3.2 Foundational CIS Controls

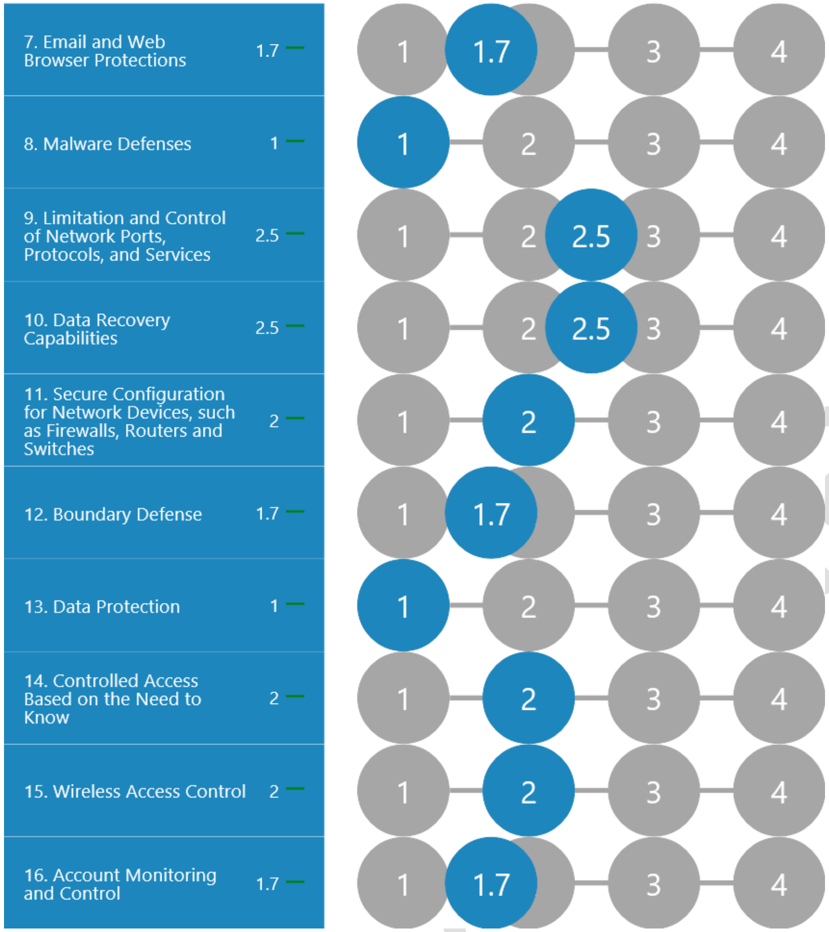
The Foundational CIS Controls are mostly focused on technically securing IT assets to the full extent of the IT environment and the detection of threats. The ten (10) Foundational CIS Controls and their objective(s) are:

Topic	Objective
7. Email and Web Browser Protections	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
10. Data Recovery Capabilities	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
13. Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
14. Controlled Access Based on the Need to know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
15. Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

3.2.1 Foundational CIS Controls - Organization Rating

The assessment has taken a measurement based on the above objectives of the Foundational CIS Controls and projected these to <Customer>‘s current position on each of the Foundational CIS Controls, resulting in a rating of:

CISv7 Foundational



3.2.2 Foundational CIS Controls - Findings and Recommendations

The detailed findings below are associated with each of the ten (10) Foundational CIS controls, and lead to the following recommendations for <Customer>:

Urgent				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
8. Malware Defenses	Are there centrally managed tools implemented to continuously scan for anti-malware and to remove malware and, keep anti-malware and signature files on workstations, servers, and mobile devices up-to-date and properly configured? Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) are enabled on all applicable systems.	Basic (1) Not implemented	Enable the default tools for antivirus, anti-malware and DEP on the organization's systems.	Microsoft Cloud App Security (CAS), Microsoft Defender ATP
8. Malware Defenses	Store events and logs of anti-virus centrally with alerting so the IT department can take actions. Reporting to identify trends is crucial for the organization.	Basic (1) Not implemented	Store the AV logs centrally and apply alerting to gain insights.	Microsoft Defender ATP, Azure Security Center, Cloud App Security
12. Boundary Defense	Do all remote login access require encryption of data in transit and multi-factor authentication (MFA)?	Basic (1) Not implemented	Enable encryption and MFA for remote login access.	Azure Multi-Factor Authentication (MFA)
13. Data Protection	Are assessments performed on data to identify sensitive information that requires the application of encryption and integrity controls? And is labeling and classification performed on all sensitive documents?	Basic (1) Not implemented	Identify sensitive information on the organization's main data sources. Apply labeling and classification.	Azure Information Protection Scanner, Data Loss Prevention, Office 365 Advanced Data Governance, Azure Information Protection P2
13. Data Protection	Has Device and Disk encryption software been applied to mobile devices and all systems that hold sensitive data?	Basic (1) Not implemented	Enable encryption on the organization's main data sources.	BitLocker, System Center Configuration Manager, Intune
16. Account Monitoring and Control	Are account and password policies enforced with Multi Factor Authentication (MFA) for all users on all systems?	Basic (1) Not defined/not implemented	Define a standard password policy definition for all the applications and infrastructure services. Start implementing MFA on all systems, increase password length if MFA is not yet available	Azure Multi-Factor Authentication (MFA), Conditional Access

High				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
7. Email and Web Browser Protections	Are Network-based URL filters (incl. DNS filtering) implemented that limit a system's ability to connect to websites not approved by the organization?	Standardized (2) Implemented for some systems	Ensure the use of the proxy server/IPS Solution by all systems within the IT infrastructure.	Microsoft Defender ATP, Proxy server/IPS solution
7. Email and Web Browser Protections	Is the Email Protected with SPF, DKIM and DMARC?	Standardized (2) SPF and DKIM records have been configured for some domains.	Create the appropriate SPF and DKIM record for all email domains.	Office 365 Advanced Threat Protection P1 and P2
7. Email and Web Browser Protections	Are malicious email attachments scanned and blocked in a sandboxed solution?	Basic (1) Not implemented	Implement an email antivirus, anti-malware solution.	Office 365 Advanced Threat Protection P1 and P2
9. Limitation and Control of Network Ports, Protocols, and Services	Are Web Application Firewalls implemented in front of critical servers to verify and validate the traffic going to the server?	Standardized (2) Implemented for some servers	Setup Web Application Firewalls (WAF) in front of any critical server.	Azure Application Gateway, Azure Web Application Firewall (WAF)
10. Data Recovery Capabilities	Does the organization have a back-up process in place where each system is automatically backed up, once per quarter a restore is being tested and verified? A backup is stored in a different site/location for disaster recovery.	Standardized (2) Back-up implemented for main systems, restore incidentally tested	Extend the backup process to include all systems, schedule Restore tests.	Azure Back-up and Site Recovery
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Are automated tools implemented to verify approved organizational (security) standards for network device configurations and detect deviations?	Standardized (2) Implemented for some network devices	Extend the network device management solution to include all the organization's network devices.	Network Device Management Solution
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Is a process implemented to install the latest stable version of any security-related updates on all network devices?	Standardized (2) A process is in place but is not scheduled or based on risks	Schedule the execution of the update process for network devices, keeping them secure.	Network Device Management Solution

High				
12. Boundary Defense	Is network segmentation applied to separate systems with different roles and restriction levels?	Standardized (2) Only servers and endpoints have been separated	Separate systems based on roles and restrictions levels.	
12. Boundary Defense	Are firewalls and network-based Intrusion Detection/Prevention IDS/IPS implemented to detect and block attacks and, malicious traffic at each of the organization's boundaries?	Standardized (2) Basic firewalls are implemented	Enable the deep packet inspection (DPI) and Intrusion Detection/Prevention functionality of the firewall if possible. Otherwise consider replacing the firewall by a more advanced model. Implement reporting on suspicious activity.	Firewall solution with IDS/IPS
14. Controlled Access Based on the Need to Know	Is Encryption in transit (SSL/TLS) implemented for all communication of sensitive information over less-trusted networks?	Standardized (2) Implemented on for some network communication	Enable encryption for all external/public network communication and internal network communication related to sensitive data.	Office 365 uses SSL/TLS encryption for data in transit
14. Controlled Access Based on the Need to Know	Is Network segmentation applied based on the label or classification level of the information stored on the servers?	Standardized (2) Implemented for some systems containing sensitive data	Apply network segmentation for all the organization's data sources.	
14. Controlled Access Based on the Need to Know	Are “Access Control Lists“ (e.g. AD Security Groups) implemented to limit the access of individuals to sensitive information based on “The Need to Know“?	Standardized (2) Basic security groups have been implemented on shares and folders	Create security groups based on the business role matrix. Ensure separate groups for read-only and read-write access.	Azure AD, PortalTalk 365
15. Wireless Access Control	Have Wireless networks been implemented which leverage Advanced Encryption Standard (AES) encryption for data in transit? Mutual, multi-factor authentication (MFA) is required to gain access to the wireless network.	Standardized (2) Wireless networks have been implemented with WPA2 (TKIP) authentication.	Switch from WAP2-TKIP to WPA2-AES authentication/encryption, or to certificate based authentication.	
15. Wireless Access Control	Are Wi-Fi Guest networks separated from the corporate network?	Standardized (2) Implemented but not physically separated from the organization's network boundaries.	Physically separate the wireless network from the organization's boundaries. Assign a separate internet connection/VLAN to the guest wireless network.	

High				
16. Account Monitoring and Control	Is a centralized authentication platform available, and used for every application, device and cloud?	Standardized (2) Implemented for the core applications and infrastructure services	Configure a single central authentication source/user directory for all applications and systems.	Azure AD
16. Account Monitoring and Control	Is Account management performed by the business, with ownership of each account, disabling dormant accounts after a set period, automatically expire accounts?	Standardized (2) Some accounts are checked by the business owner, but old/stale accounts are still lingering around	Implement business ownership of all accounts, including checks by the business/functional owner of each account, establish a process to cleanup old accounts	Azure AD Access Reviews

3.3 Organizational CIS Controls

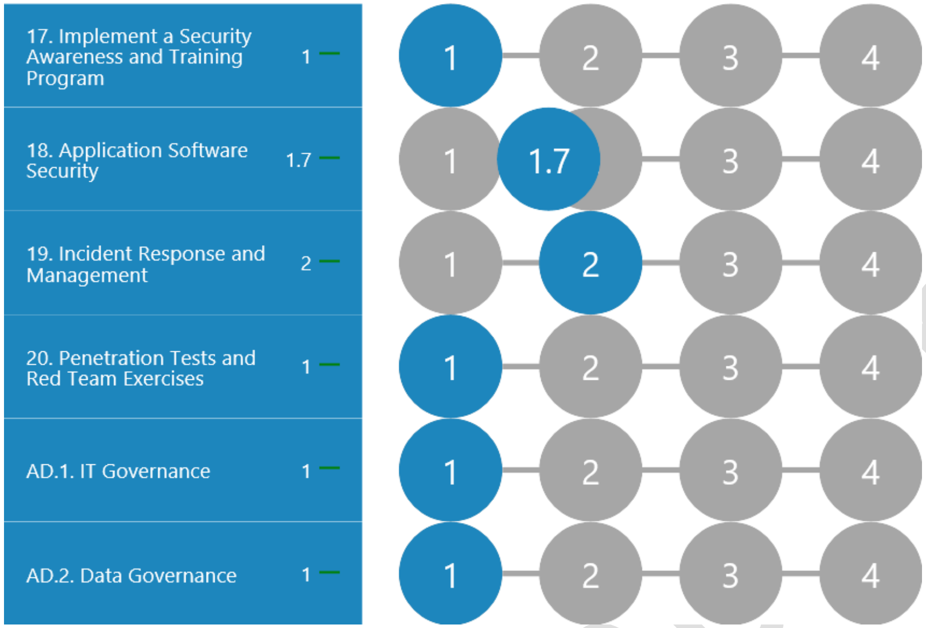
The Organizational CIS Controls are related to the processes and procedures of the organization. The Organizational CIS Controls are accompanied with high-level controls from the ISO/IEC 27001:2013 framework in addendum AD.1 and AD.2. These questions are related to IT- and data governance, and cover the areas of policies, compliancy, risk management and privacy. The four (4) Organizational CIS Controls, the two (2) Addendum Controls and their objective(s) are:

Topic	Objective
17. Implement a Security Awareness and Training Program	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
18. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
19. Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems
20. Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker
AD.1. IT Governance	Create organizational transparency and alignment by establishing a security and privacy policy framework complying with the regulatory and legal requirements applicable to the organization.
AD.2. Data Governance	Adjustment to, and adoption of privacy regulatory requirements with a risk-based approach and focus on the protection of personal identifiable information (PII).

3.3.1 Organizational CIS Controls - Organization Rating

The assessment has taken a measurement based on the above objectives of the Organization CIS Controls and Addendum controls AD.1 and AD.2, and projected these to <Customer>‘s current position on each of the controls, resulting in a rating of:

CISv7 Organizational



3.3.2 Organizational CIS Controls - Findings and Recommendations

The detailed findings below are associated with each of the four (4) Foundational CIS controls and two (2) Addendum controls, and lead to the following recommendations for <Customer>:

Urgent				
Topic	**Question**	**Answer**	**Advice**	**Advised Products**
17. Implement a Security Awareness and Training Program	Is a Security and Privacy Program established?	Basic (1) No security and privacy awareness program are available	Establish a security and privacy awareness program.	
17. Implement a Security Awareness and Training Program	Is there a Security Awareness Training Program on secure logins, social engineering, sensitive data handling, unintentional data exposure and identifying and reporting incidents?	Basic (1) No training program(s) available	Setup a basic training program for the core roles within the organization.	
18. Application Software Security	Has all third-party software been verified that it is still supported and up to date, or sufficiently hardened based on developer security recommendations?	Basic (1) Not implemented	Update all third-party software regularly.	System Center Configuration Manager (SCCM), Intune
20. Penetration Tests and Red Team Exercises	Are vulnerability scanning and penetration testing tools implemented and used together?	Basic (1) Not implemented	Implement a vulnerability scanning tool within the organization's IT infrastructure and use this as input for pen tests	System Center Configuration Manager (SCCM), Defender ATP, Azure Security Center + Pen testing tools
AD.1. IT Governance	Is there a Security and Privacy Policy defined and enforced by Management?	Basic (1) Not defined and/or documented	Create a security and privacy policy and define the processes related operational processes.	
AD.1. IT Governance	How is the segregation of duties, tasks and responsibilities regulated?	Basic (1) The segregation of tasks, responsibilities and authorizations is informally arranged.	Formalize the segregation of tasks, responsibilities and authorizations by implementing a role matrix.	
AD.1. IT Governance	Are regulatory and legal compliance continuously checked and monitored?	Basic (1) Local legislative and regulatory requirements are implemented.	Implement a review process, implement industry best practices.	Microsoft Compliance Manager

Urgent				
AD.2. Data Governance	Is Personal Identifiable Information (PII) identified throughout the organization, and is personnel aware of the rules and regulations regarding PII?	Basic (1) There is no distinct difference between data.	Make people aware of PII data, create registers to control the PII data.	Azure Information Protection Scanner, Data Loss Prevention, Office 365 Advanced Data Governance, Azure Information Protection P2
AD.2. Data Governance	Is automated Data Classification and Labeling performed by the complete organization on all documents?	Basic (1) Classification and/or labelling of data is not applied.	Define a labeling and classification policy and implement it.	Azure Information Protection Scanner, Data Loss Prevention, Azure Information Protection P2
AD.2. Data Governance	Is Data Risk Management performed at the complete organization level?	Basic (1) No risk management or assessments are performed.	Implement a basic risk management process.	Microsoft Compliance Manager (enables workflow based risk assessments)

High

Topic	Question	Answer	Advice	Advised Products
18. Application Software Security	Is Secure (In-house) development applied, for all applications, macro's, scripts and other workflows/customizations?	Standardized (2) Implemented for some developed software	Initiate a code review or extend the code review tools for all the software developed within/for the organization. Instruct software developers regarding development standards and security/privacy requirements	Code review solution
18. Application Software Security	Is Developer Production Access severely limited or completely prohibited?	Standardized (2) Implemented for some systems	Restrict developer access to all production systems of the organization.	
19. Incident Response and Management	Is an Incident Response Procedure in place, with the right reporting, data collection, management responsibilities, legal protocols and communication strategy?	Standardized (2) A basic incident response procedure is in place	Provide more details to the procedure and include the staff roles and management responsibilities, regularly test this.	Office 365 Advanced Compliance: Advanced eDiscovery
20. Penetration Tests and Red Team Exercises	Are Penetration Tests regularly performed on all enterprise systems?	Basic (1) Not performed or performed ad-hoc	Request an expert third-party specialized in penetration testing to conduct a test on all the external systems of the organization.	

4 Technical Data and Analysis

This is a fact-based summary of **Contoso‘s** (security) data from their scanned IT environment.

This information was gathered with the Cyber Security Assessment Tool (CSAT).

4.1.1 CIS Control 1: Inventory and Control of Hardware Assets

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

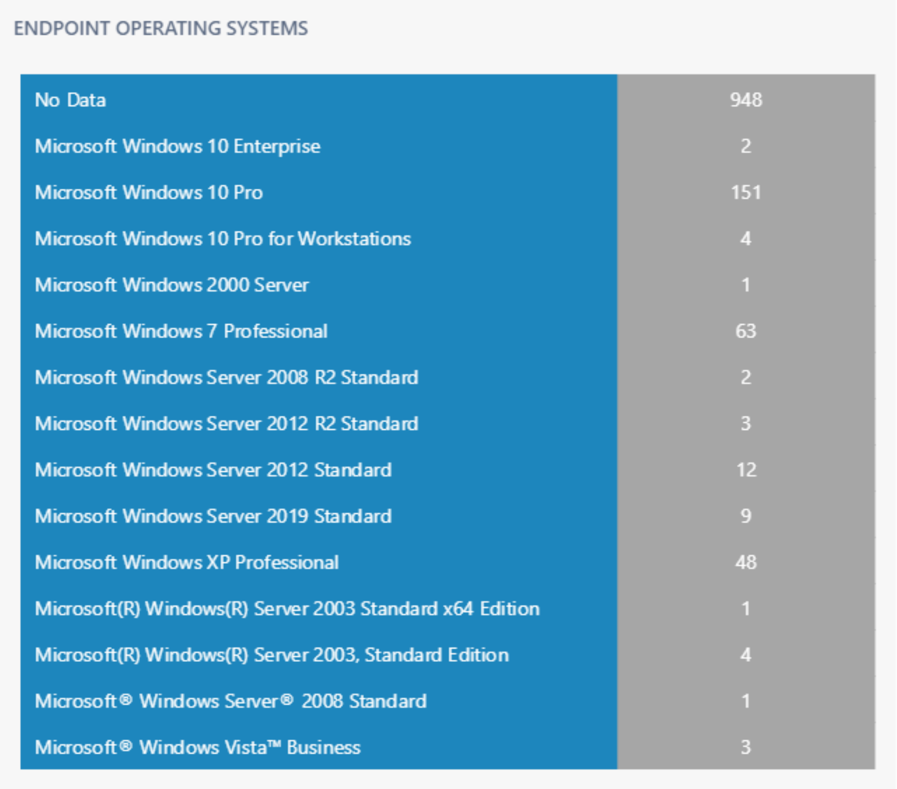
Inventory	Type	Count
Contoso’s Endpoints	Discoverable	1252
	Accessible	310
	Retrievable	304

Analysis and recommendations:

Currently there’s no discovery tool (active and passive) to identify all the devices attached to the organization's infrastructure. There are risks related to not being able to manage devices centrally, which could lead to unauthorized access or malicious activity. It’s advised utilize SCCM with network discovery method or use Intune to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory and implement port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.

4.1.2 CIS Control 2: Inventory and Control of Software Assets

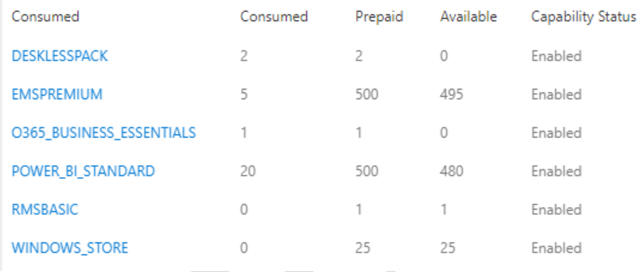
CSAT Output – Versioning Status



ENDPOINT OPERATING SYSTEMS

No Data	948
Microsoft Windows 10 Enterprise	2
Microsoft Windows 10 Pro	151
Microsoft Windows 10 Pro for Workstations	4
Microsoft Windows 2000 Server	1
Microsoft Windows 7 Professional	63
Microsoft Windows Server 2008 R2 Standard	2
Microsoft Windows Server 2012 R2 Standard	3
Microsoft Windows Server 2012 Standard	12
Microsoft Windows Server 2019 Standard	9
Microsoft Windows XP Professional	48
Microsoft(R) Windows(R) Server 2003 Standard x64 Edition	1
Microsoft(R) Windows(R) Server 2003, Standard Edition	4
Microsoft® Windows Server® 2008 Standard	1
Microsoft® Windows Vista™ Business	3

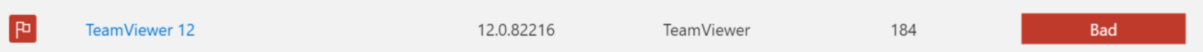
CSAT Output – Licensing Status



Consumed	Consumed	Prepaid	Available	Capability Status
DESKLESSPACK	2	2	0	Enabled
EMSPREMIUM	5	500	495	Enabled
O365_BUSINESS_ESSENTIALS	1	1	0	Enabled
POWER_BI_STANDARD	20	500	480	Enabled
RMSBASIC	0	1	1	Enabled
WINDOWS_STORE	0	25	25	Enabled

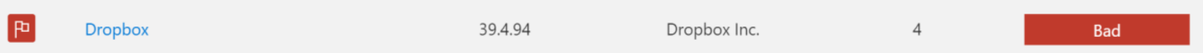
CSAT Output – Installed Applications

While a lot of the installed applications do not represent a risk, there are a few applications that could represent a risk to the endpoints. TeamViewer is installed on almost all endpoints.



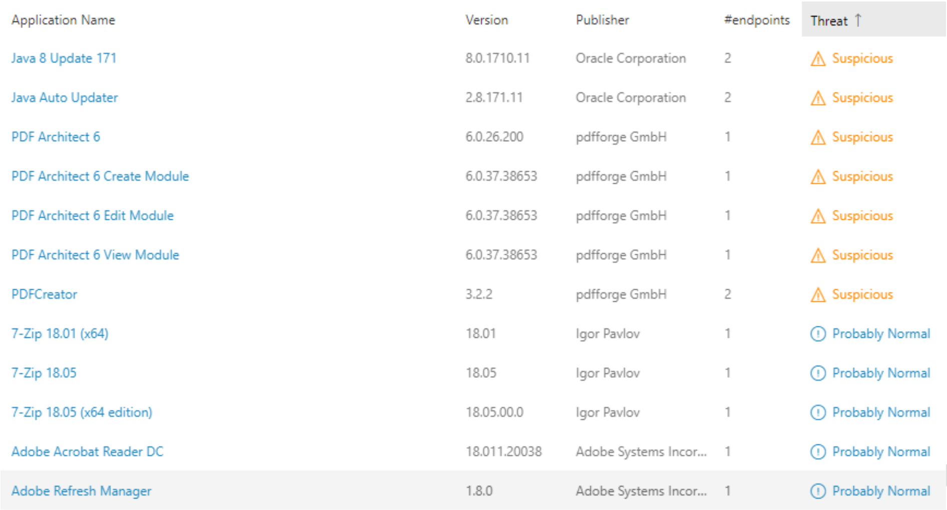
⚑	TeamViewer 12	12.0.82216	TeamViewer	184	Bad

Dropbox is installed on four laptops.



⚑	Dropbox	39.4.94	Dropbox Inc.	4	Bad

The next picture shows an overview of all the “Suspicious” and “Probably normal” applications that where found during the scan.



Application Name	Version	Publisher	#endpoints	Threat ↑
Java 8 Update 171	8.0.1710.11	Oracle Corporation	2	⚠ Suspicious
Java Auto Updater	2.8.171.11	Oracle Corporation	2	⚠ Suspicious
PDF Architect 6	6.0.26.200	pdfforge GmbH	1	⚠ Suspicious
PDF Architect 6 Create Module	6.0.37.38653	pdfforge GmbH	1	⚠ Suspicious
PDF Architect 6 Edit Module	6.0.37.38653	pdfforge GmbH	1	⚠ Suspicious
PDF Architect 6 View Module	6.0.37.38653	pdfforge GmbH	1	⚠ Suspicious
PDFCreator	3.2.2	pdfforge GmbH	2	⚠ Suspicious
7-Zip 18.01 (x64)	18.01	Igor Pavlov	1	ⓘ Probably Normal
7-Zip 18.05	18.05	Igor Pavlov	1	ⓘ Probably Normal
7-Zip 18.05 (x64 edition)	18.05.00.0	Igor Pavlov	1	ⓘ Probably Normal
Adobe Acrobat Reader DC	18.011.20038	Adobe Systems Incor...	1	ⓘ Probably Normal
Adobe Refresh Manager	1.8.0	Adobe Systems Incor...	1	ⓘ Probably Normal

Analysis and recommendations:

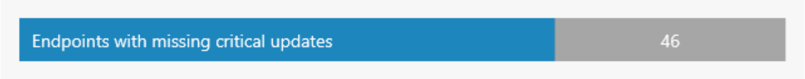
- The end of life products **Windows Server 2000**, **Windows Server 2003**, **Windows Vista** and **Windows XP** has been found, start phasing out these systems as soon as possible.
- The almost end of life products **Windows 7** and **Windows Server 2008** have been found. Create a plan to phase these operating systems (OS) out. For Windows 7 and Server 2008 applies that if you move these OS to Azure, you will receive extended Security Support.
- The version of Windows being used (**10.0.16299**) on several endpoints is not up to date. The latest version of windows 10 is **10.0.18362**. Update all the endpoints to the latest version.

Start upgrading all other software products that (almost) have reached their End of Support. See Appendix B - End of Life products for the products with the expected end of life date.

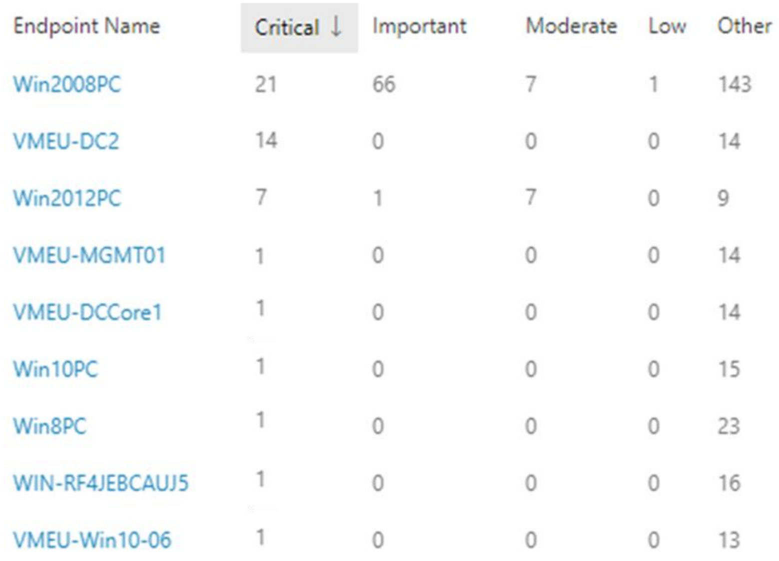
In the application list there are a few applications that were not installed by IT and can, therefore, be an issue. TeamViewer and Dropbox represent the use of shadow IT in the company infrastructure. With the use of AppLocker, or Azure Security Center, Windows Application Control you can define applications which may be installed in the company infrastructure. AppLocker can be setup with a GPO.

4.1.3 CIS Control 3: Continuous Vulnerability Management

CSAT Output – Update Status



Endpoints with missing critical updates 46



Endpoint Name	Critical ↓	Important	Moderate	Low	Other
Win2008PC	21	66	7	1	143
VMEU-DC2	14	0	0	0	14
Win2012PC	7	1	7	0	9
VMEU-MGMT01	1	0	0	0	14
VMEU-DCCore1	1	0	0	0	14
Win10PC	1	0	0	0	15
Win8PC	1	0	0	0	23
WIN-RF4JEBCAUJ5	1	0	0	0	16
VMEU-Win10-06	1	0	0	0	13

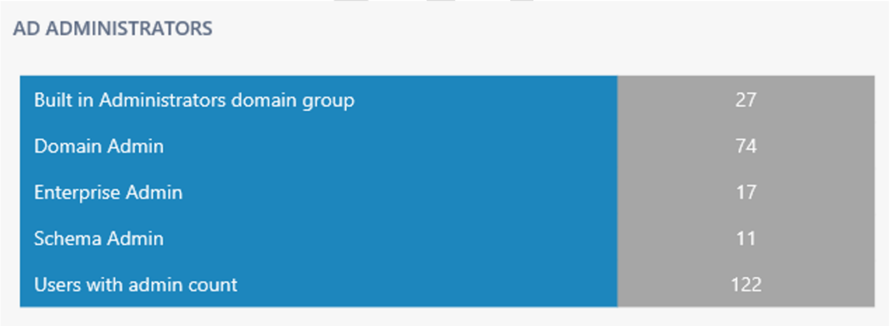
Analysis and recommendations:

- **46** Endpoints found with missing critical Security patches, roll out the available security patches as soon as possible.

Operating Systems vulnerabilities can be a potential threat to the security of the IT infrastructure. Especially if those security vulnerabilities are publicly spreading rapidly and become well known for their attack surface. Regularly applying patches and security hotfixes has therefore become an increasing priority to keep systems protected and safe. It is advised to implement tooling like SCCM, WSUS or Intune (for mobile devices) to automate the patch management process. With tooling like this you can easily gain insights on the patch status of all systems and also eases the process of enrolling security patches to the endpoints.

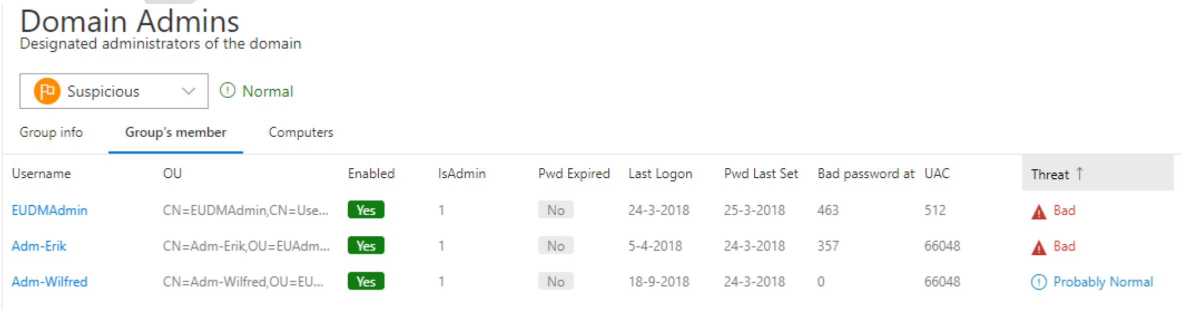
4.1.4 CIS Control 4: Controlled Use of Administrative Privileges

CSAT Output – Active Directory Administrative Groups



AD ADMINISTRATORS

Built in Administrators domain group	27
Domain Admin	74
Enterprise Admin	17
Schema Admin	11
Users with admin count	122



Domain Admins
Designated administrators of the domain

Username	OU	Enabled	IsAdmin	Pwd Expired	Last Logon	Pwd Last Set	Bad password at	UAC	Threat ↑
EUDMAdmin	CN=EUDMAdmin,CN=Use...	Yes	1	No	24-3-2018	25-3-2018	463	512	Bad
Adm-Erik	CN=Adm-Erik,OU=EUAdm...	Yes	1	No	5-4-2018	24-3-2018	357	66048	Bad
Adm-Wilfred	CN=Adm-Wilfred,OU=EU...	Yes	1	No	18-9-2018	24-3-2018	0	66048	Probably Normal

Azure Active Directory Administrative Groups

Inventory	Group name	Count
Office 365/Azure roles	Global Administrator	5
	Billing Administrator	2
	Security Administrator	5
Administrator accounts that use MFA for access	MFA enabled	0
	MFA not enabled	12

Analysis and recommendations:

AD administrative groups

- A high number of administrators was found in the **Built-in Administrators Domain** group. Members of this group have full control of the domain controllers, therefore membership should be limited as much as possible. Review these accounts and clean up old/unused accounts.

- A high number of **Domain Admins** was found. Members of this group have full control of the domain, therefore membership must be limited as much as possible. Review these accounts and clean up old/unused accounts.

- A high number of **Enterprise admins** was found. Members of this group have full control of all domains in a forest. Ideally this group should only contain 0 or 1 user. Review these accounts and clean up old/unused accounts.

- A high number of **Schema admins** was found**.** Members of this group can modify the Active Directory schema. Ideally this group should only contain 0 or 1 user. Review these accounts and clean up old/unused accounts.

Azure AD administrative groups

- Multi Factor Authentication is not enabled for any AAD administrators. Implement Azure MFA for all AAD administrators.

Administrator accounts bring high risk to a company's network, since they have access to your network, or systems and sensitive data. Therefore, it is recommended to regularly review the authorizations for administrator accounts.

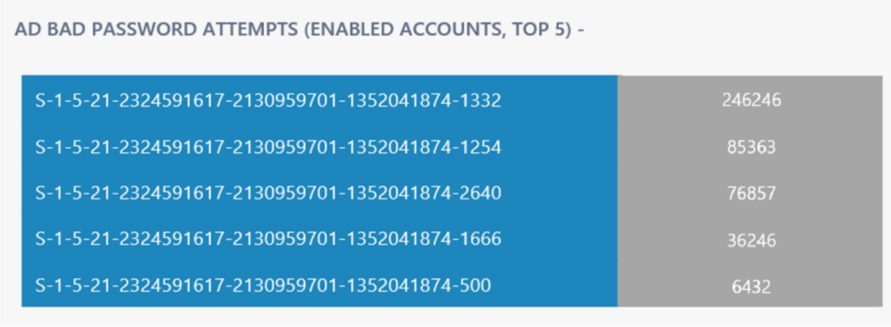
It is recommended to implement the principle of least privilege, limiting access to those who require and are authorized for it, and by allowing only enough access to perform the required job. Implement Azure Privileged Identity Management (PIM) to manage, control and monitor access to important resources. Also, implement Multi Factor Authentication for all (privileged) accounts.

4.1.5 CIS Control 5: Secure Configuration for Hardware and Software

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.6 CIS Control 6: Maintenance, Monitoring and Analysis of Audit logs

CSAT Output – Bad Password Attempts AD



AD BAD PASSWORD ATTEMPTS (ENABLED ACCOUNTS, TOP 5) -

S-1-5-21-2324591617-2130959701-1352041874-1332	246246
S-1-5-21-2324591617-2130959701-1352041874-1254	85363
S-1-5-21-2324591617-2130959701-1352041874-2640	76857
S-1-5-21-2324591617-2130959701-1352041874-1666	36246
S-1-5-21-2324591617-2130959701-1352041874-500	6432

*Usernames have been anonymized for privacy reasons.

Analysis and recommendations:

- A very high number of bad password attempts has been found. This could mean that a brute force attack has been enforced. Investigate the source of the logins and the reason that these accounts above have so many bad password attempts.

Suspicious logons and failed login events should be monitored to help and protect your organization from multiple types of advanced targeted cyber-attacks and insider threats. Recommended is to use Azure ATP or Advanced Threat Analytics (ATA) to get early warnings about possible attacks. These automatic tooling monitors against a lot of different (AD) attacks. Combine this with Azure AD Identity Protection for the cloud users.

4.1.7 CIS Control 7: Email and Web Browser Protections

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

Inventory	Used	Notes
SPF record	v=spf1 include:spf.protection.outlook.com -all	
DKIM record	Not found	
DMARC record	Not found	

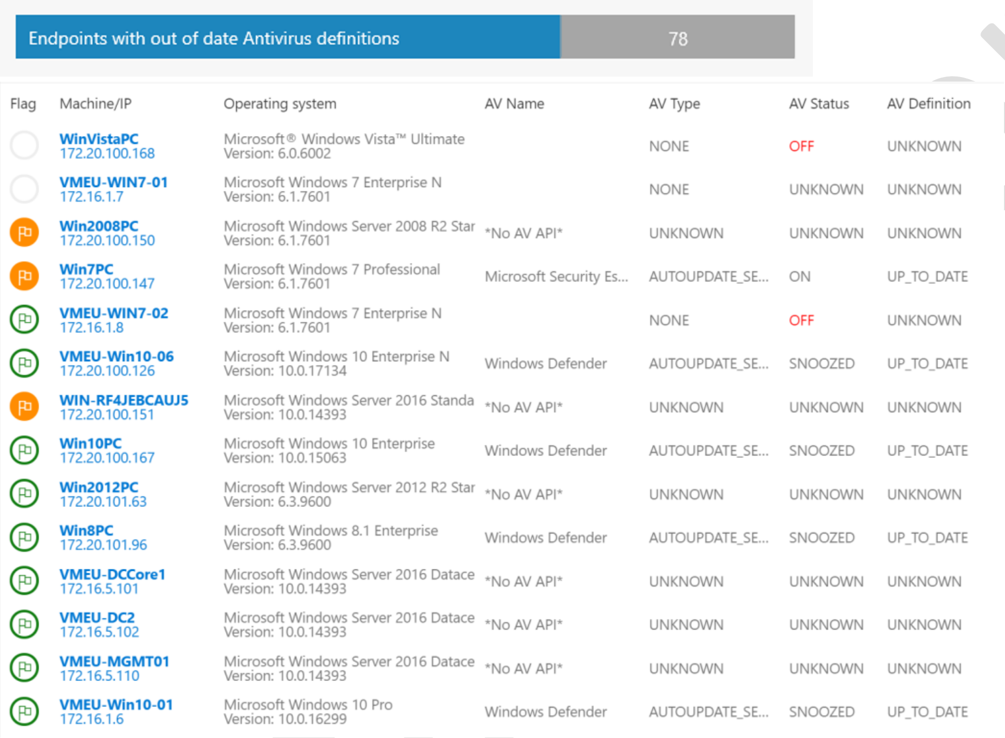
Analysis and recommendations:

- **No DKIM record was found**. This may lead to undetected email spoofing, and allow hackers to tamper or compromise the content of email. A Domain Keys Identified Mail, also known as DKIM, gives an organization the opportunity to take responsibility for a message while it is in transit. The message is signed with the organization's certificate and a signature is added to the email headers. Create the appropriate DKIM record

- **No DMARC record was found**. This will lead to email domain owners not being able to control how their email is processed, making it easier for criminals to spoof messages to appear as though they have come from a trusted address. DMARC offers linkage to the author's domain name, published policies for recipient handling of authentication failures and reporting from receivers to senders. It is recommended to create the appropriate DMARC record to help the organization to decide what to do with e-mails that fails checks and create a feedback loop to allow course correction.

4.1.8 CIS Control 8: Malware Defenses

CSAT Output – AV Status



Endpoints with out of date Antivirus definitions 78

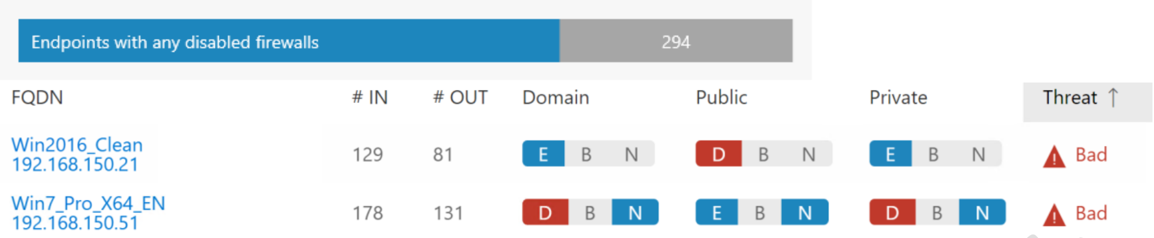
Flag	Machine/IP	Operating system	AV Name	AV Type	AV Status	AV Definition
○	**WinVistaPC** 172.20.100.168	Microsoft® Windows Vista™ Ultimate Version: 6.0.6002		NONE	OFF	UNKNOWN
○	**VMEU-WIN7-01** 172.16.1.7	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	UNKNOWN	UNKNOWN
●	**Win2008PC** 172.20.100.150	Microsoft Windows Server 2008 R2 Star Version: 6.1.7601	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
●	**Win7PC** 172.20.100.147	Microsoft Windows 7 Professional Version: 6.1.7601	Microsoft Security Es...	AUTOUPDATE_SE...	ON	UP_TO_DATE
◎	**VMEU-WIN7-02** 172.16.1.8	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	OFF	UNKNOWN
◎	**VMEU-Win10-06** 172.20.100.126	Microsoft Windows 10 Enterprise N Version: 10.0.17134	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
●	**WIN-RF4JEBCAUJ5** 172.20.100.151	Microsoft Windows Server 2016 Standa Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
◎	**Win10PC** 172.20.100.167	Microsoft Windows 10 Enterprise Version: 10.0.15063	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
◎	**Win2012PC** 172.20.101.63	Microsoft Windows Server 2012 R2 Star Version: 6.3.9600	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
◎	**Win8PC** 172.20.101.96	Microsoft Windows 8.1 Enterprise Version: 6.3.9600	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE
◎	**VMEU-DCCore1** 172.16.5.101	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
◎	**VMEU-DC2** 172.16.5.102	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
◎	**VMEU-MGMT01** 172.16.5.110	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN
◎	**VMEU-Win10-01** 172.16.1.6	Microsoft Windows 10 Pro Version: 10.0.16299	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE

Analysis and recommendations:

- There are **78** endpoints with out of date Antivirus definitions. These endpoints are vulnerable for attacks, an out of date antivirus may not be able to recognize and respond to latest threats. Recommended is to update the antivirus as soon as possible.
- There are **2** endpoints that have their antivirus disabled, check these endpoints and turn the antivirus on.

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

CSAT Output – Firewall Status



Endpoints with any disabled firewalls 294

FQDN	# IN	# OUT	Domain	Public	Private	Threat ↑
Win2016_Clean 192.168.150.21	129	81	E B N	D B N	E B N	Bad
Win7_Pro_X64_EN 192.168.150.51	178	131	D B N	E B N	D B N	Bad

Analysis and recommendations:

- **294** Endpoints found with one or more disabled Windows firewalls, it is advised to enable the firewalls on these machines.

Windows firewall provides protection from network attacks on the endpoints that pass through your perimeter network or originate inside your organization, such as Trojan horse attacks, worms, or any other type of malicious program spread through unsolicited incoming traffic.. Any infected machine that gets access to your corporate intranet can potentially make a connection to unprotected endpoints or servers and compromises it by exposing a vulnerability in a Windows service or 3rd-party application. Therefore it is advised to have the Windows firewalls enabled for a defense in depth, in case the software/hardware firewall is inactive, the Windows Firewall will take over and protect the endpoints security. It is also advised to implement a process to regularly check the firewall status and enforce policy using GP on AD.

4.1.10 CIS Control 10: Data Recovery Capability

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.11 CIS Control 11: Secure Configuration for Network Devices

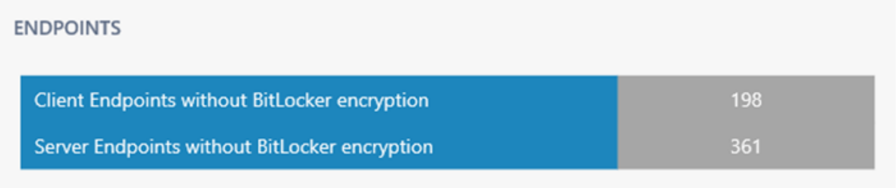
No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.12 CIS Control 12: Boundary Defense

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

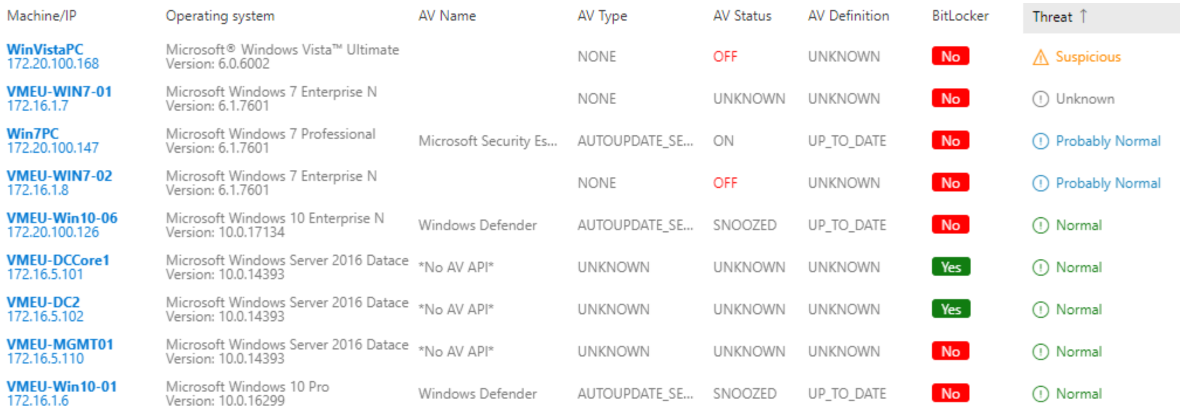
4.1.13 CIS Control 13: Data Protection

CSAT Output – Encryption Status



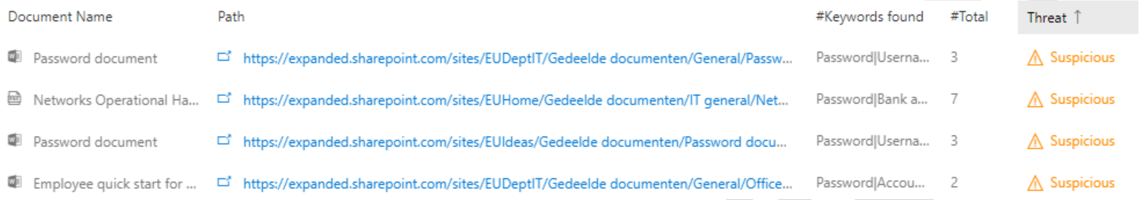
ENDPOINTS

Client Endpoints without BitLocker encryption	198
Server Endpoints without BitLocker encryption	361



Machine/IP	Operating system	AV Name	AV Type	AV Status	AV Definition	BitLocker	Threat ↑
WinVistaPC 172.20.100.168	Microsoft® Windows Vista™ Ultimate Version: 6.0.6002		NONE	OFF	UNKNOWN	No	⚠ Suspicious
VMEU-WIN7-01 172.16.1.7	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	UNKNOWN	UNKNOWN	No	ⓘ Unknown
Win7PC 172.20.100.147	Microsoft Windows 7 Professional Version: 6.1.7601	Microsoft Security Es...	AUTOUPDATE_SE...	ON	UP_TO_DATE	No	ⓘ Probably Normal
VMEU-WIN7-02 172.16.1.8	Microsoft Windows 7 Enterprise N Version: 6.1.7601		NONE	OFF	UNKNOWN	No	ⓘ Probably Normal
VMEU-Win10-06 172.20.100.126	Microsoft Windows 10 Enterprise N Version: 10.0.17134	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE	No	ⓘ Normal
VMEU-DCCore1 172.16.5.101	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	Yes	ⓘ Normal
VMEU-DC2 172.16.5.102	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	Yes	ⓘ Normal
VMEU-MGMT01 172.16.5.110	Microsoft Windows Server 2016 Datace Version: 10.0.14393	*No AV API*	UNKNOWN	UNKNOWN	UNKNOWN	No	ⓘ Normal
VMEU-Win10-01 172.16.1.6	Microsoft Windows 10 Pro Version: 10.0.16299	Windows Defender	AUTOUPDATE_SE...	SNOOZED	UP_TO_DATE	No	ⓘ Normal

CSAT Output – Potential PII Data



Document Name	Path	#Keywords found	#Total	Threat ↑
Password document	https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Passw...	Password|Userna...	3	⚠ Suspicious
Networks Operational Ha...	https://expanded.sharepoint.com/sites/EUHome/Gedeelde documenten/IT general/Net...	Password|Bank a...	7	⚠ Suspicious
Password document	https://expanded.sharepoint.com/sites/EUIdeas/Gedeelde documenten/Password docu...	Password|Userna...	3	⚠ Suspicious
Employee quick start for ...	https://expanded.sharepoint.com/sites/EUDeptIT/Gedeelde documenten/General/Office...	Password|Accou...	2	⚠ Suspicious

Analysis and recommendations:

Encryption

- **198** scanned client endpoints don’t have BitLocker encryption enabled.
- **361** scanned server endpoints don’t have BitLocker encryption enabled.

An unencrypted hard drive will pose a risk of losing data in case the device/system is lost or stolen, this applies especially to laptops. Applying hard drive encryption with BitLocker is a cost-effective way of protecting the data on stolen or lost devices. When disk encryption is applied it will prevent unauthorized access to the data storage. Some regulations, for example PCI-DSS and EU GDPR require the use of data encryption.

Create an Intune configuration policy that will enable BitLocker and store the BitLocker recovery key in the Azure Active Directory. Also create an Intune compliance policy so the client only gains access to company resources if the client has an encrypted hard disk.

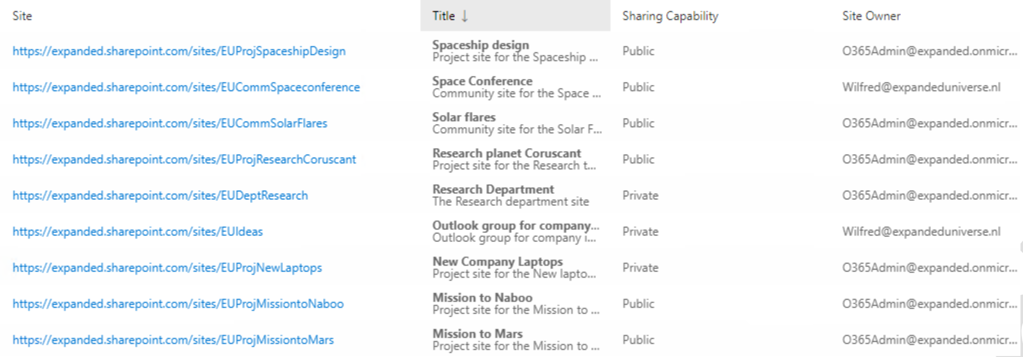
Potential PII data

- There were 4 shared documents found that require special attention. These documents contain keywords such as “password” and “username”.

Almost all endpoints are using the SharePoint library sync. The sync enables the user to easily access data they want to use offline or have quick access to, however for example the HR department has synced the entire HR site to their local devices. On the HR site are 20.464 documents with personal information about the employees. The documents in this library contain PII data which should always be encrypted. Advise is to enable BitLocker on all endpoints that contain sensitive data and apply classification and labeling on all documents that contain sensitive data with Azure Information Protection P2. To get insights in which documents contain sensitive data use Azure Information Protection scanner (for on premise) and Data Loss Prevention (for cloud).

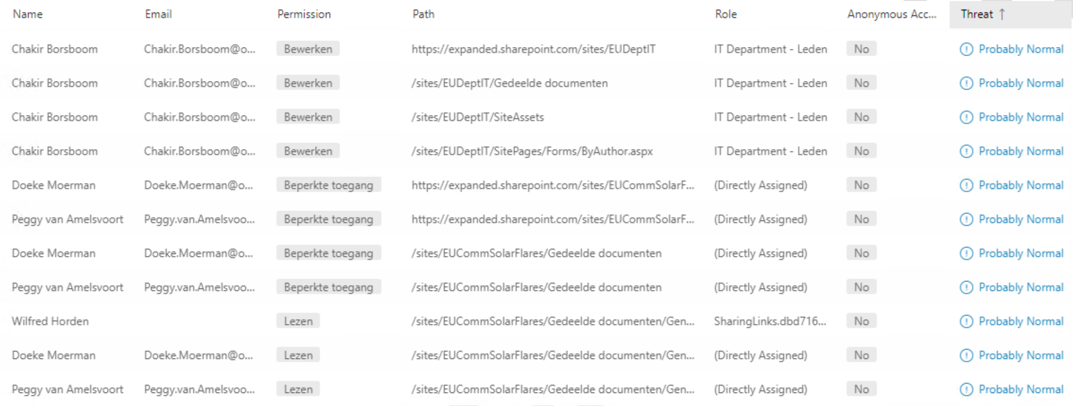
4.1.14 CIS Control 14: Controlled Access Based on the Need to Know

CSAT Output – SharePoint Site Permissions



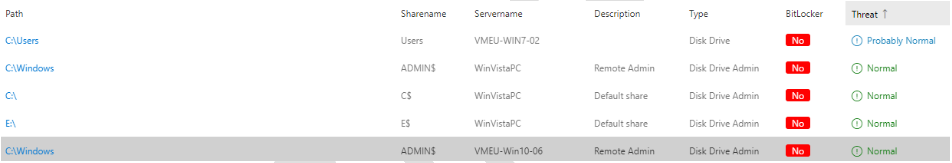
Site	Title ↓	Sharing Capability	Site Owner
https://expanded.sharepoint.com/sites/EUProjSpaceshipDesign	**Spaceship design** Project site for the Spaceship ...	Public	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUCommSpaceconference	**Space Conference** Community site for the Space ...	Public	Wilfred@expandeduniverse.nl
https://expanded.sharepoint.com/sites/EUCommSolarFlares	**Solar flares** Community site for the Solar F...	Public	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUProjResearchCoruscant	**Research planet Coruscant** Project site for the Research t...	Public	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUDeptResearch	**Research Department** The Research department site	Private	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUIdeas	**Outlook group for company...** Outlook group for company i...	Private	Wilfred@expandeduniverse.nl
https://expanded.sharepoint.com/sites/EUProjNewLaptops	**New Company Laptops** Project site for the New lapto...	Private	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUProjMissiontoNaboo	**Mission to Naboo** Project site for the Mission to ...	Public	O365Admin@expanded.onmicr...
https://expanded.sharepoint.com/sites/EUProjMissiontoMars	**Mission to Mars** Project site for the Mission to ...	Public	O365Admin@expanded.onmicr...

CSAT Output – SharePoint Externally Shared



Name	Email	Permission	Path	Role	Anonymous Acc...	Threat ↑
Chakir Borsboom	Chakir.Borsboom@o...	Bewerken	https://expanded.sharepoint.com/sites/EUDeptIT	IT Department - Leden	No	ⓘ Probably Normal
Chakir Borsboom	Chakir.Borsboom@o...	Bewerken	/sites/EUDeptIT/Gedeelde documenten	IT Department - Leden	No	ⓘ Probably Normal
Chakir Borsboom	Chakir.Borsboom@o...	Bewerken	/sites/EUDeptIT/SiteAssets	IT Department - Leden	No	ⓘ Probably Normal
Chakir Borsboom	Chakir.Borsboom@o...	Bewerken	/sites/EUDeptIT/SitePages/Forms/ByAuthor.aspx	IT Department - Leden	No	ⓘ Probably Normal
Doeke Moerman	Doeke.Moerman@o...	Beperkte toegang	https://expanded.sharepoint.com/sites/EUCommSolarF...	(Directly Assigned)	No	ⓘ Probably Normal
Peggy van Amelsvoort	Peggy.van.Amelsvoo...	Beperkte toegang	https://expanded.sharepoint.com/sites/EUCommSolarF...	(Directly Assigned)	No	ⓘ Probably Normal
Doeke Moerman	Doeke.Moerman@o...	Beperkte toegang	/sites/EUCommSolarFlares/Gedeelde documenten	(Directly Assigned)	No	ⓘ Probably Normal
Peggy van Amelsvoort	Peggy.van.Amelsvoo...	Beperkte toegang	/sites/EUCommSolarFlares/Gedeelde documenten	(Directly Assigned)	No	ⓘ Probably Normal
Wilfred Horden		Lezen	/sites/EUCommSolarFlares/Gedeelde documenten/Gen...	SharingLinks.dbd716...	No	ⓘ Probably Normal
Doeke Moerman	Doeke.Moerman@o...	Lezen	/sites/EUCommSolarFlares/Gedeelde documenten/Gen...	(Directly Assigned)	No	ⓘ Probably Normal
Peggy van Amelsvoort	Peggy.van.Amelsvoo...	Lezen	/sites/EUCommSolarFlares/Gedeelde documenten/Gen...	(Directly Assigned)	No	ⓘ Probably Normal

CSAT Output – Endpoint Shares



Path	Sharename	Servername	Description	Type	BitLocker	Threat ↑
C:\Users	Users	VMEU-WIN7-02		Disk Drive	No	ⓘ Probably Normal
C:\Windows	ADMIN$	WinVistaPC	Remote Admin	Disk Drive Admin	No	ⓘ Normal
C:\	C$	WinVistaPC	Default share	Disk Drive Admin	No	ⓘ Normal
E:\	E$	WinVistaPC	Default share	Disk Drive Admin	No	ⓘ Normal
C:\Windows	ADMIN$	VMEU-Win10-06	Remote Admin	Disk Drive Admin	No	ⓘ Normal

Analysis and recommendations:

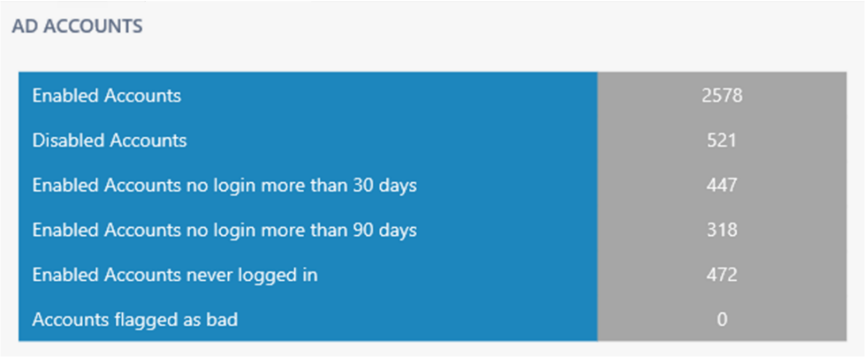
SharePoint Sites and Endpoint Shares might contain confidential data. It's important that only the rightful users have access to these SharePoint Sites and Endpoint Shares. We recommend to create procedures for the business to do attestation on user permissions and assign an owner. With this periodic check you can check if the users have the rights they need and cannot see data they aren't supposed to see.

4.1.15 CIS Control 15: Wireless Access Control

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.16 CIS Control 16: Account Monitoring and Control

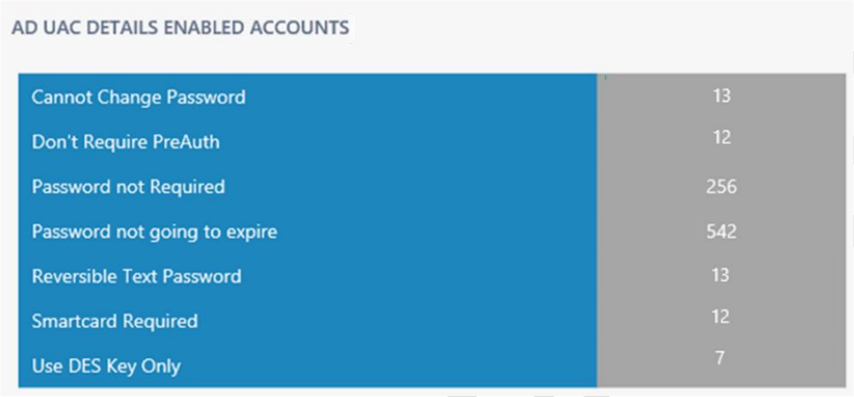
CSAT Output – AD Account Status



AD ACCOUNTS

Enabled Accounts	2578
Disabled Accounts	521
Enabled Accounts no login more than 30 days	447
Enabled Accounts no login more than 90 days	318
Enabled Accounts never logged in	472
Accounts flagged as bad	0

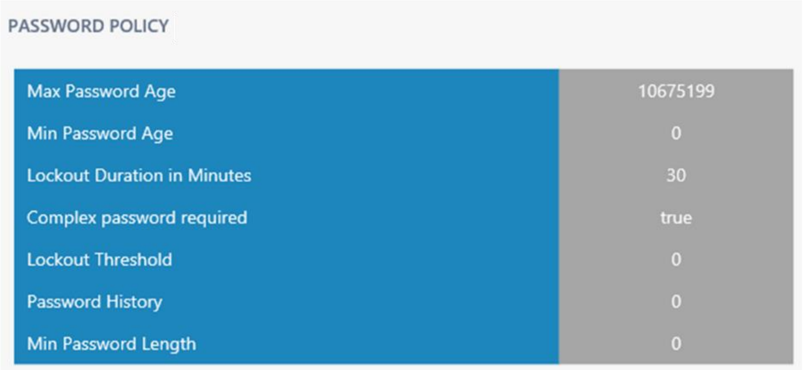
CSAT Output – AD User Account Control Flags (enabled accounts)



AD UAC DETAILS ENABLED ACCOUNTS

Cannot Change Password	13
Don't Require PreAuth	12
Password not Required	256
Password not going to expire	542
Reversible Text Password	13
Smartcard Required	12
Use DES Key Only	7

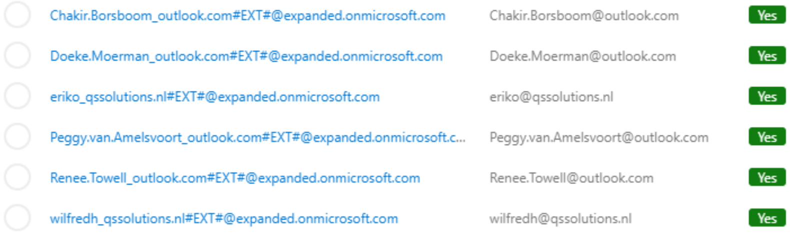
CSAT Output – AD Password policy



PASSWORD POLICY

Max Password Age	10675199
Min Password Age	0
Lockout Duration in Minutes	30
Complex password required	true
Lockout Threshold	0
Password History	0
Min Password Length	0

CSAT Output – Azure Active Directory – External Users



○	Chakir.Borsboom_outlook.com#EXT#@expanded.onmicrosoft.com	Chakir.Borsboom@outlook.com	Yes
○	Doeke.Moerman_outlook.com#EXT#@expanded.onmicrosoft.com	Doeke.Moerman@outlook.com	Yes
○	eriko_qssolutions.nl#EXT#@expanded.onmicrosoft.com	eriko@qssolutions.nl	Yes
○	Peggy.van.Amelsvoort_outlook.com#EXT#@expanded.onmicrosoft.c...	Peggy.van.Amelsvoort@outlook.com	Yes
○	Renee.Towell_outlook.com#EXT#@expanded.onmicrosoft.com	Renee.Towell@outlook.com	Yes
○	wilfredh_qssolutions.nl#EXT#@expanded.onmicrosoft.com	wilfredh@qssolutions.nl	Yes

Analysis and recommendations:

AD Account Status and AD User Account Flags

- **318** Accounts have **not logged on for 90 days** and **472** accounts have **never logged on**. Review these accounts and disable the unused accounts.

- **521** Accounts are **disabled**, clean these accounts up.

- **13** Accounts **cannot change their passwords**, review these accounts.

- **12** Accounts **don't require Kerberos pre-authentication for logon**. Kerberos pre-authentication enables protection against password-guessing attacks. Review these accounts.

- **256** Accounts have the setting **Password Not Required** enabled. This flag enables an account to logon with a blank password. Review these accounts and remove

- **542** Accounts have the setting **Password not going to expire** enabled. Older passwords are more vulnerable to being hacked. Review these accounts and remove this setting if possible.

- **13** Accounts have the setting **Reversible Text Passwords** enabled, this means that the encrypted passwords can be decrypted. Review these accounts and disable this setting.

- **12** Accounts have the setting **Smartcard required** enabled, this flag forces the user to log on using a smartcard. In case the smartcard is stolen or lost, this could potentially result into a security breach.

- **7** Accounts **use DES Key Only**, this encryption method uses 56-bit keys. It's short key length makes it vulnerable to a brute-force attack. Therefore it's advised to review these accounts and disable this UAC flag. It's advised to apply the AES (Advanced Encryption Standard) on all accounts.

Password Policy

Contoso should configure password policy to recommended practices such as:

- Maximum password age: 60 or 90 days
- Minimum password age: 1,3 or 7 days
- Account lockout duration: 30 or 60 minutes
- Password must meet complexity requirements: Enabled (true)
- Account lockout threshold: 4 or 5 invalid sign-in attempts
- Password history: 10 or 24
- Minimum password length: 8 or 12 characters

AAD External users

- There are External users found that have been invited on their personal e-mail account (Outlook). It's advised to review accounts that have been invited on their personal accounts.

It is highly recommended to implement Multi Factor Authentication (MFA) and Conditional Access to protect your users, as this is highly effective at stopping attacks.

4.1.17 CIS Control 17: Implement a Security Awareness and Training Program

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.18 CIS Control 18: Application Software Security

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.19 CIS Control 19: Incident Response and Management

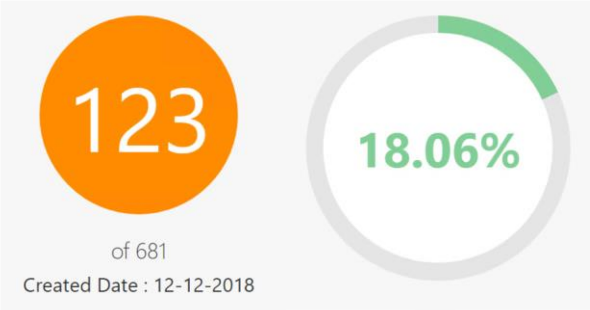
No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.1.20 CIS Control 20: Penetration Tests and Red Team Exercises

No Technical data collected in CSAT, recommendations are in the Organizational CIS Controls – Findings and recommendations.

4.2 Microsoft Secure Score

The **Contoso**'s Microsoft Secure Score retrieved from Contoso.onmicrosoft.com:



123

of 681

Created Date : 12-12-2018

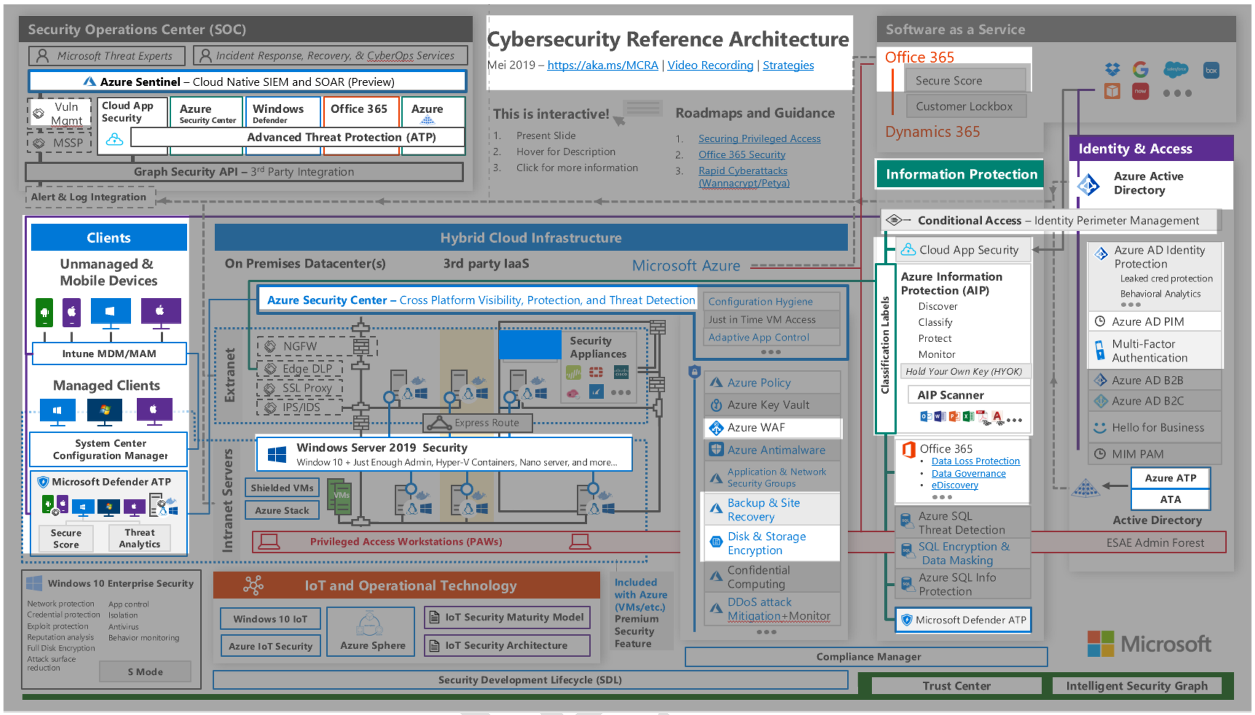
18.06%

Analysis and recommendations:

Multiple tasks from the secure score are implemented on the Office 365 environment. There are multiple tasks at the moment that can be done, for example the MFA on the administrative accounts, MFA on all users. We recommend reviewing the secure score tasks periodically and act on the tasks.

5 Appendix A - Overview of advised security software products

In this report there are one or more references made to Microsoft products that can help to solve the security findings discovered in this Assessment. For an overview of the advised products see below the “Cybersecurity Reference Architecture” as distributed by Microsoft. The highlighted items are the products advised in this report.



Source: https://gallery.technet.microsoft.com/Cybersecurity-Reference-883fb54c

6 Appendix B - End of Life products

The following products that reached their end of life were found:

End of life products	
Windows XP	
Windows Server 2000	
Windows Server 2003	
Windows 10	*Builds: 10240, 10586, 14393*
Windows Vista	

The following products with an expected end of life very soon were found:

Soon to become End of life products	
SQL Server 2008	July 2019
Windows Server 2008 R2	*January 2020*
Windows 7	*January 2020*
Exchange Server 2010	*January 2020*
Office 2010	*October 2020*
Sharepoint 2010	*October 2020*

7 Appendix C - Scope of the Assessment

The Cybersecurity Assessment was executed with the following scope:

Organization	
Customer name	Contoso
Core business activities	Health Care
Business objectives	Deliver the best care to the customer and save lives with the help of the latest technologies
Customer headquarters address	1234 Somewhere street Netherlands, Amersfoort 9876 AB
Number of employees	300
Office location(s)	Netherlands

IT environment	
Licensing programs in use	Enterprise Agreement, Direct Subscription for Office 365
Platform architecture	Hybrid
Virtualization platform(s)	Hyper-V
Core business applications	Exchange Online, Hospital information system, Office ProPlus
Additional information	Three dedicated machines are using Windows XP SP2, Contoso is in the process to replace these machines with Windows 10 version 1803.

Assessment Key dates and deadlines	
Activity	**Date**
Customer Kickoff call	16-10-2018
Complete interview series and on-site inventory collection	19-10-2018
Inventory data analysis/review	22-10-2018
Delivery of Reports	31-10-2018

Final call with customer to review all deliverables	31-10-2018

Partner Assessment participants		
Name	**Company**	**Project role**
Henri Johnson	Contoso	IT project manager
Renee Towell	Contoso	Security officer
Chakir Borsboom	QS solutions	Security consultant
Leo Richards	QS solutions	Reviewer

Interviews were conducted by **QS Solutions** with key stakeholders at **Contoso** to gather information in addition to the automated inventory of the IT infrastructure. These results are based on the answers to the questions outlined in the Cybersecurity Questionnaire. Key interviews were conducted with the following stakeholders at **Contoso**:

Interviewee	Title	Interviewer
Henri Johnson	IT Project manager	Chakir Borsboom
Renee Towell	Security officer	Chakir Borsboom
John Henson	IT Manager	Chakir Borsboom

7.1 Cybersecurity Assessment Goals

Like many organizations, **Contoso** is dealing with the major trend's IT is facing today, including the proliferation of mobile devices, the impact of social networks on organizational operation, the rapid growth of unstructured data, the accelerated adoption of the Cloud and privacy regulations. All these areas are impacted by a shifting threat landscape, meaning security programs and practices are heavily impacted across the board.

The Cybersecurity Solution Assessment provides a high-level review regarding the maturity of **Contoso's** security program based on security controls across the three domains (Basic, Foundational and Organization) contained in the CIS Controls™ Version 7 framework as published by the Center for Internet Security®.

The goals of the Cybersecurity Assessment are to:

- Initiate a foundation for protecting IT assets, and for promoting modern cybersecurity practices in a holistic, integrated way.
- Align with the security "recommended practices" of a well-known and highly regarded security-framework as the foundation for a cybersecurity program.
- Project a security pathway to move to the cloud where internal controls around areas such as authentication, authorization, and data protection will be even more critical.
- Provide recommendations based on the interviews and facts found during the scan of the IT environment.
- Uncover critical issues related to cybersecurity.
- Establish a prioritized action list, based on the criticality of the findings which can serve as a short-term roadmap in the cybersecurity program of the organization.

7.2 Inventory Tools

To conduct an inventory of **Contoso's** IT infrastructure (Technical Topics) the Cyber Security Assessment Tool (CSAT) was used to determine the IT assets and their current state providing as input for the assessment, analysis and report. In addition, the following tools were used:

- Manual inventory and the Cybersecurity Questionnaire

7.3 Cyber Security Assessment Tool

The Cyber Security Assessment Tool (CSAT) is a software product developed by experienced security experts to quickly assess the current status of your organization's security and recommend improvements based on facts. The tool collects relevant data from the IT environment by scanning e.g. endpoints, Active Directory and SharePoint Online. Additionally, CSAT uses a questionnaire to collect data about policies and other key indicators.

CSAT

Organizations are looking for a way to check their security status simple and quickly. They want insight into their vulnerabilities, based on data from the organization's IT infrastructure and Office 365. The Cyber Security Assessment Tool (CSAT) from QS solutions provides this through automated scans and analyses. This is the basis on which the CSAT scan provides recommendations and a short-term action plan in this report to improve your security. It's the perfect way to maximize security and demonstrate that your organization takes security seriously. This is also important given the EU GDPR and other privacy regulations.

8 Appendix D - Assessment background

8.1 Introduction

Hybrid IT strategies - integration between the traditional, on-premises IT infrastructures and Cloud platforms - have become a standard for every organization. This has expanded the scope for cybersecurity practices. The traditional mindset towards IT security, which was often minimalistic and static by nature, is no longer satisfactory in the Cloud era as the threat landscape is expanding, shifting and evolving in a much faster pace. Business ownership of security, and clear instructions on the needed level of security needed are key to protecting the company's assets.

This expanded scope and requires a solid cybersecurity program and practice that is aligned with today's threats and risks, which have changed significantly in the past years:

Traditional IT Environments	Modern IT Environments
"Script Kiddies" and Cyber crimes	Cyber espionage; Cyber warfare
Individual cybercriminals	(Foreign) sponsored actions with nearly unlimited resources by large hacker groups
Attacks on the *Fortune 500* and multi-nationals	All sectors are targeted, even SME organizations
Corporate owned and tightly managed devices	(Un-)managed Bring Your Own Device (BYOD) and/or Choose Your Own Device (CYOD) policies
Business/Commercial centric strategy demands	Privacy centric strategy is mandatory
Security practice to protect IT assets	Data protection to ensure privacy

End-user demands have changed rapidly and the way people work is no longer determined by the organization but by the mindset of a user based on its own experiences with everyday Cloud services and the endless possibilities associated with them. Data is also stored on a wide variety of locations and users expect to have access to corporate data and applications from anywhere, at any time from any device. This creates new security risks because nearly every part of an organization's IT environment is exposed.

Security is relative to the threats and risks an organization faces; there is no absolute security. That which is good for one organization can be overkill for another, a one-size fits all security program does not exist. A maturity-based approach can help to address these variations in security threats and IT risk management.

To establish a measurable security framework a solid foundation of security "recommended practices" is needed. For this reason, the Cybersecurity Assessment is using the **CIS Controls™ (v7)** security framework published by the **Center for Internet Security®** (CIS) (http://www.cisecurity.org). See: Appendix D - Assessment background

During the Cybersecurity Assessment, **Contoso‘s** cybersecurity practices level has been measured by answering a Questionnaire. The measurement was scoped on the practices at the Basic, Foundational and Organizational control domains of the CIS Control™ (v7) security framework.

Besides the measurement through the Questionnaire, relevant security related data was collected from **Contoso**'s IT environment. With this measurement through the Questionnaire, and with the analysis of the collected data, a list of findings, recommendations, action items and a compiled short-term roadmap is provided to improve the cybersecurity program and practices of **Contoso**.

8.2 Control Framework background (CIS)

This security framework is constructed out of **three** domains. The CIS Controls™ (v7) are segregated in domains to provide alignment and guidance throughout the implementation and afterwards in operation. Starting at the **Basic** controls which define the scope and set a baseline for implementation, followed by the **Foundational** domain which covers those essential and important measures to protect IT assets. The **Organizational** domain provides process and procedural guidance with pro-active and mitigative controls to help protect the organization from cyberthreats.

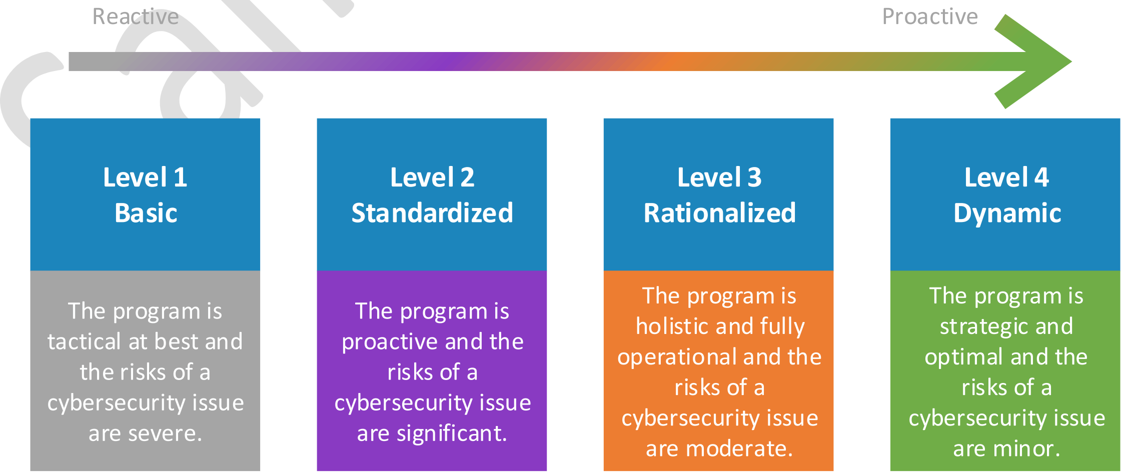
The CIS Controls™ (v7) take a community-based (as opposed to specific enterprise-based) approach to the notion of a risk assessment. Instead of starting from the viewpoint of a specific enterprise (e.g., an agency or a facility), the CIS Controls™ (v7) were created using a consensus risk assessment process. This consensus risk assessment integrates the judgment of a large group of experts from government, industry, and academia regarding the common and pervasive threats and vulnerabilities that are typically found in large enterprises.

Since the CIS Controls™ (v7) were derived from the most common attack patterns and vetted across a very broad community of governments and industries, with very strong consensus on the resulting set of controls, it serves as a very strong basis for high-value actions. The framework does not attempt to replace comprehensive IT and security risk management frameworks. The CIS Controls™ (v7), instead, provide focus and priority to a smaller number of actionable controls with high-leverage and high-payoff.

For the Cybersecurity Assessment, the technical CIS Controls™ (v7) are extended with high-level controls from the ISO/IEC 27001:2013 framework as an addendum on the Organizational control domain. A selection of controls is taken from ISO/IEC 27001:2013 as a beneficiary addition for the customer within the context of the assessment. These questions are related to IT- and data governance, and cover the areas of policies, compliancy, risk management and privacy.

8.3 SOM Model

To achieve this goal, the Cybersecurity Assessment utilizes a Maturity Model to communicate the findings and recommendations. The maturity model construct for the Cybersecurity Assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM). The below reflects the levels:



Level 1 Basic

The program is tactical at best and the risks of a cybersecurity issue are severe.

Level 2 Standardized

The program is proactive and the risks of a cybersecurity issue are significant.

Level 3 Rationalized

The program is holistic and fully operational and the risks of a cybersecurity issue are moderate.

Level 4 Dynamic

The program is strategic and optimal and the risks of a cybersecurity issue are minor.

The complete score of the company is determined by the lowest score in the organization, for example if most processes are at Level 3, but one process is at Level 1, the whole organization is rated at Level 1.

To achieve this goal, the Cybersecurity Assessment utilizes a Maturity Model to communicate the findings and recommendations. The maturity model construct for the Cybersecurity Assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM).