Release Notes

Product	CSAT
Version	1.8.2
Release date	25-01-2021

1. System requirements and prerequisites

CSAT has the following System requirements and prerequisites

1.1. System requirements

The following Operating Systems are supported:

- Windows 10 Professional or Enterprise, build 1803 or newer
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2 (supported, however not recommended)

The minimum requirements for the CSAT server are:

Windows updates	Up to date with the latest Windows updates
Azure Size	A2 or equivalent
CPU	Four CPU cores from one CPU socket
Memory	3.5 GB
Hard disk	At least 50 GB free space
.NET Framework	Version 4.6 or higher

The recommended requirements for the CSAT server are:

Windows updates	Up to date with the latest Windows updates
Azure Size	D4s_v3 or equivalent
CPU	Four CPU cores from one CPU socket
Memory	16 GB
Hard disk	(Azure Premium) SSD with at least 80 GB free space
.NET Framework	Version 4.6 or higher

The targeted endpoints have the following requirements:

- .NET version 3.0 or higher is required
- If you are using IPS and or IDS solutions, please ensure that CSAT traffic is not blocked. When this process is blocked not all endpoints can be scanned
- Antivirus software should allow the execution of the CSAT.exe, cmat_dwnld.exe in the C:\windows\temp\csat folder, as well as the cmd.exe and certutil.exe.

2. Installation, configuration

For the installation of CSAT and all the prerequisites check the CSAT installation manual. This manual contains all information necessary to install and run CSAT.

3. CSAT version 1.8.0 release information

3.1. New Features

- Update .NET core to 3.1.8

- Collect Office 365 audit log setting
- Added support for Active Directory LDAP over SSL scanning
- Collect Azure Active Directory Organizational relationships
- Collect Azure Active Directory Multi factor authentication settings from the Azure Active Directory user accounts
- Collect audit logging data on Windows Server
- Added specific data collection from Azure
  - Read Azure Subscription information
  - Collect Azure Security Center recommendations
  - Collect Azure Secure Score
- Show notification when license is expired
- Collect SharePoint online and OneDrive global sharing settings
- Added threat score for the external users when private mail is used
- Collect Active Directory Password Security Objects
- SSH collects the uptime for Linux machines
- Limit services and analysis menu items based upon the used license type
- Collect the following data for Teams assessments:
  - Collect the total number of Yammer activity
  - Collect Skype for business users
  - Collect SharePoint Online subsite, hubs and active users

3.2. Bugfixes and changes

- Changed the Azure AD roles to reflect the Azure AD role names
- Changed the scan level and browser scan options from the config file to the settings screen
- Updated the license expired notification
- Updated view of the Secure score, UI now shows all incomplete items
- Fixed endpoint count in Firewall CSV export
- Changed the name of the report generation when a Teams license is used
- Fixed an issue where the RDP security level was not shown within the reports screen
- Added support for IP v6 on the Enumeration Service
- Updated the deployment service to ensure endpoint scanning will work when TLS 1.0 and or TLS 1.1 are disabled (TLS 1.2 is now supported)
- Updated progress view for the Active Directory scan, Microsoft cloud scan and SharePoint On-Premises scan
- Added the tenant name for the Microsoft cloud scan report generation
- Changed the left Analysis menu sorting to alphabetical
- Updated the Azure Active Directory risk event widget
- Changed the Azure Active Directory Application creation for the Microsoft cloud scan from the PowerShell script to the CSAT settings UI
- Updated the collection of the firewall settings to include the settings from the registry

3.3. CSAT 1.8.1

- Changed the available questionnaire for the Secure teamwork assessment
- Fixed an issue where there was an issue with the report generation of the teamwork questionnaire
- Updated the Azure scan to collect the Azure Security Recommendation description
- Updated the German translation

3.4. CSAT 1.8.2

- Fixed an issue with the Microsoft Secure Score and the Azure Secure Score, This because the API changed
- Fixed an issue where there was an issue with the Microsoft Cloud scan if the tenant did not have any Azure Active Directory Premium P1 or P2 license(s)

3.5. Known issues

- Scanning the Edge browser history is not supported by Microsoft APIs
- Windows Servers do not return Antivirus data through the Microsoft Security Center API, only detection is if Windows Defender is enabled
- Externally shared data is only returned for document directly shared with a person. Detecting Anonymous shared documents is not possible in SharePoint, as every document has an anonymous sharing link
- The SharePoint Online scan requires “Full control” role. This is because of the Microsoft SharePoint Search API (which we use for the PII search), The API only allows searches with the Full Control permission. When you lower the permission the PII scan will not work
- Status updates from the csat.exe during a scan in the portal are only displayed in English

4. CSAT update from 1.7 to 1.8

With this 1.8 release, you can update a previous CSAT version to the current version. Download the CSAT installation package to the machine where CSAT is currently installed. Start the executable using the account that installed CSAT and it will automatically update CSAT from v1.7 to v1.8. If you want to upgrade from an earlier version to 1.7, get in touch with our email support: sc.csat@qssolutions.nl.

5. Questionnaire changes

In the CSAT 1.8 release, there are several changes made to the questionnaire. The following changes are made in the CIS questionnaire

- Added question – “Are privileged accounts monitored for suspicious behavior, such as unsuccessful logins and changes in groups that have administrative privileges assigned?”
- Added question – “Are users prevented from installing unauthorized browser and email client plugins, and add-on applications?”
- Added question – “Do you have a business continuity and disaster recovery (BCDR) strategy?”
- Added question – “Does the board receive cyber security reports and are risks communicated to the higher management?”
- Added question – “Do you have a plan/roadmap in place to improve cyber security that is supported by the higher management and is the plan/roadmap in line with the business strategy?”
- Added question – “Do you have an internal security audit available and is the performance of the security controls assessed to verify they continue to meet control objectives?”
- Added question – “Is Data Classification and Labeling performed throughout the organization each of the business units, departments and teams?”
- Added question – “how are the policies regarding data storage, retention and archiving in place?”
- Added question – “Do you have risk management processes in place that addresses: the identification and measurement of potential risks, mitigating controls (measures taken to

reduce risk), and the acceptance or transfer of the remaining (residual) risk after mitigation steps have been applied?"

- Added question – "Do you perform vendor risk management on suppliers and third parties that have (privileged) access to your systems and data?"
- Updated question and advised products – "Does every administrator have a dedicated personal admin account and dedicated administrative workstation, separated from their normal user account, secured with MFA and Just in Time access?"
- Updated question advised products – "Are assessments performed on data to identify sensitive information that requires the application of encryption and integrity controls?"
- Updated question advised products – "Has Device and Disk encryption software been applied to mobile devices and all systems that hold sensitive data?"
- Updated question – "Is Network segmentation applied based on the label or classification level of the information stored on the systems?"
- Removed the question "Is Data Risk Management performed at the complete organization level?"

The following changes are made in the Quickscan questionnaire

- Removed question – "Do you have a business continuity and disaster recovery (BCDR) strategy?"