CIS-CAT Pro Assessor: Extraction Guide Tip Sheet

CIS CAT Pro Assessor 4.60

mastercard

Table of content

1. Tool Description

CIS-CAT Pro Assessor is a Java-based tool that scans a target system's configuration settings and reports the system's compliance to the corresponding CIS Benchmark. The results generated are only presented in machine-readable format.

2. Licensing requirements

The CIS-CAT Pro Assessor tool is available for download from the Integrations tab in the "Cyber Quant" Assessment Portal.

The CIS-CAT Pro Assessor tool must be deleted once the configuration files export is completed.

3. Who should use the document

This document is for "Cyber Quant CyMA" users participating in an organizational cyber risk and security assessment using Mastercard's "Cyber Quant Cyber Risk Quantification" platform.

The document is also targeted at experienced IT and cyber professionals who will extract technology infrastructure configuration files for the "Cyber Quant CyMA" cyber risk and security assessment.

4. Requirements & permissions

- Machine Requirements:
  - Windows server or client OS (it cannot be executed on a Linux machine).
  - CIS-CAT Pro Assessor requires a Java Runtime Environment (JRE) at or above version 1.8. The JRE package is available from the "Cyber Quant" portal – link on page 5.
- User Requirements:
  - Windows machine for the execution of the tool.
  - Network expert experienced with local and remote connections to the organizational technological assets.

- Access Requirements:
  - Administrative permissions to execute the CIS-CAT Pro Assessor.
  - Administrative permissions to connect to the organizational technological assets.

5. High-level process flow

The "CIS-CAT Pro Assessor" tool is downloaded from a provided link as a zip document and extracted in the C:\ drive.

The tool is executed with administrative permissions to get the required access to all system configurations.

A basic local scan assesses a local Windows machine containing the tool and generates an "ARF XML" format report.

A remote advanced scan is performed to assess a CentOS via SSH and generate an "ARF XML" format report.

Finally, the reports are imported into "CyMA" for analysis.

6. Tool Download Instructions

1. Decide on the target machine to download CIS-CAT Pro Assessor. **A Windows OS (client or server) must power the target machine.**

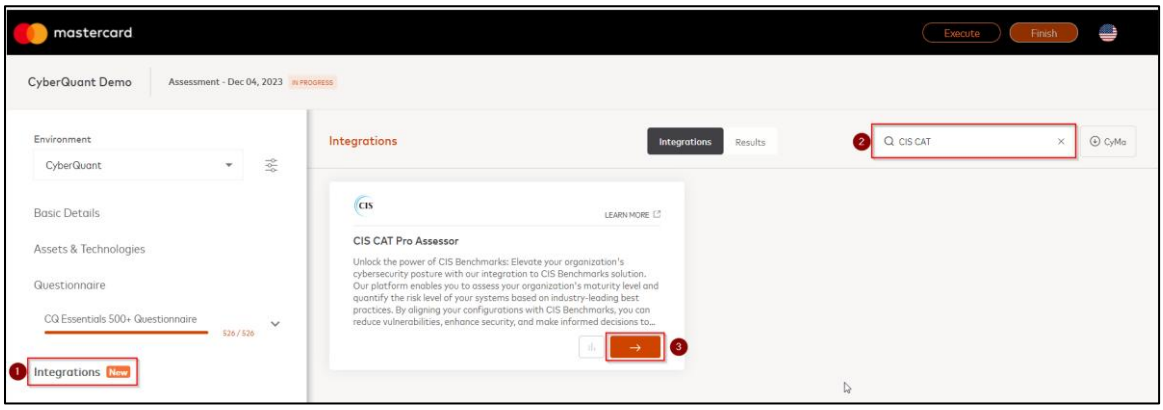
   There are 2 execution options for the CIS-CAT Pro Assessor:

   a. Downloading and executing on multiple target machines - this is best for organizations that have highly segmented and divided responsibility in the management of systems. This option will require multiple extraction sessions to collect all the required evaluations. **(DISCUSS WITH YOUR SYSADMIN)**

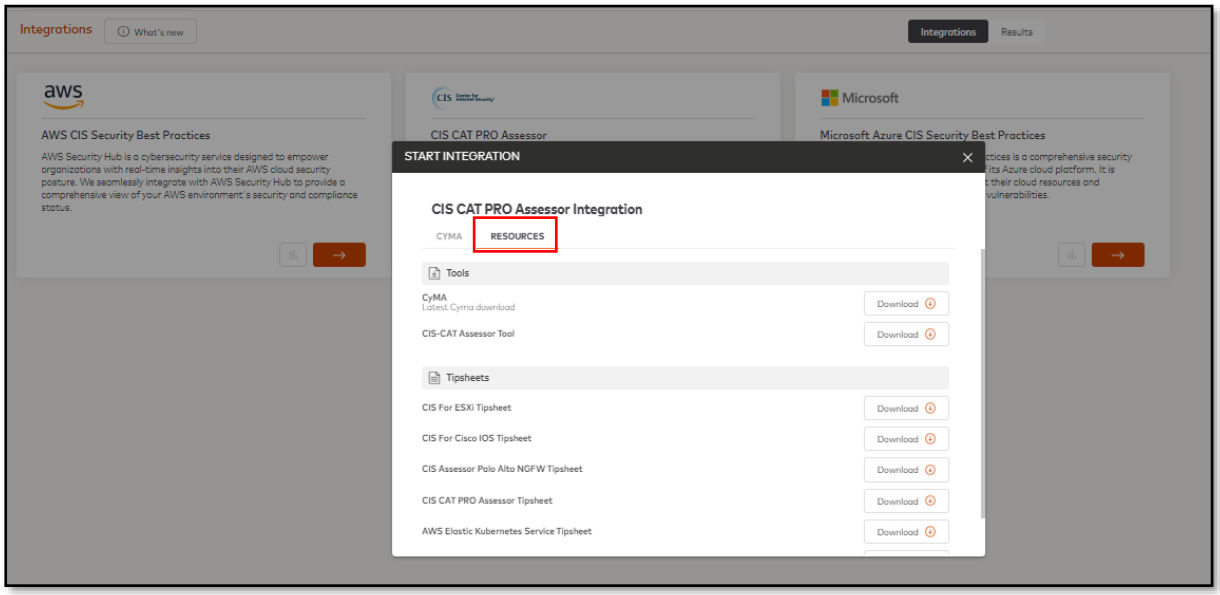
   b. Downloading and executing on a single central machine - the extraction can be run on the local machine and may also be used to connect to additional target systems (based on necessary permissions and access rights) to extract configurations during a

single session, however, the run time for this single session may be longer than option 1.

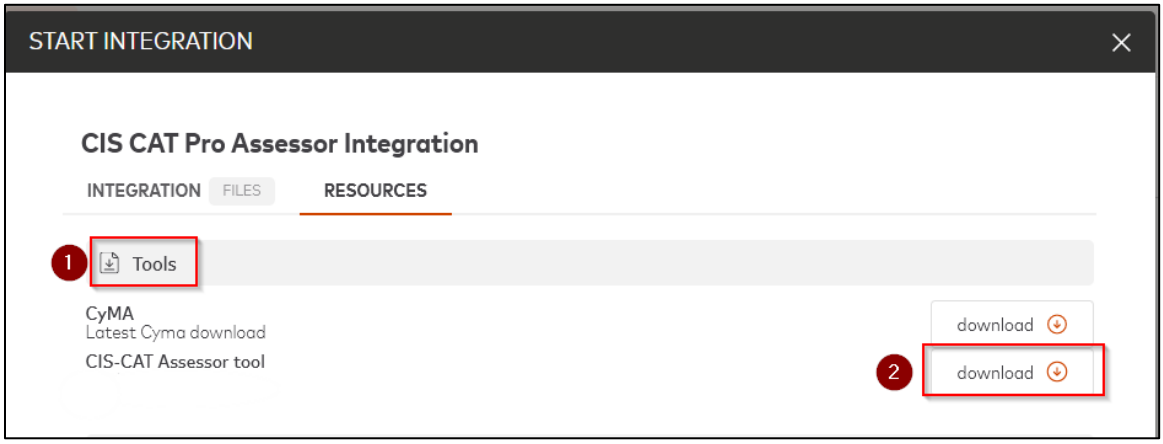
2. Browse to the "**Cyber Quant**" and login to the portal. Open one of the assessments and navigate to the integrations page (1). Search for "CIS CAT" (2) and click on the arrow (3) to open its resources windows.



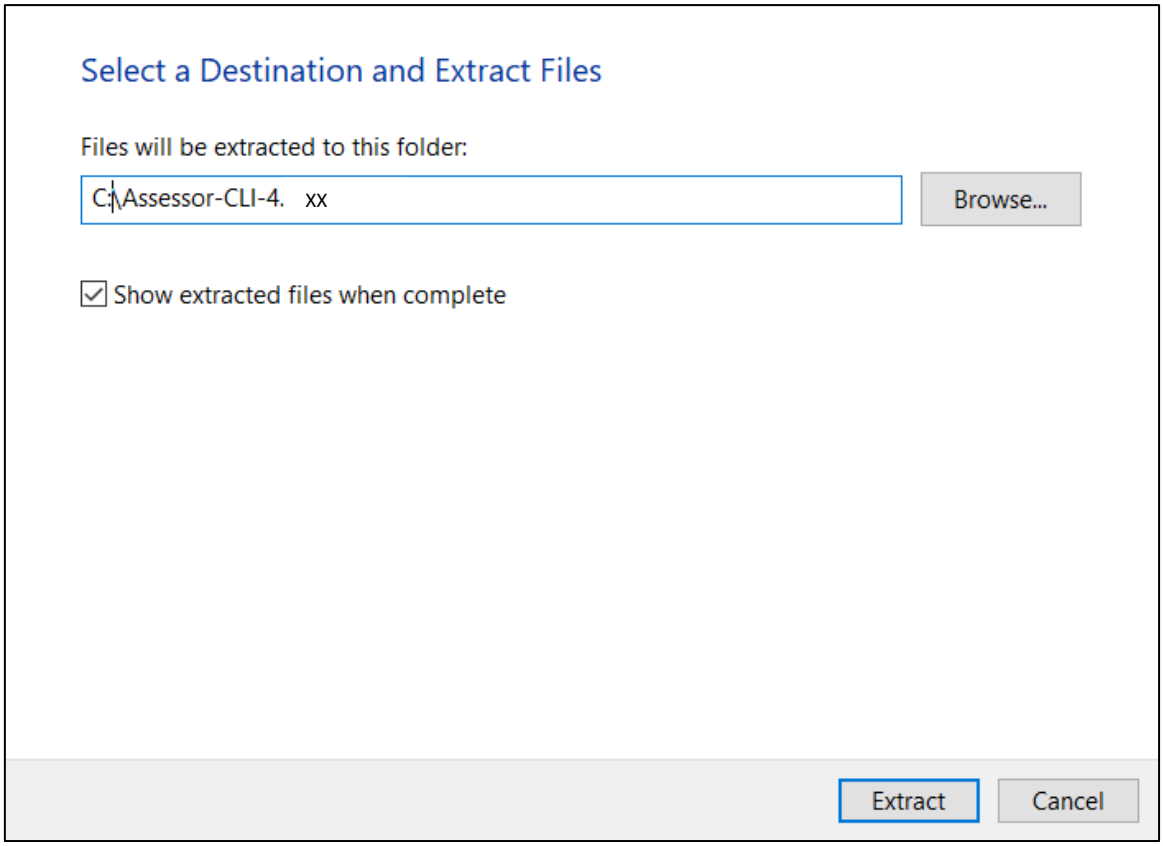
3. Open the "RESOURCES" tab.



4. Under "Tools" (1), press "download" (2) next to the "CIS-CAT Assessor tool".



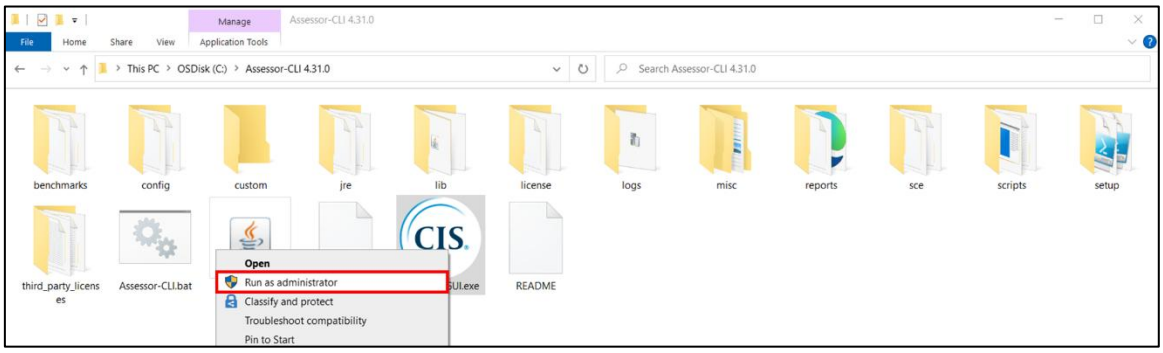
5. Extract the contents of the downloaded zip file to a preferred folder. A recommended location is the C:\ drive.



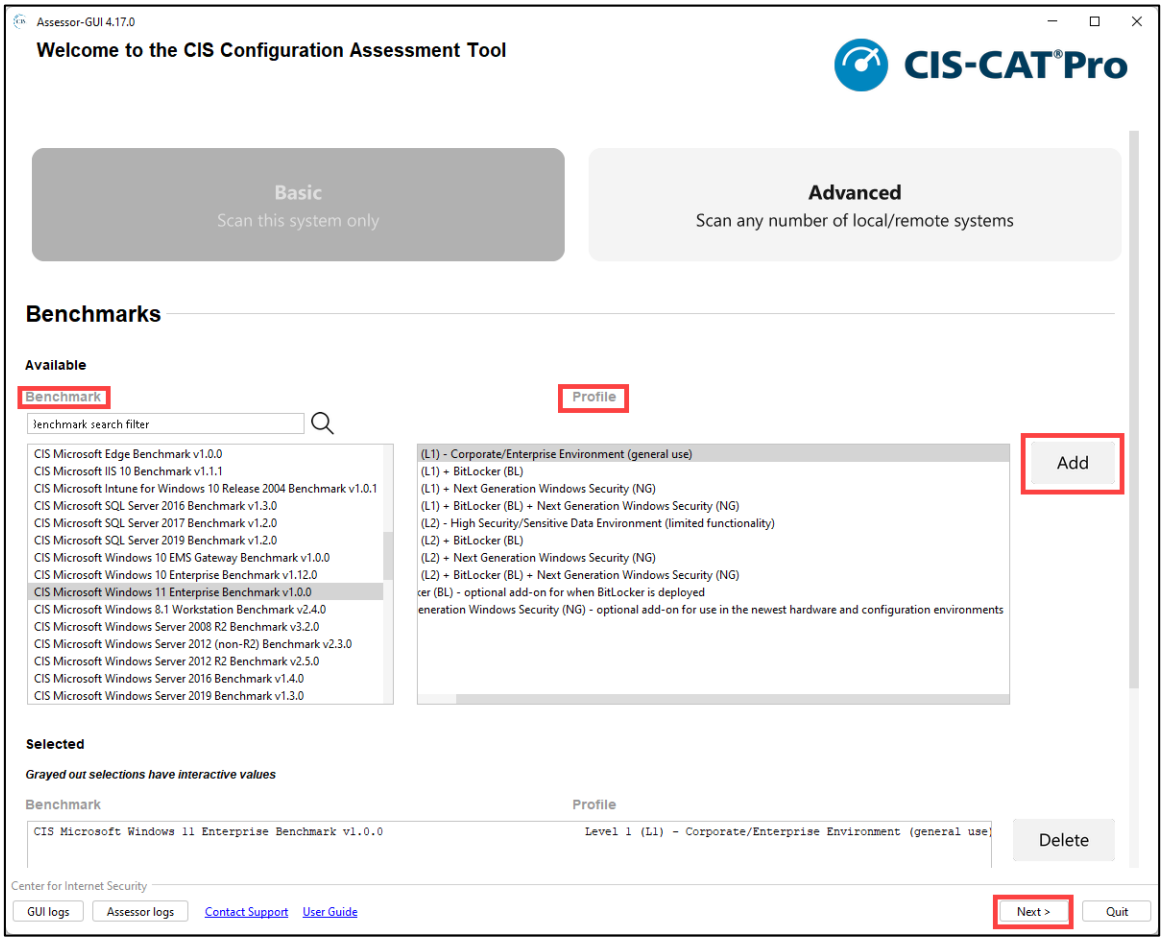
6. For a local scan proceed to section 7 "Local Configuration Scan" and for the remote proceed to section 8 "Remote Configuration Scan".

7. Local Configuration Scan

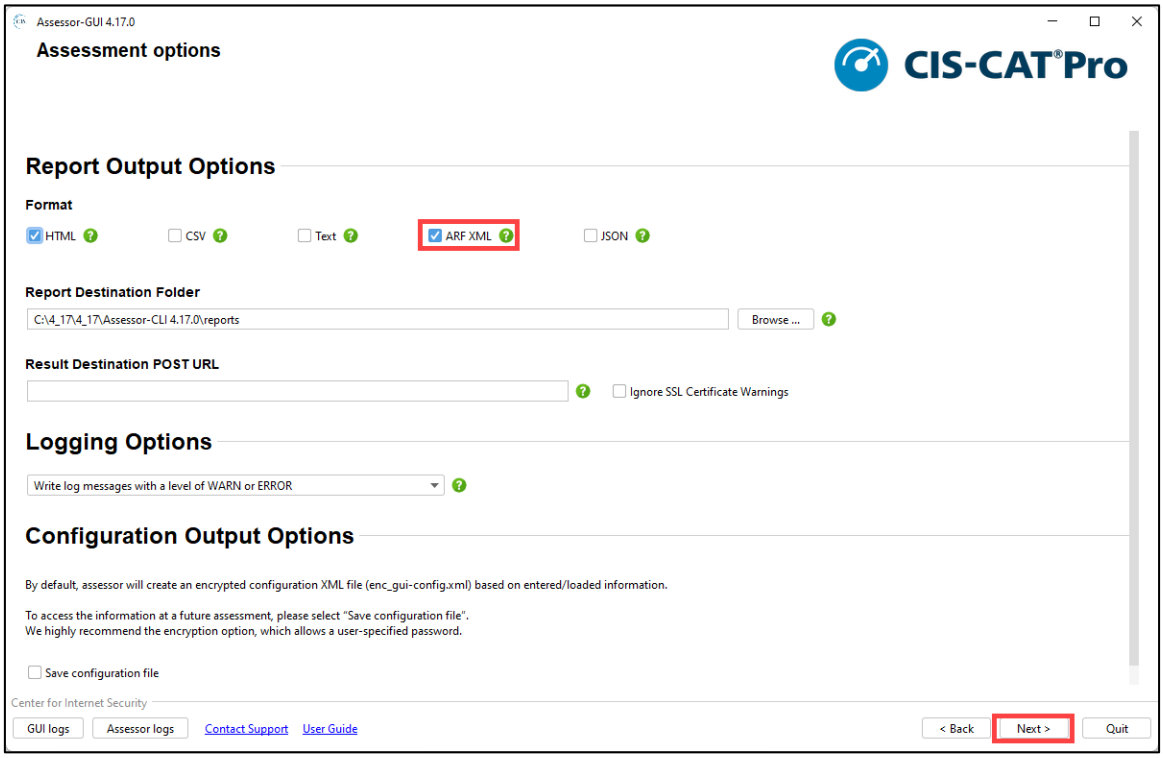
1. Open the "Assessor-CLI 4.xx" folder inside the extracted files and execute "Assessor-GUI.exe" as administrator. Accept the user account control dialog box (proceed normally if it does not appear), it may require administrative credentials.



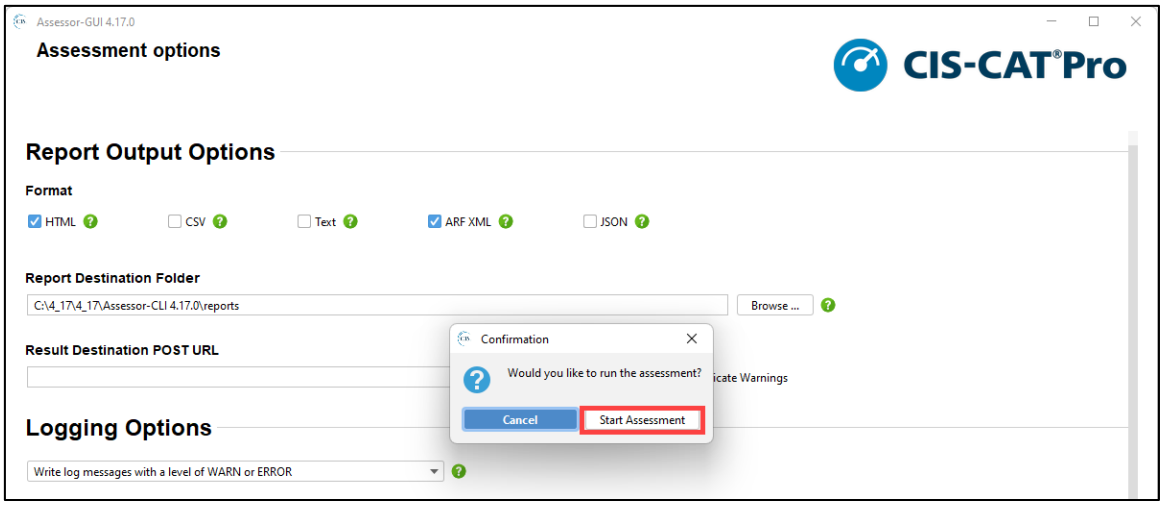
2. Click on "Basic," select the desired "Benchmark" and "Profile," click "Add" and then "Next" (*refer to* ***Appendix B*** *for an overview of the benchmark options*).



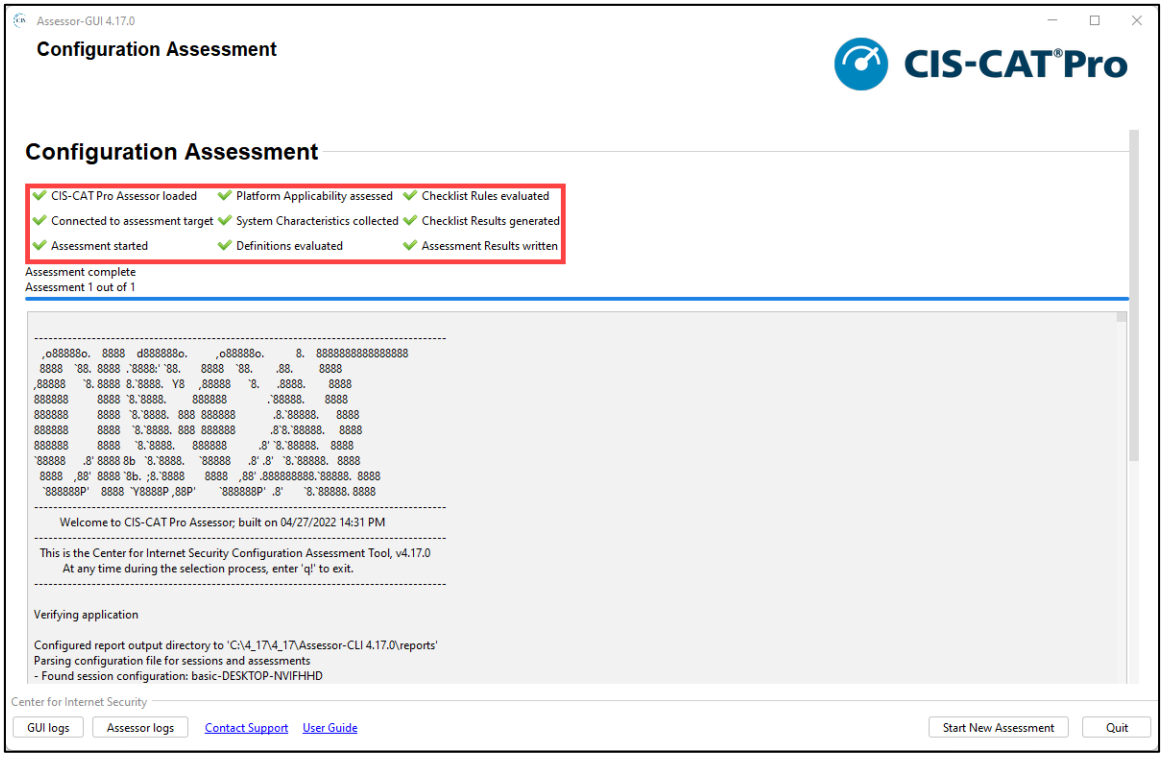
3. Select the "ARF XML" format (this is the only format supported by "CyMA") and the destination to save the report into and click "Next." In addition, an "HTML" format can be also selected to generate a human friendly repot. **It is recommended to store it in the default "C:\Assessor-CLI\reports" to avoid long paths which may cause errors**.



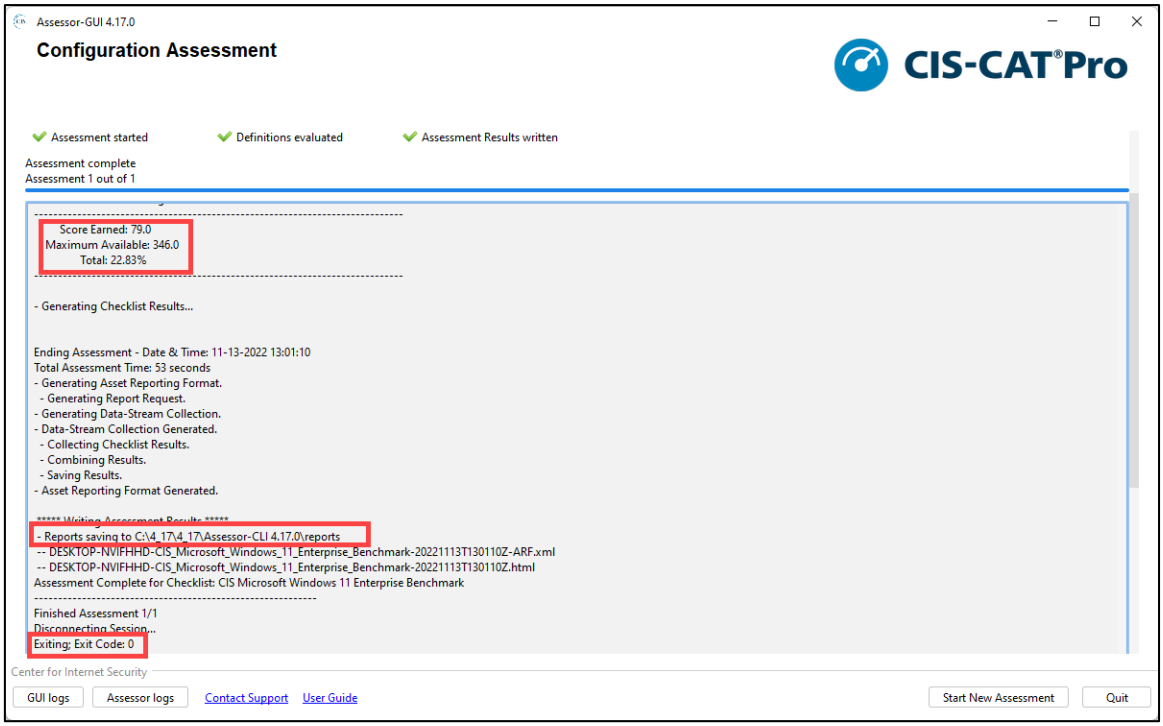
4. Click on "Start Assessment" to execute it.



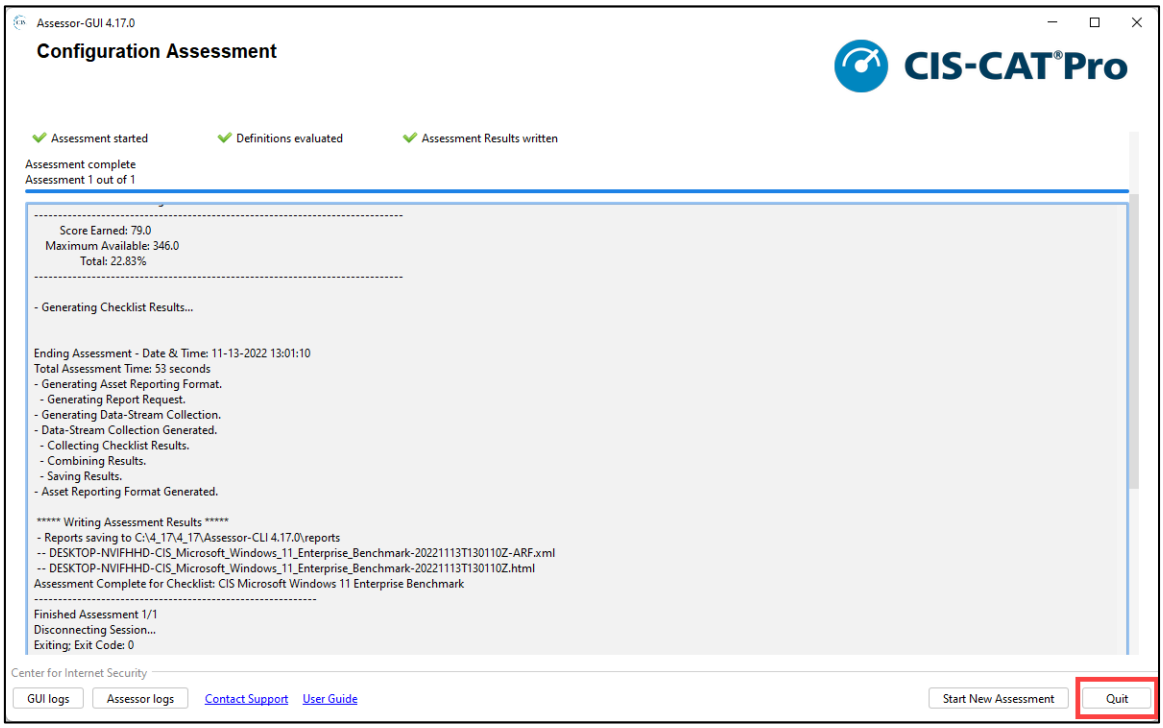
5. The assessment may take several minutes to execute while displaying its progress.



6. Once the assessment finishes, it displays information such as a score, the location of the generated reports and whether it was successful or not. An exit code of 0 indicates a successful execution, while 1 indicates an error (refer to Appendix C for assessment completion error checks and types).

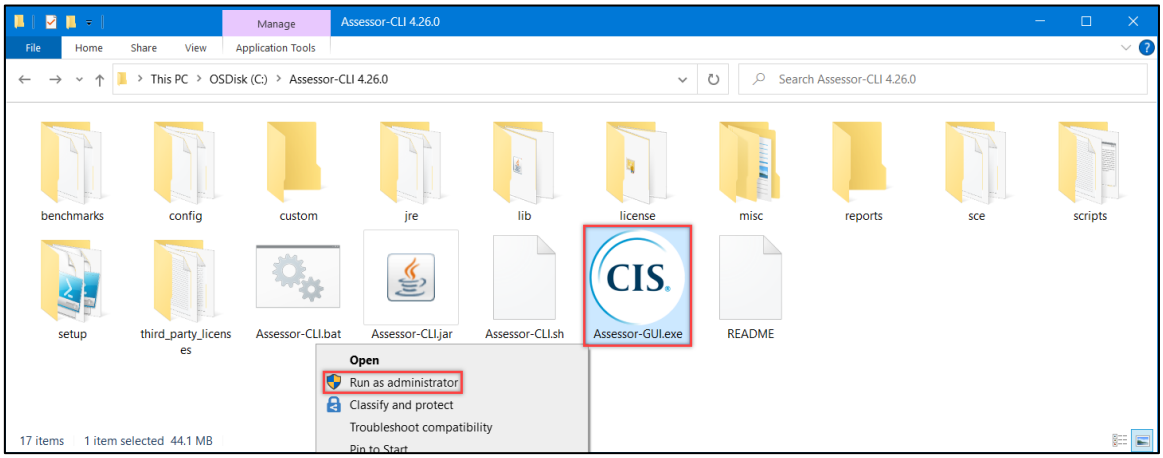


7. Click "Quit" after a successful assessment to close the "CIS-CAT Pro Assessor" tool.

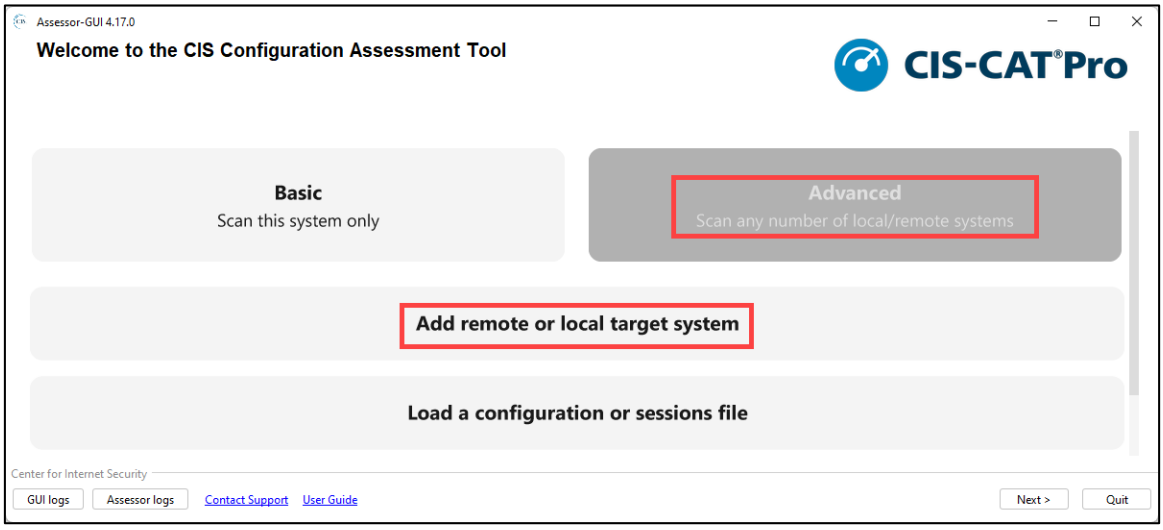


8. Remote Configuration Scan

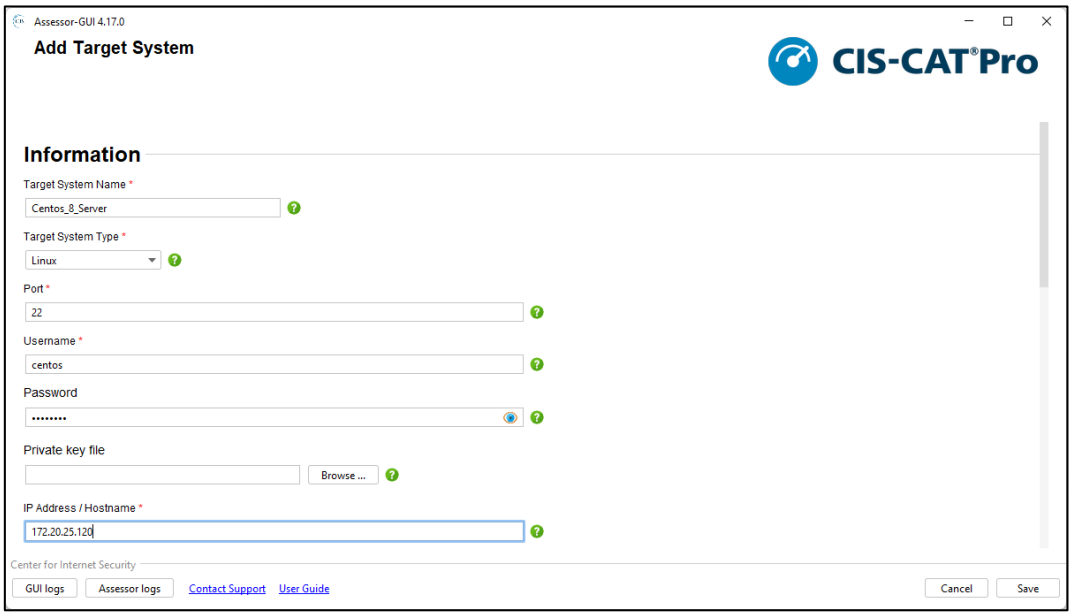
1. Open the "Assessor-CLI 4.xx" folder inside the extracted files and execute "Assessor-GUI.exe" as administrator. Accept the user account control dialog box (proceed normally if it does not appear), it may require administrative credentials.



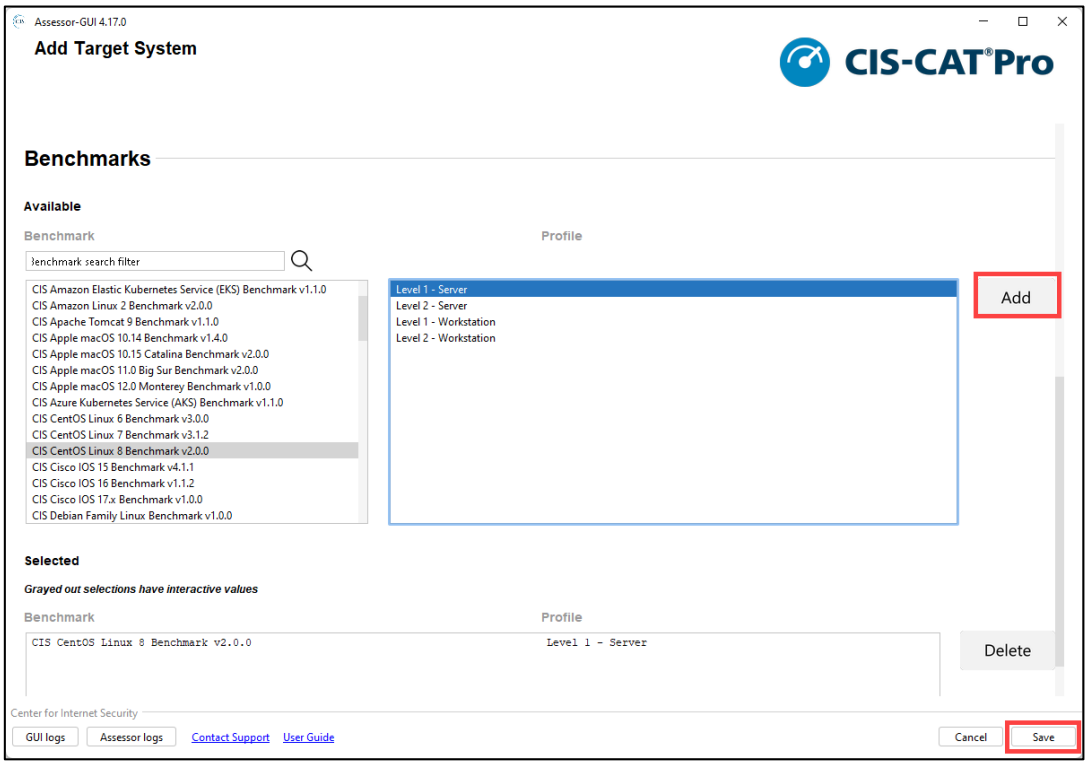
2. Click on "Advanced" and then on "Add remote or local target system." Several target systems can be added at the same time; each will require discrete addresses and credentials to retrieve the benchmarks and profiles.



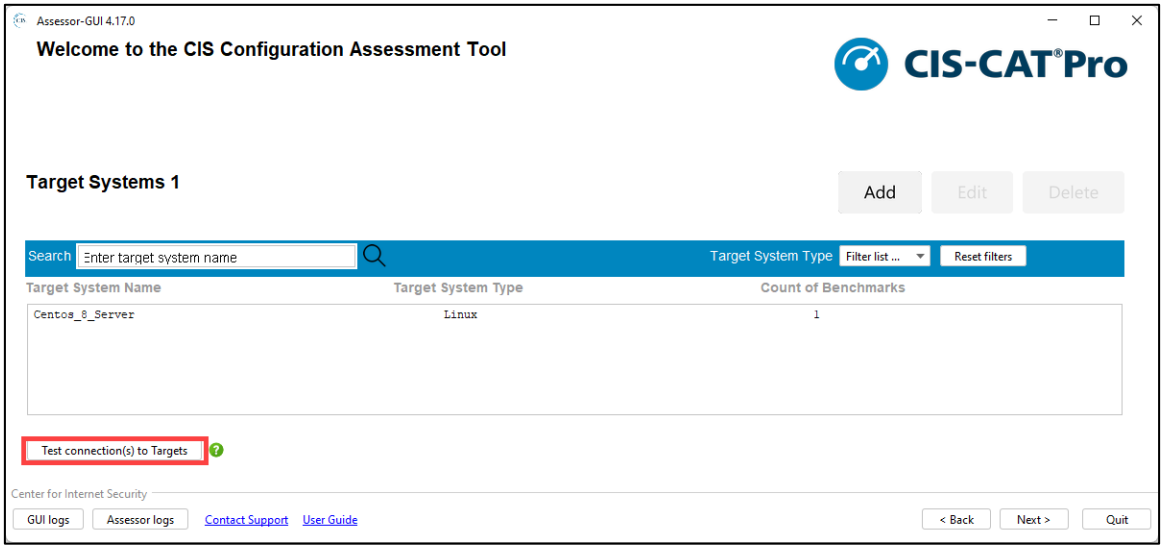
3. Fill in the information required for the remote connection (*for information regarding the fields refer to* ***Appendix D – Connection Fields Overview***).



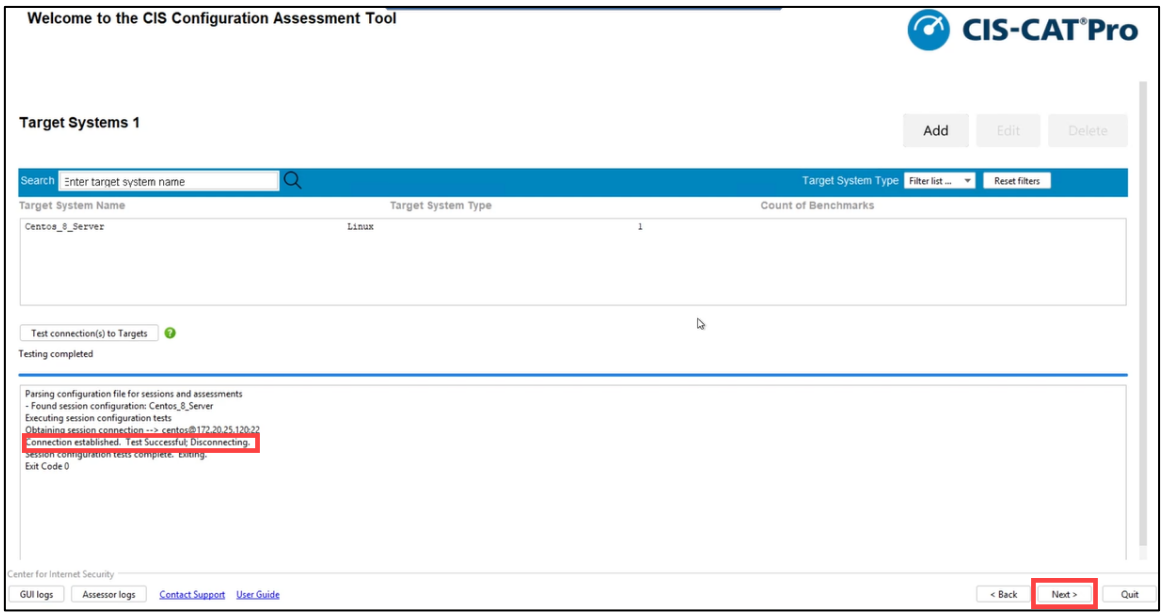
4. Select the desired "Benchmark" and "Profile," click "Add" and then "Save" *(Refer to* ***Appendix B – Connection Fields Overview*** *for an overview of the benchmark options).*



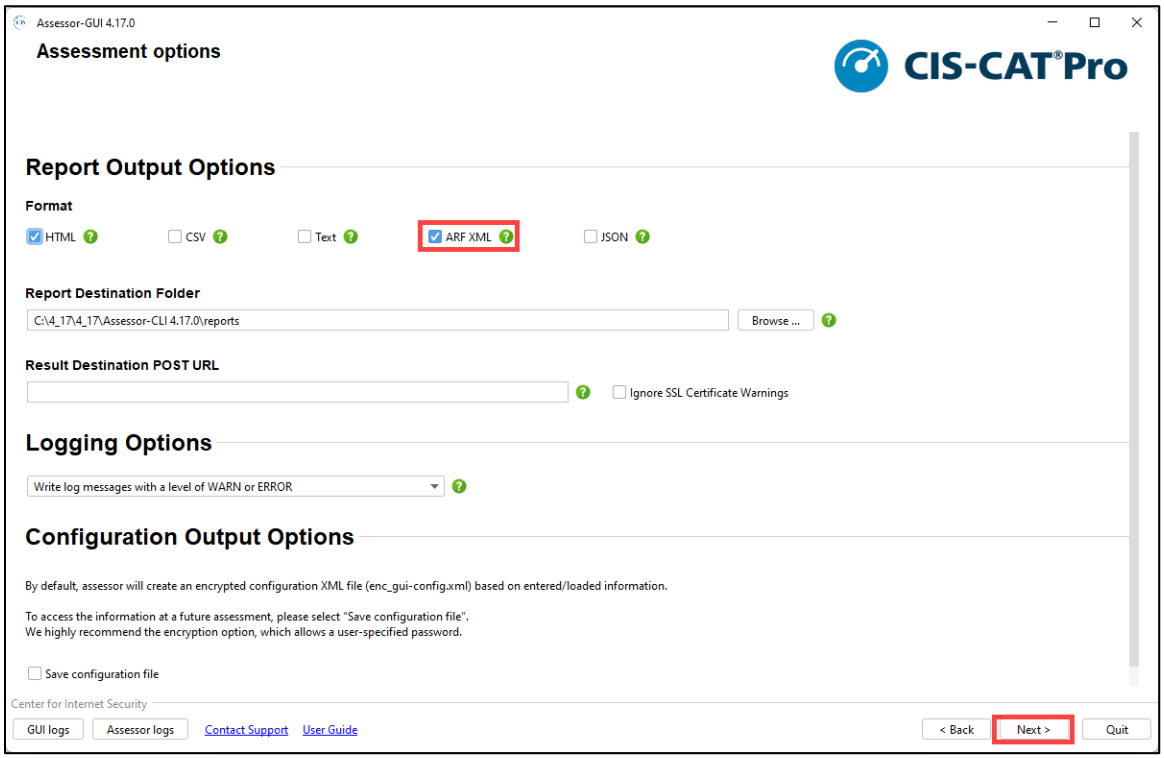
5. Click on "Test connection(s) to Targets" to verity that the information provided in the previous step is correct and the target can be reached.



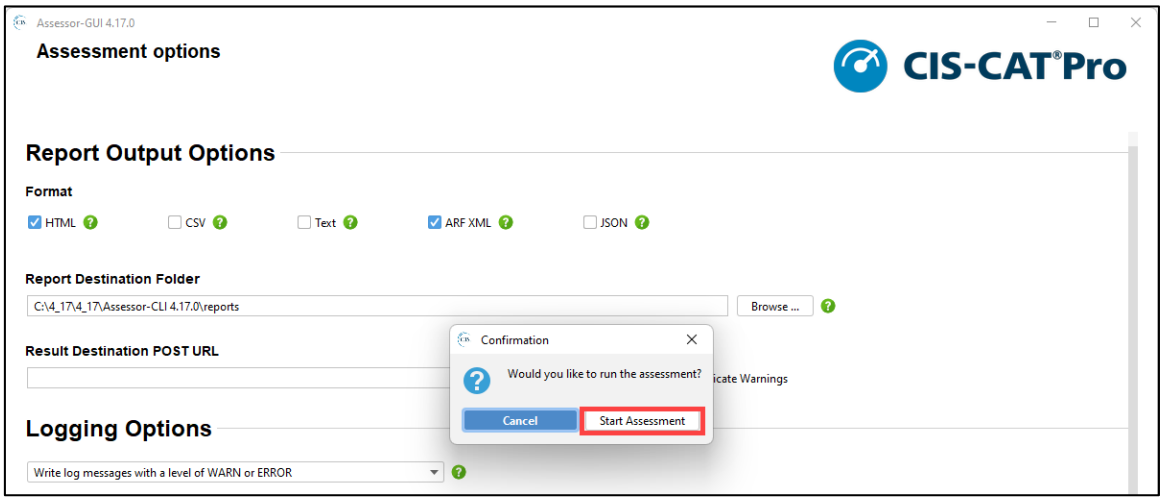
6. If the information filled in for the connection is correct, the test displays a message of "Connection established." Click "Next" to proceed.



7. Select the "ARF XML" format (this is the only format supported by "CyMA") and the destination to save the report into and click "Next." In addition, an "HTML" format can be also selected to generate a human friendly repot. **It is recommended to store it in the default "C:\Assessor-CLI 4.xx\reports" to avoid long paths which may cause errors**.

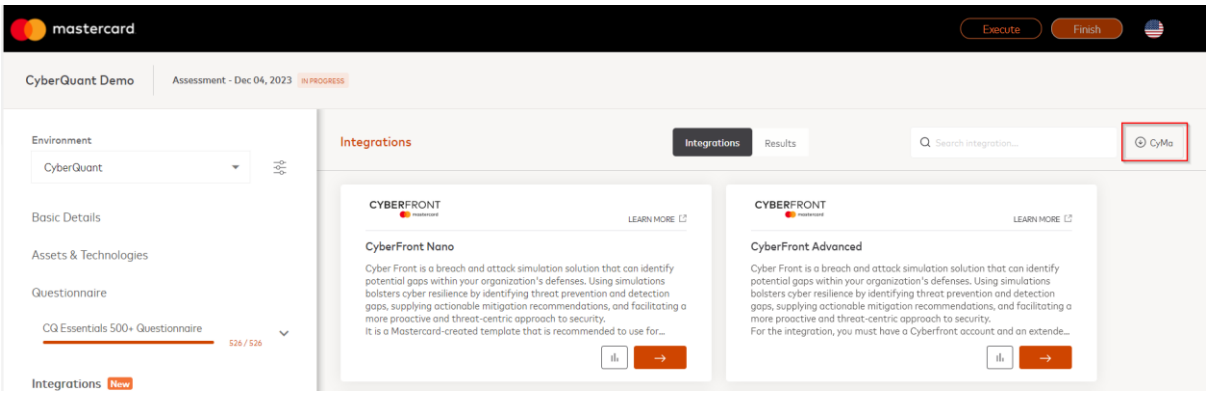


8. Click on "Start Assessment" to execute it. **Once it finished, follow the same steps as displayed in section 7 steps 5-7**.

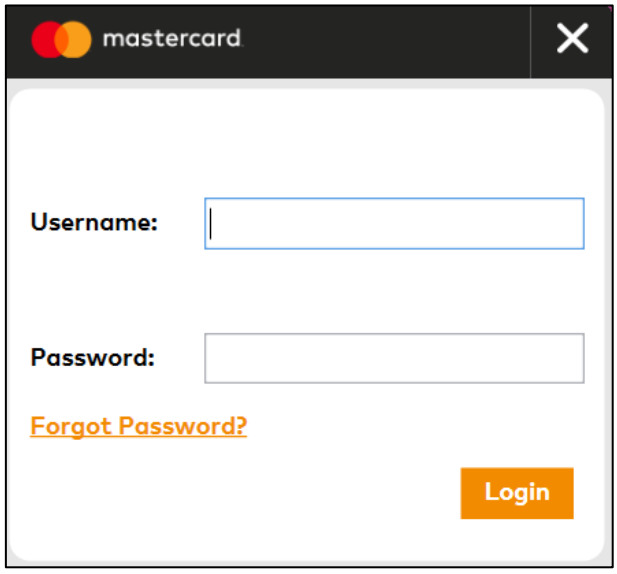


9. Open and Review Integration Results

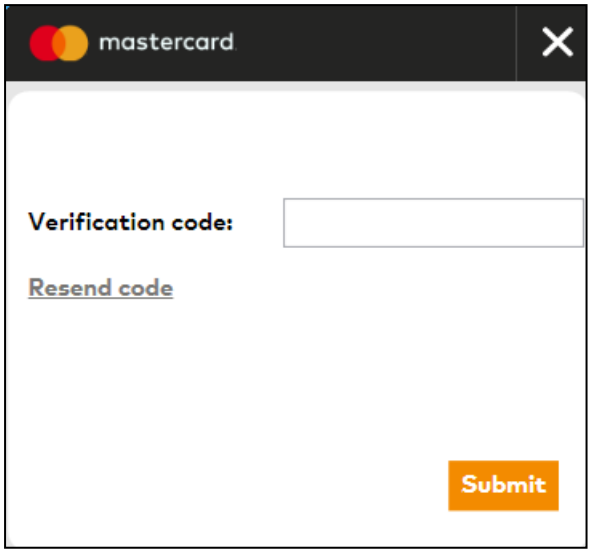
1. CyMA is Available to download from the integration page.



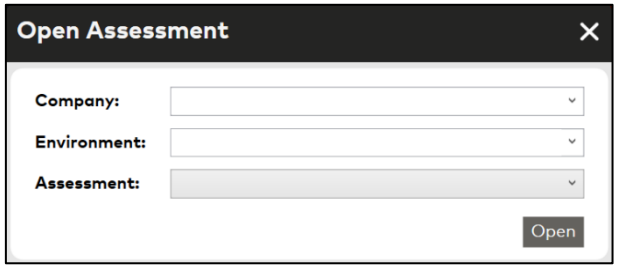
2. After Installation, Execute the "Cyber Quant CyMA" software and log in.



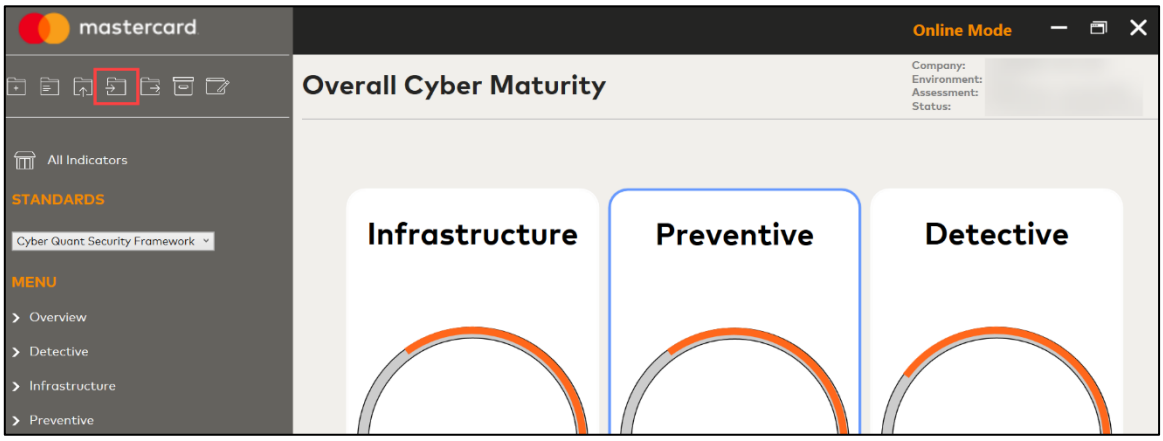
3. Enter the verification code sent to the account's email address.



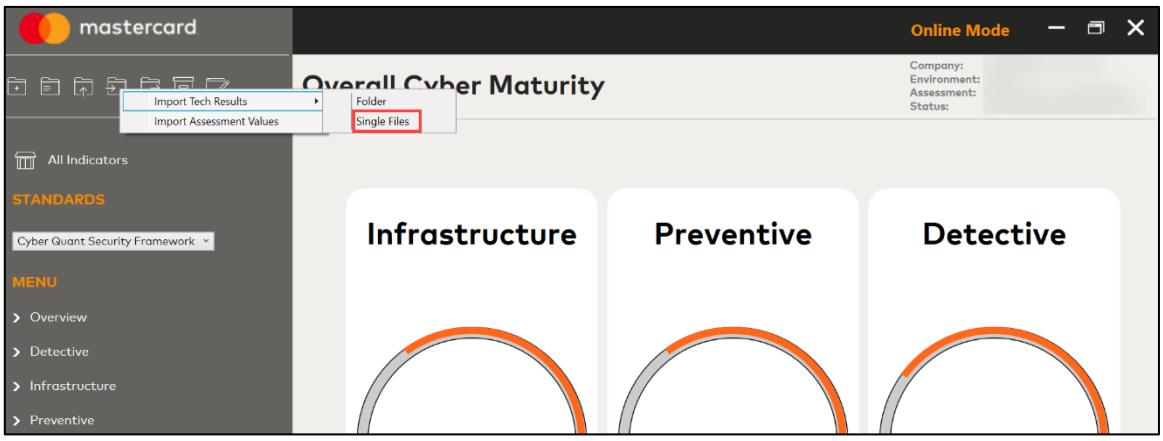
4. Select the desired company, environment, and assessment to import the report.



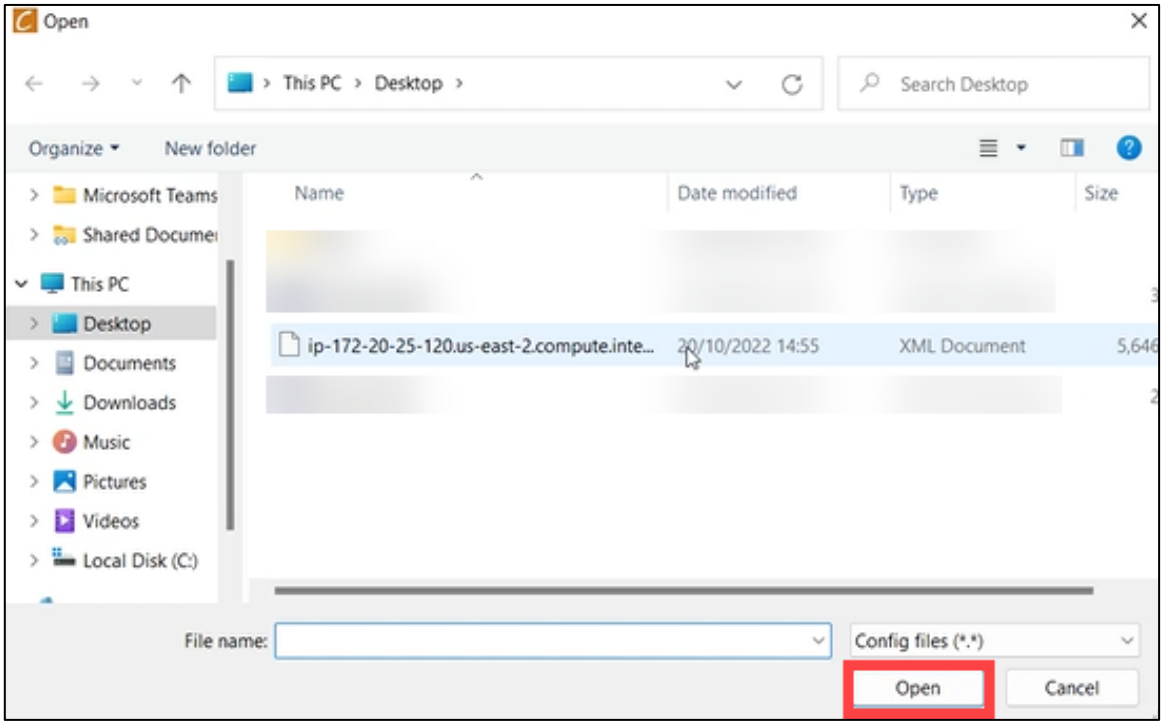
5. Click on the "Import Files" icon on the top left of the screen.



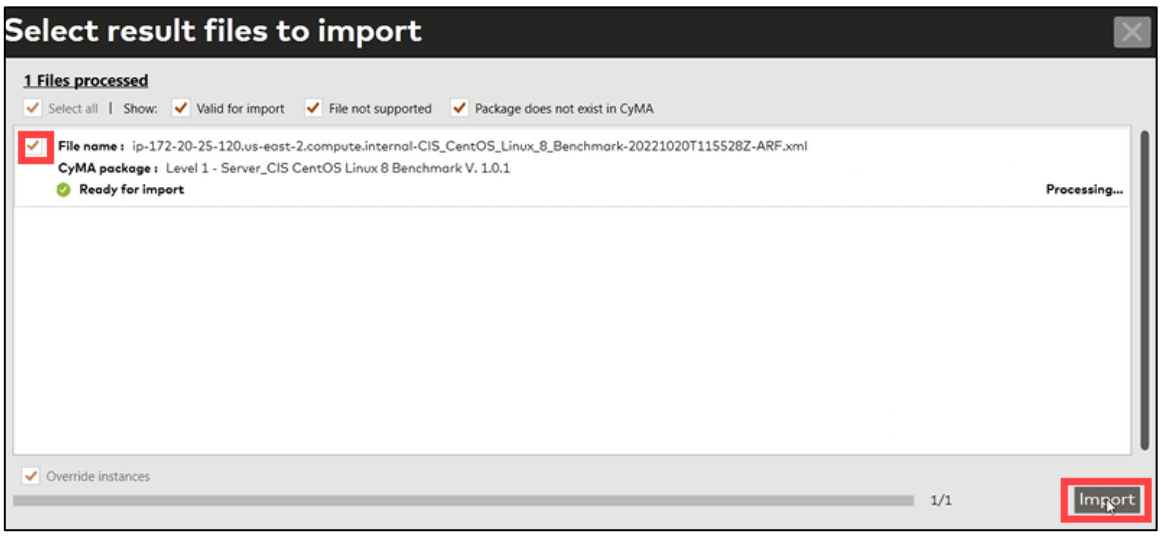
6. Hover over "Import Tech Results" and click "Single File."



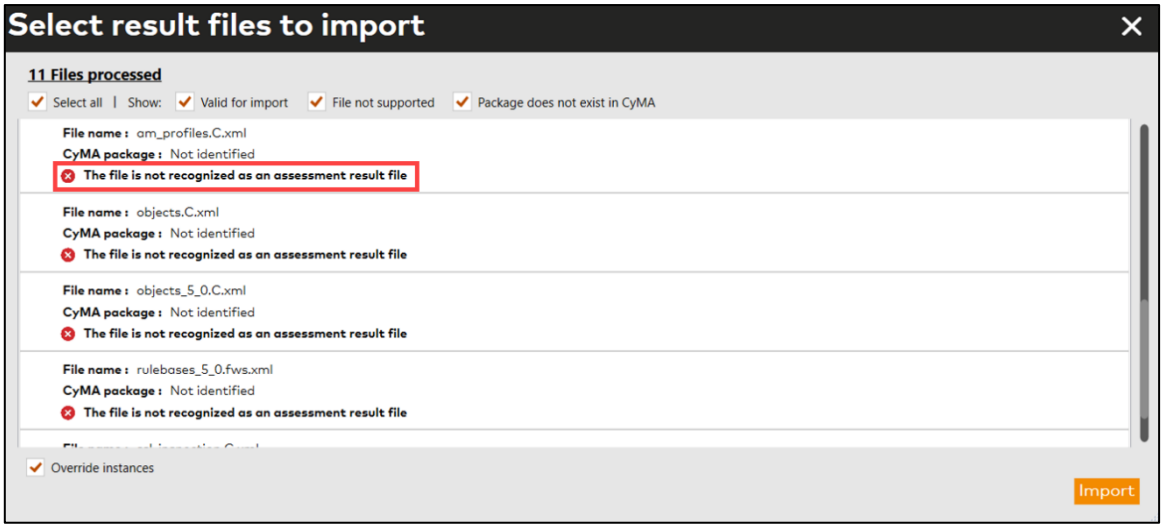
7. Locate the created report and open it.



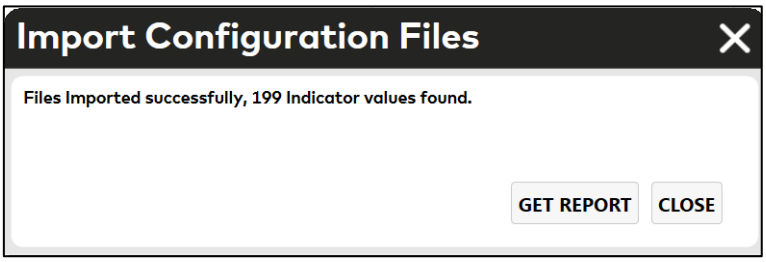
8. Once the report is open, select the file and click "Import." The following screen displays information regarding import errors and packages associated with the imported files.



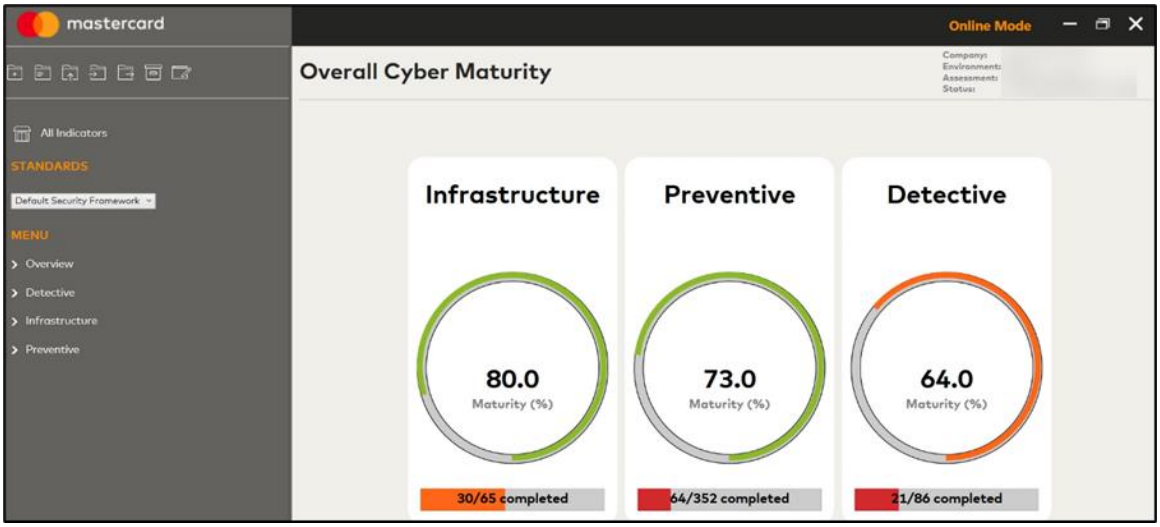
A red mark is displayed below the package in case of an error.



9. Upon successful import, a confirmation notice is displayed, click "CLOSE." **Please note that the number of indicators may vary based on the input configuration files**.



10. The assessment results are now available for review.



Appendix Section

Appendix A - CIS-CAT Pro Assessor Benchmark Overview

Most CIS Benchmarks include multiple configuration profiles.

A Profile describes the configurations assigned to benchmark recommendations. In some of the benchmarks, there are multiple levels to select from:

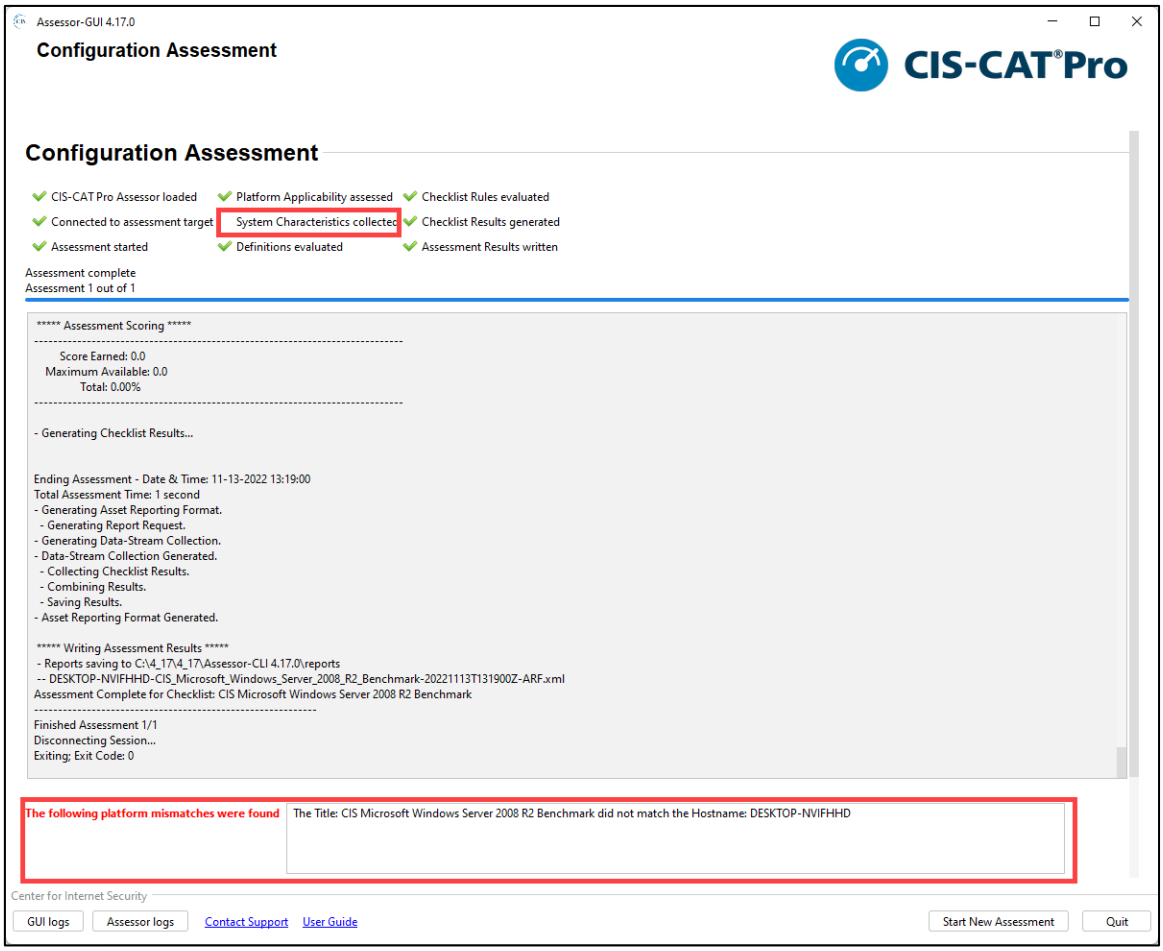
- Level 1 - considered a base recommendation that can be implemented and designed not to have an extensive performance impact.
- Level 2 profile represents a strict security profile applied to the system; it includes all the policies that exist in Level 1. This means selecting the Level 2 profile does not require selecting Level 1 also.

Suppose the assessed system serves multiple roles, such as BitLocker, Next Generation windows Security (NG), Microsoft SQL Server, etc. it is possible to select additional relevant modules to be included in the assessment (For a correct assessment, it is important to choose the right profile).

CIS-CAT Pro Assessor tool allows the selection of as many profiles as needed for the same assessment. The selected benchmarks and profiles are displayed in the SELECTED section and can be edited.

Appendix B - Assessment Completion Error Check and Error Types

After the Extraction process, the tool may display one or more messages as can be seen in the image below. These messages inform that some of the selected benchmarks may not have been found during the search/extraction. These must be resolved otherwise the extract will not be exportable to "CyMA."



If encountered, please check that the selected benchmark profiles match the system's type and version. Further details can be found on the mismatched profile by reviewing the log in the "Configuration Assessment" progress screen. Please ask the IT team to verify that the system parameters are correct. If the issue is not resolved, contact "Cyber Quant" support.

Appendix C – Connection Fields Overview

To perform a remote connection, there are several fields that is necessary to fill in:

1. Target system name – a chosen name that is displayed in the report, it does not have to match the assessed machine's name.
2. Target system type – should match the assessed target system (Windows, Linux, Local, Cisco, Palo Alto).
3. Port - the port must be accepted by the remote system. For Linux or Cisco specify SSH port (default 22), and WinRM for Windows system (default HTTP 5985, HTTPS 5986).
4. Username, Password or Certificate - The specified user should be an administrator or with elevated privilege in the target system. If a certificate is available, it can be used with the secret key passphrase for the private key file.
5. IP address / Hostname – the target machine IP address or DNS name.

Appendix D – CIS-CAT Host System Requirements

- JRE or JDK for command line/centralized assessments.
    - If using just GUI, JRE is embedded so no additional Java needed.
    - Stable version 8 or 11 of JRE or JDK (free OpenJDK also supported) present on host or accessed via network share.
    - Newer Java builds may work in certain environments; however Technical Support will not be able to help with troubleshooting as CIS focuses on implementation of stable, non-proprietary versions.
    - Some users have experienced issues with proprietary Java versions and headless Java versions.
    - 64-bit Java recommended for faster performance
    - Java versions 9+ will receive "WARNING: An illegal reflective access operation has occurred". This can be ignored and will not halt the assessment.
    - OpenJDK (free and open source) implementations are supported. We have found this website easy to navigate. The official source is OpenJDK.
- Remote scanning requires unrestricted access from the CIS-CAT host system to the assessed target system.
- Windows remote and local assessments require a 64-bit operating system.

Recommended Minimum:

Depending on your organization's use of CIS-CAT Pro Assessor, the actual server specifications mentioned below could vary.

- 2 GHz dual processor
- 4 GB of RAM

For more details, refer to CIS website:

https://ciscat-assessor.docs.cisecurity.org/en/latest/User%20Guide%20-%20Assessor/

Appendix E – CIS Implementation Groups

What are the CIS Implementation Groups (IGs)?

IGs are the recommended guidance to prioritize implementation of the CIS Controls. To assist organizations of every size, IGs are divided into three groups: IG1, IG2 and IG3. They are based on the risk profile and resources an organization has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards (previously referred to as CIS Sub-Controls), that they need to implement. There are 153 Safeguards in CIS Controls v8.

Every organization should start with IG1. IG1 provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action if that is warranted. Building upon IG1, we then identified an additional set of Safeguards for organizations with more resources and expertise, but also greater risk exposure. This is IG2. Finally, the rest of the Safeguards make up IG3.

These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

CIS Implementation Groups:

- IG1: Is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise to thwart general, non-targeted attacks. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks. It consists of **56 safeguards**.

- IG2: Assists enterprises in managing the IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity. It consists of **74 safeguards**.

- IG3: Assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks. It consists of **23 additional cyber defense safeguards.**

Appendix F – Cyber Quant Supported Technologies

The following list presents Cyber Quant supported technologies and collection methods:

ID	Technology	Classification
1	APIVoid	Threat Assessment
2	AWS CIS Security Best Practices	Cloud Services
3	AWS Foundational Security Best Practices	Cloud Services
4	AWS Resource Tagging Standard	Cloud Services
5	Check Point R80.20 - R81.x	Firewall
6	CIS AKS Optimized Azure Linux 2 Benchmark v1.1.0	Operating System
7	CIS AKS Optimized Azure Linux 3 Benchmark v1.0.0	Operating System
8	CIS Alibaba Cloud Linux 3 Benchmark v2.0.0	Operating System
9	CIS AlmaLinux OS 10 Benchmark v1.0.0	Operating System
10	CIS AlmaLinux OS 8 Benchmark v4.0.0	Operating System
11	CIS AlmaLinux OS 9 Benchmark v2.0.0	Operating System
12	CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.8.0	Kubernetes
13	CIS Amazon Linux 2023 Benchmark v1.0.0	Operating System
14	CIS Amazon Linux 2 Benchmark v3.0.0	Operating System
15	CIS Amazon Linux 2 STIG Benchmark v2.0.0	Operating System
16	CIS Apache HTTP Server 2.4 Benchmark v2.3.0	Web Server
17	CIS Apache Tomcat 10.1 Benchmark v1.1.0	Web Server
18	CIS Apache Tomcat 11 Benchmark v1.0.0	Web Server
19	CIS Apache Tomcat 9 Benchmark v1.2.0	Web Server
20	CIS Apple macOS 12.0 Monterey Benchmark v4.0.0	Operating System
21	CIS Apple macOS 12.0 Monterey Cloud-tailored Benchmark v1.1.0	Operating System
22	CIS Apple macOS 13.0 Ventura Benchmark v4.0.0	Operating System
23	CIS Apple macOS 13.0 Ventura Cloud-tailored Benchmark v1.1.0	Operating System
24	CIS Apple macOS 14.0 Sonoma Benchmark v3.0.0	Operating System
25	CIS Apple macOS 14.0 Sonoma Cloud-tailored Benchmark v1.1.0	Operating System
26	CIS Apple macOS 15.0 Sequoia Benchmark v2.0.0	Operating System
27	CIS Apple macOS 15.0 Sequoia Cloud-tailored Benchmark v1.0.0	Operating System
28	CIS Apple macOS 26 Tahoe Benchmark v1.0.0	Operating System
29	CIS Azure Compute Microsoft Windows Server 2019 Benchmark v1.0.1	Operating System
30	CIS Azure Compute Microsoft Windows Server 2022 Benchmark v1.0.0	Operating System
31	CIS Azure Kubernetes Service (AKS) Benchmark v1.8.0	Kubernetes
32	CIS Cisco IOS XE 16.x Benchmark v2.2.0	Network Devices OS

33	CIS Cisco IOS XE 17.x Benchmark v2.2.1	Network Devices OS
34	CIS Cisco IOS XR 7.x v1.0.1	Network Devices OS
35	CIS Cisco NX-OS Benchmark v1.2.0	Network Devices OS
36	CIS Controls Assessment Module Windows 10 v1.0.3	Operating System
37	CIS Controls Assessment Module Windows Server v1.0.0	Operating System
38	CIS Debian Linux 11 Benchmark v2.0.0	Operating System
39	CIS Debian Linux 11 STIG Benchmark v1.0.0	Operating System
40	CIS Debian Linux 12 Benchmark v1.1.0	Operating System
41	CIS Debian Linux 13 Benchmark v1.0.0	Operating System
42	CIS Docker Benchmark v1.8.0	Containers
43	CIS ExtremeNetworks-SLX-OS-20.X.X Benchmark v1.0.1	Network Devices OS
44	CIS FortiGate 7.4.x Benchmark v1.0.1	Network Devices OS
45	CIS Google Chrome Group Policy Benchmark v1.0.0	Web Browser
46	CIS Google Kubernetes Engine (GKE) Autopilot Benchmark v1.3.0	Kubernetes
47	CIS Google Kubernetes Engine (GKE) Benchmark v1.9.0	Kubernetes
48	CIS HPE Aruba Networking CX Switch Benchmark v1.0.1	Network Devices OS
49	CIS Kubernetes Benchmark v1.12	Kubernetes
50	CIS Kubernetes V1.20 Benchmark v1.0.1	Kubernetes
51	CIS Kubernetes V1.23 Benchmark v1.0.1	Kubernetes
52	CIS Linux Mint 22 Benchmark v1.0.0	Operating System
53	CIS Microsoft 365 Foundations Benchmark v6.0.1	Cloud Services
54	CIS Microsoft Defender Antivirus Benchmark v1.0.0	Application
55	CIS Microsoft Edge Benchmark v4.0.0	Web Browser
56	CIS Microsoft IIS 10 Benchmark v1.2.1	Web Server
57	CIS Microsoft Intune for Edge Benchmark v1.0.0	Cloud Services
58	CIS Microsoft Intune for Office Benchmark v1.1.0	Cloud Services
59	CIS Microsoft Intune for Windows 10 Benchmark v4.0.0	Cloud Services
60	CIS Microsoft Intune for Windows 11 Benchmark v4.0.0	Cloud Services
61	CIS Microsoft Office Enterprise Benchmark v1.2.0	Application
62	CIS Microsoft SQL Server 2019 Benchmark v1.5.2	Databases
63	CIS Microsoft SQL Server 2022 Benchmark v1.2.1	Databases
64	CIS Microsoft Windows 10 EMS Gateway Benchmark v3.0.0	Operating System
65	CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0	Operating System
66	CIS Microsoft Windows 10 Stand-alone Benchmark v4.0.0	Operating System
67	CIS Microsoft Windows 11 Enterprise Benchmark v5.0.0	Operating System

68	CIS Microsoft Windows 11 Stand-alone Benchmark v4.0.0	Operating System
69	CIS Microsoft Windows Server 2016 Benchmark v4.0.0	Operating System
70	CIS Microsoft Windows Server 2019 Benchmark v4.0.0	Operating System
71	CIS Microsoft Windows Server 2019 Stand-alone v3.0.0	Operating System
72	CIS Microsoft Windows Server 2022 Benchmark v4.0.0	Operating System
73	CIS Microsoft Windows Server 2022 Stand-alone Benchmark v1.0.0	Operating System
74	CIS Microsoft Windows Server 2025 Benchmark v1.0.0	Operating System
75	CIS Microsoft Windows Server 2025 Stand-alone v1.0.0	Operating System
76	CIS MongoDB 6 Benchmark v1.2.0	Databases
77	CIS MongoDB 7 Benchmark v1.2.0	Databases
78	CIS MongoDB 8 Benchmark v1.0.0	Databases
79	CIS Mozilla Firefox ESR GPO Benchmark v1.0.0	Web Browser
80	CIS NGINX Benchmark v2.1.0	Web Server
81	CIS Oracle Cloud Infrastructure Container Engine for Kubernetes(OKE) Benchmark v1.8.0	Kubernetes
82	CIS Oracle Database 19c Benchmark v2.0.0	Databases
83	CIS Oracle Database 23ai Benchmark v1.1.0	Databases
84	CIS Oracle Linux 10 Benchmark v1.0.0	Operating System
85	CIS Oracle Linux 8 Benchmark v4.0.0	Operating System
86	CIS Oracle Linux 9 Benchmark v2.0.0	Operating System
87	CIS Oracle MySQL Community Server 8.0 Benchmark v1.2.0	Databases
88	CIS Oracle MySQL Community Server 8.4 Benchmark v1.1.0	Databases
89	CIS Oracle MySQL Enterprise Edition 8.0 Benchmark v1.5.0	Databases
90	CIS Oracle MySQL Enterprise Edition 8.4 Benchmark v1.1.0	Databases
91	CIS Palo Alto Firewall 10 Benchmark v1.3.0	Firewall
92	CIS Palo Alto Firewall 11 Benchmark v1.1.0	Firewall
93	CIS PostgreSQL 13 Benchmark v1.3.0	Databases
94	CIS PostgreSQL 14 Benchmark v1.3.0	Databases
95	CIS PostgreSQL 15 Benchmark v1.2.0	Databases
96	CIS PostgreSQL 16 Benchmark v1.1.0	Databases
97	CIS PostgreSQL 17 Benchmark v1.0.0	Databases
98	CIS Red Hat Enterprise Linux 10 Benchmark v1.0.1	Operating System
99	CIS Red Hat Enterprise Linux 8 Benchmark v4.0.0	Operating System
100	CIS Red Hat Enterprise Linux 8 STIG Benchmark v2.0.0	Operating System
101	CIS Red Hat Enterprise Linux 9 Benchmark v2.0.0	Operating System
102	CIS Red Hat OpenShift Container Platform Benchmark v1.9.0	Kubernetes
103	CIS Rocky Linux 10 Benchmark v1.0.0	Operating System
104	CIS Rocky Linux 8 Benchmark v3.0.0	Operating System

105	CIS Rocky Linux 9 Benchmark v2.0.0	Operating System
106	CIS SUSE Linux Enterprise 12 Benchmark v3.2.1	Operating System
107	CIS SUSE Linux Enterprise 15 Benchmark v2.0.1	Operating System
108	CIS Ubuntu Linux 20.04 LTS Benchmark v3.0.0	Operating System
109	CIS Ubuntu Linux 20.04 LTS STIG Benchmark v2.0.0	Operating System
110	CIS Ubuntu Linux 22.04 LTS Benchmark v3.0.0	Operating System
111	CIS Ubuntu Linux 22.04 LTS STIG Benchmark v1.0.0	Operating System
112	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0	Operating System
113	CIS Ubuntu Linux 24.04 LTS STIG Benchmark v1.0.0	Operating System
114	CIS Visual Studio Code GPO Benchmark v1.0.0	Application
115	CIS VMware ESXi 6.7 Benchmark v1.4.0	Virtualization / Hypervisor
116	CIS VMware ESXi 7.0 Benchmark v1.5.0	Virtualization / Hypervisor
117	CIS VMware ESXi 8.0 Benchmark v1.2.0	Virtualization / Hypervisor
118	CrowdStrike Exposure Management Vulnerabilities	Crowdstrike Vulnerabilities Integration
119	Crowdstrike ZTA	Extended detection and response (XDR)
120	Cyber Front	Breach and Attack Simulation
121	Fortigate 6.2.x-7.2	Firewall
122	Google Cloud Platform	Cloud Services
123	McAfee ePo Endpoint Security 5.10	Endpoint Antimalware
124	Microsoft 365 Defender	Cloud Services
125	Microsoft Azure Defender for Cloud - Recommendations	Cloud Services
126	Microsoft Azure Defender for Cloud - Regulatory Compliance	Cloud Services
127	Microsoft Cloud Security Benchmark	Cloud Services
128	Microsoft Exchange 2013 - 2016	Mail Services
129	Microsoft Office 365	Cloud Services
130	MX Toolbox	Threat Assessment
131	Okta	Authentication & Authorization Services
132	Picus	Breach and Attack Simulation
133	Qualys VMDR Vulnerability Management, Detection, and Response	Vulnerability Scan
134	Qualys SCA Security Configuration Asssessment	Secure Configuration & Compliance
135	Qualys WAS	Web Application Vulnerability Scan
136	RiskRecon	Third Party Risk Monitoring
137	Symantec Endpoint Protection 12.1.X-14.2.X	Endpoint Antimalware
138	Tenable IO	Vulnerability Management & Security Configuration & Compliance
139	Tenable Nessus	Vulnerability Management & Security Configuration & Compliance
140	WhatIsMyBrowser	Threat Assessment

Appendix G – CIS-Assessor User Guide Links

Guide	External Link
CIS-CAT Pro Assessor v4 configuration guide	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#cis-cat-pro-assessor-configuration-guide
CIS-CAT Pro Assessor v4 benchmark coverage	https://ciscat-assessor.docs.cisecurity.org/en/latest/Coverage%20Guide/#cis-cat-pro-assessor-coverage-guide
CIS-CAT Pro Assessor v4 GUI	https://ciscat-assessor.docs.cisecurity.org/en/latest/User%20Guide%20-%20Assessor/#graphical-user-interface-gui
About the HTML Report	https://ciscat-assessor.docs.cisecurity.org/en/latest/User%20Guide%20-%20Assessor/#report-about-the-html-report
CIS-CAT Pro Assessor v4 results legend	https://ciscat-assessor.docs.cisecurity.org/en/latest/User%20Guide%20-%20Assessor/#console-assessment-results
Remote export Microsoft Windows configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#remote-setup-microsoft-windows
Remote export Unix /Linux / MACOS configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#remote-setup-unixlinuxosx
Remote export from Cisco Network Devices configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#remotelocal-setup-cisco-network-device
Databases assessment configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#database-assessment
Kubernetes Assessment	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#kubernetes-assessment
Apache Tomcat Assessment configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#apache-tomcat-9-assessment
VMware ESXi Assessment configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#vmware-esxi-assessment
Red Hat OpenShift Container Platform Assessment configuration	https://ciscat-assessor.docs.cisecurity.org/en/latest/Configuration%20Guide/#red-hat-openshift-container-platform-assessment