CSAEC

CyberScan — Cyber Server Audit Engine Core

CyberScan User Guide

A practical guide to your Windows security assessment

Version 1.0 | August 2026
Microsoft Windows 10 or later | 64-bit

Document information

Field	Value
Document title	CyberScan User Guide
Product	CyberScan - Cyber Server Audit Engine Core
Organisation	CSAEC
Version	1.0
Publication date	August 2026
Document code	CS-UG-EN-1.0
Language	English
Intended audience	Business users, independent professionals, small-business owners, office personnel, and first-level IT personnel
Classification	Public distribution

Table of contents

This contents list follows the document section order. Page numbers are provided in the footer for navigation.

1. Introduction

CyberScan - Cyber Server Audit Engine Core provides an understandable overview of security settings and exposure on a Windows workstation. It runs twelve structured checks, shows an overall score, and explains what deserves attention.

> Important
> CyberScan is a preliminary assessment and decision-support application. It does not replace antivirus software, professional testing, continuous monitoring, or qualified cybersecurity advice.

2. What CyberScan does

- Runs twelve local security checks.
- Shows a score from 0 to 100 and a classification.
- Explains individual findings and suggests general next actions.
- Offers local AI-assisted guidance without requiring a cloud AI subscription.
- Lets you decide whether to prepare and share a report with CSAEC.

3. Intended users

CyberScan is suitable for small and medium-sized businesses, independent professionals, IT administrators, cybersecurity consultants, organisations preparing cyber-risk questionnaires, and anyone seeking an initial Windows security posture overview.

4. System requirements

Area	Requirement
Operating system	Microsoft Windows 10 or later, 64-bit edition
Environment	A standard Windows desktop environment
Storage	Sufficient local storage for the application, security components, and local AI model
Permissions	Suitable user permissions for system and network security checks
Hardware note	Detailed hardware requirements may vary according to the selected application build and local AI configuration.

5. Installing CyberScan

Installation steps may vary by the authorised distribution package.

General installation procedure

- Obtain CyberScan from the authorised CSAEC distribution source.
- Confirm that the package is intended for 64-bit Windows 10 or later.
- Close unnecessary applications and follow the instructions supplied with the package.
- Approve only prompts that you understand and that identify the expected publisher or source.
- Start CyberScan after installation completes.

> Warning
> Do not disable security controls or bypass organisational policy to complete installation. Ask your IT administrator if a prompt, source, or permission request is unexpected.

6. Starting the application

Open CyberScan from the installed application entry or authorised package location. Some checks need suitable permissions. If a result is unavailable, do not assume that the control is healthy; review the message and contact IT support if needed.

7. Understanding the main interface

Area	What it shows
Overall score	A 0-100 summary and the current classification.
Control cards	One card for each of the twelve security checks.
Progress area	The check currently running and completed results.
Finding detail	Status, plain-language explanation, and general action.
Recheck actions	Options to repeat one control or all controls.
Wiki and AI	Explanatory content and local AI-assisted guidance.
Report and contact	User-controlled ways to prepare a report or request support.

8. Starting a security scan

Run a complete assessment

- Open CyberScan.
- Select the option to start a scan if the assessment does not begin automatically.
- Keep the application open while all twelve checks run.
- Review the overall score only after the scan is complete.
- Open every warning or high-attention finding before deciding what to do.

9. Understanding scan progress

Checks may finish at different times. Network and vulnerability-oriented checks can take longer because visibility depends on active services and network conditions. A completed scan reflects only the condition detected at that moment.

> Note
> Closed or filtered services can reduce visibility. A completed scan does not prove that the workstation has no vulnerabilities.

10. Understanding the overall security score

The score summarises the twelve controls. Individual findings are more important than the total alone because different weaknesses can have very different business impacts.

Score	Classification	Interpretation
85-100	Good	A sound baseline is indicated; review every finding and maintain controls.
60-84	Improvement Recommended	One or more controls merit attention and prioritised follow-up.
0-59	At Risk	Material weaknesses may be present; timely validation and action are recommended.

Result colours and severity

Presentation	Meaning	What to do
Green / OK	The available indicators meet the baseline.	Maintain the control and read any notes.
Amber / Warning	The control may need improvement or the result is limited.	Investigate and plan a suitable action.
Red / High attention	A material weakness may be present.	Validate promptly and seek help if the action is significant.

Do not use the score as proof
A high score does not guarantee security, certification, regulatory compliance, or cyber-insurance acceptance.

11. The twelve security checks

1. Windows Firewall Status

Confirms whether host firewall protection is active and appropriately configured at a high level. A disabled or unsuitable firewall can increase exposure to unsolicited connections.

Typical next step: Enable and review Windows firewall protection using approved organisational settings. Validate exceptions before changing them.

Keep in mind: The result is a point-in-time configuration indicator and does not prove that every rule is appropriate.

2. Disk Encryption Status

Evaluates whether storage protection indicates that data at rest is encrypted. Unencrypted storage can expose business data if a device is lost, stolen, or accessed without authorisation.

Typical next step: Use an organisation-approved disk-encryption configuration and preserve recovery information securely.

Keep in mind: The check does not assess every key-management, recovery, or escrow practice.

3. Operating System Security and Integrity

Reviews available indicators of operating-system integrity and security configuration. Weakened integrity controls can make unauthorised changes harder to prevent or detect.

Typical next step: Apply supported security settings and investigate unexpected changes with qualified personnel.

Keep in mind: Coverage depends on the Windows edition, permissions, and information available to the application.

4. Local Network Port Exposure

Uses network-oriented inspection, including Nmap where available, to identify reachable local ports and services. Unnecessary listening services may increase the attack surface.

Typical next step: Confirm business need, restrict access, and remove or reconfigure unneeded services after impact review.

Keep in mind: Filtered or closed services and local network conditions can affect visibility.

5. Local Network Device Discovery

Discovers devices visible on the current local network segment using available network information. Unknown devices can indicate unmanaged assets, guest access, or a need for inventory review.

Typical next step: Compare results with an authorised asset list and investigate unexplained devices.

Keep in mind: Discovery is not a complete inventory; segmentation, filtering, and sleeping devices can hide assets.

6. Automatic Screen-Lock Configuration

Evaluates whether an automatic lock and re-authentication policy is configured. An unattended, unlocked workstation can permit unauthorised access.

Typical next step: Adopt a suitable inactivity timeout and require authentication on return, consistent with business policy.

Keep in mind: The check does not assess user behaviour or every policy source.

7. Windows Security Update Configuration

Reviews the configuration indicators available for Windows security updates. Delayed security updates can leave known weaknesses unaddressed.

Typical next step: Maintain an approved update process, test business-critical changes, and resolve persistent failures.

Keep in mind: Configuration status does not prove that every update is installed successfully.

8. Antivirus or Endpoint Protection Status

Evaluates available indicators of antivirus or endpoint protection status. Missing, disabled, or outdated protection can reduce detection and response capability.

Typical next step: Enable a supported protection solution, verify updates, and review alerts according to policy.

Keep in mind: CyberScan is not an antivirus or EDR platform and does not replace their monitoring.

9. Backup Configuration

Reviews available indicators that a backup configuration exists. Without usable backups, recovery from ransomware, failure, or accidental deletion may be difficult.

Typical next step: Maintain protected backups and test restoration regularly using approved procedures.

Keep in mind: Configuration alone does not prove backup completeness, integrity, isolation, or restorability.

10. Wireless and Bluetooth Exposure

Reviews available indicators of wireless interface and Bluetooth exposure. Unnecessary discoverability or active interfaces can increase nearby attack opportunities.

Typical next step: Disable unused interfaces and limit discoverability according to operational needs.

Keep in mind: Radio state and discoverability can change after the assessment.

11. Known Vulnerability Assessment

Uses vulnerability-oriented checks, including Nmap components where available, against detected services. Potentially vulnerable services may permit compromise or unauthorised access.

Typical next step: Validate findings, prioritise by exposure and impact, then apply vendor-supported mitigation.

Keep in mind: Results can include false positives or false negatives and are not proof of exploitability.

12. Local Web Service Vulnerability Assessment

Uses Wapiti where available to assess locally exposed web services for selected vulnerability classes. Weak local web services may expose data or enable attacks through the workstation.

Typical next step: Validate findings in an authorised context, then update, reconfigure, or remove affected services.

Keep in mind: Only reachable services are assessed; coverage is not equivalent to a full web application penetration test.

12. Reviewing a single finding

Review procedure

- Open the control card.
- Read the status and plain-language explanation.
- Review any detected host, port, service, or vulnerability detail.
- Read the limitation before treating the result as confirmed.
- Use the recommended action as a starting point, not an automatic instruction.
- Ask qualified personnel before making disruptive or business-critical changes.

13. Rechecking controls

Recheck one control

Use the recheck action on that control card after you have changed a setting or when the earlier result was limited.

Recheck all controls

Use the complete recheck after several changes or when you want a new point-in-time overview. The new results replace the previous displayed scan state.

> Warning
> Do not change firewall rules, encryption, endpoint protection, update settings, backups, network services, or radio configuration without understanding operational impact.

14. Asking the AI assistant

The integrated local AI assistant helps users understand security findings and provides general remediation guidance without requiring a cloud-based AI subscription.

Ask about a finding

- Open a finding that is not marked OK.
- Select the option to ask the AI assistant.
- Review the pre-filled question and submit it.
- Read the answer together with the original finding and limitation.
- Verify the advice before applying any system change.

> AI caution
> AI responses may contain errors. The assistant is informational, does not autonomously modify Windows settings, and does not automatically remediate vulnerabilities.

15. Using the Security Wiki

The Security Wiki opens a dedicated window with explanatory cybersecurity content and the AI chat. You can keep it open while reviewing the main assessment. Language changes are designed to remain consistent across the interface.

16. Generating a security report

Prepare a report

- Complete or recheck the assessment.
- Review individual findings and remove misunderstandings where possible.
- Select the report action.
- Check the score, findings, assessment time, and any sensitive details.
- Save or share the report only through an authorised business process.

17. Sending a report to CSAEC

The sharing action prepares a message in the default email client. CyberScan does not automatically submit the report to CSAEC. Review the recipient, subject, body, attachments, and sensitive information, then deliberately send the message if you choose.

18. Requesting emergency assistance

Use the emergency contact action when a serious finding or active concern requires urgent professional review. The action prepares a message; it does not guarantee immediate response or replace your organisation's incident-response procedure.

> Possible active incident
> If you suspect ongoing compromise, follow your organisation's incident-response instructions. Avoid deleting evidence or making uncoordinated changes.

19. Privacy and local processing

CyberScan uses a local-first processing approach. Core checks and scan-result processing are designed to run on the workstation, and the AI assistant is designed to operate locally. No report is automatically sent to CSAEC. Opening an email client or using an optional external component may involve third-party software or services.

20. Recommended user actions

- Prioritise red findings and important warnings by business impact.
- Confirm significant findings before changing production settings.
- Maintain supported Windows updates and endpoint protection.
- Protect backups and test restoration.
- Repeat the assessment after approved changes.
- Use qualified cybersecurity assistance when the risk or remedy is unclear.

21. Troubleshooting

Issue	What you can do
A check does not complete	Wait briefly, then recheck. Confirm suitable permissions and contact IT if the issue repeats.
Network results look incomplete	Confirm that you are on the expected network. Filtering and segmentation can hide devices or services.
The AI is unavailable	Allow local model initialisation to finish. Availability can depend on the installed build and local configuration.
The email action does not open	Confirm that a default email application is configured in Windows.
A language change appears incomplete	Change the language again or restart CyberScan. The cached results can be redrawn without rescanning.

22. Frequently asked questions

Does CyberScan remove threats?

No. It assesses selected controls and provides decision support; it does not automatically remediate vulnerabilities.

Is a Good score proof of compliance?

No. The score is not a certification, formal audit, regulatory guarantee, or insurance decision.

Are network findings always complete?

No. Filtering, inactive devices, permissions, and segmentation can affect visibility.

Does CyberScan send my report automatically?

No. Sharing requires a deliberate user action and review in the email client.

23. Limitations

- The assessment is point-in-time and limited to twelve defined controls.
- Vulnerability checks can produce false positives and false negatives.
- A completed scan does not prove absence of vulnerabilities.
- Backup configuration does not prove successful recovery.
- AI output may contain errors.
- Professional validation may be required for significant findings.

24. Glossary and support

Term	Plain-language meaning
Control	One of the twelve security checks.
Endpoint protection	Separate security software that detects or blocks harmful activity.
Local-first	Designed to process core information on the workstation and minimise external transmission.
Port	A network communication point used by a service.
Severity	An indication of how much attention a finding may need.
Vulnerability	A weakness that could be used to affect confidentiality, integrity, or availability.

Support information

Use the authorised CSAEC contact details included with your CyberScan distribution. Include the assessment time and relevant finding details, but review confidential information before sending.