

CyberGuardian XDR

User Guide

Enterprise cybersecurity for organizations of any size



CyberGuardian XDR - detects and neutralizes threats in real time

MITRE ATT&CK Coverage

NIS2 Compliance Support

SSL A+

Windows EDR / XDR

cyberguardian.bg | cgs.xdr@gmail.com

What is CyberGuardian XDR?

Next-generation extended detection and response platform

CyberGuardian XDR is a next-generation extended detection and response platform built for organizations that require enterprise-grade protection without enterprise-grade complexity. Installed on Windows machines, it provides real-time threat detection, automated response, MITRE ATT&CK coverage, NIS2 compliance support, and a bilingual BG/EN interface - all through one lightweight agent that installs in minutes.

1. Dashboard

This is the first page you see - the entire security picture on one screen. Three key numbers show the current state: total incidents, critical incidents, and unopened incidents. The Needs Your Attention section automatically prioritizes what requires immediate action. Security Posture Score summarizes the health of your entire infrastructure in one number. The system also recognizes when one technique dominates detections and points you to FP Control for tuning.

THIS GIVES YOU

An answer to the question "Am I safe?" in seconds, without navigating through ten screens.

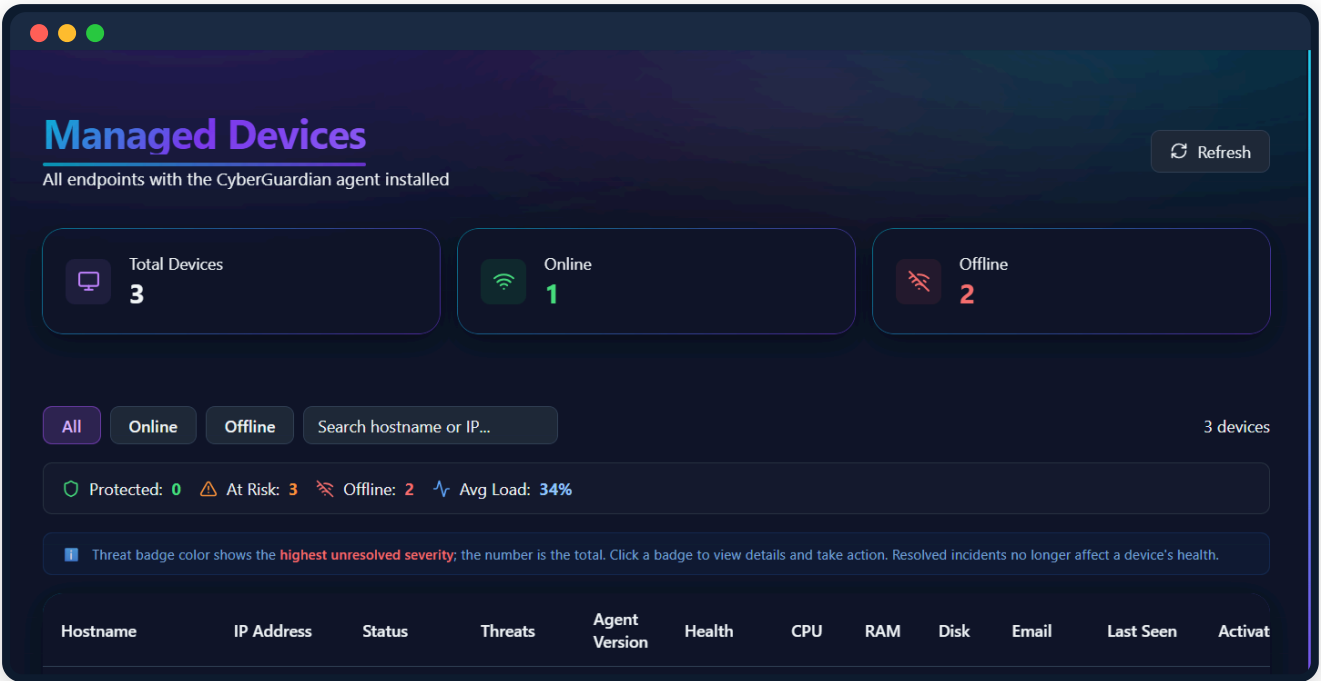


2. Managed Devices

A central view of all computers with the agent installed. You can see the total number of devices, how many are online and offline right now. For each device: network address, connection status, detected threats by severity, agent version, CPU, memory and disk usage, and the last active time. Color-coded threat indicators show the most severe unresolved incident. Search and filtering by name or status take you to a specific machine in seconds.

THIS GIVES YOU

See the status of every computer in the organization from one place instead of checking each machine separately.



3. Crash Telemetry

If an agent on any computer encounters a serious problem, it reports it automatically and you see it immediately with full context. When the same issue affects several machines, the system groups them so you can instantly distinguish a widespread problem from an isolated case. The Contact Support button sends the request directly by email with ready diagnostics. When everything is fine, the page shows "All agents healthy".

THIS GIVES YOU

Resolve problems while they are still small instead of discovering them too late.



Crash Telemetry

Your agents automatically report crashes here, so you can spot and resolve issues early

Contact Support

Refresh



All agents healthy

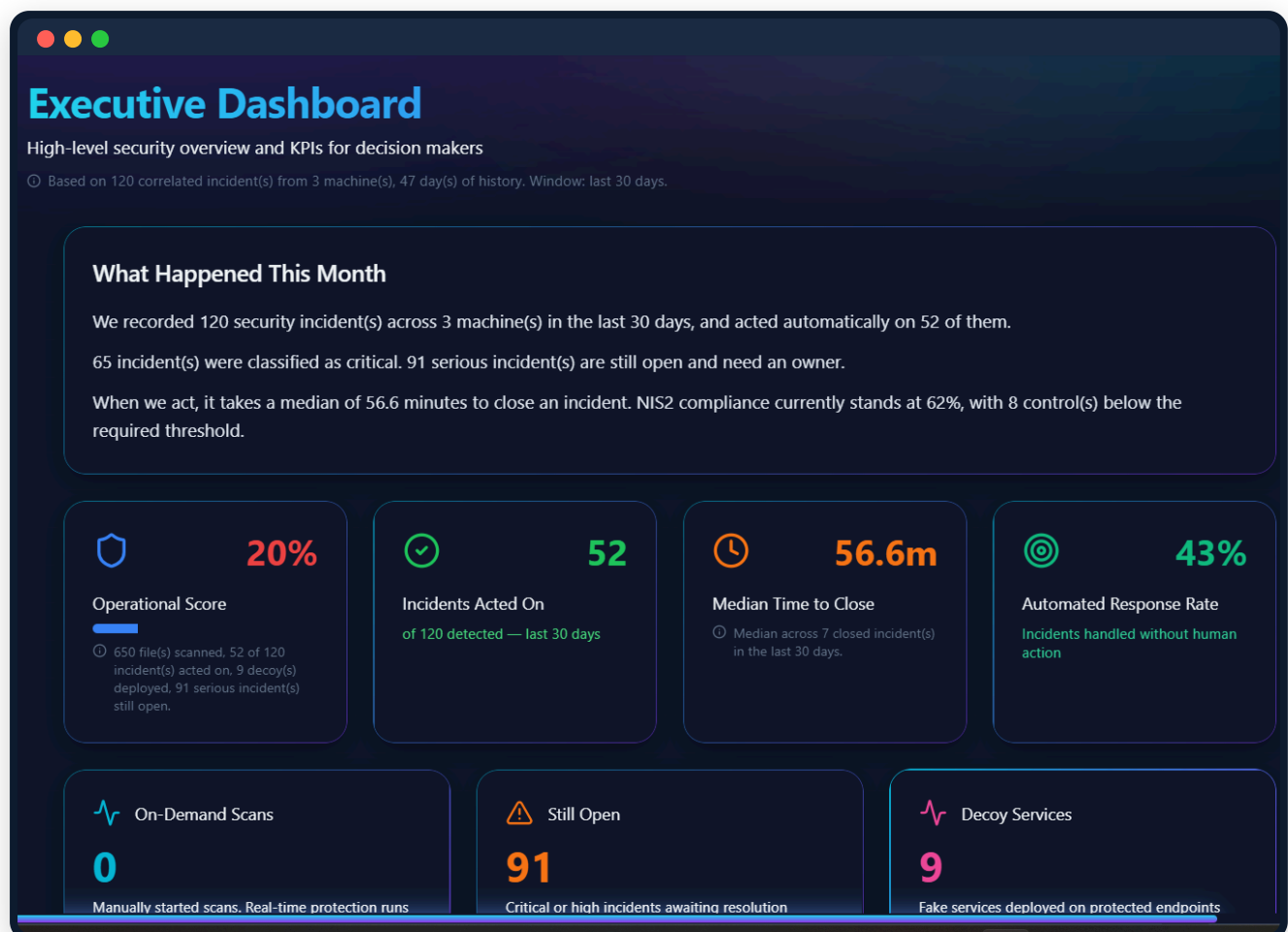
No crashes reported. Your agents send a report the moment they panic, so this page stays empty as long as your devices are stable.

4. Executive Dashboard

The management page summarizes the month in plain language: how many incidents were recorded, how many were handled automatically, and how many remain open. Key indicators include Operational Score, the share of incidents with automated response, and average incident resolution time. NIS2 Board Risk Overview translates technical compliance into board-level language - readiness percentage and the number of controls below the required threshold.

THIS GIVES YOU

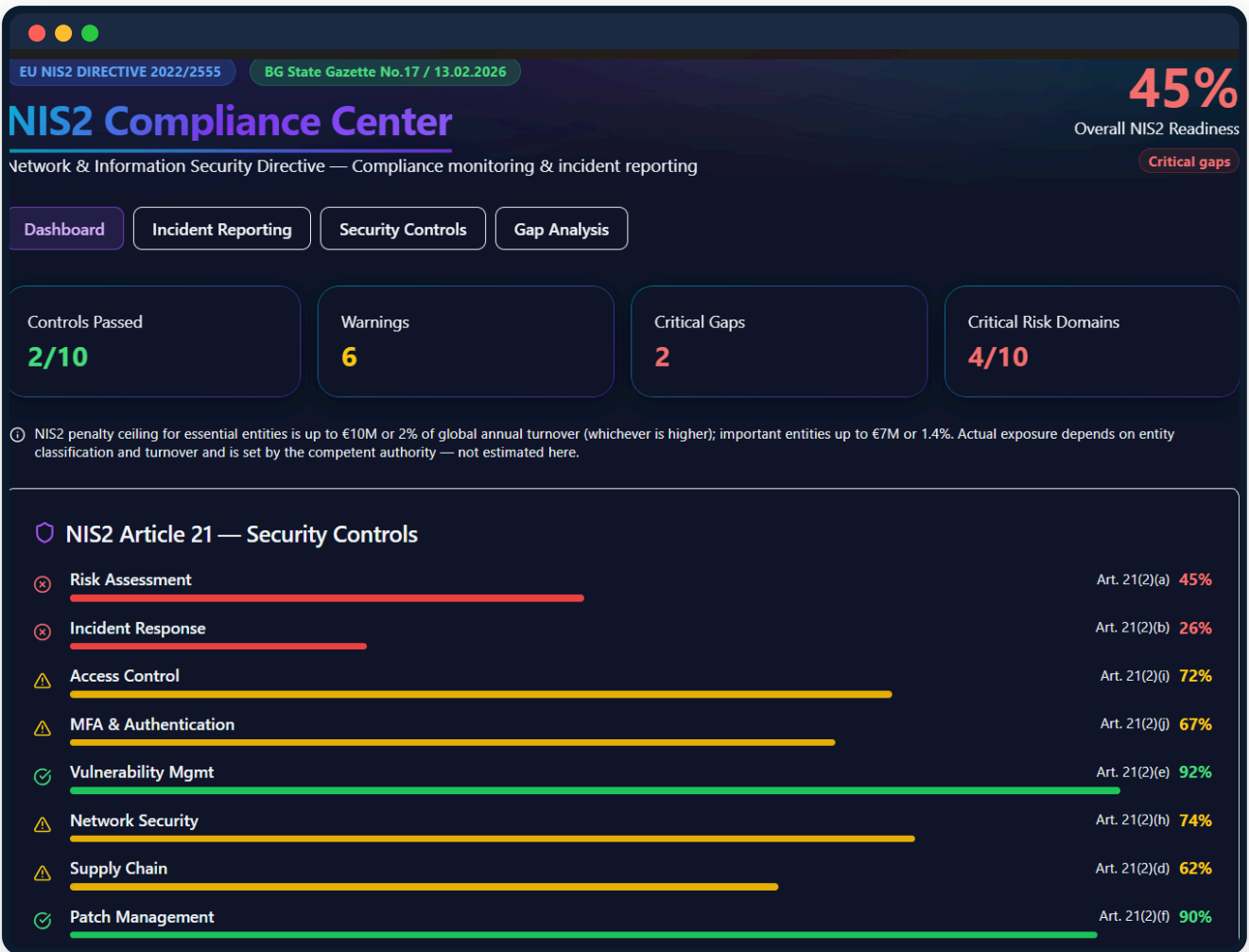
Management understands within minutes what happened and where the organization stands against the requirements - without translation from the technical team.



5. NIS2 Compliance

Built-in automated assessment against NIS2 Article 21 and the Bulgarian Cybersecurity Act (State Gazette No. 17 / 13.02.2026)

CyberGuardian XDR helps assess the organization against applicable requirements. Penalties for non-compliance can reach up to EUR 10,000,000 depending on the entity category and applicable regime. The platform supports work across the 10 control domains under Article 21, generates structured reports, and automates the Article 23 incident timeline.



NIS2 Compliance Overview

Real-time assessment against the mandatory controls under Article 21. Gap Analysis provides a prioritized action plan.

Know where you stand before the audit.

Audit Evidence Vault

Forensic evidence for every event. Export to PDF, CSV or JSON.

At audit time - one click, not a week of digging.

Vulnerability Scanner

Scans the inventory against the national vulnerability database in real time.

Know which programs are exploitable before the attacker does.

Patch Management

Tracks applied and overdue security updates and the status of automatic updates.

Close the most common door to compromise.

Network Security

Full firewall audit across the three profiles, with risk-based port classification.

Access Control

Finds passwordless accounts, excessive administrator privileges and unused accounts.

See open doors before someone else does.

Catch "forgotten" accounts - a favorite attacker entry point.

MFA & Authentication

Checks Windows Hello, remote-access protection and password protection in memory.

A stolen password alone is no longer enough.

Incident Response

Monitors the security log in real time for failed logons and privilege escalation.

You see the break-in attempt at the first knock.

Supply Chain Security

Scans applications for malware, unverified publishers and outdated versions.

Know what is actually installed and what creates risk.

Risk Assessment

Combines results from all NIS2 domains into a weighted score.

One number for the board, details for the technical team.

Cyber Hygiene & Training

Automated audit of screen lock, USB media and protection settings.

Small gaps that lead to major breaches - caught early.

NIS2 Executive Report

Structured compliance report for review and preparation before submission to CERT-BG.

Evidence preparation and reporting become significantly faster.

Policy Generator

Generates ready-to-use Word security policy documents tailored to your company.

Mandatory documents in minutes instead of weeks.

Training Tracker

Centralized register of mandatory training with validity tracking.

At an audit, show the register instead of collecting certificates from email.

Backup Security Monitor

Automatically checks whether you have an active, protected and up-to-date backup, including a remote copy.

When the worst happens, you have something to restore from.

Threats

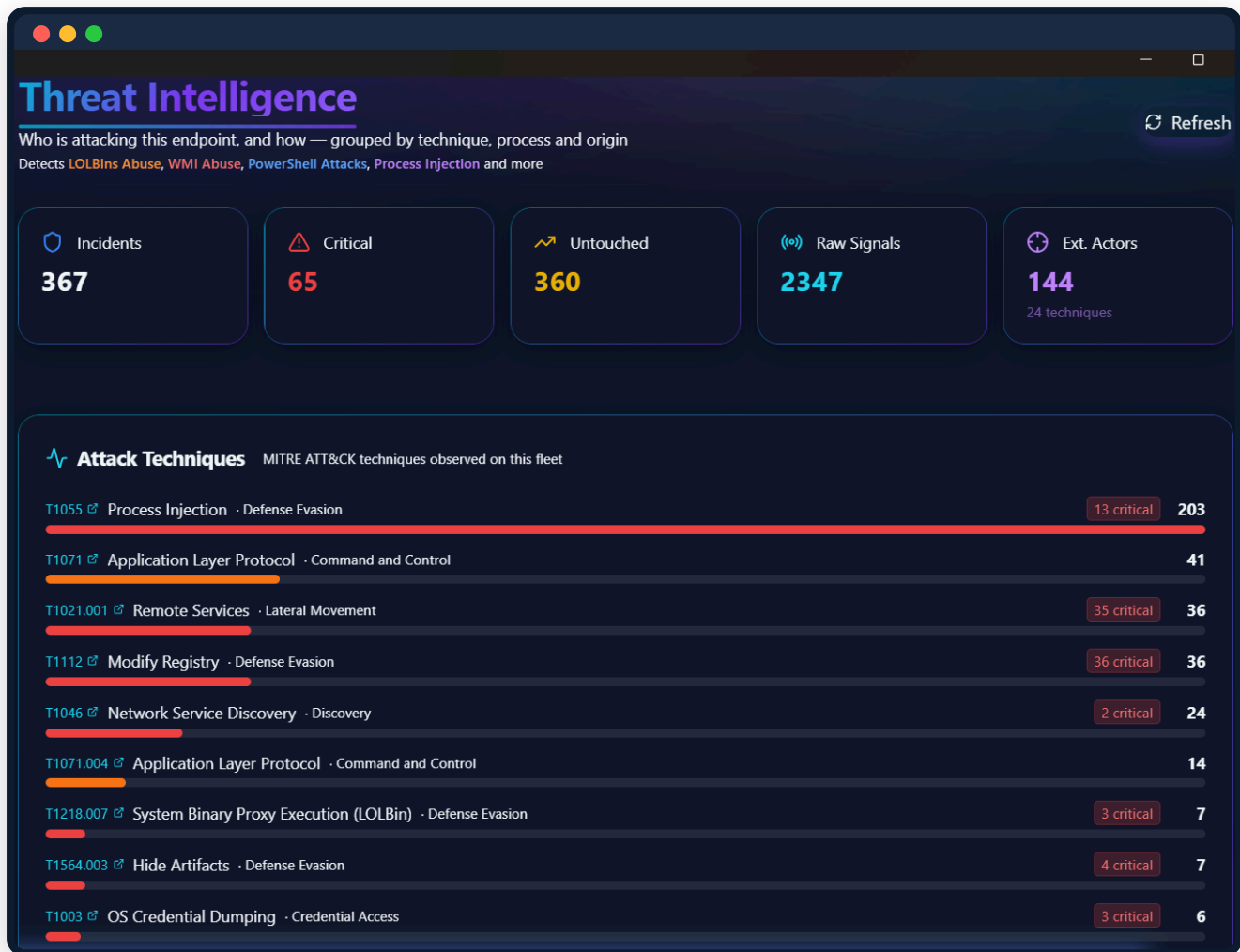
A complete picture of threats - from signals to attacker techniques and threat intelligence

6. Threats — Threat Intelligence

All detected threats are collected here - from abuse of system tools and PowerShell to code-injection attempts. You can see the total number of incidents, critical incidents, untouched incidents and Raw Signals, plus the number of unique External Actors. Attack Techniques shows every MITRE ATT&CK technique observed across the fleet, with incident counts and criticality. The AI Response Playbook button generates a personalized response guide.

THIS GIVES YOU

Never face a threat asking "What now?" - the system tells you exactly what to do.

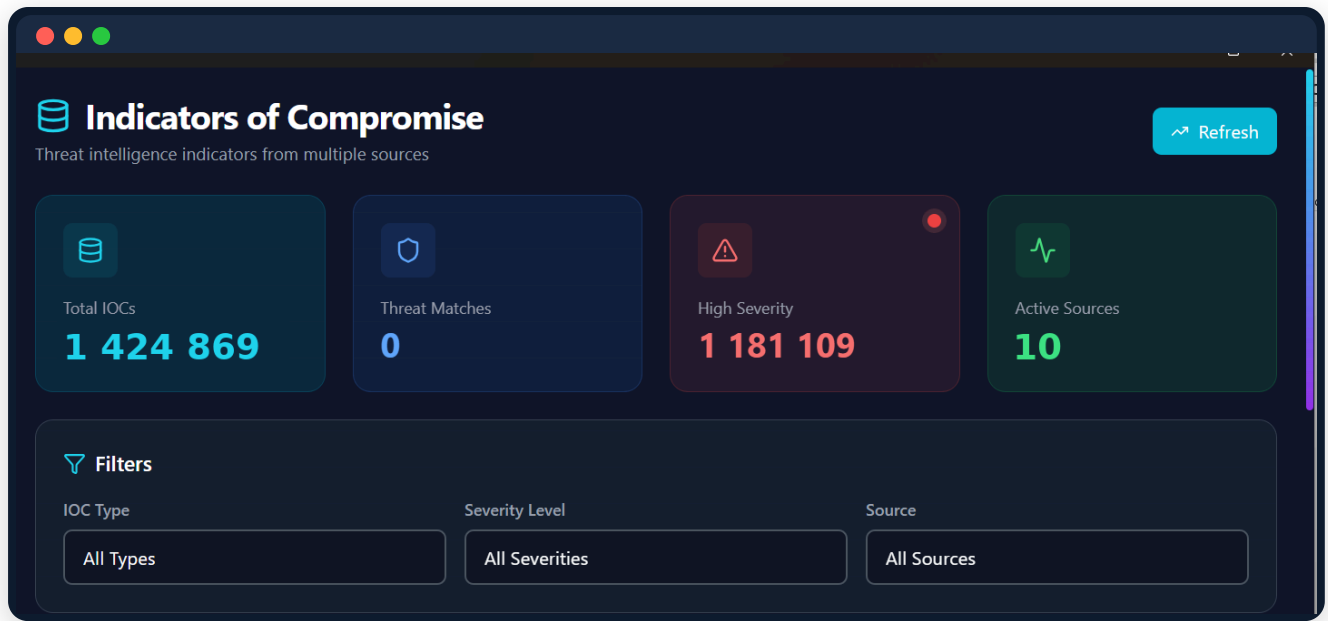


7. Threats — Indicators of Compromise (IOCs)

The Indicators of Compromise database contains approximately 1,424,869 active records from 10 independent feeds. Every IP, domain or file hash associated with known malicious activity is here. When multiple independent sources report the same indicator, confidence in it rises automatically. Filter by IOC type, severity and source.

THIS GIVES YOU

Newly disclosed global indicators reach the system through automatic updates.



8. Threats — Threat Intelligence Feeds

The system is fed by leading global threat-intelligence sources - more than 1,000,000 active indicators of compromise, updated automatically every 6 hours. You can see each source, its status and the number of IOCs it contributes. When several independent sources report the same threat, confidence in it increases automatically.

THIS GIVES YOU

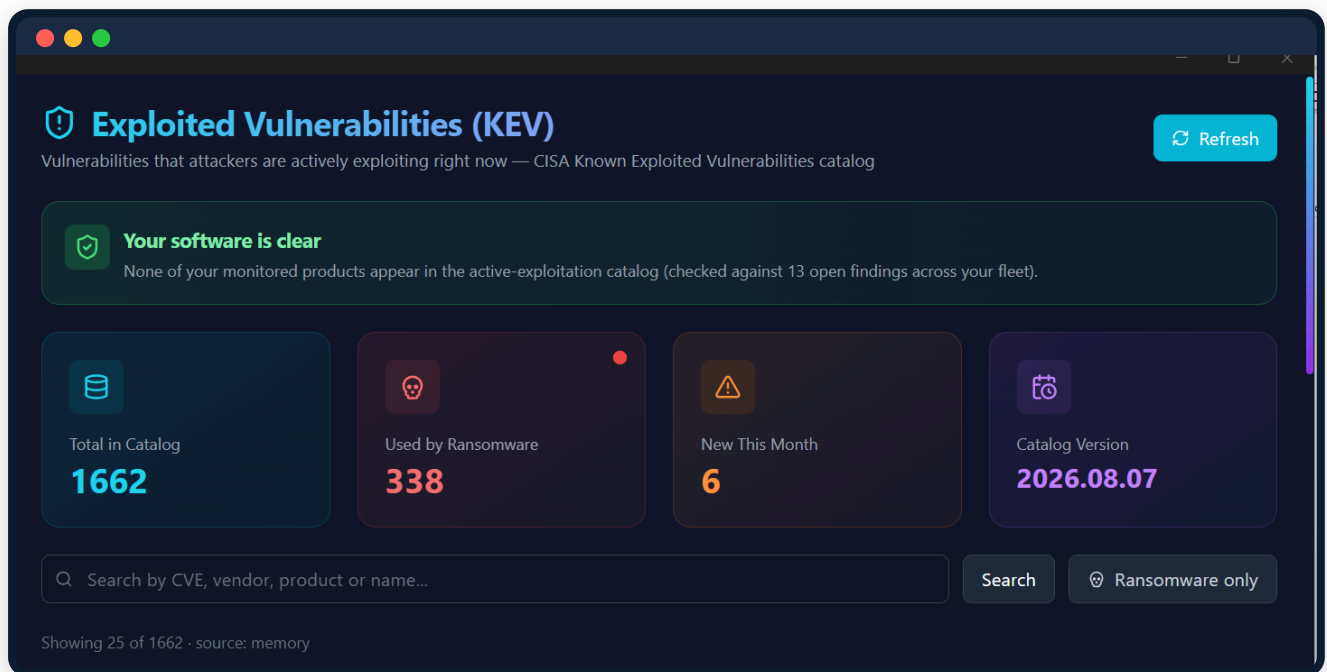
Newly disclosed indicators are added through automatic threat-intelligence updates.

9. Threats — Exploited Vulnerabilities (KEV)

Thousands of vulnerabilities are discovered every month, but only a small share are actively exploited by attackers. This page tracks exactly those in CISA's Known Exploited Vulnerabilities catalog. The system compares the catalog with the software on your computers and alerts you on a match. The current catalog contains 1,662 entries, of which 338 are linked to ransomware. Ransomware-related vulnerabilities are marked as most urgent.

THIS GIVES YOU

A concrete answer to "Am I at risk right now?" - so you focus effort where the danger is real.



Detection

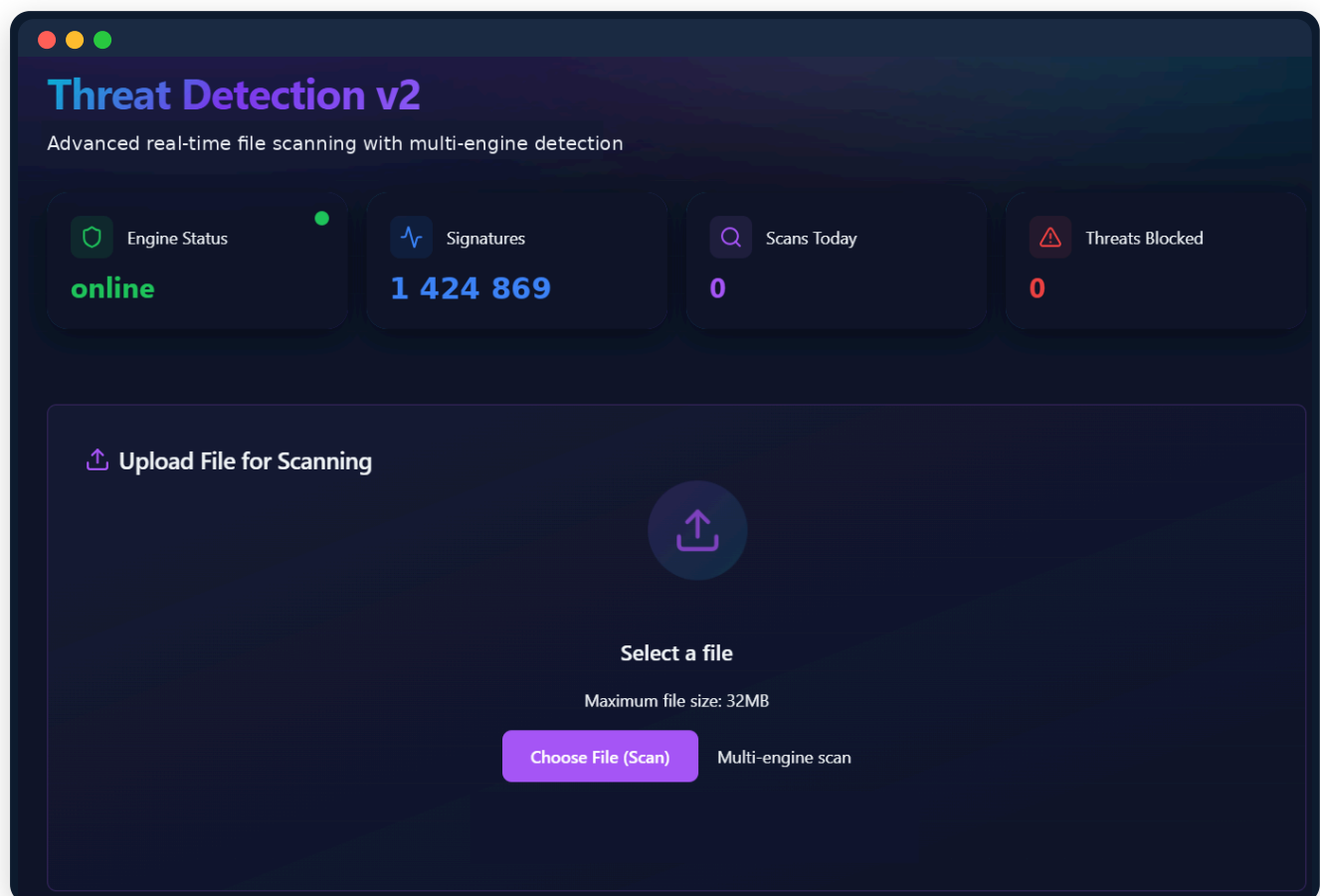
Multi-layer threat detection - signatures, behavior and real-time blocking

10. Detection — Threat Detection v2

Here you manage threat detection itself. You can see the size of the active detection base (shown in the interface as Signatures) - approximately 1,424,869 records - and the operating mode. You can upload a specific file for checking through Multi-Engine Scan (signatures, entropy analysis, PE inspection and cloud lookup).

THIS GIVES YOU

See not only that something was detected, but exactly what the system did - blocked it, remediated it, or only monitored it.



11. Detection — Runtime Blocking

Runtime Blocking watches everything executed on the computer in real time. When it detects suspicious behavior, it reacts immediately: the process is terminated (Killed), the change is reversed after detection (Remediated), or the event is logged for review (Detected). Every event is linked to a MITRE ATT&CK technique and Risk Score.

THIS GIVES YOU

The threat is stopped at execution time - not after the damage has already been done.

Runtime Blocking

Total events: 10

Disable Blocking

Runtime Blocking ACTIVE

Behavioral & signature engine — live process termination enabled

Killed — live process terminated

Remediated — change reverted after the fact

Detected — logged, no termination

PID

Process

Reason

MITRE

Risk Score

Time

Status

12. Detection — Process Tree

A visual map of everything currently running on the computer - 246 processes arranged in a parent-child hierarchy. The system automatically highlights suspicious relationships: a program started by an unexpected parent, a code-injection attempt, or abuse of legitimate tools. Automatic refresh runs every 30 seconds.

THIS GIVES YOU

Attackers like to hide behind legitimate processes - here, their camouflage becomes visible at a glance.

Process Tree

Live process hierarchy · Anomaly detection · MITRE ATT&CK mapping

246 Processes

All Clear

Search process, PID, user...

All Processes · Click to see anomalies

20:52:37 u

Auto 30s

Refresh

PROCESS NAME

PID

CPU

MEMORY

USER

ANOMALY

STATUS

[System Process]

0

0.0%

0 MB

N/A

RUNNING

System

4

0.6%

13 MB

N/A

RUNNING

Registry

176

0.0%

42 MB

N/A

RUNNING

smss.exe

720

0.0%

1 MB

N/A

RUNNING

Memory Compression

4012

0.0%

311 MB

N/A

RUNNING

CyberGuardian XDR | cyberguardian.bg | cgs.xdr@gmail.com

© 2026 CyberGuardian Security EOOD

Protection & Scans

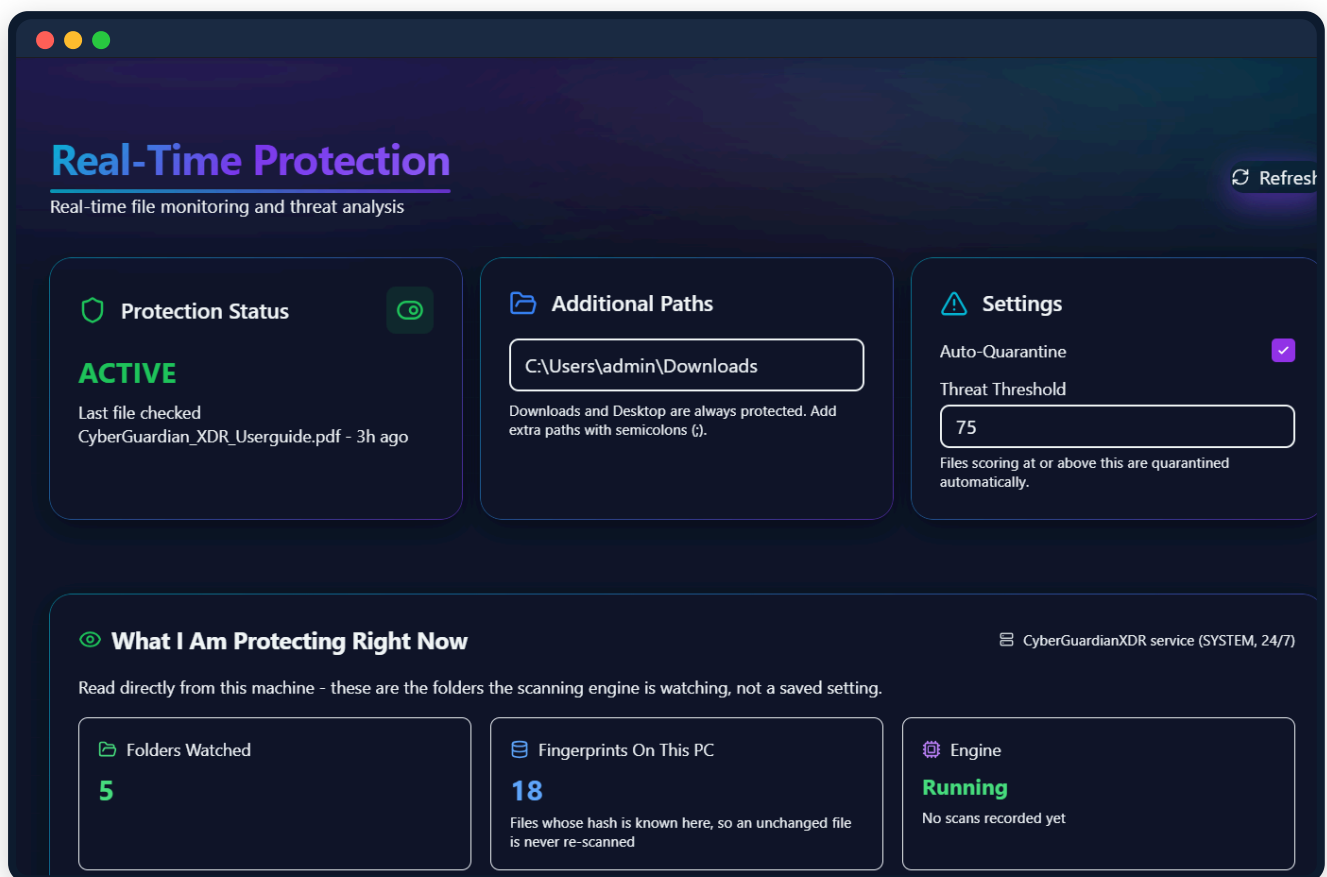
Real-time file protection and on-demand scanning

13. Real-Time Protection

This page continuously monitors the file system - every change is analyzed automatically as it happens. Dangerous files are sent to quarantine automatically, without your intervention. You can set the sensitivity (Threat Threshold) to control how strictly automatic action is applied. What I Am Protecting Right Now shows exactly which folders are being monitored and how many file fingerprints the system has stored on that machine.

THIS GIVES YOU

Peace of mind that the computer protects itself 24/7 - even when nobody is watching the screen.



14. Scans — Security Scans

Start a computer scan whenever you want. Three profiles are available: Quick Scan (~2 min, 100 files), Standard Scan (~10 min, 1,000 files) and Deep Scan (~30+ min, 10,000 files). Suspicious of a specific file? Upload it and the system analyzes it through Multi-Engine File Scanner. The data does not leave your machine - scanning is local.

THIS GIVES YOU

Control in your hands - check anything suspicious immediately while routine scans run by themselves.

Security Scans

Run on-demand scans and review your scan history

[Refresh](#) [Run Scan Now](#)



Advanced File Analysis

Upload any file for deep multi-engine threat analysis



Multi-Engine File Scanner

Deep multi-engine threat analysis



Click to upload or drag and drop
Any file type supported



Quick Scan Profiles

Start a scan instantly with predefined profiles optimized for different scenarios



Quick Scan

Fast scan of critical system files

⌚ Duration

~2 minutes

📁 Max Files

100

🔄 Recursive

No

Extensions:

.exe .dll .bat .ps1 +3

Start Scan



Standard Scan

Balanced scan for regular use

⌚ Duration

~10 minutes

📁 Max Files

1000

🔄 Recursive

Yes

Extensions:

.exe .dll .bat .ps1 +4

Start Scan



Deep Scan

Comprehensive scan of entire system

⌚ Duration

~30+ minutes

📁 Max Files

10 000

🔄 Recursive

Yes

Extensions:

*

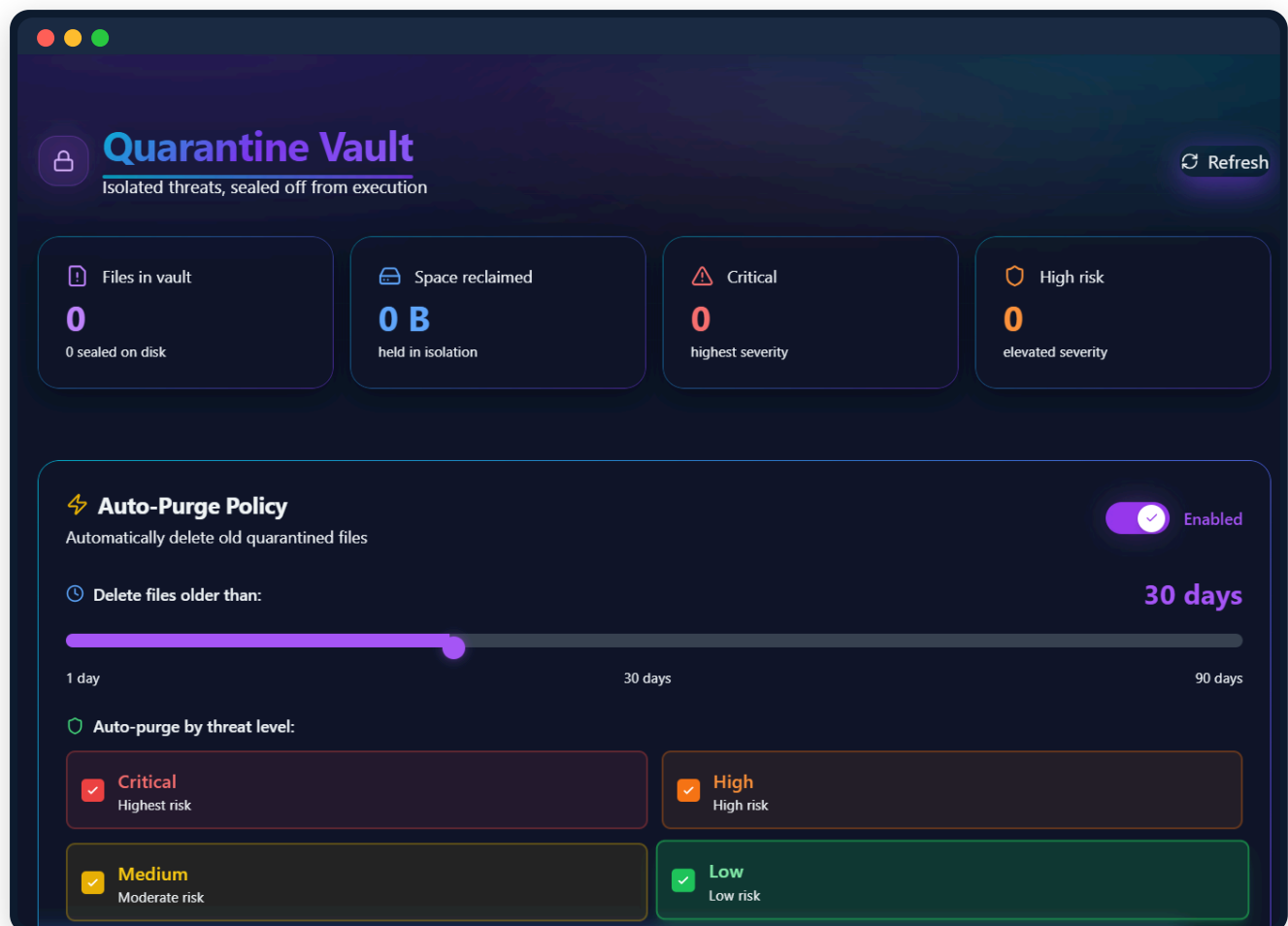
Start Scan

15. Quarantine Vault

Captured dangerous files are stored here - isolated, safe, but not deleted. You can see the number of files in the vault, storage used and severity levels. Auto-Purge Policy automatically cleans old entries according to a period you define (1-90 days) and threat severity. Every file can be reviewed and restored in case of a false positive.

THIS GIVES YOU

The captured file is neutralized, but nothing is lost - a false positive can be restored with one click.



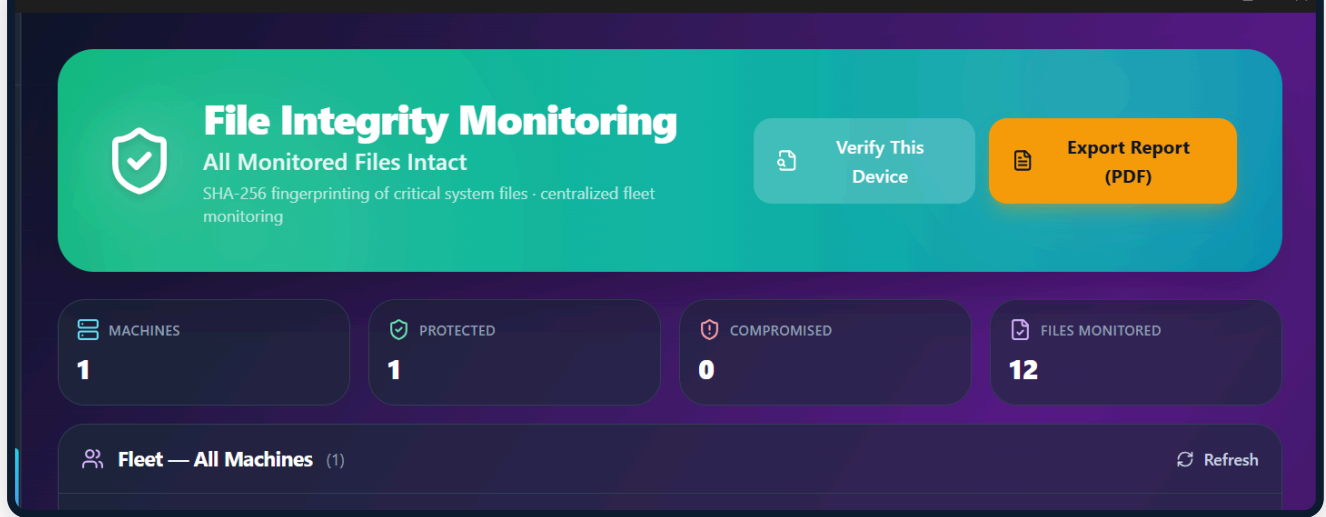
16. File Integrity Monitoring

Monitors critical system files for unauthorized changes using cryptographic checksums (SHA-256). A fleet-wide view shows the number of protected, compromised and monitored files. For a selected machine, you can see a detailed breakdown and generate a PDF report or start verification.

THIS GIVES YOU

Silent replacement of system files becomes visible immediately - on every machine in the fleet, with a single check.





17. Tamper Protection

The first goal of a serious attacker is often to disable your protection. This page shows an overall Protection Score (100/100) and four protection layers: Config Integrity (VALID), Ransomware Canary (ARMED - 3 decoys active), Watchdog (ACTIVE), and Process Protection (ACTIVE - 13 critical processes protected). Protection includes self-defense mechanisms.

THIS GIVES YOU

Multi-layer protection designed to make silent disablement harder, with visibility into the attack techniques it is built to resist.



Remediation

Complete removal of malware and persistence mechanisms

18. Malware Remediation

A standard antivirus deletes the file, but malware can leave persistence anchors in the system - in the registry, services and scheduled tasks. Four specialized tools remove them thoroughly: Registry Cleanup scans and removes malicious registry entries with automatic backup before deletion; Services Cleanup finds and stops malicious Windows services; Tasks Cleanup removes malicious scheduled tasks; and Deep Quarantine performs full analysis and removal. Everything runs locally - data does not leave the machine.

THIS GIVES YOU

Reduce the risk of the threat returning after a restart.



Malware Remediation

Advanced tools for complete malware removal and system cleanup

7 active threats

Refresh Stats

Registry Entries

0

Suspicious entries found

Services

1

Malicious services

Scheduled Tasks

6

Suspicious tasks

Quarantined

0

Deep Quarantine backups

Registry Cleanup

Available

Scan and remove malicious Windows registry entries

✓ Scan autorun registry keys

✓ Detect suspicious entries

✓ Automatic backup before removal

✓ One-click restore

Open Module

Services Cleanup

Available

Identify and remove malicious Windows services

✓ Enumerate all services

✓ Detect suspicious services

✓ Stop and delete services

✓ Service backup

Open Module

Tasks Cleanup

Available

Scan and clean malicious scheduled tasks

✓ Scan Task Scheduler

✓ Identify malicious tasks

✓ Remove suspicious tasks

✓ Task backup

Open Module

Deep Quarantine

Available

Complete malware removal with deep scanning

✓ Deep file analysis

✓ Registry reference scan

✓ Service dependency check

✓ Complete removal

Open Module

CyberGuardian XDR | cyberguardian.bg | cgs.xdr@gmail.com

© 2026 CyberGuardian Security EOOD

Insights

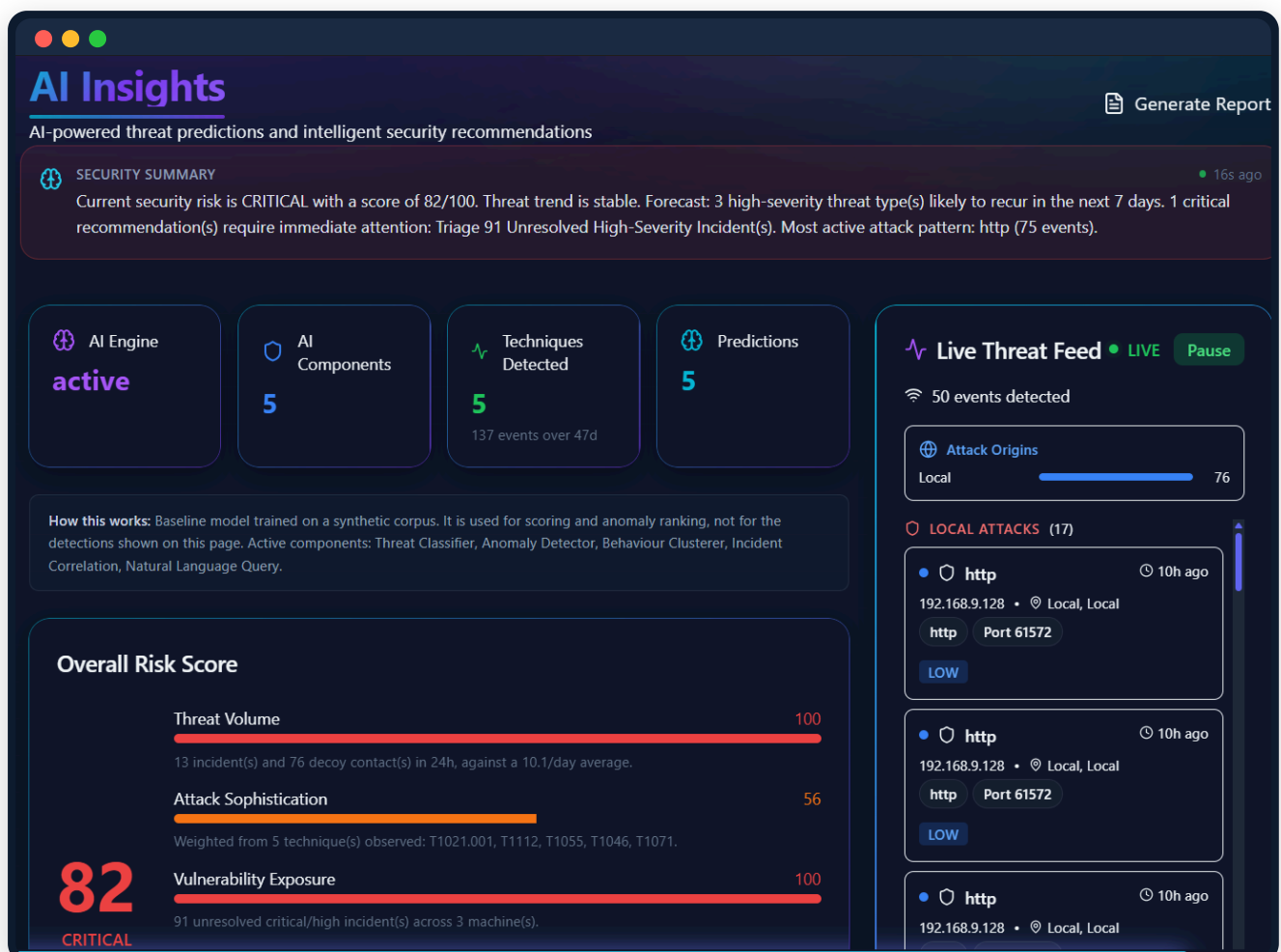
Artificial intelligence analyzes risk and provides a ready action plan

19. AI Insights

AI continuously analyzes all data from your environment and provides a short natural-language summary of the current risk and what needs attention first. Overall Risk Score from 0 to 100 is broken down into five factors: Threat Volume, Attack Sophistication, Vulnerability Exposure, Incident Frequency and Security Posture. Live Threat Feed shows incoming threats in real time, classified by origin.

THIS GIVES YOU

Clearly see how exposed you are right now and why, instead of interpreting charts and numbers yourself.



20. Predictive Threat Timeline & What-If Simulator

Predictive Threat Timeline shows whether attack activity is rising or falling over the last 24 hours, 7 days or 30 days. What-If Simulator is a planning tool: model a hypothetical scenario - attack type, intensity and duration - and see how your current defenses would perform. The tool is explicitly identified as a simulation, not as a measurement of the live environment.

THIS GIVES YOU

Know not only what is happening, but where the trend is heading - and plan proactively.

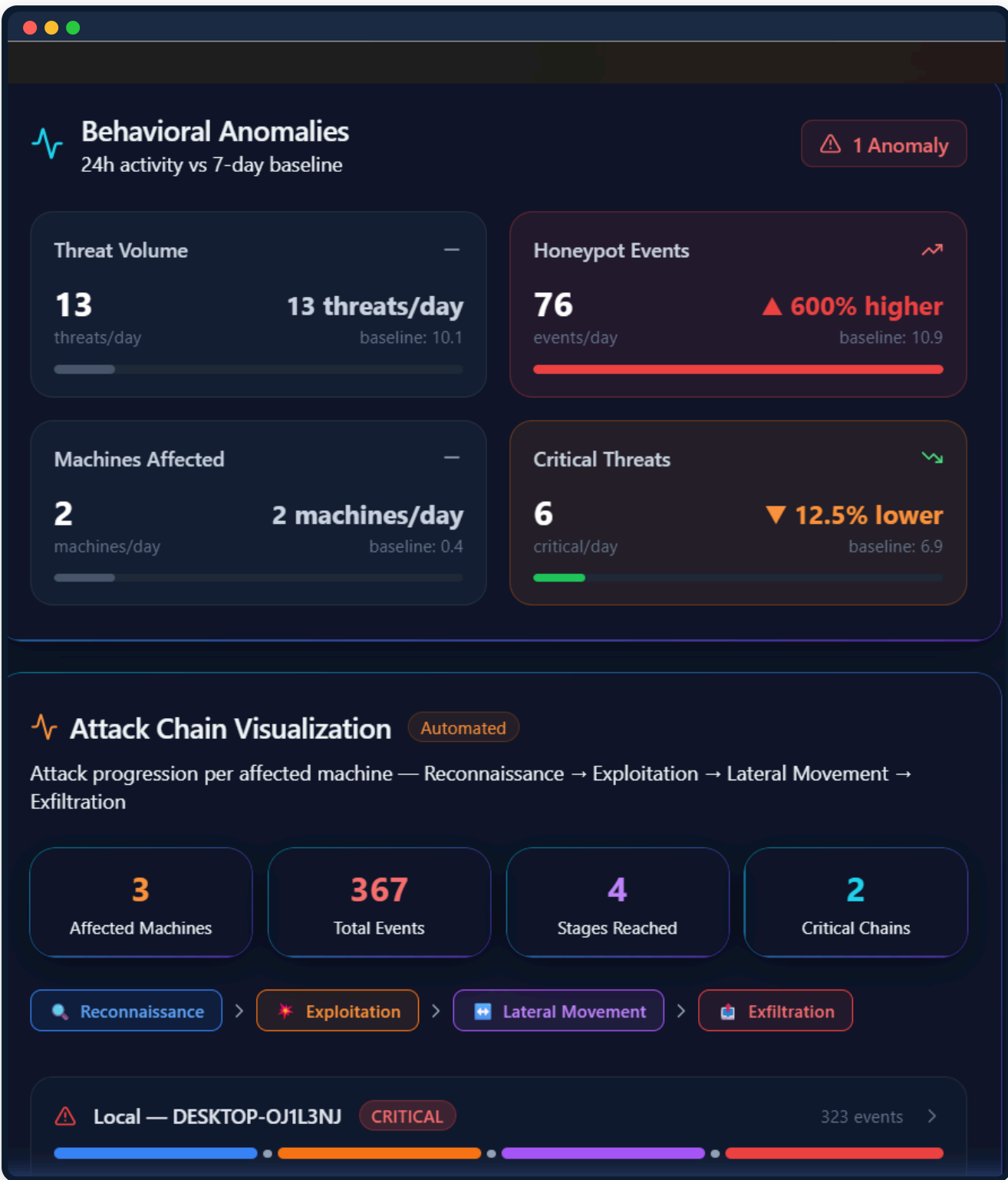


21. Behavioral Anomalies & Attack Chain Visualization

Behavioral Anomalies compares the last 24 hours with a 7-day baseline, showing whether threat volume, honeypot events, affected machines and critical threats are above or below normal. Attack Chain Visualization tracks attack progress per machine: Reconnaissance > Exploitation > Lateral Movement > Exfiltration, with the number of affected machines, total events and critical chains.

THIS GIVES YOU

See not just individual incidents, but the full attack picture - what stage it has reached and which machines are affected.



22. AI Recommendations

AI turns the analysis into a concrete task list ordered by priority. For each recommendation, you can see why it was suggested, the expected implementation time, complexity, and the expected security impact - including a direct link to the relevant NIS2 requirement. Filter by priority and sort by importance.

THIS GIVES YOU

Not just a list of problems - a ready action plan, with priority and estimated effort for every step.

The screenshot shows a dark-themed window titled "AI Recommendations" with a lightbulb icon. At the top, there are three filters: a search bar labeled "Search recommendation", a dropdown menu set to "All Priorities", and another dropdown menu set to "Sort by Priority". Below the filters, a recommendation card is displayed. The card has a red warning icon and the title "Triage 91 Unresolved High-Severity Incident(s)". It features three tags: "critical" (in a red pill), "Incident Response" (in a dark pill), and "Pending" (with a clock icon in a dark pill). The main text states: "91 critical or high incident(s) detected on your machines are still open. Each one should be reviewed, contained or dismissed as a false positive. Unreviewed incidents are the most common way a real intrusion stays hidden." Below this, a small icon and text say "Based on 91 events in open incidents on your machines right now". Two metrics are shown in separate boxes: "Implementation 22.8h" and "Complexity Low". The "Impact" section states: "Closes the gap between detection and response, which is what NIS2 Article 23 reporting timelines depend on". Below the impact, four NIS2-related requirements are listed in pill-shaped buttons: "NIS2 Art. 23", "NIST CSF RS.AN-1", "ISO 27001 A.16.1.5", and "CIS Controls 17.4". At the bottom of the card, there are three buttons: a green "Implement" button with a checkmark, a blue "Learn More" button with a book icon, and a grey "Dismiss" button with an 'X' icon.

AI Recommendations

Search recommendation | All Priorities | Sort by Priority

⚠ Triage 91 Unresolved High-Severity Incident(s)

critical Incident Response Pending

91 critical or high incident(s) detected on your machines are still open. Each one should be reviewed, contained or dismissed as a false positive. Unreviewed incidents are the most common way a real intrusion stays hidden.

Based on 91 events in open incidents on your machines right now

Implementation **22.8h** | Complexity **Low**

Impact: Closes the gap between detection and response, which is what NIS2 Article 23 reporting timelines depend on

NIS2 Art. 23 | NIST CSF RS.AN-1 | ISO 27001 A.16.1.5 | CIS Controls 17.4

✓ Implement | Learn More | Dismiss

ML Models & Incidents

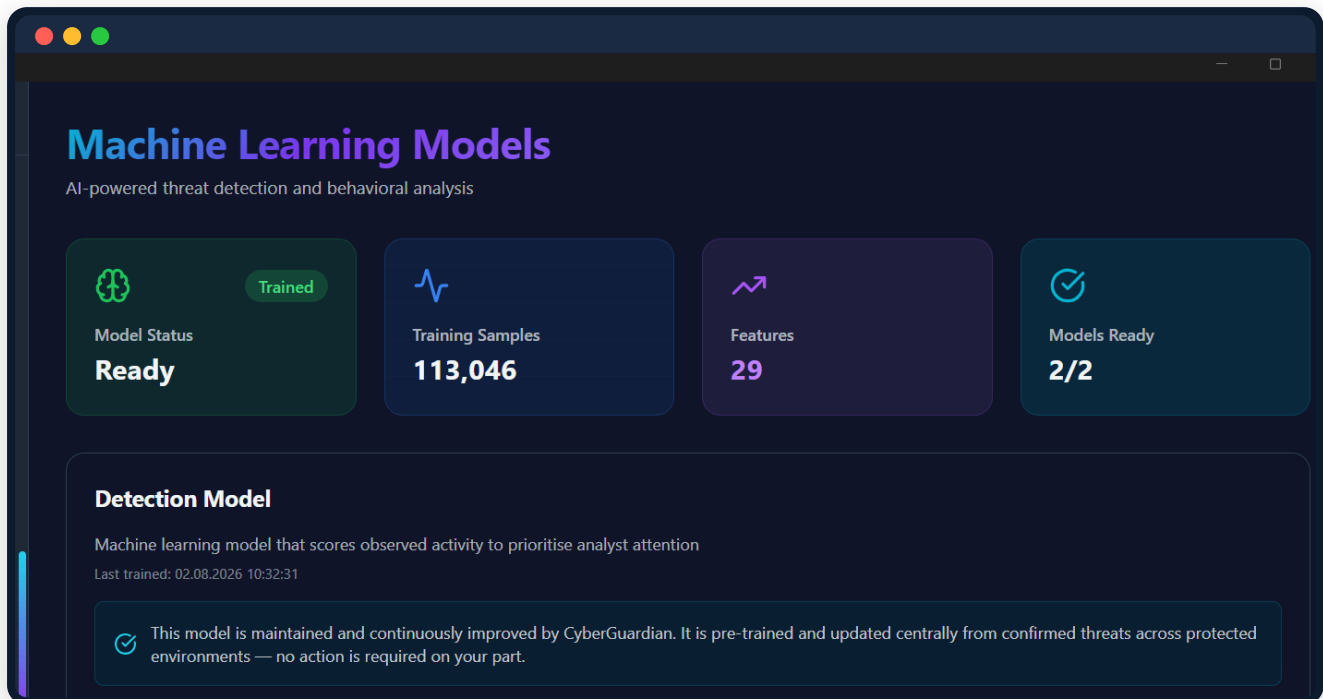
Machine learning behind detections and correlated incidents with NIS2 reporting

23. Machine Learning Models

Here you can see and manage the AI behind detections - model status (Ready / Trained), number of training samples and independent features used for decisions. Current state: 113,046 training samples, 29 features, 2/2 models ready. The models are maintained and updated centrally by CyberGuardian using confirmed threats from protected environments - no action is required on your side.

THIS GIVES YOU

AI models refreshed with confirmed training data - without manual maintenance on your side.



24. Correlated Incidents

Most serious attacks are not a single event, but a chain of steps. This page links separate signals into common incidents with severity, confidence and Auto-Response status. Response Performance shows average time to acknowledge, contain and resolve incidents. For an incident requiring reporting under NIS2 Article 23, the 24h Early Warning, 72h Notification and Final Report actions are directly available next to it.

THIS GIVES YOU

Manage the entire incident response, with the NIS2 clock in front of you, from one page.

Correlated Incidents

Attack chain reasoning — isolated signals connected into incidents

Active Incidents

113

Auto-Response

52

High Confidence

12

Suppressed (FP)

5

🕒 Response Performance

Mean time to acknowledge

—
from 0 incidents

Mean time to contain

—
from 0 incidents

Mean time to resolve

—
from 0 incidents

Never picked up

0
of 0 open

Averages are computed only from incidents that actually reached each milestone. A dash means no incident has reached it yet — it is not a zero.

Each incident shows the machine, AI risk level, confidence and verdict. Expand the incident to see the full Attack Storyline - every event in chronological order with its MITRE technique. NIS2 deadlines show the countdown to the reporting deadline. You can add a note to the audit trail, mark the incident as a False Positive, or resolve it.

Active Incidents

All Machines

INC-20260810-0385

MITKOLAPTOP

Suspicious

Living off the Land (LOTL)

HIGH
AI risk

HIGH
confidence

Confirmed
verdict

8 events

NIS2 Art. 23 report:

24h Warning

72h Notification

Final Report

Resolve

Suppress (FP)

Always expected here

Description

PIDs

MITRE

First Seen

Multiple LOLBins used in sequence

33816, 24360, 10036

T1046 T1218.007

10.08.2026 16:51:54

Move to:

Investigating

False Positive

Nobody has picked this up yet

Add a note for the audit trail (optional)

Save note

NIS2 deadlines:

24h early warning: 19h 54m left

72h notification: 67h 54m left

Attack Storyline — 8 events

HIGH T1046

16:51:54 u.

Port scan detected: 16 inbound TCP connections from IP 192.168.192.92 in 60s

Process: 192.168.192.92

HIGH T1046

16:51:54 u.

Port scan detected: 16 inbound TCP connections from IP 192.168.192.92 in 60s

Process: 192.168.192.92

25. FP Control

The system distinguishes legitimate system processes from disguised threats using Suppression Rules and Trusted Processes. Suppression Rules let you define process + parent process + reason combinations for which the alert is suppressed automatically. Trusted Processes adds processes by name and SHA256 hash. Current state: 14 rules, 6 trusted processes, 5 automatically suppressed.

THIS GIVES YOU

Reduce false positives and direct the team toward more likely real threats.



FP Control Layer

False Positive suppression — enterprise-grade alert accuracy

Suppression Rules

14

Trusted Processes

6

Auto-Suppressed

5

Active Incidents

113

Suppression Rules

Add New Rule

Process (e.g. powershell.exe)

Parent (e.g. vscode.exe)

Reason (e.g. IDE terminal)

+ Add Rule

powershell.exe ← vscode.exe
VSCode terminal
built-in



powershell.exe ← code.exe
VSCode internal
built-in



Trusted Processes

Add Trusted Process

Process name (e.g. MsMpEng.exe)

SHA256 hash (optional)

Reason (e.g. Windows Defender)

+ Add Trusted

Windows Defender
built-in



Windows Security Health
built-in

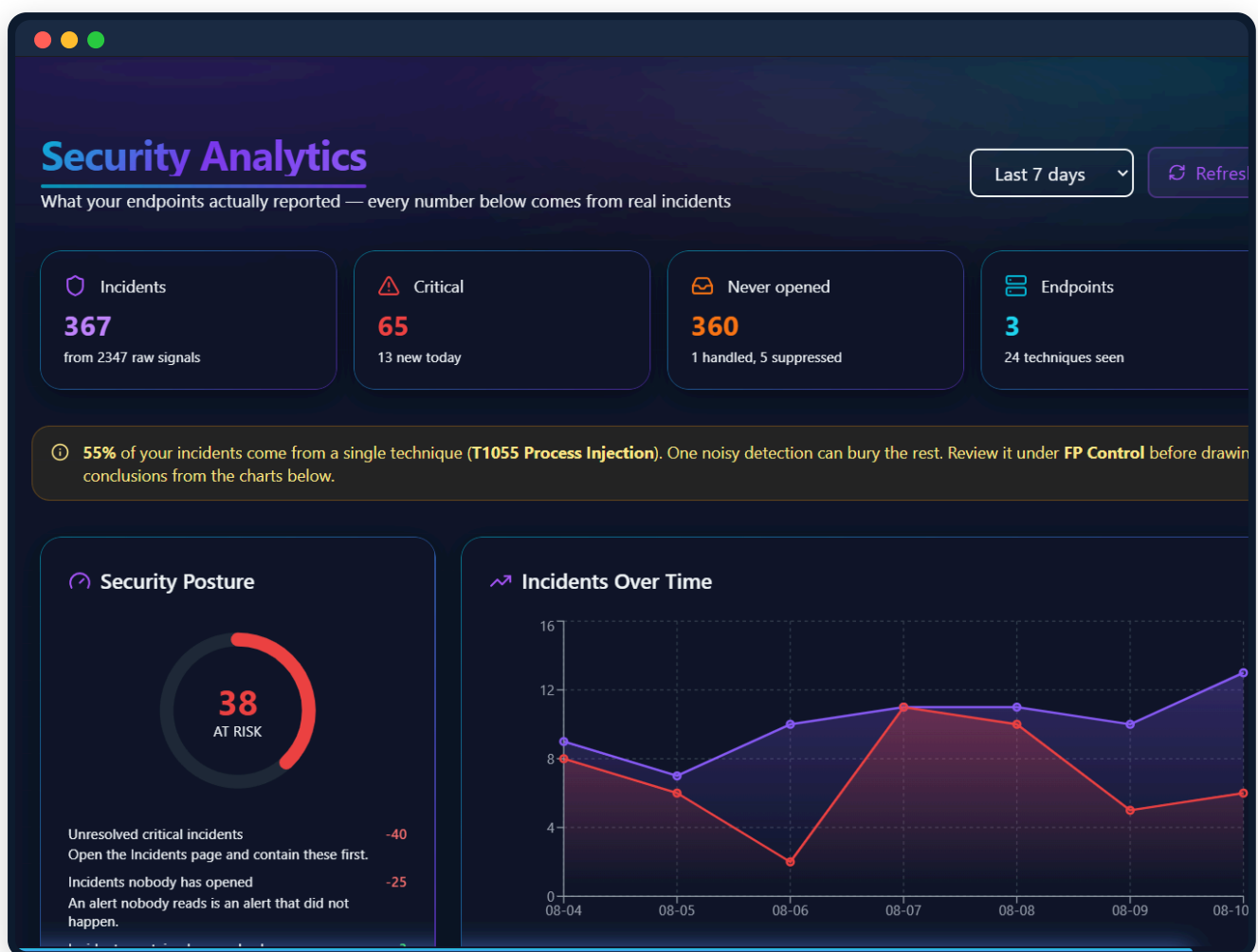


26. Security Analytics

A consolidated picture of everything your devices actually reported - not forecasts, but data from real incidents. See incidents, critical incidents, unopened incidents and triggered endpoints for the selected period (7 days / month). Security Posture Score summarizes health in one number. If a single technique dominates the statistics, the system explicitly points it out and links to FP Control. The Incidents Over Time chart shows the trend by day.

THIS GIVES YOU

Rely on real data from your environment - and get a warning when a noisy detection may distort the picture.



27. Email & Phishing Scanner

Phishing is attack vector No. 1. The scanner connects to your mailbox through an App Password and analyzes every email in multiple layers - checking URLs, domains and attachments against more than 1,000,000 malicious indicators. Settings are available in the separate Settings section. You can see Scanner Status, the number of scanned emails, detected phishing attempts and safe emails.

THIS GIVES YOU

A suspicious email can be flagged before the employee clicks.

Email & Phishing Scanner

Scan your inbox for phishing attempts and malicious emails

[Go to Settings](#)

Scanner Status

Not Setup



Total Scanned

0



Phishing Detected

0



Safe Emails

0





No Email Accounts Configured

Add an email account in Settings to start scanning for phishing emails

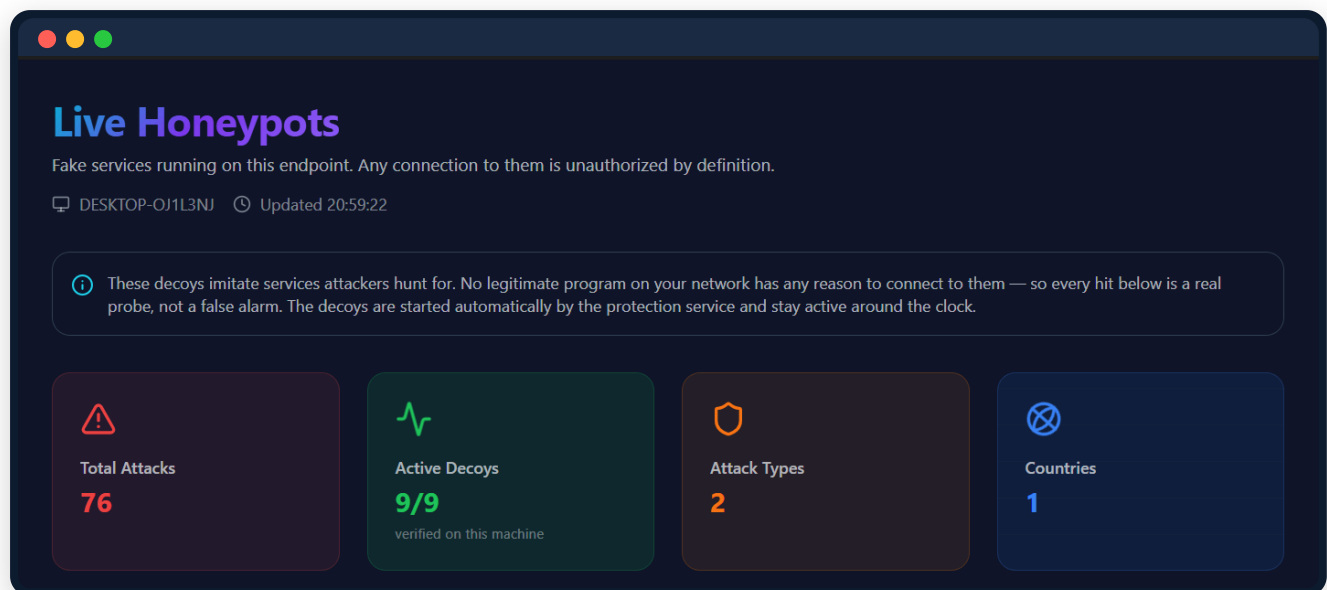
[Go to Settings](#)

28. Live Honeypots

Decoys are fake services running on the endpoint that look real to an attacker. Any connection to them is treated as highly suspicious, because legitimate applications normally have no reason to use them. Current view: 76 total attacks, 9/9 active decoys verified on this machine, 2 attack types from 1 source. Decoys are started automatically by the protection service and run continuously.

THIS GIVES YOU

Turn the game around - the attacker thinks they are attacking you, but actually shows you how and from where.



29. Performance Monitor

Real-time machine health and optimization recommendations. Health Score from 0 to 100 shows overall health. See CPU Usage, Memory Usage, Disk Usage and Top Process in real time. The system identifies bottlenecks and suggests specific improvements. Export Report generates a PDF with the full health analysis.

THIS GIVES YOU

Protection that monitors itself not to get in the way - clearly see that the computer is performing well.



Performance Monitor

Real-time health of this machine and optimization insights

Export Report

Refresh

System Health Overview

Live status of this machine



POOR

Uptime: 101h 9m



CPU USAGE

16.6%



8 cores @ 2803 MHz



MEMORY USAGE

78.7%



12.4 GB / 15.8 GB



DISK USAGE

71.7%



134.4 GB free of 475.1 GB



TOP PROCESS

msedgewebvi...



PID: 4744
CPU: 53.8%
Memory: 179.4 MB

30. Process Protection & Monitoring

This page protects running programs against tampering. It monitors Service Status (Running), Total Processes (247) and Suspicious Processes (0) in real time. Advanced Monitoring is active in Production mode with Auto-Monitoring and provides manual Trigger Scan and Dismiss Alerts options. Anti-Termination makes it harder for malware to disable protection, while Self-Healing restores it automatically after a crash.

THIS GIVES YOU

Protection designed to make silent disablement harder - one of an attacker's first objectives.



31. Software Updates

See the exact agent version (current: 2.0.2 Sentinel, Built August 10, 2026) and the full update history: 2 Major, 0 Minor and 2 Patch versions. Update Health shows when the last check occurred, how many updates are installed and which channel is used (Stable). Automatic updating is managed from here.

THIS GIVES YOU

Your protection stays up to date - and you can prove it with a complete audit-ready history.





Software Updates

Keep your CyberGuardian AI secure and up-to-date



Current Version

Actively protecting your system

2.0.2

Sentinel

Built on August 10, 2026

MAJOR
2

MINOR
0

PATCH
2

UPDATE HEALTH

LAST CHECKED
Just now

INSTALLED
1 updates

CHANNEL
Stable



Update Status

Check for the latest security updates

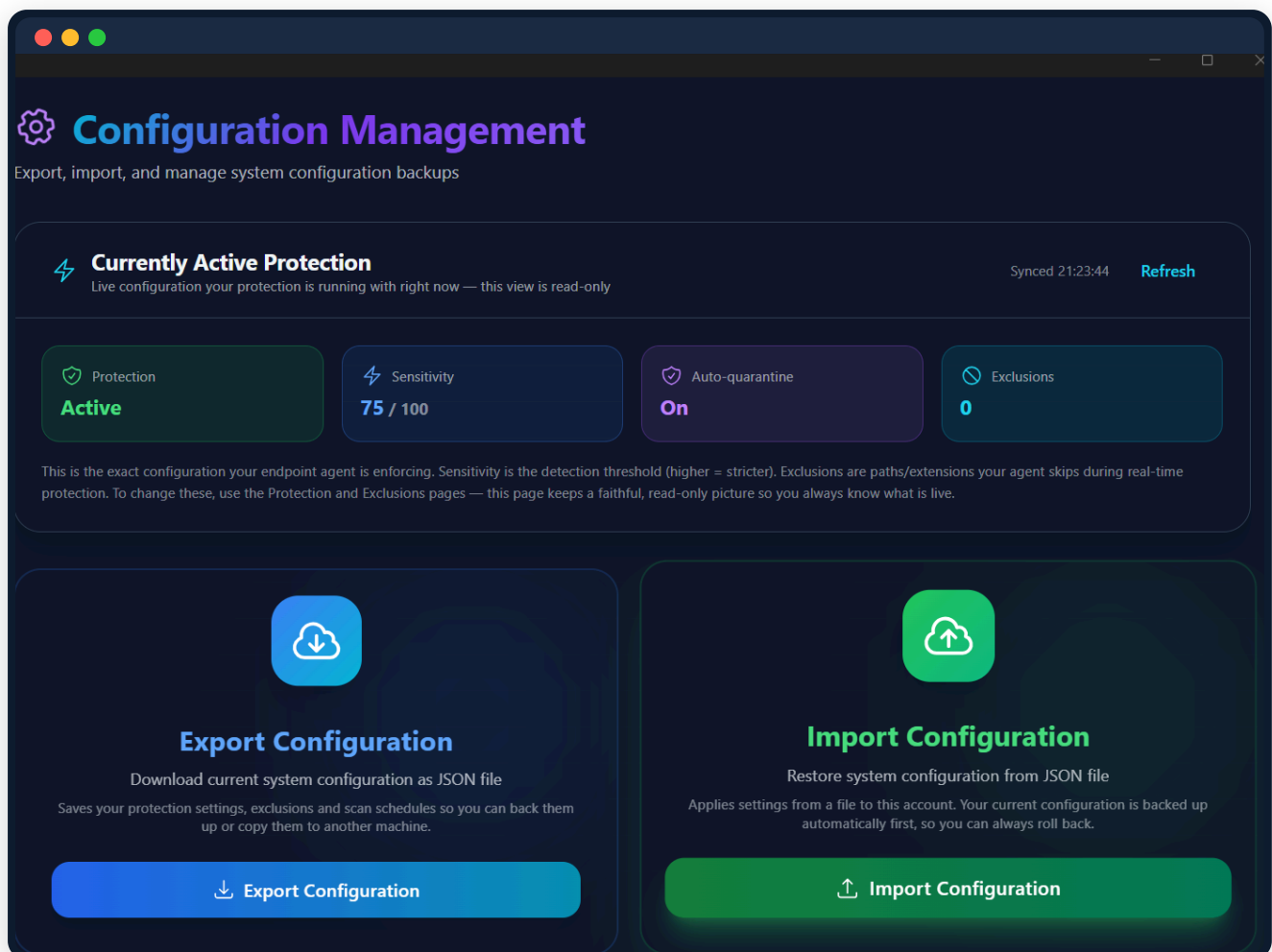
Check for Updates

32. Configuration Management

This page shows the exact configuration currently applied by the agent - in real time and in view-only mode. You can see Protection (Active), Sensitivity (75/100), Auto-quarantine (On) and Exclusions (0). Export Configuration downloads the current settings as a JSON file, useful for backup or copying to another machine. Import Configuration loads settings from a file with automatic backup before the change.

THIS GIVES YOU

Know exactly which configuration is running on each machine - and transfer or restore it in seconds.



33. Settings

Manage notifications (Email Alerts, Desktop Alerts, Critical Only, Alert Sound) and visual preferences (Compact Mode, Animations). Email Alerts send a summary of new incidents to the licensed email address. Desktop Alerts show a native Windows notification when a new threat appears in Live Feed.

THIS GIVES YOU

Configure the system to notify you in the way you work - without noise, but also without missed alerts.



Settings

Configure your CyberGuardian preferences and system settings

Notifications

Email Alerts

Sends a summary email to your license contact address when new incidents are detected.
Requires a contact email on your license.



Desktop Alerts

Shows a native desktop notification when a new threat appears in the live feed.



Critical Only

Limits alerts to CRITICAL and HIGH incidents only. Off by default so you don't miss anything.



Alert Sound

Plays a sound in the app when a new threat appears in the live feed.



Appearance

Compact Mode

Reduce spacing and padding



Animations

Enable smooth animations



34. Settings — Organization Profile

The organization profile stores the data needed for NIS2 reports: Organization Name, EIK/Bulstat, Address, Contact Person, Contact Email, CERT-BG ID and System Description. NIS2 Profile Completeness shows what percentage is filled in. These data automatically populate all NIS2 reports.

THIS GIVES YOU

Enter your organization details once - and they automatically feed all NIS2 reports from then on.



Organization

NIS2 Profile Completeness

1/17 • 6%

These details feed your NIS2 compliance reports. Fill them all in to be report-ready.

Organization Name

Your Organization

EIK / Bulstat

123456789

Address

1 Example St, Sofia

Contact Person

John Doe

Contact Email

security@example.com

CERT-BG ID

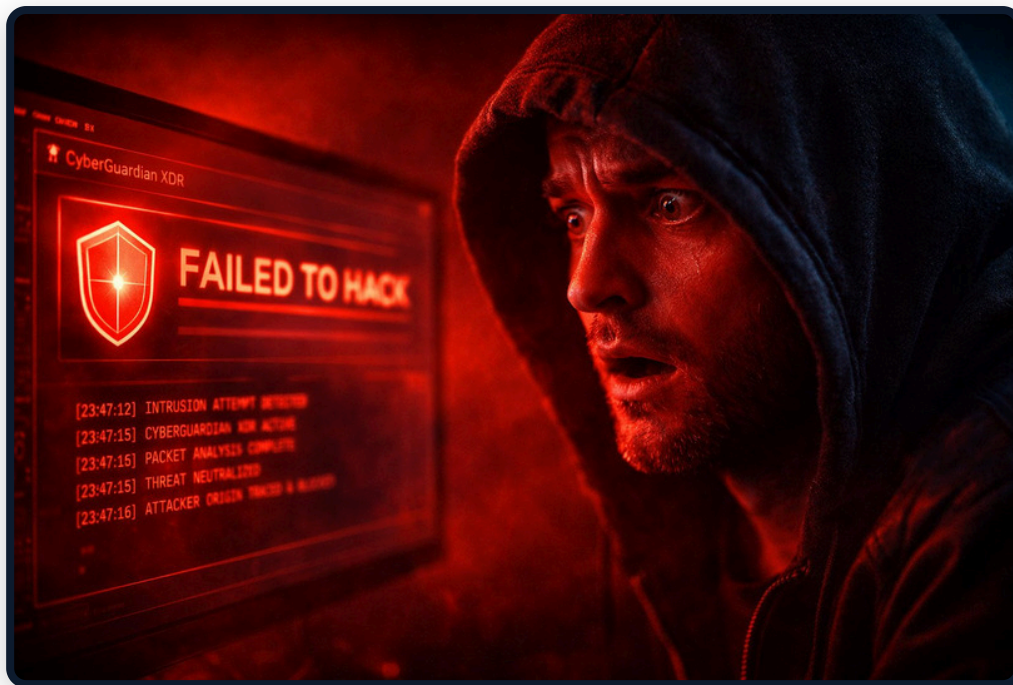
CERT-BG-XXXX

System Description

Critical network infrastructure for...

35. What you get with CyberGuardian XDR

What you get	What it means for you
Dashboard - Security Operations Center	All protection on one screen - incidents, critical issues, unopened items and Security Posture Score
Managed Devices (Fleet)	All machines in one place - status, health, threats and agent version
Crash Telemetry	A problem on any machine becomes visible immediately, centrally, with ready diagnostics
Executive Dashboard	Management sees risk, trends and NIS2 status in plain language
NIS2 Compliance - 15 modules	NIS2 evidence and reports for review before submission
Threat Intelligence + IOC (1M+)	Newly disclosed indicators are added through automatic updates
Exploited Vulnerabilities (KEV)	See whether your software is under real attack right now - not an abstract list
Detection v2 + Runtime Blocking	The threat is stopped at execution time - not after damage is done
Process Tree	Attacker camouflage behind legitimate processes - visible at a glance
Real-Time Protection	The computer protects itself 24/7 - even when nobody is watching the screen
Tamper Protection (100/100)	Four protection layers make silent disablement harder
File Integrity Monitoring	Silent replacement of system files becomes visible immediately on every machine
Malware Remediation	Removes files and persistence mechanisms
AI Insights + ML Models	Explained risk, trends and a ready action plan
Live Honeypots (9 active)	Suspicious activity against decoys is visible separately
Email & Phishing Scanner	Protection against attack vector No. 1 - directly in email, before the click
FP Control + Security Analytics	Reduces false positives and points you toward more likely threats.



"FAILED TO HACK" - CyberGuardian XDR detected and blocked the simulated attack.

36. Contact and licensing

cgs.xdr@gmail.com • cyberguardian.bg

Business / Professional: from EUR 199/year* | Enterprise: custom quote

Monday - Friday, 09:00 - 18:00 | Critical incidents: initial response within 2 hours

* Starting price and licensing scope are specified in the quote. NIS2 features support compliance and do not represent regulatory certification.

CyberGuardian XDR is a product of CyberGuardian Security EOOD, Bulgaria. All rights reserved © 2026.