

CyberGuardian XDR

Ръководство за потребителя

Корпоративна киберзащита за организации от всякакъв мащаб



CyberGuardian XDR — засича и неутрализира заплахи в реално време

MITRE ATT&CK Coverage

NIS2 Compliance Support

SSL A+

Windows EDR / XDR

cyberguardian.bg | cgs.xdr@gmail.com

Какво е CyberGuardian XDR?

Платформа от ново поколение за разширено засичане и реакция

CyberGuardian XDR е платформа от ново поколение за разширено засичане и реакция, създадена за организации, които изискват корпоративна защита без корпоративна сложност. Инсталирана на Windows машини, осигурява засичане на заплахи в реално време, автоматична реакция, покритие на MITRE ATT&CK framework, подкрепа за NIS2 и двуезичен интерфейс БГ/ЕН — от един лек агент, инсталиращ се за минути.

1. Dashboard

Това е първата страница, която виждате — цялата картина на защитата ви на един екран. Три ключови числа показват моментното състояние: общ брой инциденти, критичните и непрегледаните. Разделът Needs Your Attention автоматично приоритизира какво изисква действие веднага. Security Posture Score обобщава здравето на цялата ви инфраструктура в едно число. Системата разпознава и кога едната техника доминира в детекциите — и ви насочва към FP Control за прецизиране.

ТОВА ВИ ДАВА

отговор на въпроса „в безопасност ли съм?“ за секунди, без да обикаляте десет екрана.

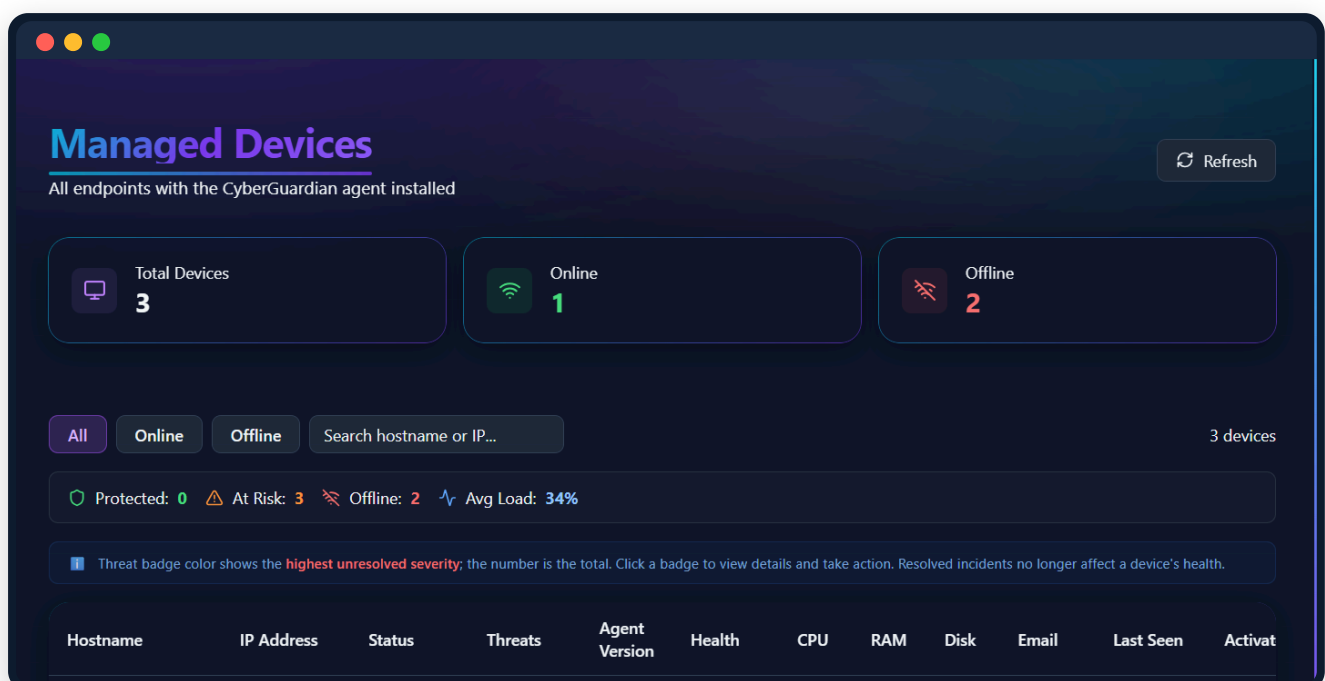


2. Managed Devices

Централен изглед на всички компютри с инсталиран агент. Виждате общия брой устройства, колко са онлайн и колко офлайн в момента. За всяко устройство — адрес в мрежата, статус на връзката, брой открити заплахи по ниво на сериозност, версия на агента, натоварване на процесора, паметта и диска и кога последно е било активно. Цветните индикатори за заплахи показват най-сериозния нерешен инцидент. Търсене и филтриране по име или статусви извеждат конкретна машина за секунди.

ТОВА ВИ ДАВА

виждате състоянието на всеки компютър в организацията от едно място — вместо да проверявате всяка машина поотделно.



3. Crash Telemetry

Ако агент на някой компютър срещне сериозен проблемой автоматично докладва това и вие го виждате веднага, с пълния контекст. Когато един и същ проблем засегне няколко машини, системата ги групира — веднага личи кое е широко разпространено и кое е единичен случай. Бутонът Contact Support изпраща заявката директно по имейл с готовата диагностика. Когато всичко е наред, страницата показва „All agents healthy“.

ТОВА ВИ ДАВА

решавате проблемите, докато са малки, вместо да ги откривате късно.



Crash Telemetry

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

Contact Support

Refresh



All agents healthy

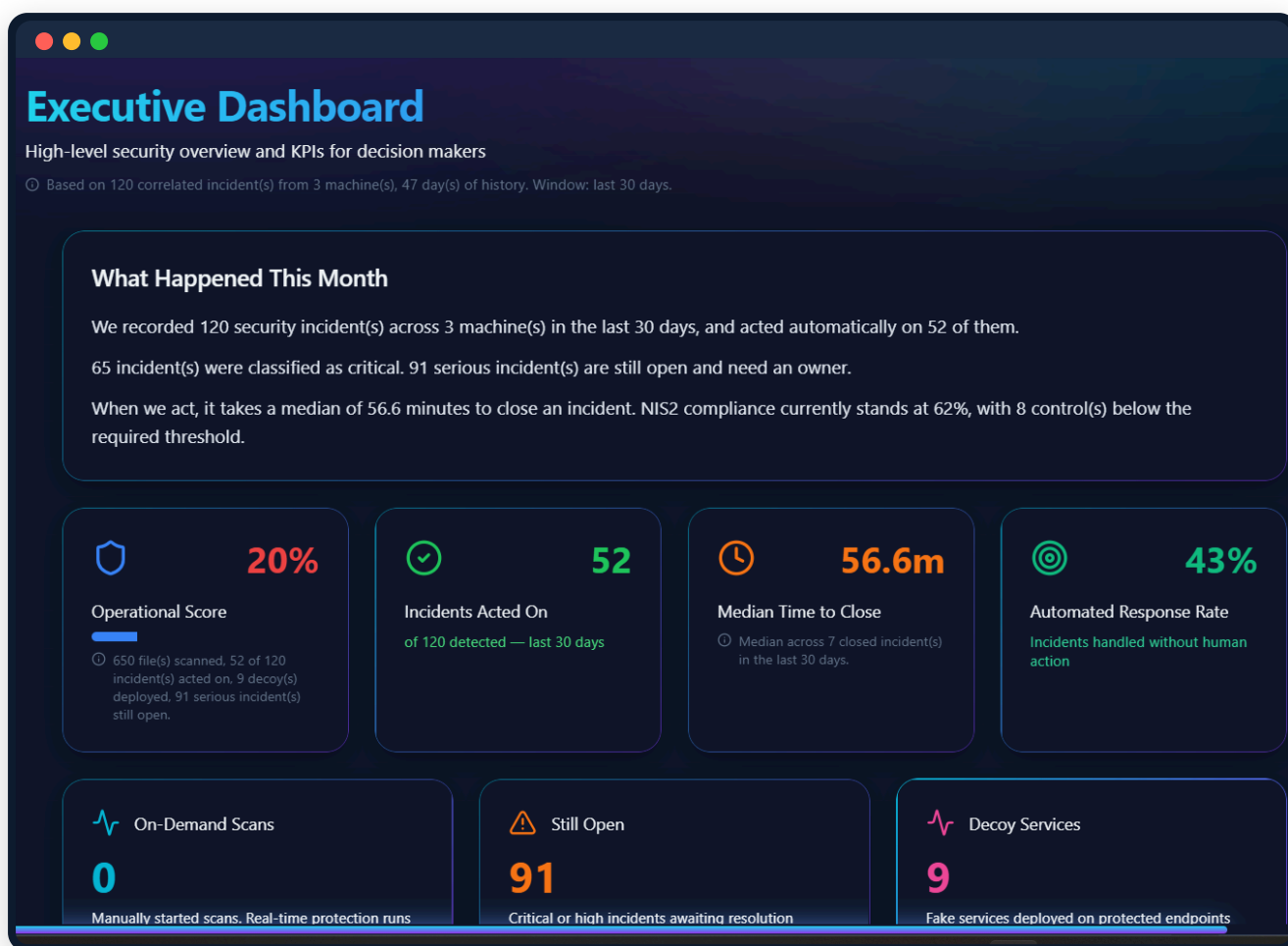
No crashes reported. Your agents send a report the moment they panic, so this page stays empty as long as your devices are stable.

4. Executive Dashboard

Страницата за ръководството обобщава месеца на разбираем език: колко инцидента са регистрирани, колко от тях са обработени автоматично, колко остават отворени. Ключови показатели: Operational Score, дял на инцидентите с автоматична реакция и средно време за приключване на инцидент. NIS2 Board Risk Overview превежда техническото съответствие на бордов език — процент на готовност и брой контроли под изискуемия праг.

ТОВА ВИ ДАВА

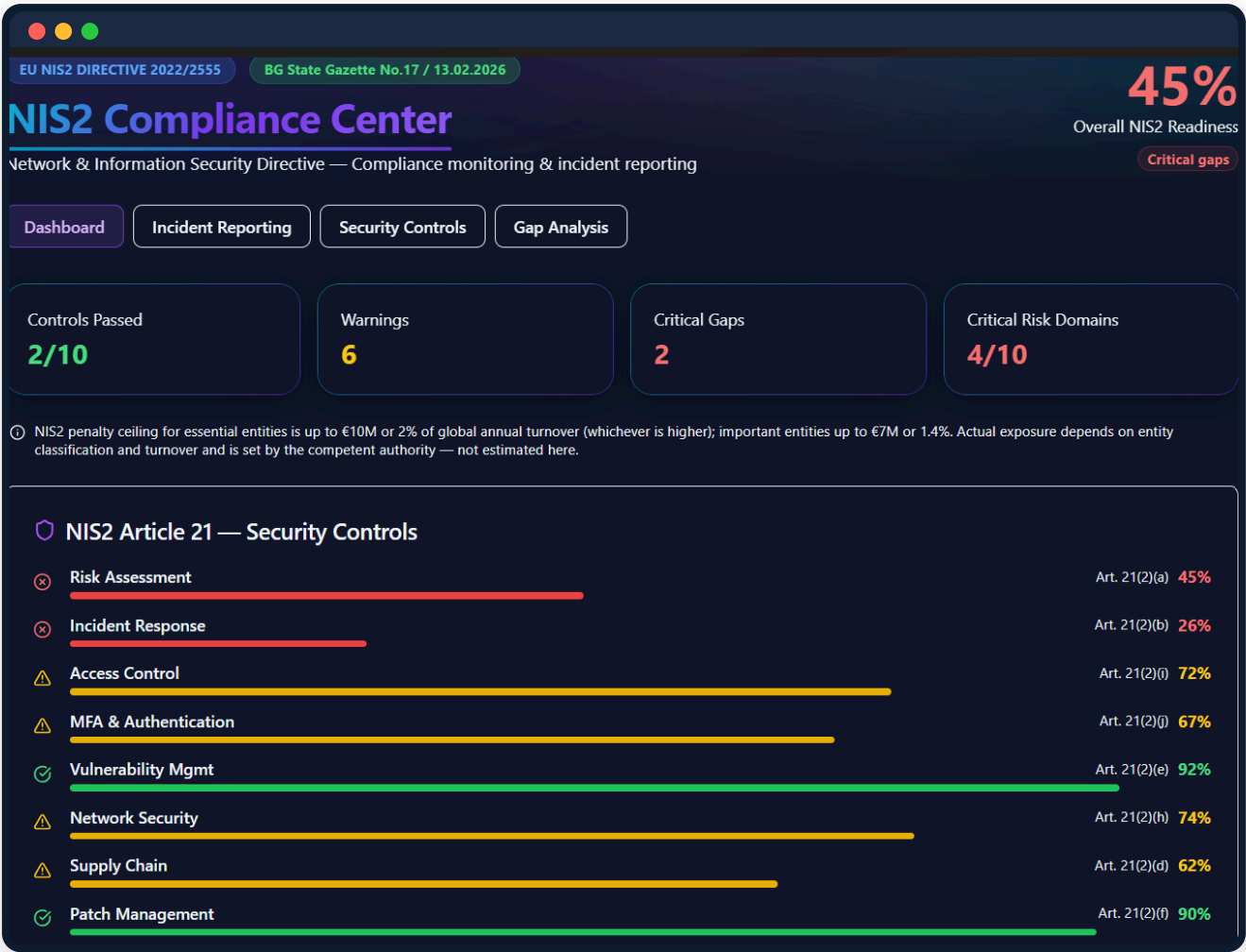
ръководството разбира за минути какво се е случило и къде стои организацията спрямо изискванията за превод от техническия екип.



5. NIS2 Compliance

Вградена автоматична проверка спрямо изискванията на Директива NIS2 чл. 21 и Закона за киберсигурност (ДВ бр. 17 / 13.02.2026)

CyberGuardian XDR подпомага оценката на организацията спрямо приложимите изисквания. Санкциите при несъответствие могат да достигнат до €10 000 000 според категорията на субекта и приложимия режим. Платформата подпомага работата по 10-те контролни домейна по чл. 21, генерира структурирани доклади и автоматизира хронологията по чл. 23 при инцидент.



Виждалте отворените врати преди някой друг.	Хващате „забравените“ акаунти — любимия вход на хакерите.
MFA & Authentication Проверява Windows Hello, защитата на отдалечения достъп и защитата на паролите в паметта. Открадната парола сама по себе си престава да е достатъчна.	Incident Response Следи журнала за сигурност в реално време за неуспешни влизания и повишаване на права. Опитът за пробив се вижда още при „чуването“.
Supply Chain Security Сканира приложенията за зловреден софтуер, невалидирани издатели и остарели версии. Знаете какво реално е инсталирано и кое е риск.	Risk Assessment Събира резултатите от всички NIS2 домейни в един претеглен резултат. Едно число за борда, детайлите за техническия екип.
Cyber Hygiene & Training Автоматизиран одит на заключване на екрана, USB носители и защитни настройки. Малките пропуски, през които стават големите пробиви — хванати навреме.	NIS2 Executive Report Структуриран compliance доклад за преглед и подготовка за подаване към CERT-BG. Подготовката на доказателства и отчетност става значително по-бърза.
Policy Generator Генерира готови Word документи с политики по сигурност, персонализирани за вашата компания. Задължителните документи за минути вместо седмици.	Training Tracker Централизиран регистър на задължителните обучения с проследяване на валидността им. При проверка показвате регистъра — не събирате сертификати по имейли.
Backup Security Monitor Проверява автоматично дали имате активен, защитен и актуален backup, включително отдалечено копие. Когато най-лошото се случи, има от какво да се възстановите.	

Threats

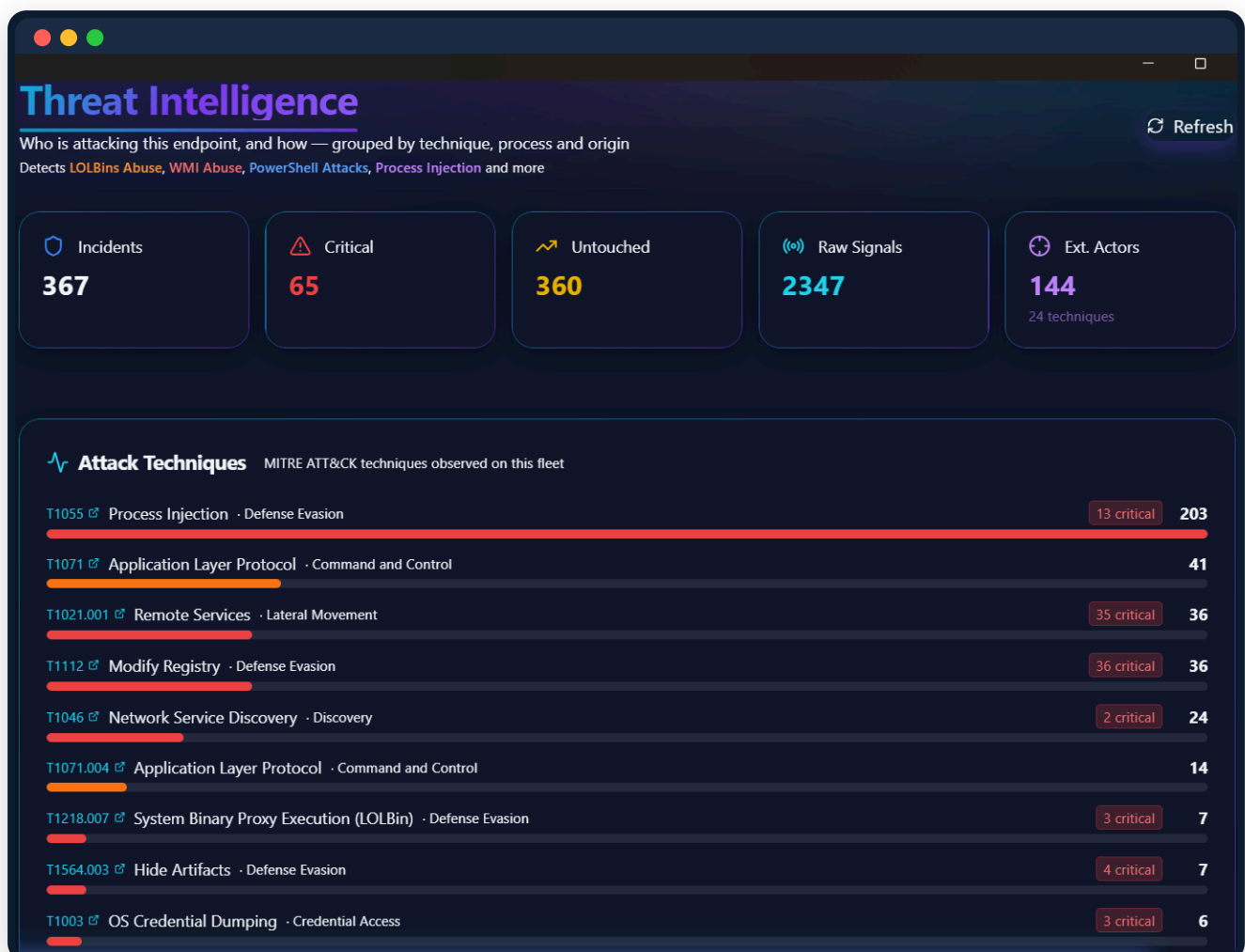
Пълна картина на заплахите — от сигнали до атакуващи техники и разузнавателни данни

6. Threats — Threat Intelligence

Тук се събират всички засечени заплахи — от злоупотреба със системни инструменти и PowerShell до опити за инжектиране на код. Виждате общия брой инциденти, критичните, необработените и Raw Signals, плюс броя на уникалните External Actors. Attack Techniques показва всяка MITRE ATT&CK техника, засечена във флота, с брой инциденти и критичност. Бутонът AI Response Playbook генерира персонализиран наръчник за реакция.

ТОВА ВИ ДАВА

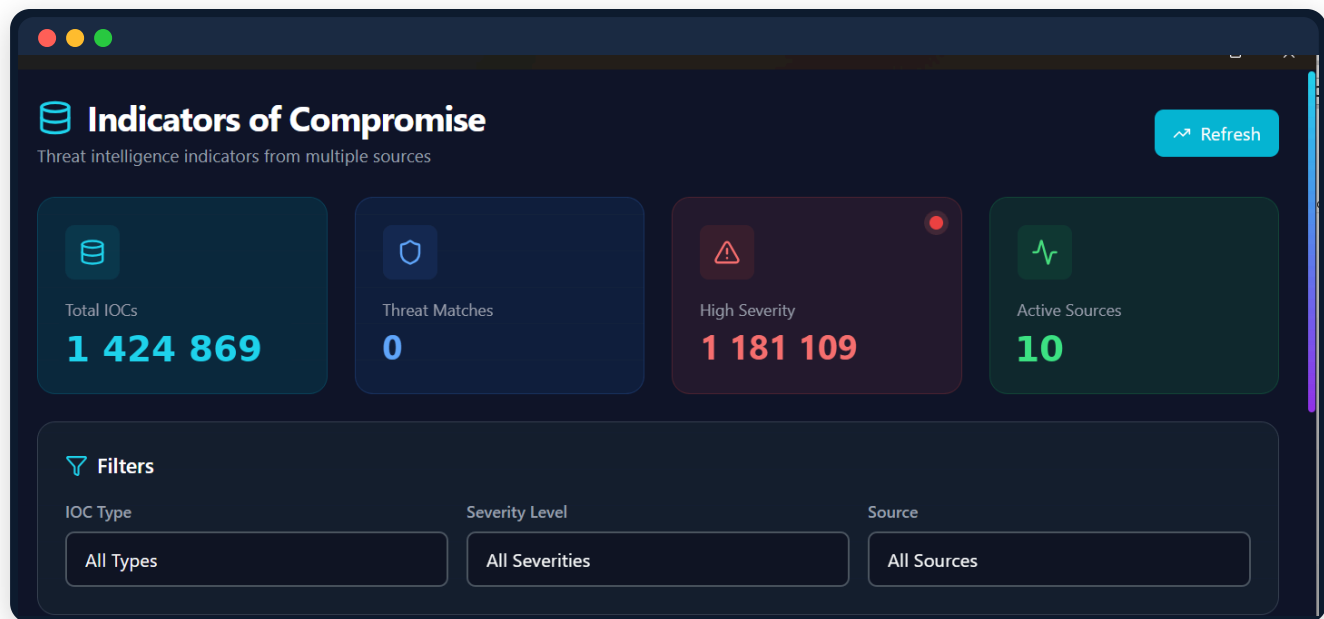
никога не стоите пред заплахата с въпроса „и сега какво?“ — системата ви казва какво точно да направите.



7. Threats — Indicators of Compromise (IOCs)

Базата данни с индикатори за компрометиране съдържа около 1 424 869 активни записа от 10 независими източника. Всяко IP, домейн или файлов хеш, свързан с известна злонамерена дейност, е тук. Когато няколко независими източника докладват един и същ индикатор, доверието в него расте автоматично. Филтрирате по тип IOC, ниво на сериозност и източник.

ТОВА ВИ ДАВА



8. Threats — Threat Intelligence Feeds

Системата се захранва с данни от водещите световни източника за заплахи — над 1 000 000 активни индикатора за компрометиране, обновявани автоматично на всеки 6 часа. Виждате всеки източник, статуса му и броя IOC-ове, които носи. Когато няколко независими източника докладват една и съща заплаха, доверието в нея се повишава автоматично.

ТОВА ВИ ДАВА

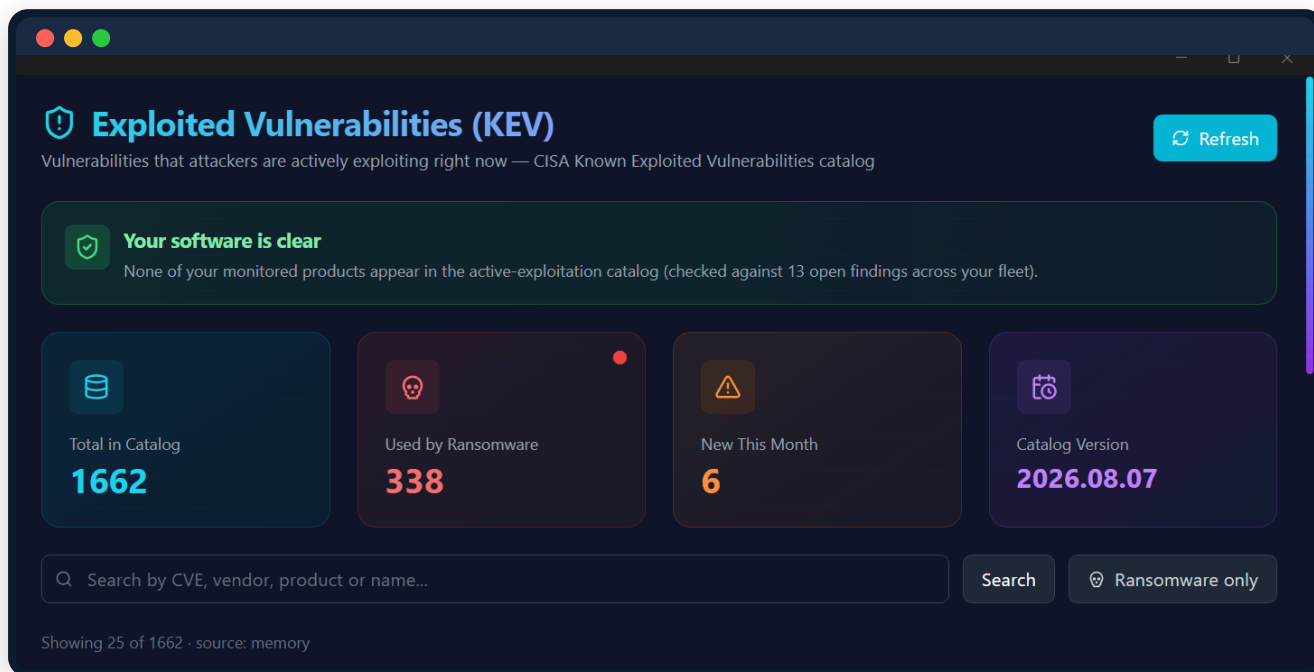
новоразкрити индикатори се добавят при автоматичните обновявания на threat intelligence.

9. Threats — Exploited Vulnerabilities (KEV)

Всеки месец се откриват хиляди уязвимости, но само малка част се използват реално от атакуващи. Тази страница следи именно тях — от каталога Known Exploited Vulnerabilities на CISA (държавен американски източник) Системата сверява каталога със софтуера на вашите компютри и ви предупреждава при съвпадение. В момента каталогът съдържа **1 662** записа, от които **338** са свързани с ransomware. Ransomware уязвимостите са маркирани като най-спешни.

ТОВА ВИ ДАВА

конкретен отговор на „застрашен ли съм точно аз, точно сега?“ — насочвате усилията там, където опасността е реална.



Detection

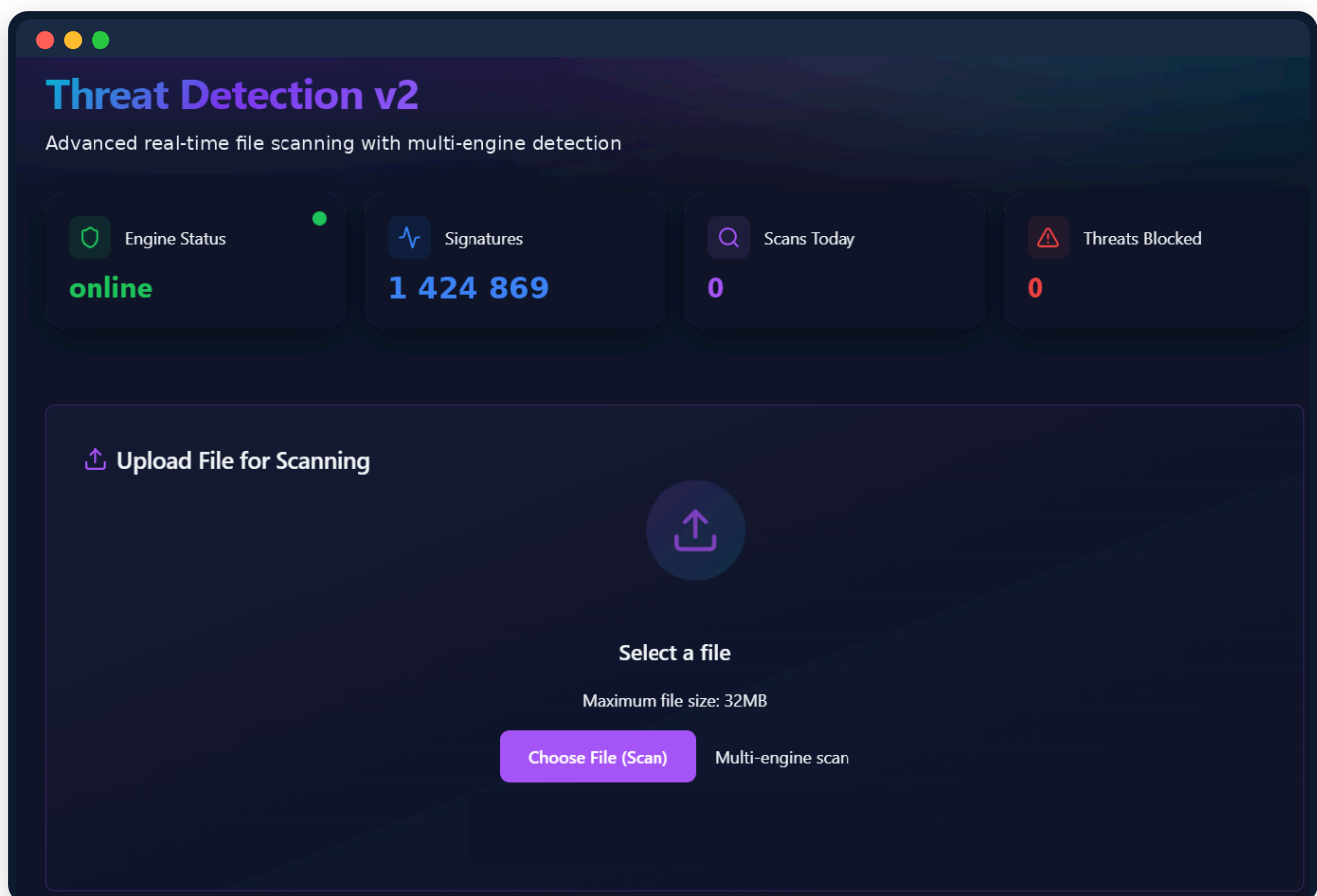
Многослойно засичане на заплахи — сигнатури, поведение и реално-времево блокиране

10. Detection — Threat Detection v2

Тук управлявате самото засичане на заплахи. Виждате размера на активната база за засичане (показана в интерфейса като Signatures) - около 1 424 869 записа - и режима на работа. Сканирането комбинира сигнатури, анализ на ентропията, PE инспекция и облачна проверка. Можете да качите конкретен файл за проверка чрез Multi-Engine Scan.

ТОВА ВИ ДАВА

виждате не само че нещо е засечено, а точно какво е направила системата — спряно, отменено или само под наблюдение.

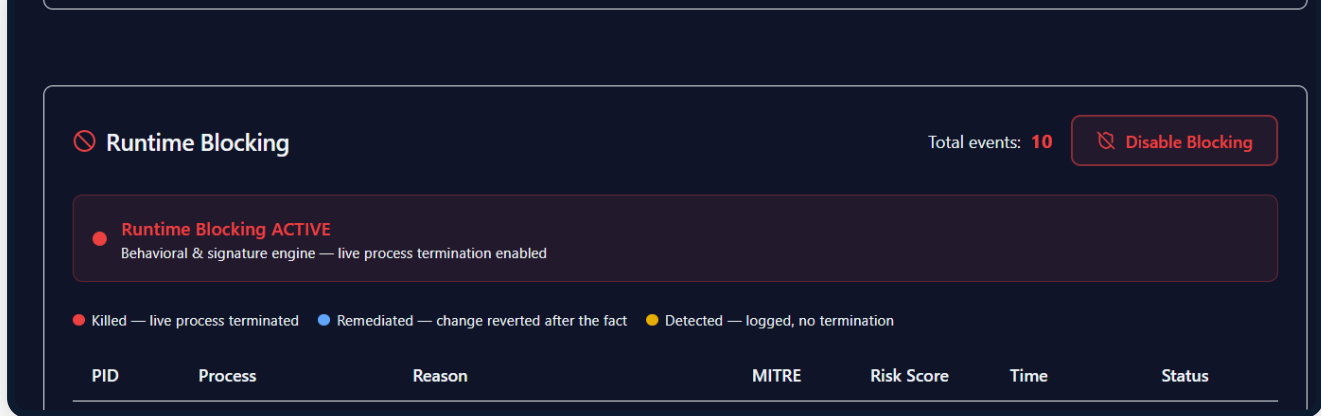


11. Detection — Runtime Blocking

Runtime Blocking следи всичко, което се изпълнява на компютъра в реално време. Когато засече подозрително поведение, реагира незабавно: процесът е спрян напълно (Killed), промяната е отменена след установяване (Remediated) или събитието е записано за преглед (Detected). Всяко събитие е свързано с MITRE ATT&CK техника и Risk Score.

ТОВА ВИ ДАВА

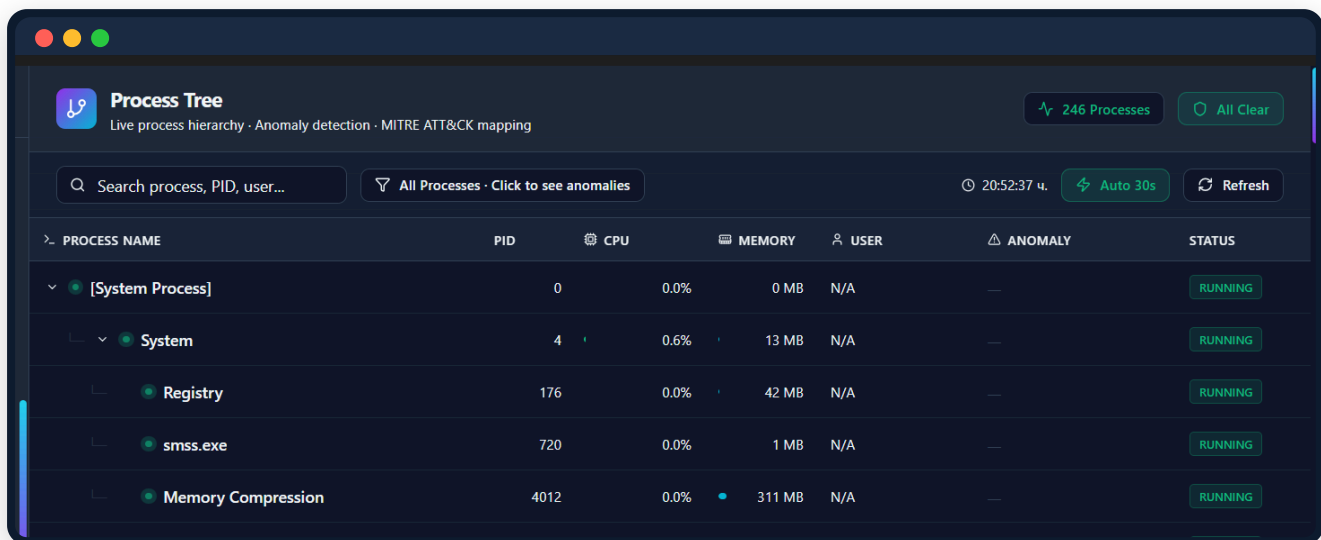
запахата е спряна в момента на изпълнение — не след като вредата вече е нанесена.



12. Detection — Process Tree

Визуална карта на всичко, което работи на компютъра в момента — 246 процеса, наредени по йерархия родител-дете. Системата автоматично маркира подозрителните връзки: програма, стартирана от неочакван родител, опит за инжектиране на код, злоупотреба с легитимни инструменти. Автоматично опресняване на всеки 30 секунди.

ТОВА ВИ ДАВА
хакерите обичат да се крият зад легитимни процеси — тук маскировката им става видима с един поглед.



Protection & Scans

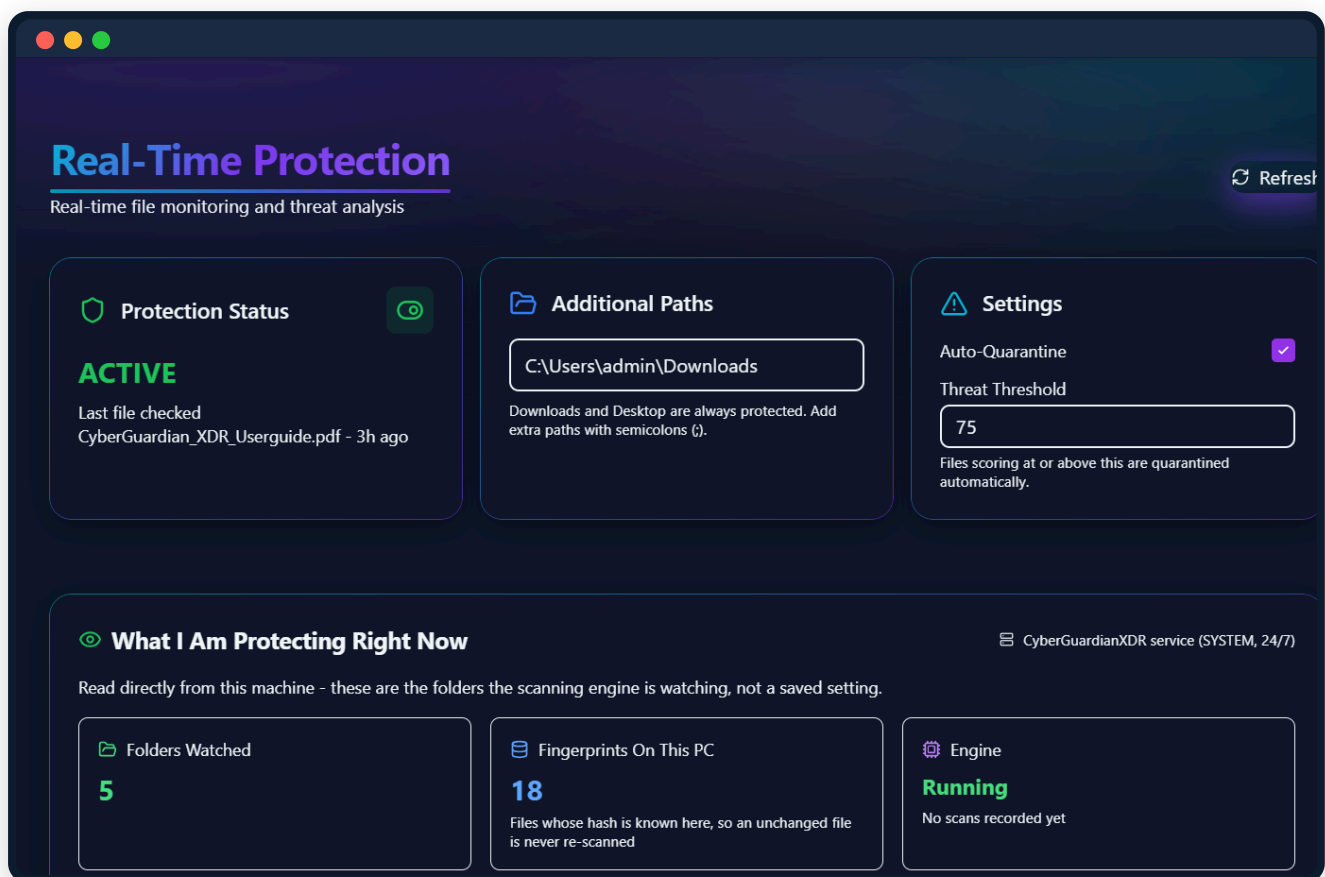
Реално-времева защита на файловете и ръчно сканиране при нужда

13. Real-Time Protection

Тази страница следи файловата система непрекъснато — всяка промяна се анализира автоматично в момента, в който се случи. Опасните файлове отиват в карантина сами, без ваша намеса. Настройвате чувствителността (Threat Threshold) — колко строго да се прилага автоматичното действие. Разделът What I Am Protecting Right Now показва точно кои папки са под наблюдение и колко файлови отпечатъка е запомнила системата на тази машина.

ТОВА ВИ ДАВА

спокойствие, че компютърът се пази сам 24/7 — дори когато никой не гледа екрана.



14. Scans — Security Scans

Оттук стартирате проверка на компютъра, когато пожелаете. Три профила: Quick Scan (~2 мин, 100 файла), Standard Scan (~10 мин, 1 000 файла) и Deep Scan (~30+ мин, 10 000 файла). Съмнявате се в конкретен файл? Качвате го и системата го анализира чрез Multi-Engine File Scanner. Данните не напускат машината ви — сканирането е локално.

ТОВА ВИ ДАВА

контрол в ръцете ви — проверявате всичко подозрително веднага, а рутинните проверки вървят сами.

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:

*

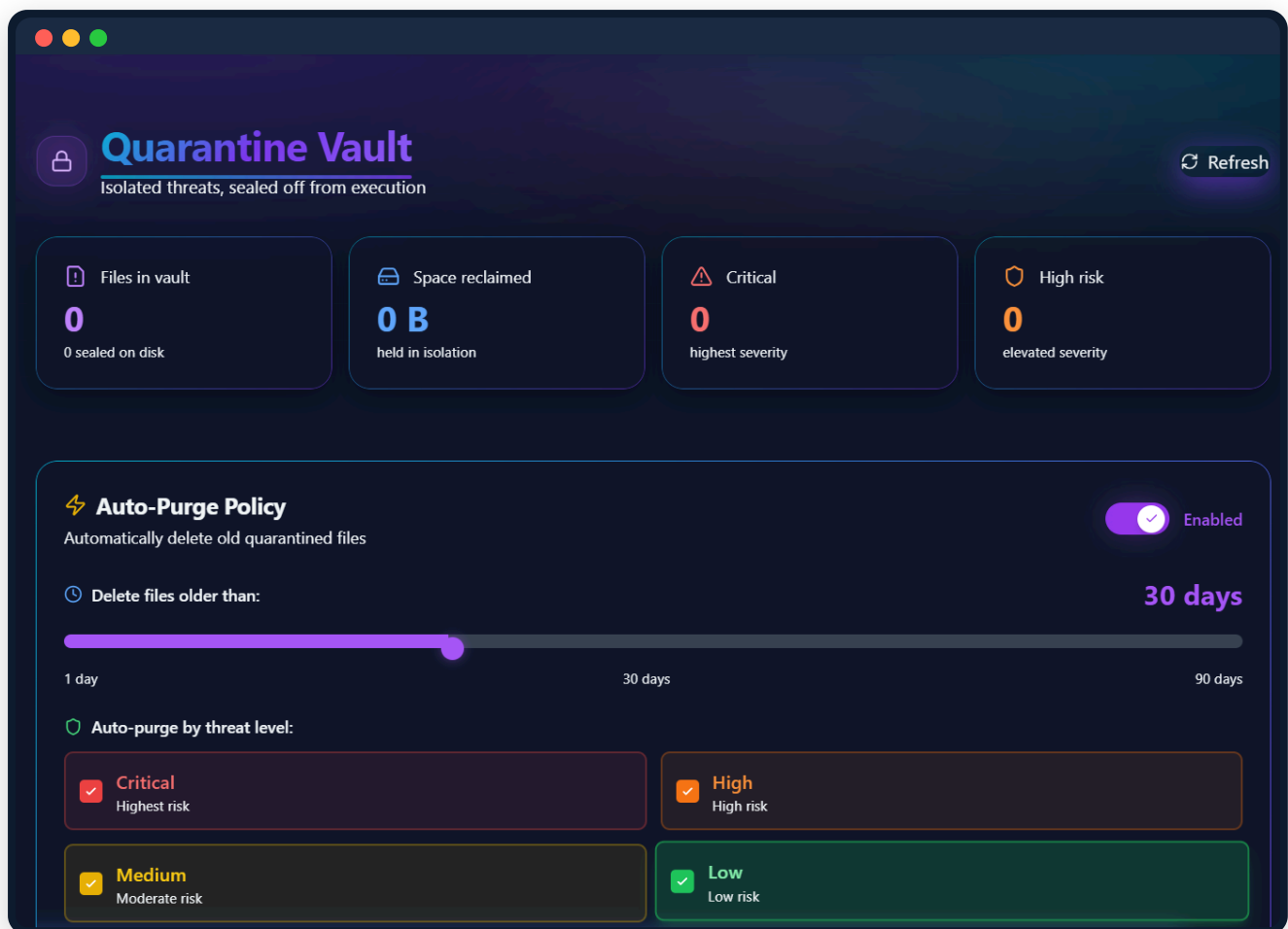
Start Scan

15. Quarantine Vault

Тук отиват заловените опасни файлове — изолирани, безопасни, но не изтрити. Виждате броя файлове в хранилището, заетото място и нивата на сериозност. Auto-Purge Policy автоматично почиства стари записи по зададен от вас период (1–90 дни) и ниво на заплаха. Всеки файл може да бъде прегледан и възстановен при фалшива аларма.

ТОВА ВИ ДАВА

заловеното е обезвредено, но нищо не е загубено — фалшива аларма се възстановява с един клик.



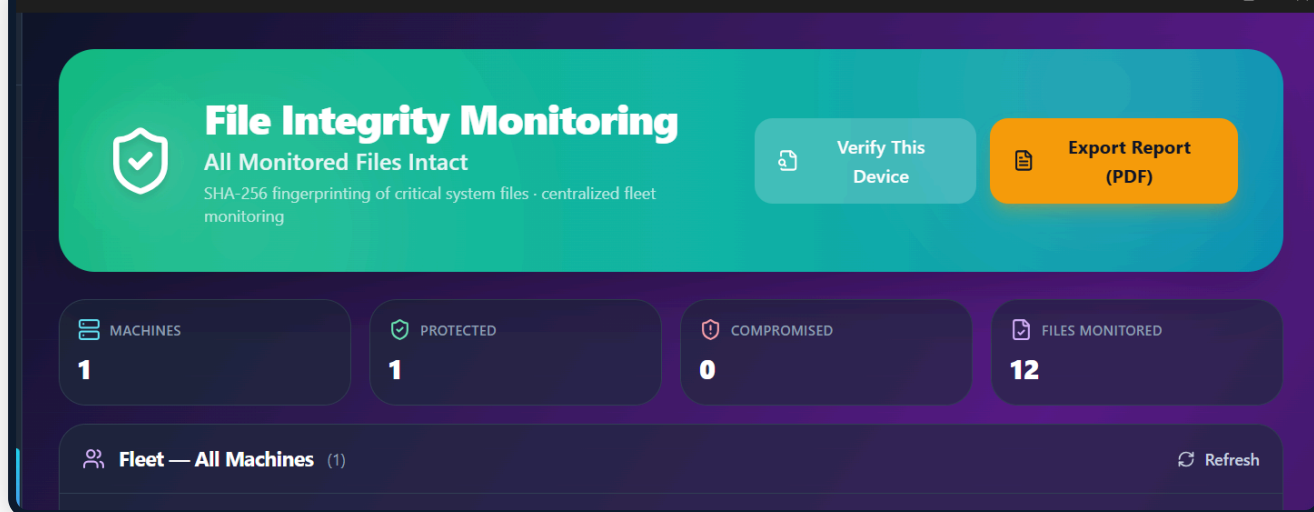
16. File Integrity Monitoring

Следи критичните системни файлове за неотризирани промени чрез криптографски контролни суми (SHA-256). Обобщен fleet изглед на всички машини: брой защитени, компрометирани и наблюдавани файлове. За избрана машина виждате детайлна разбивка и можете да генерирате PDF доклад или да стартирате верификация.

ТОВА ВИ ДАВА

тихите подмени на системни файлове стават видими веднага — на всяка машина във флота, с една проверка.





17. Tamper Protection

Първата цел на всеки сериозен хакер е да изключи защитата ви. Тази страница показва обобщен Protection Score (100/100) и четири защитни пласта: Config Integrity (VALID), Ransomware Canary (ARMED — 3 капана активни), Watchdog (ACTIVE) и Process Protection (ACTIVE — 13 критични процеса пазени). Защитата включва механизми за самозащита.

ТОВА ВИ ДАВА

многослойна защита, проектирана да затруднява тихото изключване - с видимост към техниките на атака, срещу които работи.



Remediation

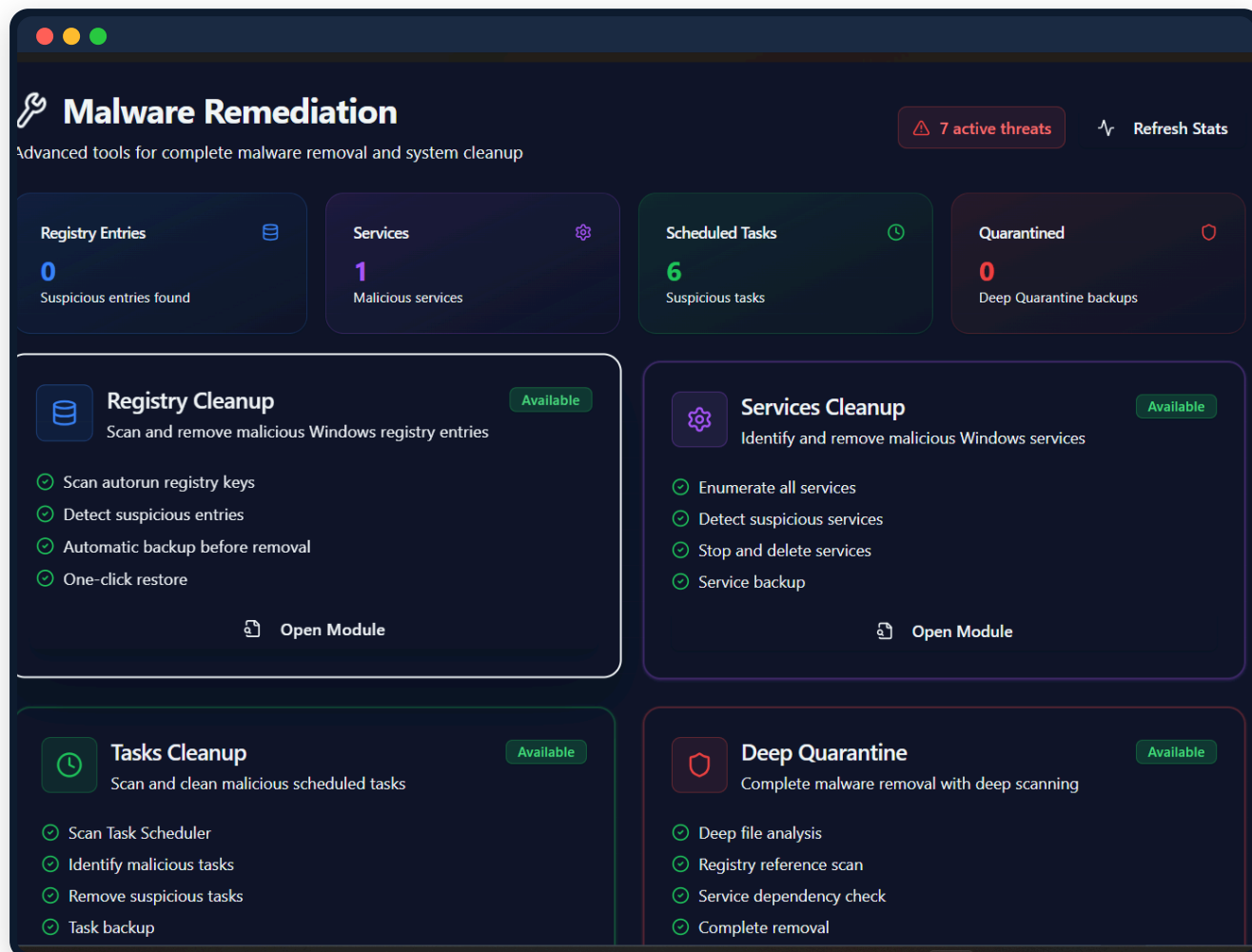
Цялостно отстраняване на зловреден софтуер и механизми за устойчивост

18. Malware Remediation

Стандартният антивирус трие файла, но зловредният софтуер оставя котви в системата — в регистъра, услугите и задачите. Четири специализирани инструмента ги премахват из корен: Registry Cleanup (сканира и премахва злонамерени записи в регистъра с автоматичен backup преди изтриване), Services Cleanup (открива и спира злонамерени Windows услуги), Tasks Cleanup (премахва злонамерени планирани задачи) и Deep Quarantine (пълнен анализ и отстраняване). Всичко работи локално — данните не напускат машината.

ТОВА ВИ ДАВА

намалявате риска заплахата да се възстанови след рестарт.



Insights

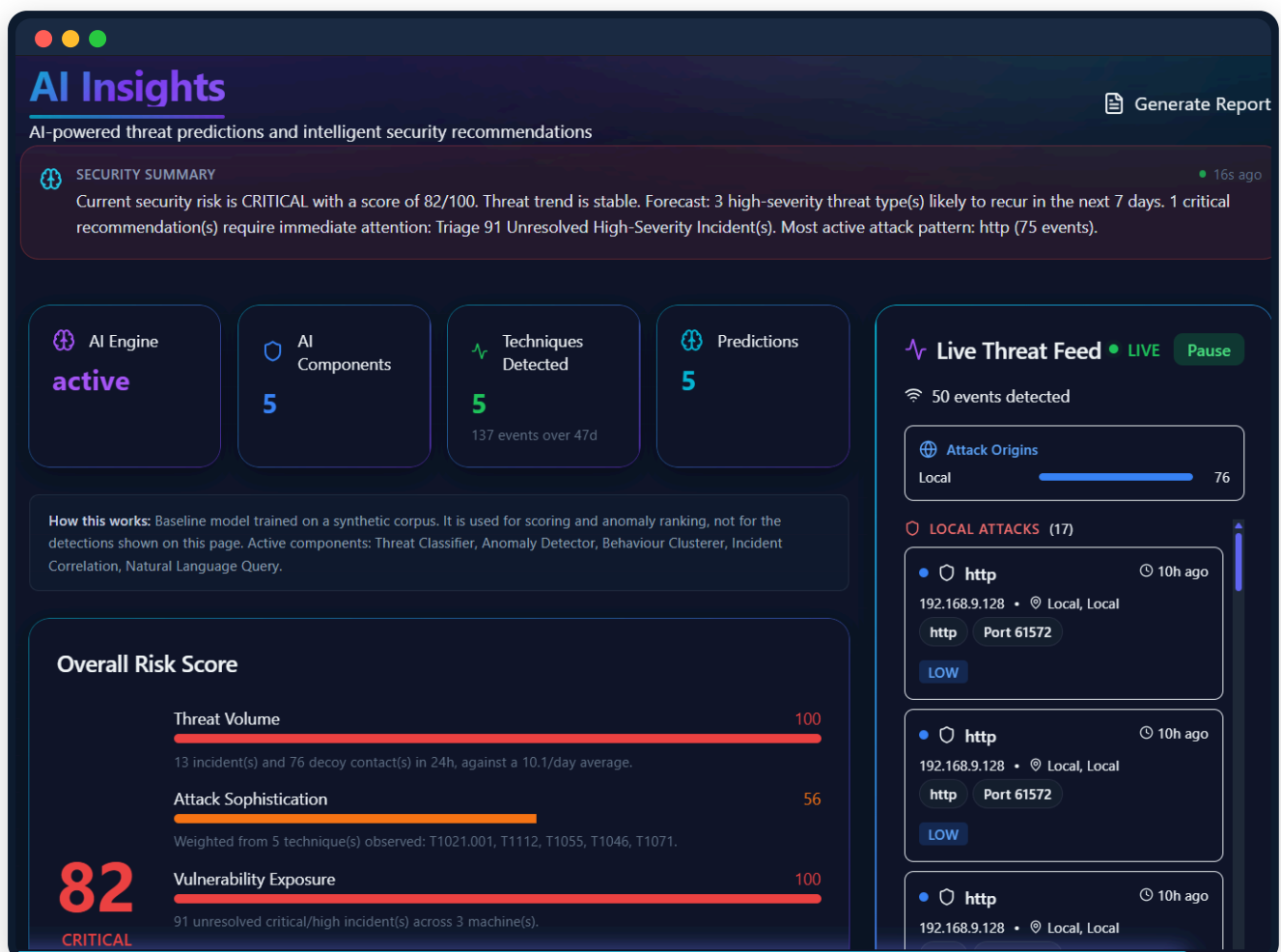
Изкуствен интелект анализира рисковете и дава готов план за действие

19. AI Insights

Тук изкуственият интелект анализира непрекъснато всички данни от средата ви и дава кратко обобщение на естествен език — какъв е рискът в момента и кое изисква внимание първо. Overall Risk Score от 0 до 100 се разбива на пет съставни фактора: Threat Volume, Attack Sophistication, Vulnerability Exposure, Incident Frequency и Security Posture. Live Threat Feed показва постъпващите заплахи в реално време с класификация по произход.

ТОВА ВИ ДАВА

виждате ясно колко сте застрашени в момента и защо — вместо да тълкувате сами графики и числа.

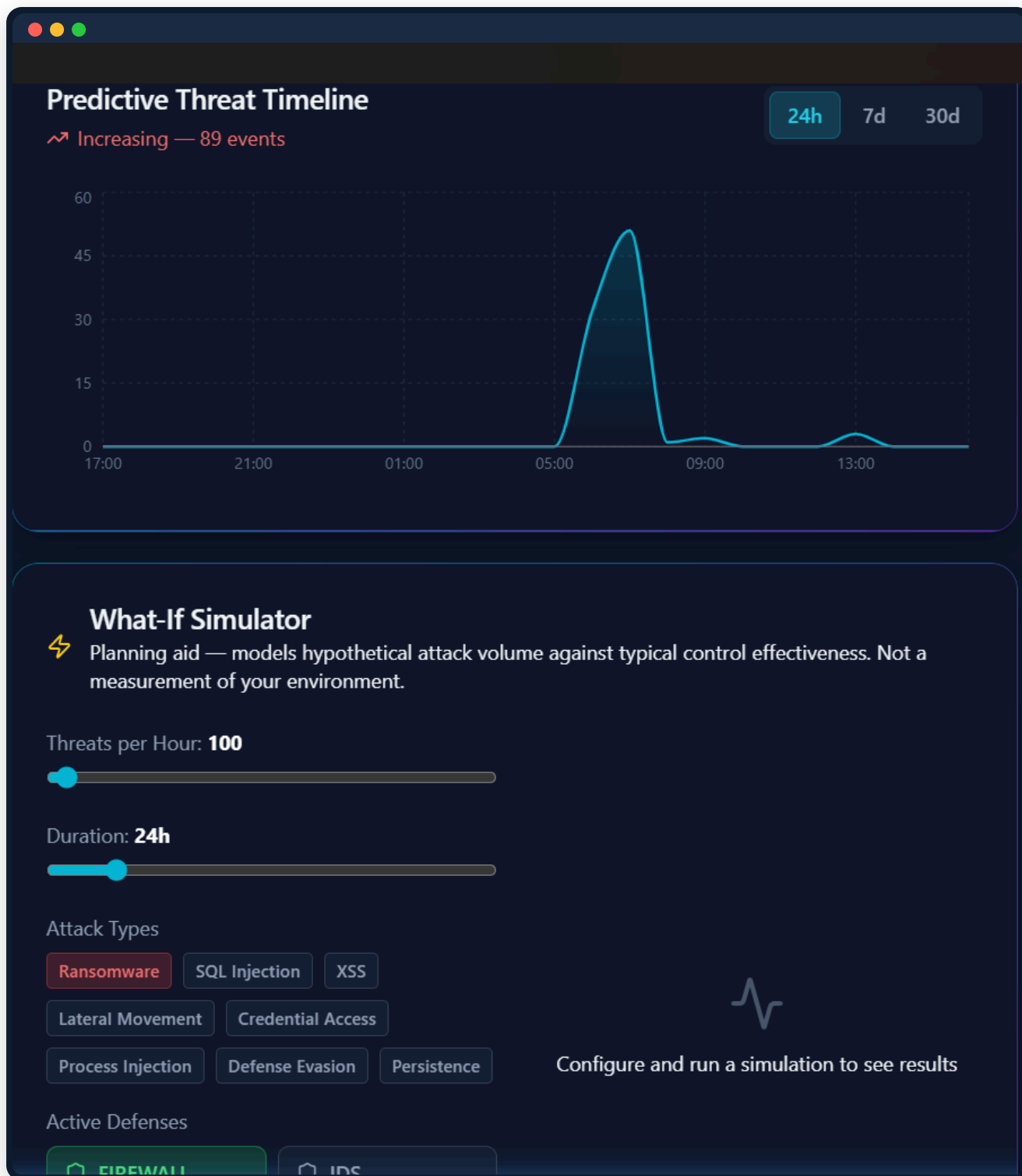


20. Predictive Threat Timeline & What-If Simulator

Predictive Threat Timeline показва как расте или спада активността на атаки в последните 24ч, 7 дни или 30 дни. What-If Simulator е инструмент за планиране: моделирате хипотетичен сценарий — вид атака, интензитет, продължителност — и виждате как текущите ви защити биха се справили. Инструментът е изрично обозначен като симулация, не като измерване на реалната среда.

ТОВА ВИ ДАВА

знаете не само какво се случва, но и накъде се движи тенденцията — и можете да планирате превантивно.



21. Behavioral Anomalies & Attack Chain Visualization

Behavioral Anomalies сравнява последните 24 часа с 7-дневната база — показва дали обемът на заплахите, honeypot събитията, засегнатите машини и критичните заплахи са над или под нормалното. Attack Chain Visualization проследява прогреса на атаката по машина: Reconnaissance → Exploitation → Lateral Movement → Exfiltration, с брой засегнати машини, общо събития и критични вериги.

ТОВА ВИ ДАВА

виждате не само отделни инциденти, а пълната картина на атаката — на кой етап е и кои машини са засегнати.



22. AI Recommendations

Изкуственият интелект превръща анализа в конкретен списък задачи, подредени по приоритет. За всяка препоръка виждате защо е предложена, очакваното време за изпълнение, сложността и какъв ефект ще има върху сигурността ви — включително директна връзка към съответното NIS2 изискване. Филтрирате по приоритет и сортирате по важност.

ТОВА ВИ ДАВА

не просто списък с проблеми — готов план за действие, с приоритет и оценка на усилияето за всяка стъпка.

 **AI Recommendations**

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

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

© 2026 CyberGuardian Security EOOD

ML Models & Incidents

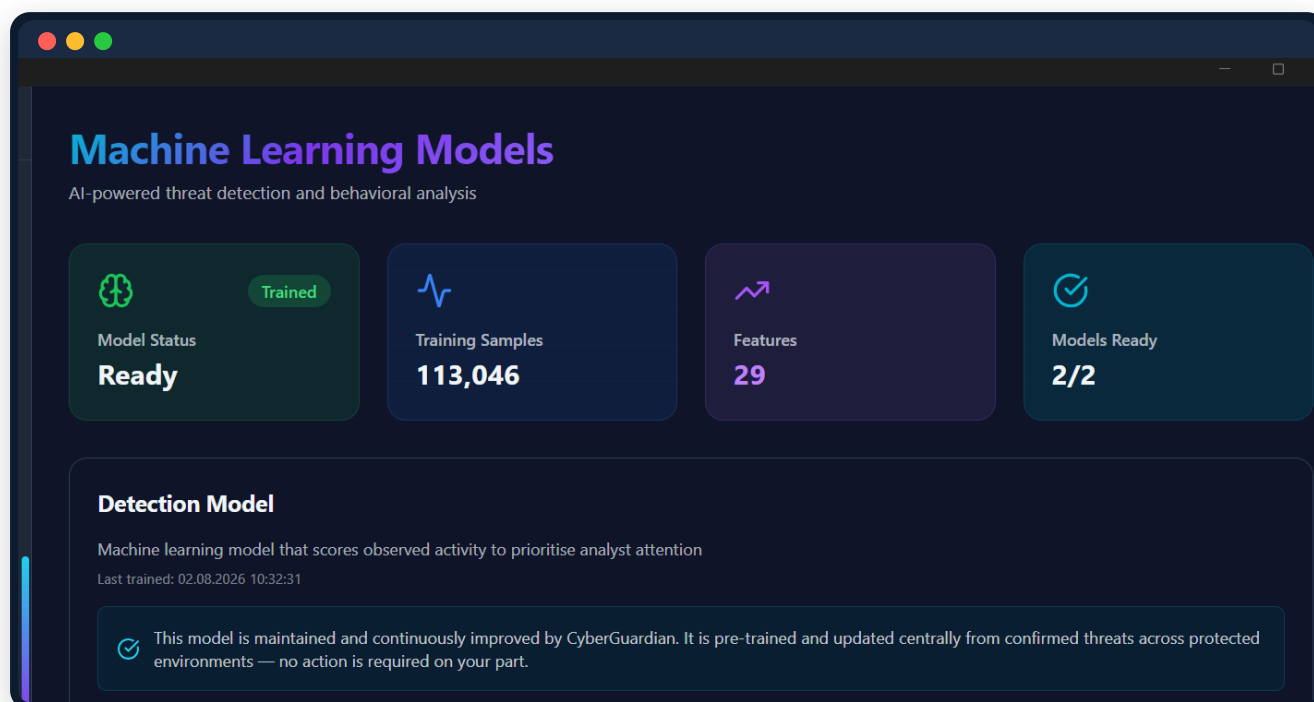
Машинно обучение зад детекциите и корелирани инциденти с NIS2 докладване

23. Machine Learning Models

Тук виждате и управлявате изкуствения интелект зад детекциите — статус на моделите (Ready / Trained), брой обучаващи проби и независими характеристики, по които се вземат решенията. В момента: **113 046** обучаващи проби, **29** характеристики, **2/2** модела готови. Моделите се поддържат и обновяват централно от CyberGuardian от потвърдени заплахи в защитените среди — не е необходимо действие от ваша страна.

ТОВА ВИ ДАВА

AI модели, които се обновяват с потвърдени обучаващи данни - без ръчна поддръжка от ваша страна.



24. Correlated Incidents

Повечето сериозни атаки не са едно събитие, а верига от стъпки. Тази страница свързва отделните сигнали в общи инциденти с ниво на сериозност, достоверност и Auto-Response статус. Response Performance показва средното време за признаване, овладяване и разрешаване на инциденти. При инцидент, изискващ докладване по NIS2 чл. 23, бутоните за 24ч ранно предупреждение, 72ч уведомление и Final Report са директно до него.

ТОВА ВИ ДАВА

управлявате целия отговор на инцидента, с часовника по NIS2 пред очите си, от една страница.



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.

Всеки инцидент показва: машина, ниво на AI риск, достоверност и вердикт. Разгъвате инцидента и виждате пълния Attack Storyline — всяко събитие по хронологичен ред с MITRE техника. NIS2 deadlines показват обратното броене до крайния срок за докладване. Можете да добавите бележка към audit trail, да маркирате като False Positive или да разрешите инцидента.

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 ч.

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 ч.

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

Process: 192.168.192.92

25. FP Control

Системата разграничава легитимните системни процеси от маскираните заплахи чрез Suppression Rules и Trusted Processes. Suppression Rules позволяват да дефинирате комбинации процес + родителски процес + причина, при които алармата се потиска автоматично. Trusted Processes добавя процеси по име и SHA256 хеш. В момента: 14 правила, 6 доверени процеса, 5 автоматично потиснати.

ТОВА ВИ ДАВА

намаляват фалшивите положителни сигнали и насочват екипа към по-вероятните реални заплахи.



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

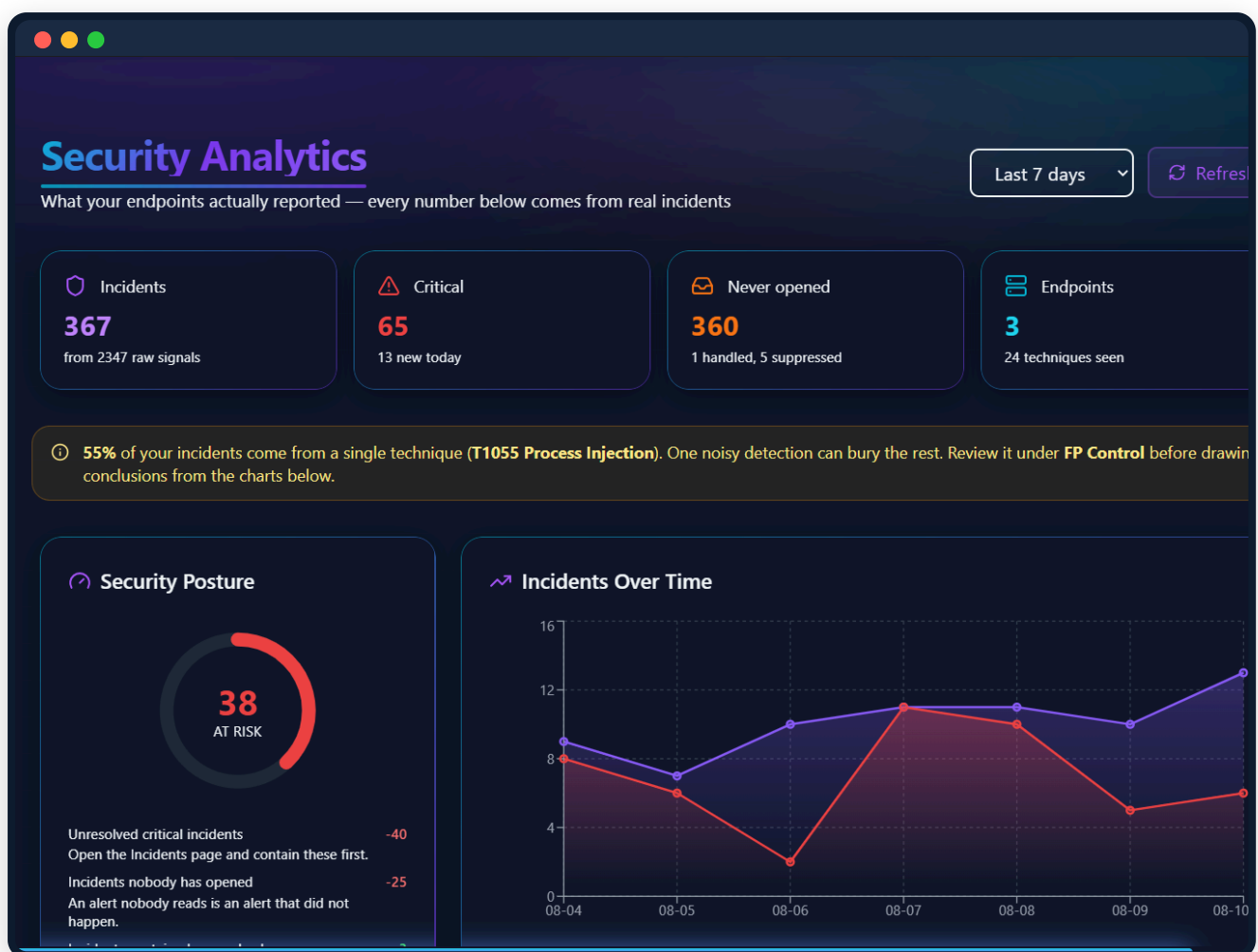


26. Security Analytics

Обобщена картина на всичко, което устройствата ви реално са докладвали — не прогнози, а данни от реални инциденти. Виждате инциденти, критичните, непрегледаните и задействаните endpoints за избран период (7 дни / месец). Security Posture Score обобщава здравето в едно число. Ако една-единствена техника доминира в статистиката, системата изрично го посочва и препраща към FP Control. Графиката Incidents Over Time показва тенденцията по дни.

ТОВА ВИ ДАВА

разчитате на реални данни от вашата среда — и системата сама ви предупреждава, когато шумна детекция може да изкриви картината.



27. Email & Phishing Scanner

Фишингът е атакуващ вектор №1. Скенерът се свързва с пощата ви чрез App Password и анализира всяко писмо многослойно — проверка на URL-и, домейни и прикачени файлове спрямо над 1 000 000 злонамерени индикатора. Настройките са в отделния раздел Settings. Виждате Scanner Status, броя сканирани писма, открити фишинг опити и безопасни писма.

ТОВА ВИ ДАВА

подозрителното писмо може да бъде маркирано преди служителят да кликне.

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

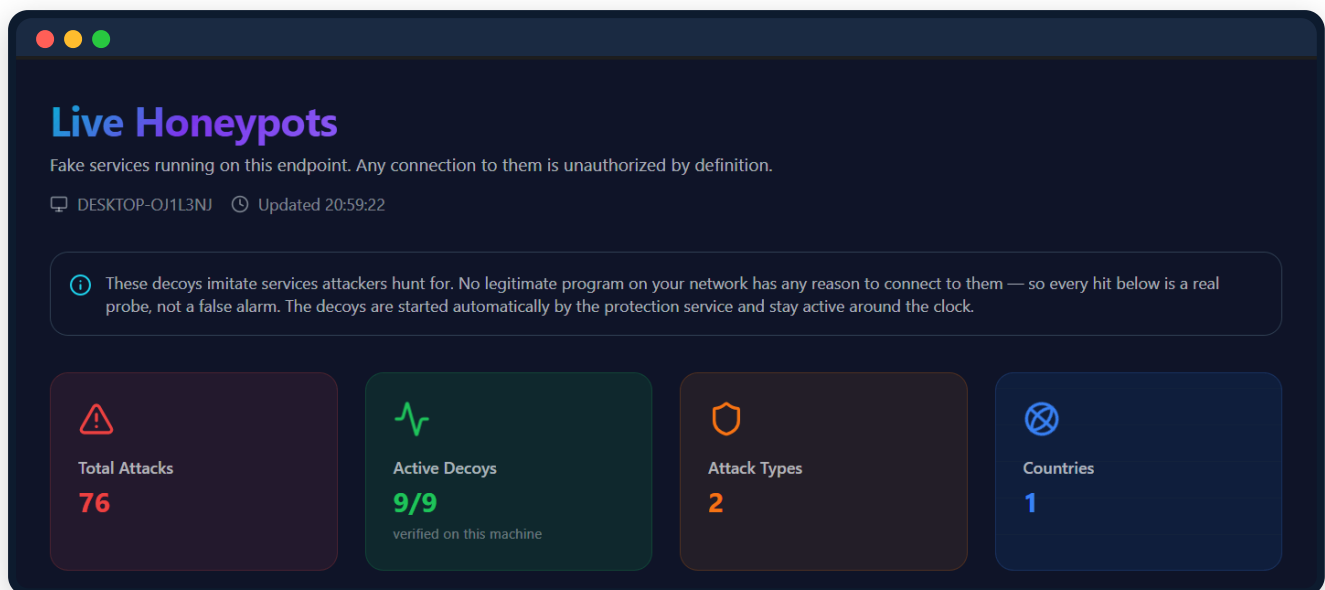
[Go to Settings](#)

28. Live Honeypots

Примамките са фалшиви услуги, работещи на endpoint-а, които изглеждат истински за атакуващия. Всяко свързване с тях се третира като силно подозрително, тъй като легитимните приложения по правило нямат причина да ги използват. Виждате: 76 общо атаки, 9/9 активни примамки (верифицирани на тази машина), 2 типа атаки от 1 страна. Примамките се стартират автоматично от защитната услуга и работят денонощно.

ТОВА ВИ ДАВА

обръщате играта — хакерът си мисли, че ви атакува, а всъщност ви показва точно как и откъде атакува.



29. Performance Monitor

Реално-времево здраве на машината и препоръки за оптимизация. Health Score от 0 до 100 показва общото здраве. Виждате CPU Usage, Memory Usage, Disk Usage и Top Process в реално време. Системата идентифицира тесните места и предлага конкретни подобрения. Export Report генерира PDF с пълния health анализ.

ТОВА ВИ ДАВА

защита, която следи да не пречи — виждате черно на бяло, че компютърът работи добре.



Performance Monitor

Real-time health of this machine and optimization insights

Export Report

Refresh

System Health Overview

Live status of this machine



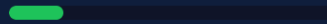
POOR

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

Тази страница пази работещите програми от манипулация. Следи в реално време: Service Status (Running), Total Processes (247) и Suspicious процеси (0). Advanced Monitoring е активен в Production режим с Auto-Monitoring и дава опции за ръчно Trigger Scan и Dismiss Alerts. Anti-Termination затруднява опитите на зловреден софтуер да изключи защитата, а Self-Healing я възстановява автоматично при срив.

ТОВА ВИ ДАВА

защита, проектирана да затруднява тихото изключване - една от първите цели на атакуващия.



31. Software Updates

Виждате точната версия на агента (текуща: 2.0.2 Sentinel, Built August 10, 2026) и пълната история на обновленията: 2 Major, 0 Minor, 2 Patch версии. Update Health показва кога е проверено последно, колко обновления са инсталирани и кой канал се използва (Stable). Автоматичното обновяване се управлява от тук.

ТОВА ВИ ДАВА

защитата ви е винаги актуална — и можете да го докажете с пълна одит-готова история.





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

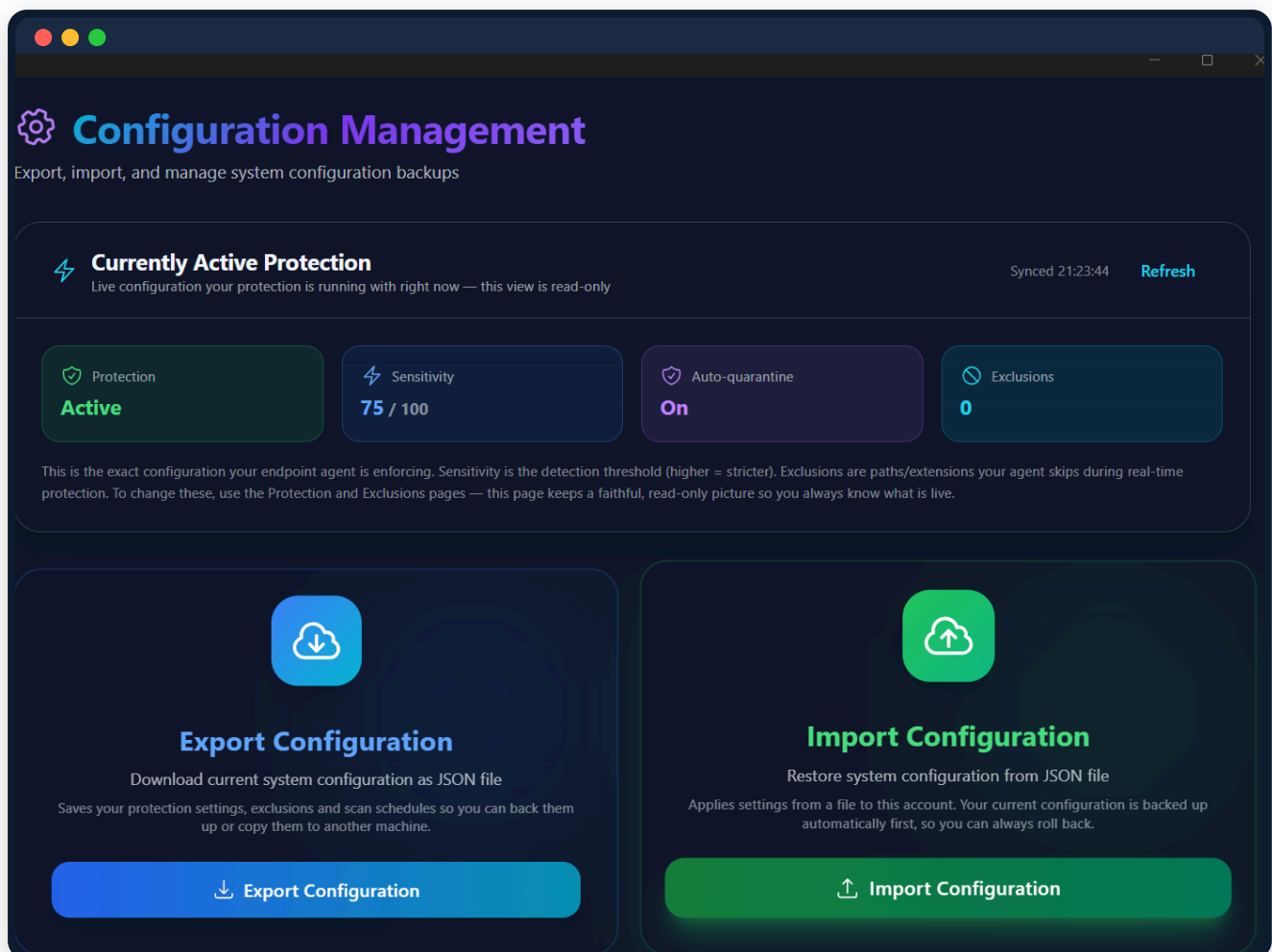
Check for Updates

32. Configuration Management

Тази страница показва точната конфигурация, която агентът прилага в момента - в реално време, в режим за преглед. Виждате: Protection (Active), Sensitivity (75/100), Auto-quarantine (On) и Exclusions (0). Export Configuration сваля текущите настройки като JSON файл - полезно за backup или копиране към друга машина. Import Configuration зарежда настройки от файл с автоматичен backup преди промяната.

ТОВА ВИ ДАВА

знаете точно каква конфигурация работи на всяка машина — и можете да я прехвърлите или възстановите за секунди.



33. Settings

Тук управлявате известията (Email Alerts, Desktop Alerts, Critical Only, Alert Sound) и визуалните предпочитания (Compact Mode, Animations). Email Alerts изпращат обобщение при нови инциденти към лицензия имейл. Desktop Alerts показват нативна Windows нотификация при нова заплаха в Live Feed.

ТОВА ВИ ДАВА

настройвате системата да ви уведомява по начина, по който работите — без шум, но и без пропуснати аларми.



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

Отделният профил на организацията събира данните, нужни за NIS2 докладите: Organization Name, EIK/Bulstat, Address, Contact Person, Contact Email, CERT-BG ID и System Description. NIS2 Profile Completeness показва какъв процент е попълнен. Тези данни захранват автоматично всички NIS2 доклади.

ТОВА ВИ ДАВА

попълвате данните на организацията си веднъж — и те захранват автоматично всички NIS2 доклади оттам нататък.



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

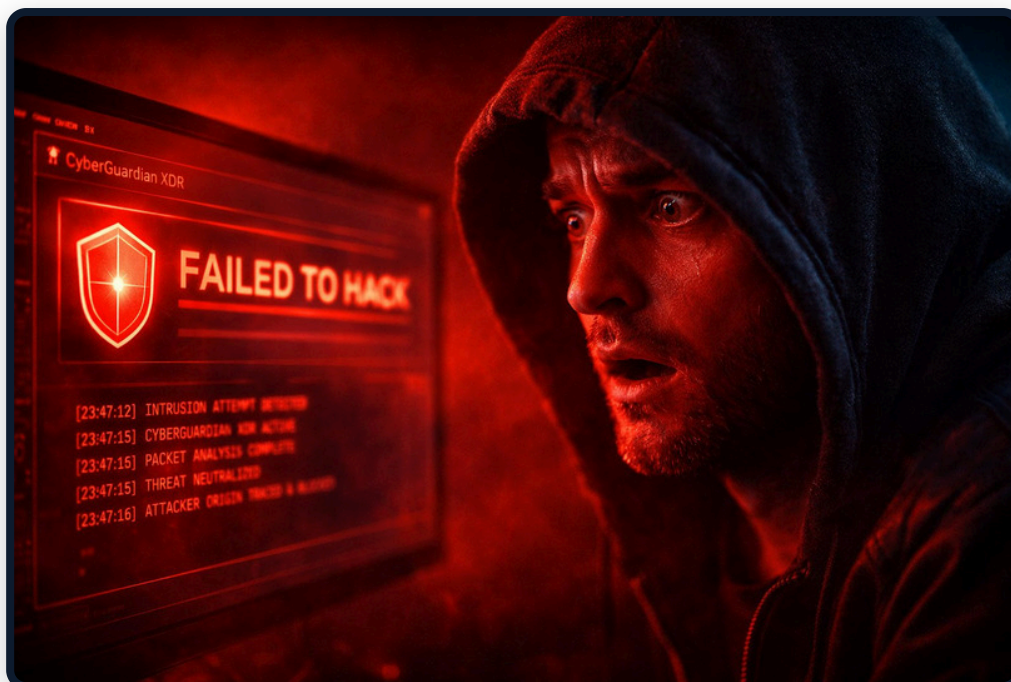
CERT-BG-XXXX

System Description

Critical network infrastructure for...

35. Какво получавате с CyberGuardian XDR

Какво получавате	Какво означава за вас
Dashboard — Security Operations Center	Цялата защита на един екран — инциденти, критични, непрегледани и Security Posture Score
Managed Devices (Fleet)	Всички машини на едно място — статус, здраве, заплахи, версия на агента
Crash Telemetry	Проблем на която и да е машина — видим веднага, централно, с готова диагностика
Executive Dashboard	Ръководството вижда риск, тенденции и NIS2 статус на разбираем език
NIS2 Compliance — 15 модула	NIS2 доказателства и доклади за преглед преди подаване
Threat Intelligence + IOC (1M+)	Новоразкрити индикатори се добавят при автоматични обновявания
Exploited Vulnerabilities (KEV)	Виждате дали ваш софтуер е под реална атака точно сега — не абстрактен списък
Detection v2 + Runtime Blocking	Запахата е спряна в момента на изпълнение — не след нанесена вреда
Process Tree	Хакерската маскировка зад легитимни процеси — видима с един поглед
Real-Time Protection	Компютърът се пази сам 24/7 — дори когато никой не гледа екрана
Tamper Protection (100/100)	4 защитни пласта затрудняват тихото изключване на защитата
File Integrity Monitoring	Тихите подмени на системни файлове — видими веднага на всяка машина
Malware Remediation	Премахва файлове и persistence механизми
AI Insights + ML Models	Обяснен риск, тенденции и готов план за действие
Live Honeypots (9 активни)	Подозрителната активност срещу примамките се вижда отделно
Email & Phishing Scanner	Защита от атакуващ вектор №1 — директно в пощата, преди клик
FP Control + Security Analytics	Намалява фалшивите сигнали и насочва към по-вероятните заплахи.



„FAILED TO HACK“ - CyberGuardian XDR засече и блокира симулираната атака.

36. Контакт и лицензиране

cgs.xdr@gmail.com • cyberguardian.bg

Business / Professional: от €199/год.* • Enterprise: персонална оферта

Понеделник - Петък, 09:00 - 18:00 ч. • Критични инциденти: първоначален отговор до 2 часа

* Началната цена и лицензият обхват се уточняват в офертата. NIS2 функциите подпомагат съответствието и не представляват регулаторен сертификат.

CyberGuardian XDR е продукт на CyberGuardian Security EOOD, България. Всички права запазени © 2026.