



**SECURITY
DAYS**

ESET IŠ ARTI: KAIP KEIČIASI TECHNOLOGIJA

Lukas Apynis,
Baltimax vyresnysis kibernetinio saugumo inžinierius, ESET ekspertas

Your technology and progress, our passion to protect

1bn+

protected users worldwide

500k+

protected business customers

176

covered countries and territories

30+

years of cybersecurity experience

800+

cybersecurity researchers
and technology experts

11

research and development centers

2300+ EMPLOYEES

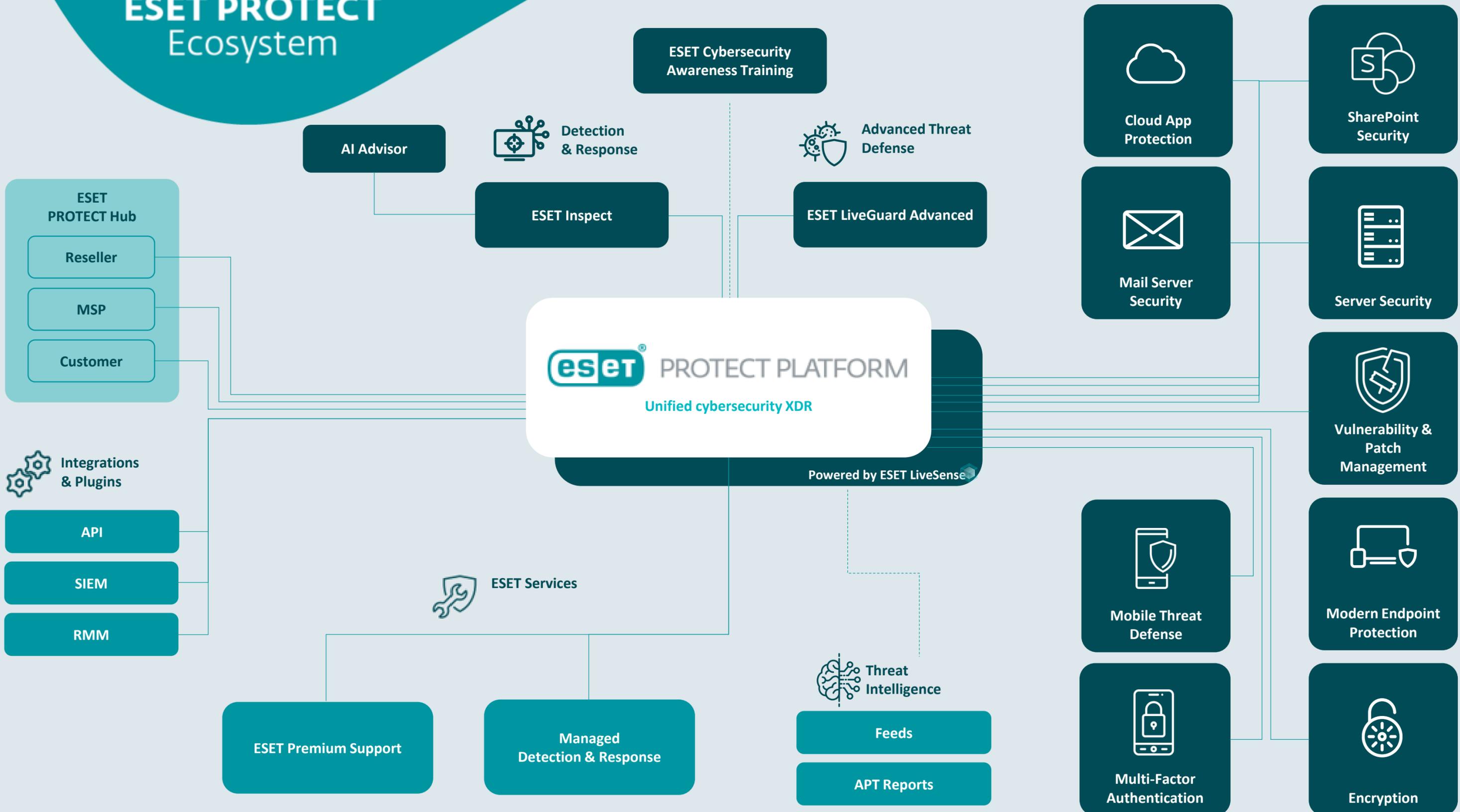
23 OFFICES

- ISO 27001 Certified
- ISO 9001 Certified
- SOC 2 Certified

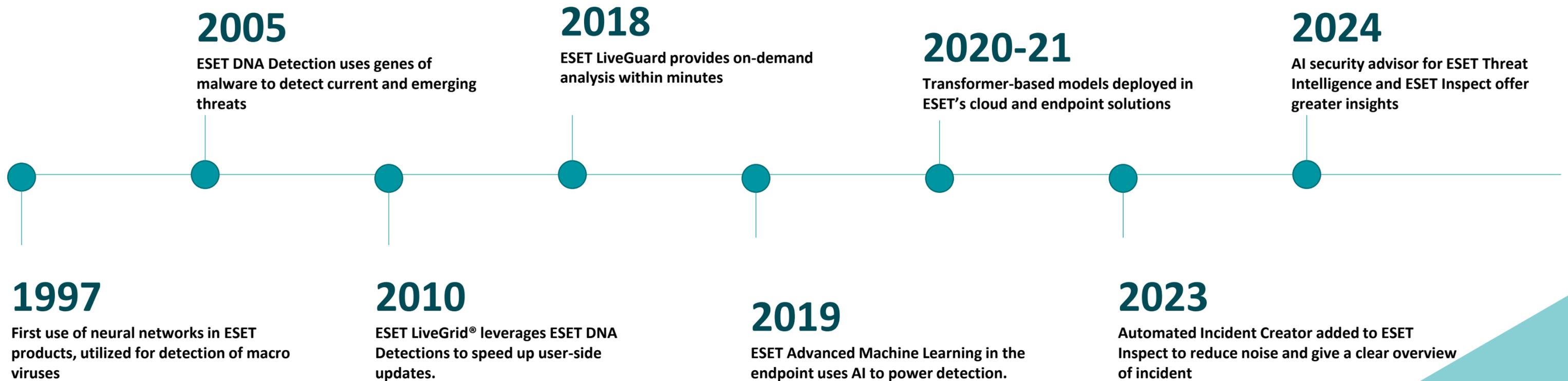


SOC 2 Type 2
Certified

ESET PROTECT Ecosystem



ESET has been using AI/ML for over 25 Years





ESET PROTECT – Unified XDR Platform

Solution Tier	ESET PROTECT Entry	ESET PROTECT Advanced	ESET PROTECT Complete	ESET PROTECT Enterprise	ESET PROTECT Elite
Modules	Management Console	Management Console	Management Console	Management Console	Management Console
	Modern Endpoint Security	Modern Endpoint Security <small>Incl. Ransomware Remediation</small>			
	Server Security	Server Security	Server Security	Server Security	Server Security
		Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense
		Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense
		Full Disk Encryption	Full Disk Encryption	Full Disk Encryption	Full Disk Encryption
			Mail Security		Mail Security
			Cloud App Protection		Cloud App Protection
			Vulnerability & Patch Management		Vulnerability & Patch Management
				Extended Detection & Response	Extended Detection & Response
					Multi-Factor Authentication



NOD Baltic Paslaugos

Premium Support

Techninio palaikymo sąlygos

- Premium palaikymas
- Inžinieriaus pagalba (Starter)
- Esamos situacijos įvertinimas
- Diegimas ir atnaujinimas
- Inžinieriaus konsultacija

NOD Baltic MDR ir kt. paslaugos

Kibernetinės saugos paslaugos

- Aptikimas ir reagavimas (MDR)
- Kibernetinio incidento tyrimas
- Atsparumo įsilaužimams testavimas

Ransomware remediation/rollback

- Advanced setup
 - Protections 6
 - Real-time file system protection
 - HIPS 2
 - Cloud-based protection 3
 - Network access protection 1
 - Email client protection
 - Web access protection
 - Browser protection
 - Device control
 - Document protection
 - Scans
 - Updates 2
 - Connectivity
 - Troubleshooting
 - Remote management
 - User interface 3
- Default

Mode set after learning

Log all blocked operations

Notify when changes occur

- Self-Defense
- Deep Behavioral Inspection
- Ransomware Shield
 - Enable Ransomware Shield
 - Enable Intel® Threat Detection

Ransomware Remediation

Restore files after a ransomware attack

List of excluded folders

List of protected file types [Edit](#)

List of protected file types

- aif
- cda
- mid
- midi
- mp3
- ogg
- wav
- wma
- wpl
- 7z
- arj
- deb
- pkg

Add Edit Delete Import Export

OK Cancel

OK Cancel

Geriausia konfigūruoti centrinės valdymo konsolės politiką

VERSLO PRODUKTŲ NAUJI FUNKCIONALUMAI

- ESET LiveGuard Advanced
- ESET Server Security
- ESET Endpoint Security
- ESET Inspect
- ESET PROTECT Cloud
- ESET Full Disk Encryption
- ESET Mail Security
- ESET Cloud Office Security
- ESET Secure Authentication
- ESET PROTECT Hub
- ESET Threat Intelligence
- ML / AI ir kitos vidinės technologijos
- ESET Connect (API)

ESET LiveGuard Advanced (Sandbox)

eset LIVEGUARD

Tuesday, March 5, 2024

Malware

SHA-1 4DBEDE1A5A0E1DFCC1D322B26FD275866B33EFE8
 SHA-256 5E3AD38FB50CAB6CB5841BF906B00A465F855695402ECB982963894678CCA733
 Category Executable

[↓ DOWNLOAD PDF](#)



File
Details

File name KTB_FOREIGN_REMITTANCE.pdf.scr
 SHA-1 4DBEDE1A5A0E1DFCC1D322B26FD275866B33EFE8 [↗](#)
 SHA-256 5E3AD38FB50CAB6CB5841BF906B00A465F855695402ECB982963894678CCA733 [↗](#)
 Category Executable
 Size 1.06 MB



Sandbox
Details

Country Slovakia
 File path C:\Windows\System32\drivers\etc\KTB_FOREIGN_REMITTANCE.pdf.scr

Analyzed behaviors 12

DETECTION	DETAIL	# OF REASONS
Startup list modified	The sample has added a new entry to the Windows Startup application list.	1 ▼
Blocked URL detected	The sample communicated with a URL on an ESET blacklist.	1 ▼
Hidden code detection	The sample contains hidden code to hide its functionality.	0
Files created in the Program Files folder	The sample has created new files in the Program Files folder.	1 ▼
Machine Learning detection	The sample behaves very similarly to known malware.	0

ESET LiveGuard Advanced (Sandbox)

Analyzed behaviors 12

DETECTION	DETAIL	# OF REASONS	
Startup list modified	The sample has added a new entry to the Windows Startup application list.	1	▼
Blocked URL detected	The sample communicated with a URL on an ESET blocklist.	1	▼
Hidden code detection	The sample contains hidden code to hide its functionality.	0	
Files created in the Program Files folder	The sample has created new files in the Program Files folder.	1	▲
	C:\Program Files (x86)\DHCP_Subsystem\dhcpcss.exe		
Machine Learning detection	The sample behaves very similarly to known malware.	0	
Detected dropper	The sample has dropped or downloaded a file that was detected as malicious.	1	▼
Malware detected without execution	The sample has been detected as malicious without execution.	1	▼
Script execution	The sample has executed a script (BAT, JS, VBS, etc.).	1	▼
Running process injection	The sample has tried to inject code into a running process.	1	▼
Running process enumeration	The sample has enumerated all running processes on the system.	2	▼
Network communication	The sample has tried to contact another computer over a network or listen for connections from other computers.	1	▼
Executed file deleted by sample	The sample has executed a file and deleted it afterward.	1	▼

ESET LiveGuard Advanced (Sandbox)

Type to search...

Process Operations API Logs

All processes

- [-] CREATE PROCESS <SAMPLE> (7012)
"C:\Windows\System32\drivers\etc\<SAMPLE>" /S
 - [-] PROCESS 1
 - [-] CREATE PROCESS WSCRIPT.EXE (6120)
"C:\Windows\System32\WScript.exe" "C:\Users\ADMINI~1\AppData\Local\Temp\RarSFX0\qhmf.vbe"
 - + PROCESS 3
 - [-] REGISTRY 4
 - Set **AutoDetect** (6120)
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 - Set **IntranetName** (6120)
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 - Set **ProxyBypass** (6120)
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 - Set **UNCAsIntranet** (6120)
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
 - + OTHER 3
 - + FILE 17

ESET LiveGuard Advanced (Sandbox)

Process	Operations	API Logs
+ WERMGR.EXE (6732) 366		
C:\Windows\system32\wermgr.exe -upload		
<pre>"cmd": "C:\Windows\system32\wermgr.exe -upload", "image": "C:\Windows\system32\wermgr.exe", "pid": 6732, "calls": [</pre>		
+ SHTASKS.EXE (604) 10		
schtasks.exe" /create /f /tn "DHCP Subsystem Task" /xml "C:\Users\Administrator\AppData\Local\Temp\tmp667B.tmp		
<pre>"cmd": "schtasks.exe" /create /f /tn "DHCP Subsystem Task" /xml "C:\Users\Administrator\AppData\Local\Temp\tmp667B.tmp", "image": "C:\Windows\SysWOW64\schtasks.exe", "pid": 604, "calls": [</pre>		

ESET Server Security for Linux 12.0

ADDED: Patch Management

ADDED: Network Isolation

ADDED: Kubernetes support in Container security

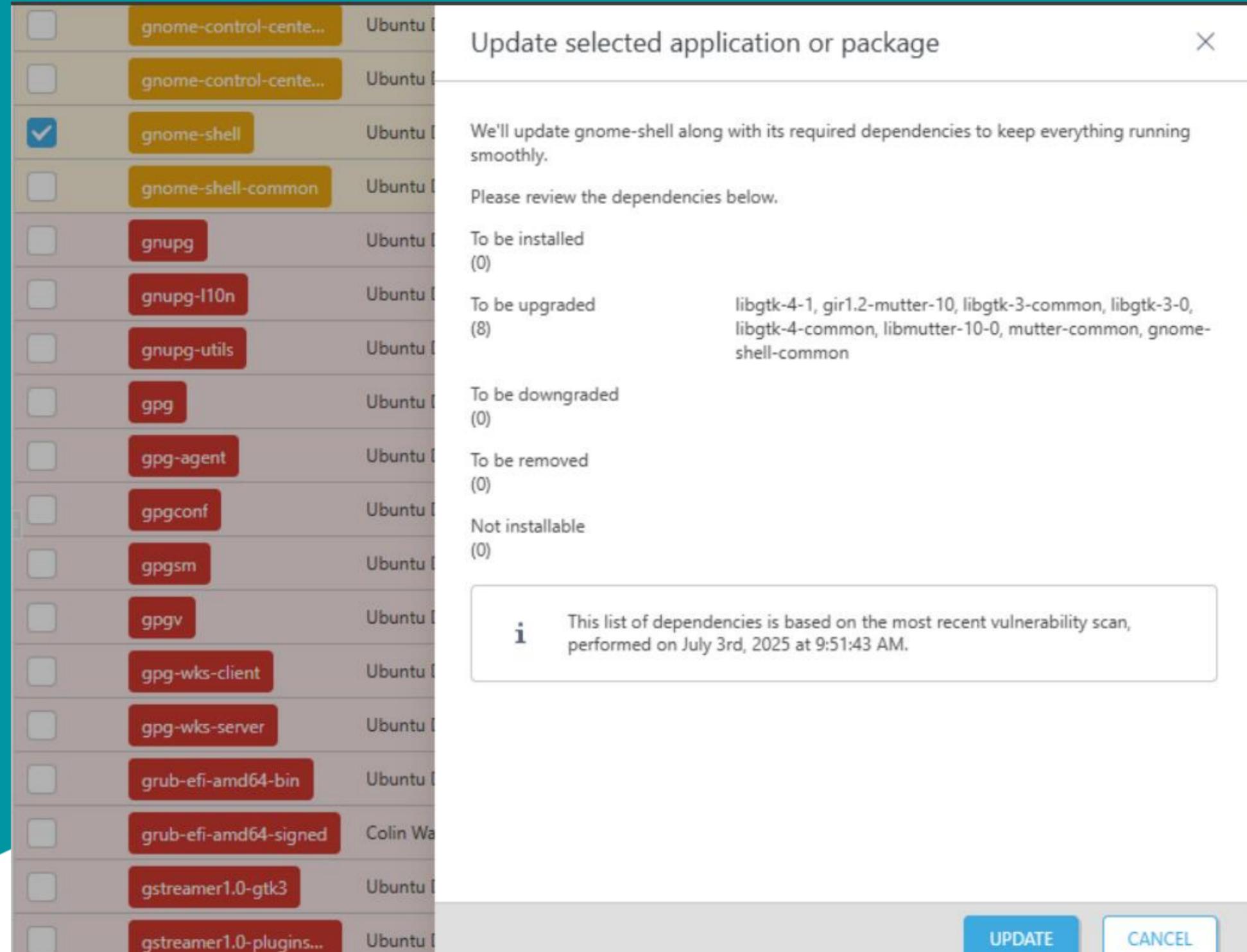
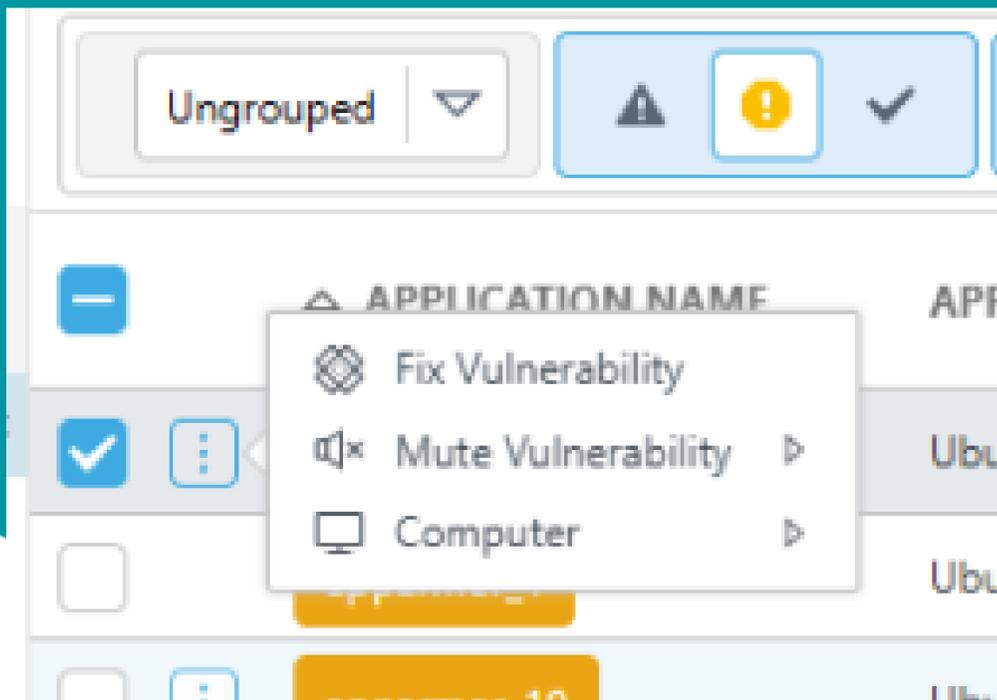
ADDED: RHEL 10 support

ADDED: AlmaLinux 10 support

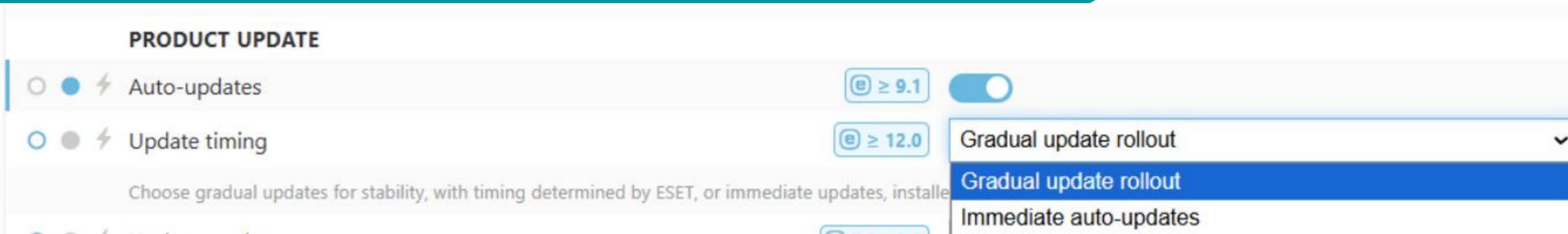
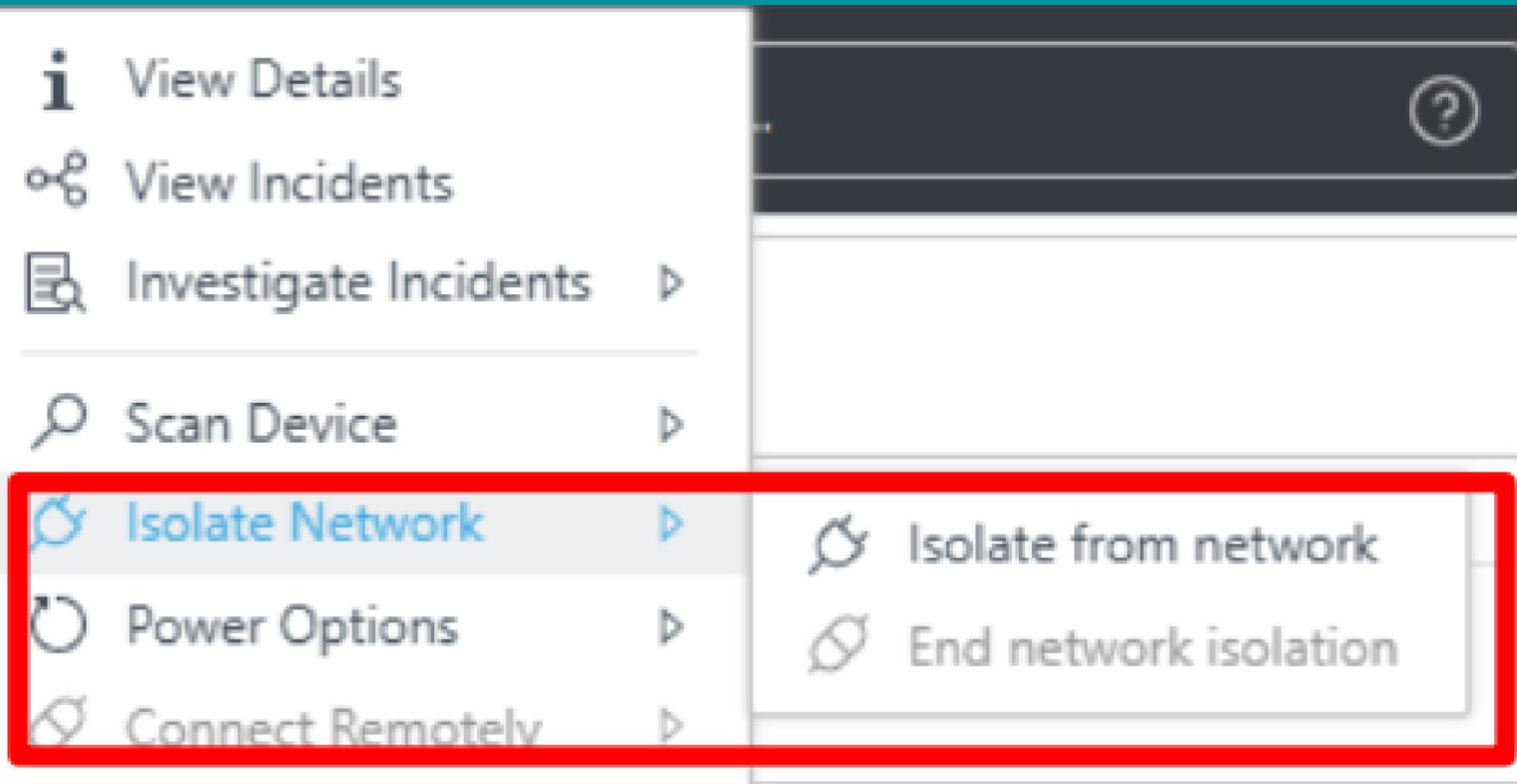
ADDED: Rocky Linux 10 support

ADDED: Auto-updates for testing environments

ESET Server Security for Linux 12.0



ESET Server Security for Linux 12.0



Endpoint Security for macOS v8.0

CPU: Apple M (ARM) ir Intel (x86) architektūra

Vienas produktas.

Šiuo atnaujinimu norėjome pašalinti būtinybę spręsti, kurį produktą atsisiųsti. Įdiegime mechanizmą, kuris dabar leidžia naudoti tik vieną produktą.

Produkto pavadinimas yra „ESET Endpoint Security“.

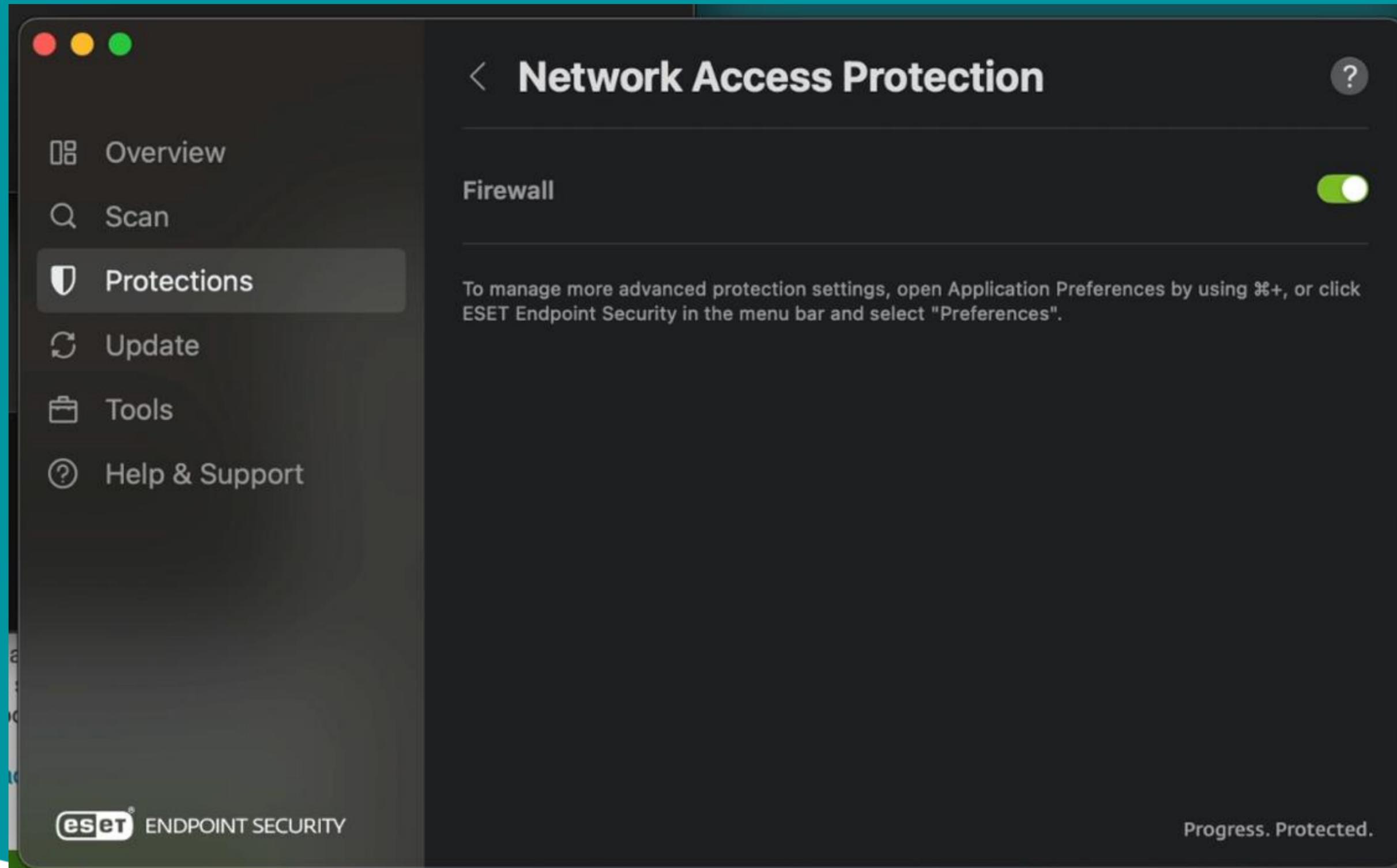
PRIDĖTA: integracija su ESET LiveGuard Advanced

PRIDĖTA: pažeidžiamumo ir pataisų valdymas

PRIDĖTA: ugniasienės konfigūravimas valdomose aplinkose

PRIDĖTA: galimybė izoliuoti kompiuterį nuo tinklo – iš PROTECT & Inspect

Endpoint Security for macOS v8.0



Endpoint Security for macOS v8.0

Add rule

Name

Enabled

<input type="checkbox"/> ACTION	<input type="checkbox"/> Log rule	Block
<input type="checkbox"/> OS		Mac
<input type="checkbox"/> APPLICATION		Any
<input type="checkbox"/> DIRECTION		In
<input type="checkbox"/> IP PROTOCOL		TCP & UDP
<input checked="" type="checkbox"/> LOCAL HOST		Any
IP sets	Edit	
IP	<input type="text"/>	<input type="button" value="i"/>
<input type="checkbox"/> LOCAL PORT		Any
<input type="checkbox"/> REMOTE HOST		Any
<input type="checkbox"/> REMOTE PORT		Any
<input type="checkbox"/> PROFILE		Any

Endpoint Security for macOS v9.0

Palaikymas naujajai macOS 26 versijai

HTTPS svetainių ir srauto nuskaitymo palaikymas

Įrenginių valdymo funkcija (device control)

ESET Inspect v2.7

Tinklo izoliacija Linux* sistemai

„SentBytes“ funkcija dabar yra prieinama taisyklėse

Native ARM EI Connector macOS sistemoms

Pridėta palaikoma versija: Oracle Linux 9

Aptikimo sluoksnio patobulinimai ir greitaveikos optimizavimai

Viena konsolē visiems saugumo sprendimams

eSet PROTECT
🔔

🔍
QUICK LINKS ▾
🔗 HELP ▾
👤 LUKAS APYNIS
🚪 LOGOUT

DASHBOARD

COMPUTERS

INCIDENTS

VULNERABILITIES

Patch Management

Detections

Reports

Tasks

Installers

Configuration

Notifications

Status Overview

Platform Modules

More

Submit Feedback

COLLAPSE

Dashboard

Status Overview
Incidents
ESET LiveGuard
ESET Vulnerability & Patch Management
ESET Cloud Office Security
Detections
ESET MDR
Computers
Antivirus detections
Firewall detections
ESET applications

Computer status 155

Error

🚨 **65** Affected Computers

Warning

⚠️ **26** Affected Computers

Incident status 389

High severity

🔴 **54**

Medium severity

🟡 **320**

Top functional problems

Most impactful active incidents

Name	Computers	Status
Multiple Malware Detecti...	7	Open
Multiple Malware Infecti...	6	Open
Multiple Malware Detecti...	5	Open
Detection of MSIL/Disabl...	4	Open
Detection and Cleanup o...	4	Open

Top vulnerable applications

Application name	Affected computers	Total vulnerabilities	Overall Impact
Microsoft Windows 10 Pro	11	10099	54%
Microsoft Windows 10 Enterprise Evaluation	1	3647	22%
Microsoft Windows 11 Enterprise Evaluation	5	1212	7%
Adobe Acrobat DC Continuous	1	392	2%
Microsoft Visual Studio	11	339	2%

Computer connection status

Computer management status

Platform modules

Version status

WeLiveSecurity

Supply-chain dependencies: Check your resilience blind spot

August 12th, 2025

Does your business truly understand its dependencies, and how to mitigate the risks posed by an attack on them?

Viena konsole visiems saugumo sprendimams

ESET PROTECT
🔔

🔍
QUICK LINKS ▾
🔗 HELP ▾
👤 LUKAS APYNIS
🚪 LOG

- 🏠 DASHBOARD
- 💻 COMPUTERS
- 🔗 INCIDENTS
- 🛡️ VULNERABILITIES
- 🔄 Patch Management
- ⚠️ Detections
- 📄 Reports
- 📁 Tasks
- 📦 Installers
- ⚙️ Configuration
- 🔔 Notifications
- 📊 Status Overview
- 📁 Platform Modules
- ⋮ More

Dashboard

Status Overview
Incidents
ESET LiveGuard
ESET Vulnerability & Patch Management
ESET Cloud Office Security
Detections
ESET MDR
Computers
Antivirus detections
Firewall detections
ESET applications

Active incidents

All active incidents

🔗 389

High severity

📈 54

Medium severity

📈 320

Low severity

📉 15

Number of created incidents over time 7d

Date	High severity	Medium severity	Low severity
08/09/2025	0	0	0
08/10/2025	0	0	0
08/11/2025	0	3	0
08/12/2025	0	0	0
08/13/2025	0	0	0
08/14/2025	0	0	0
08/15/2025	0	0	0

Latest active incidents

Creation time	Name	Computers	Detections	Status
Aug 12, 2025, 8:19:40 AM	Multiple Malicious A...	1	39	Open
Aug 12, 2025, 8:19:38 AM	Execution of Multipl...	1	10	Open
Aug 12, 2025, 8:19:30 AM	Webshell AV Detecti...	1	26	Open
Aug 6, 2025, 7:36:20 PM	HackTool Detected [I...	1	2	Open
Aug 6, 2025, 7:15:30 PM	Multiple Malware De...	1	87	Open

Top impacted computers

Computer name	Incidents	Group	Last seen
desktop-aaofdt8	17	Student15	Jun 27, 2025, 2:56:03 PM
desktop-tlonn2r	13	Student23	Aug 16, 2025, 12:50:01 PM
windev2407eval	12	Student25	Jul 25, 2025, 2:31:11 PM
desktop-52t26o9	10	Student12	Aug 11, 2025, 4:53:38 PM
desktop-52t26o9	10	Lost & found	Apr 15, 2025, 9:14:19 PM

Most impactful active incidents

Name	Computers	Status
Multiple Malware Detections and Cleanings on win10flarevm	7	Open
Multiple Malware Infections Cleaned on desktop-nn44lnp	6	Open
Multiple Malware Detections from 7-Zip Extraction on desktop-52t26o9	5	Open
Detection of MSIL/Disabler.DR and MSIL/Spy.RedLine.A on desktop-2h0v9i5	4	Open

Active incidents by status

Open	389
In progress	0
Waiting for input	0

Closed incident resolution

True positive	33
False positive	3
Canceled	0
Suspicious	3

Submit Feedback

COLLAPSE

ESET Protect - Incidents

< BACK

Dashboard >

Detection of MSIL/Disabler.DR and MSIL/Sp...

INSPECT →

Overview

Detections (11)

Affected Computers (4)

Incident Timeline



Detection of MSIL/Disabler.DR and MSIL/Spy.RedLine.A on desktop-2h0v9i5

Severity	High
Status	Open
Creation time	04/09/2025, 7:47 PM
Last update	04/09/2025, 8:21 PM
Author	ESET
Tags	Select tags



Company impact

Computers	4
Executables	5 View in ESET Inspect
Processes	9 View in ESET Inspect

Comments

[+ Add comment](#)

Description

On computer AGIL, malware MSIL/Disabler.DR was detected from the untrusted executable Ir074206.exe located in folder a (6), which has a malicious reputation and is associated with multiple executables: zimu3272.exe, zizx4343.exe, and it296434.exe located at %DESKTOP%\a (6). Additionally, on computer desktop-2h0v9i5, user simon executed Windows File Explorer - explorer.exe, which accessed the malicious executable zimu3272.exe, triggering the detection of MSIL/Disabler.DR. Furthermore, the same user simon executed explorer.exe again, which accessed another malicious executable kp696044.exe from %HOME%\downloads\samples4\a (6)/zimu3272.exe, leading to the detection of malware MSIL/Spy.RedLine.A.

IMPORTANT: Generated by AI. Verify information for accuracy.

ESET Protect Cloud

Dashboard

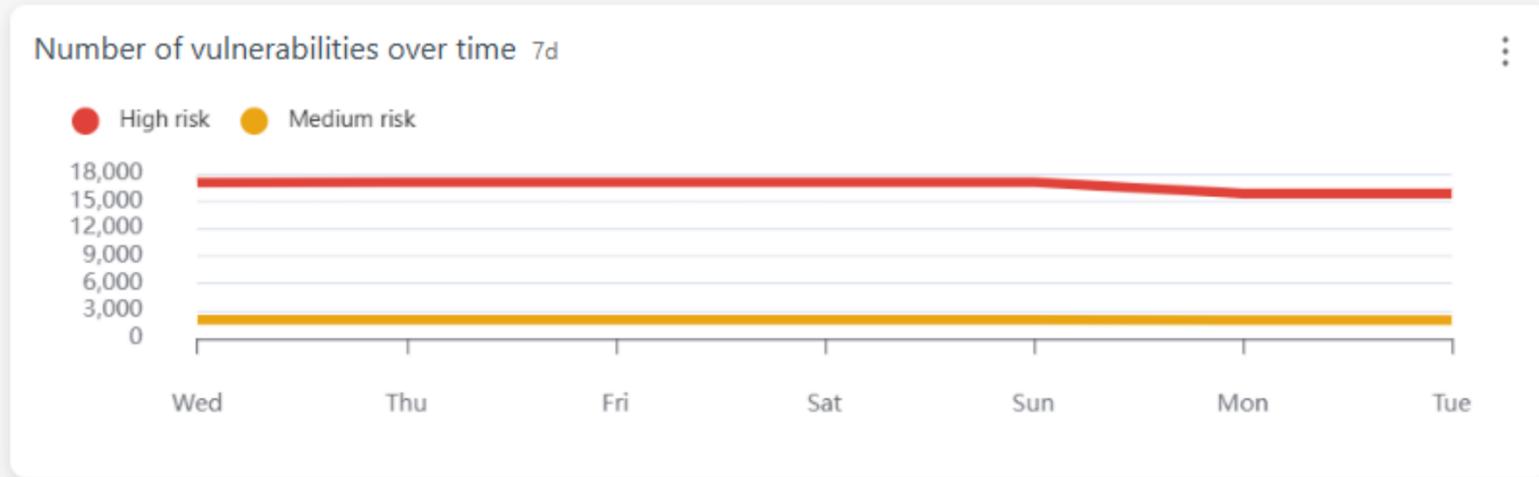


- Status Overview
- Incidents
- ESET LiveGuard
- ESET Vulnerability & Patch Management**
- ESET Cloud Office Security
- Detections
- ESET MDR
- Computers
- Antivirus detections
- Firewall detections
- ESET applications

Number of vulnerabilities

High-risk score including 48 muted
16,231 vulnerabilities

Medium-risk score including 1 muted
2,105 vulnerabilities



Top vulnerable computers

Computer name	Computer type	High-risk vulnerabilities	Medium-risk vulnerabilities	Total vulnerabilities
[Redacted]	Desktop	3500	220	3,720
[Redacted]	Desktop	1751	198	1,949
[Redacted]	Desktop	1222	45	1,267
[Redacted]	Desktop	1177	44	1,221
[Redacted]	Desktop	1031	184	1,215

Top vulnerable computers by OS vulnerabilities

Computer name	OS name	High-risk OS vulnerabilities	Medium-risk OS vulnerabilities	Total OS vulnerabilities
[Redacted]	Microsoft Windows 10 E...	3428	219	3,647
[Redacted]	Microsoft Windows 10 P...	1659	193	1,852
[Redacted]	Microsoft Windows 10 P...	1217	44	1,261
[Redacted]	Microsoft Windows 10 P...	1096	44	1,140
[Redacted]	Microsoft Windows 10 P...	933	179	1,112

Top vulnerable applications

Application name	Affected computers	Total vulnerabilities	Overall Impact
Microsoft Windows 10 Pro	11	10099	54%
Microsoft Windows 10 Enterprise Evaluation	1	3647	22%
Microsoft Windows 11 Enterprise Evaluation	5	1212	7%

Top outdated applications with available patches

Application name	Affected computers
Microsoft Visual C++ 2015-2022 Redistributable	25
Microsoft .NET Desktop Runtime 8.0	12
Wireshark	12

ESET Protect Cloud

127.0	38	CVE-2024-10460
127.0	38	CVE-2024-10461
127.0		
127.0		
127.0		
127.0		
127.0		
127.0		
127.0		
120.0.1		
120.0.1	66	CVE-2024-10459
120.0.1	38	CVE-2024-10460
120.0.1	38	CVE-2024-10461

CVEs covered by ESET

Enter a specific CVE ID to check if it's covered by ESET.

✓ CVE-2023-20867 is covered by ESET.
⚠ CVE-2023-20867 was found in your environment on 4 computers.

SEARCH CANCEL

ESET Protect Cloud

The dashboard is divided into two main sections: Quarantine and Vulnerability & Patch Management. The Quarantine section includes a 'New Report Template' button and two overview cards: 'Detailed quarantined objects' and 'Quarantined objects'. The Vulnerability & Patch Management section includes two overview cards: 'Patch management overview' and 'Vulnerability scans overview'.

Quarantine

- New Report Template**
- Detailed quarantined objects**
Detailed overview of quarantined objects
- Quarantined objects**
Unique objects quarantined by security products

Vulnerability & Patch Management

- Patch management overview**
An overview of OS and application patches applied via Patch Management
- Vulnerability scans overview**
An overview of performed vulnerability scans and detected vulnerabilities on computers

The 'Computers' management interface shows a table of devices. A context menu is open over the selected device, listing various actions such as 'View Details', 'Isolate Network', and 'Power Options'. The 'Isolate Network' option is currently selected, and a sub-menu is visible with 'Isolate from network' and 'End network isolation' options.

NAME	OS NAME	SECURITY PRODUCT	OS
linux-endpoint-rhel9	RedHat	ESET Endpoint Antivirus	64

- View Details
- View Incidents
- Investigate Incidents
- Scan Device
- Isolate Network**
 - Isolate from network
 - End network isolation
- Power Options
- Connect Remotely
- Update Device
- Platform modules
- Perform Tasks
- Send Wake-Up Call
- Manage Device
- Tags...
- Mute
- Audit Log

ESET Protect Cloud

The screenshot displays the ESET Protect Cloud interface. At the top, there is a navigation bar with the ESET logo, 'PROTECT', a search bar, and user information. Below this is a breadcrumb trail: < BACK Incidents > Suspicious processes executed memoryscanne... > Possible Windows Vault enumeration using ...

The main content area features a process flow diagram showing the following sequence:

- explorer.exe (6056) - 16 min ->
- powershell.exe (2872) - 24 ms ->
- vaultcmd.exe (11700) ->
- Possible Windows Vault e...

Below the diagram is an 'Overview' section with two panels:

Incident Details:

- Icon:** Possible Windows Vault enumeration using vaultcmd [D0441]
- Detection category:** ESET Inspect Rules (with a link to 'See rule details')
- MITRE ATT&CK® techniques:** T1555.004 - Credentials from Password Stores: Windows Credential Manager
- Triggered event:** ProcessCreated (%SYSTEM%\windowspowershell\v1.0\powershell.exe)
- User name:** sta

Host Information:

- OS name:** Microsoft Windows 11 Pro (10.0.22635.5305)
- Parent group:** eset
- Last connected:** 6 minutes ago - Jul 9, 2025, 3:07:19 PM
- Network isolation:** Not isolated

At the bottom, there is a 'Description' section with a 'RESPOND TO INCIDENT' button and an 'ACTIONS' dropdown menu.

ESET Protect Cloud

The screenshot shows the ESET Protect Cloud interface. The top navigation bar includes the ESET logo, the word "PROTECT", a search bar with the placeholder "Type to search ...", and a "QUICK LINKS" dropdown. The left sidebar contains a navigation menu with items: DASHBOARD, COMPUTERS (with a red "5" badge), INCIDENTS, VULNERABILITIES (with a red "99+" badge), Patch Management, Detections, Reports, Tasks, Installers, Configuration (highlighted), Notifications, Status Overview, Platform Modules (with a blue "23" badge), and More. At the bottom of the sidebar is a "Submit Feedback" button and a "COLLAPSE" button.

The main content area is titled "Configuration" and has two tabs: "Basic setup" (selected) and "Advanced setup". A sub-menu on the left lists "ESET Security Product", "ESET LiveGuard", and "ESET Vulnerability & Patch Management" (highlighted). The main content area displays the "ESET Vulnerability & Patch Management" configuration page. It includes a descriptive paragraph, a "Review and adjust the security settings" section with a link to "Learn more on ESET Help", and three toggle switches: "Auto-enable Vulnerability & Patch Management on new and existing devices" (checked), "Auto-patch management for applications" (checked, with a green "Recommended" badge), and "Operating system auto-updates" (checked, with a green "Recommended" badge). There are two information boxes: one about current limitations for Windows Server, Linux, and macOS, and another about creating a custom policy for auto-patch behavior. At the bottom of the configuration area are "BACK", "NEXT", and "APPLY" buttons.

Configuration

Basic setup | Advanced setup

ESET Security Product

ESET LiveGuard

ESET Vulnerability & Patch Management

ESET Vulnerability & Patch Management

Vulnerability and Patch Management proactively identifies and remediates vulnerabilities on your company's devices by patching outdated applications and operating systems. This improves overall network security and mitigates the risk of exploitation of vulnerabilities by cyber attackers. [Learn more](#) about ESET Vulnerability & Patch Management.

Review and adjust the security settings that will always be applied to all devices connected to ESET PROTECT. [Learn more on ESET Help.](#)

Auto-enable Vulnerability & Patch Management on new and existing devices [?](#)

i **Current limitations:** Our Windows Server and Linux products (for endpoints and servers) don't support automated patch management or OS auto-updates. ESET Endpoint Security for macOS doesn't support OS patching.

Auto-patch management for applications [?](#) **Recommended**

Operating system auto-updates **Recommended**

i To further customize auto-patch behavior, such as to avoid unwanted updates, create a new custom policy.

BACK

NEXT

APPLY

DASHBOARD

COMPUTERS

INCIDENTS

VULNERABILITIES

Patch Management

Detections

Reports

Tasks

Installers

Configuration

Notifications

Status Overview

Platform Modules

More

Submit Feedback

COLLAPSE

Configuration

Basic setup

Advanced setup

ESET Security Product

ESET LiveGuard

ESET Vulnerability & Patch Management

ESET Security Product Recommended

Review and adjust the security settings that will always be applied to all devices connected to ESET PROTECT. [Learn more on ESET Help.](#)

Lock security settings with a password e ≥ 7.0 ?

Password

Password

Automatically resolve problems e ≥ 9.1 ?

after 1 day

Always install ESET security product on existing and new devices ?

Always activate ESET security product on existing devices ?

ESET Endpoint Antivirus/Security

v11.1

V12

Ransomware Remediation



Support for ESET Vulnerability & Patch management v1.3



└ Deploy optional (non-CVE) patches



└ Auto-patch threshold limiter



└ Direct patch action for vulnerabilities



└ Other changes (console-side management)

N/A

N/A

Support for ESET HUB migrations



Private LiveGuard support



Pro-active presentation mode



Network isolation exclusions



Automatic End-of-Life upgrades



Support for Intel® NPU



Firewall rules in GPO



Advanced setup reorganization



ESET Endpoint Antivirus/Security 12.1 (Windows)

- **Perėjimas prie prenumeratos modelio**

Modifikacijos ir atnaujinimai, leidžiantys pereiti prie šiuolaikinio prenumeratos verslo modelio.

- **Ransomware Remediation/Rollback**

Apsaugos sluoksnio evoliucija, konfigūracijos ir tolesni sluoksnių tarpusavio aptikimo patobulinimai (ESET LiveGuard).

- **Automatiniai atnaujinimai testavimo aplinkoms**

Geriausia praktika yra ta, kad visi programinės įrangos atnaujinimai gamybos aplinkoje turi būti dar kartą patikrinti testavimo tinklo segmente, kad būtų galima susidoroti su netikėtomis situacijomis. Mūsų automatiniai atnaujinimai atitiks šias kategorijas (testavimo ir gamybos segmento politiką) ir taip pat leis vartotojui atidėti priminimą ilgiau nei 24 valandoms, jei galutinis perkrovimo terminas yra daugiau nei savaitė.

- **Pažeidžiamumų ir pataisų valdymo modulio atnaujinimai v1.4**

- **OAuth 2.0 authentication support for email notification forwarding.**

Naujas autentifikavimo metodas, elektroninių laiškų pranešimams siųsti naudojant „Microsoft“ paskyras.

- **Kiti pokyčiai ir patobulinimai**

ESET Full Disk Encryption v2.0

Enable single sign-on

e ≥ 2.0



When single sign-on (SSO) is enabled, the user's password requirements are enforced by a Windows policy and not ESET Full Disk Encryption. This includes "User can change password", "Password characters" and "Password expiry" policies. However, the password character settings continue to apply when recovery passwords are generated. Additionally, the invalidate password task will not apply. Use the Windows "User must change password on next logon" option within Active Directory instead.

Startup password ?

Enable startup password

Startup password

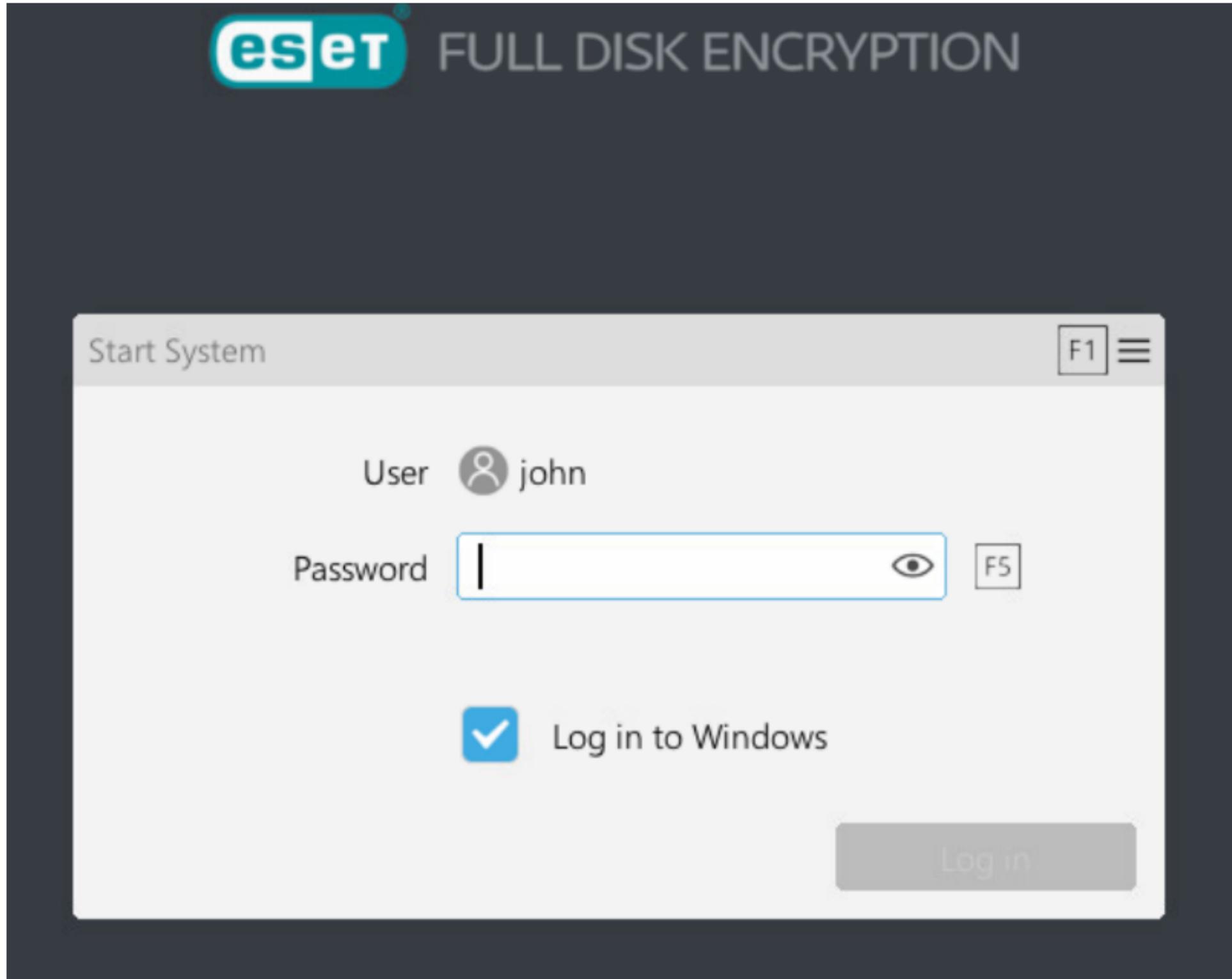
Confirm startup password

● *Startup password must be at least 8 and at most 127 characters long.*

ESET Full Disk Encryption v2.0



ESET Full Disk Encryption v2.0



ESET Full Disk Encryption v2.1

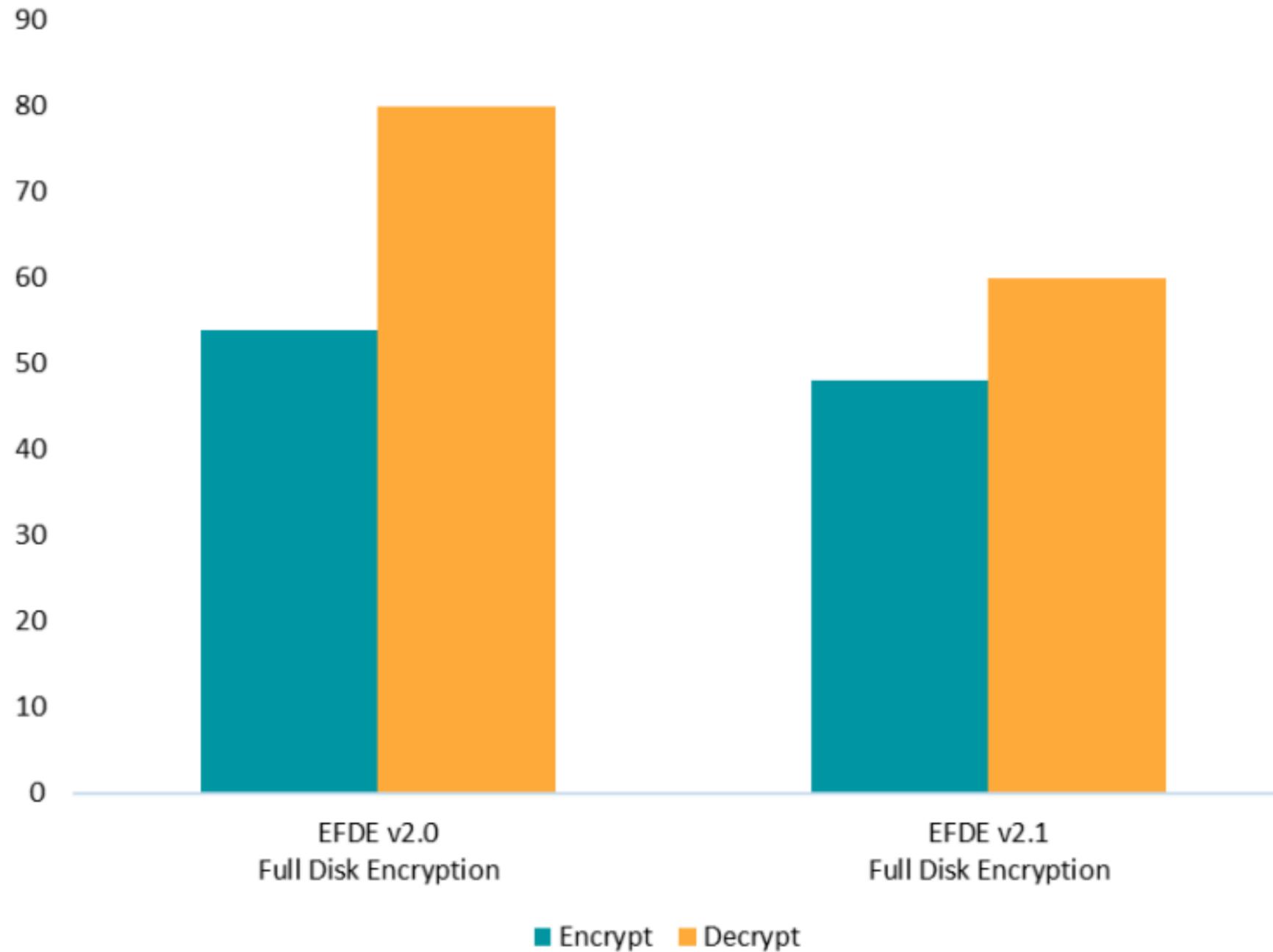
⚡ Enable encryption  

⚡ Encrypt and decrypt used space only  

Speeds up encryption and decryption by targeting only the disk space that contains data. Only recommended for new systems.

ESET Full Disk Encryption v2.1

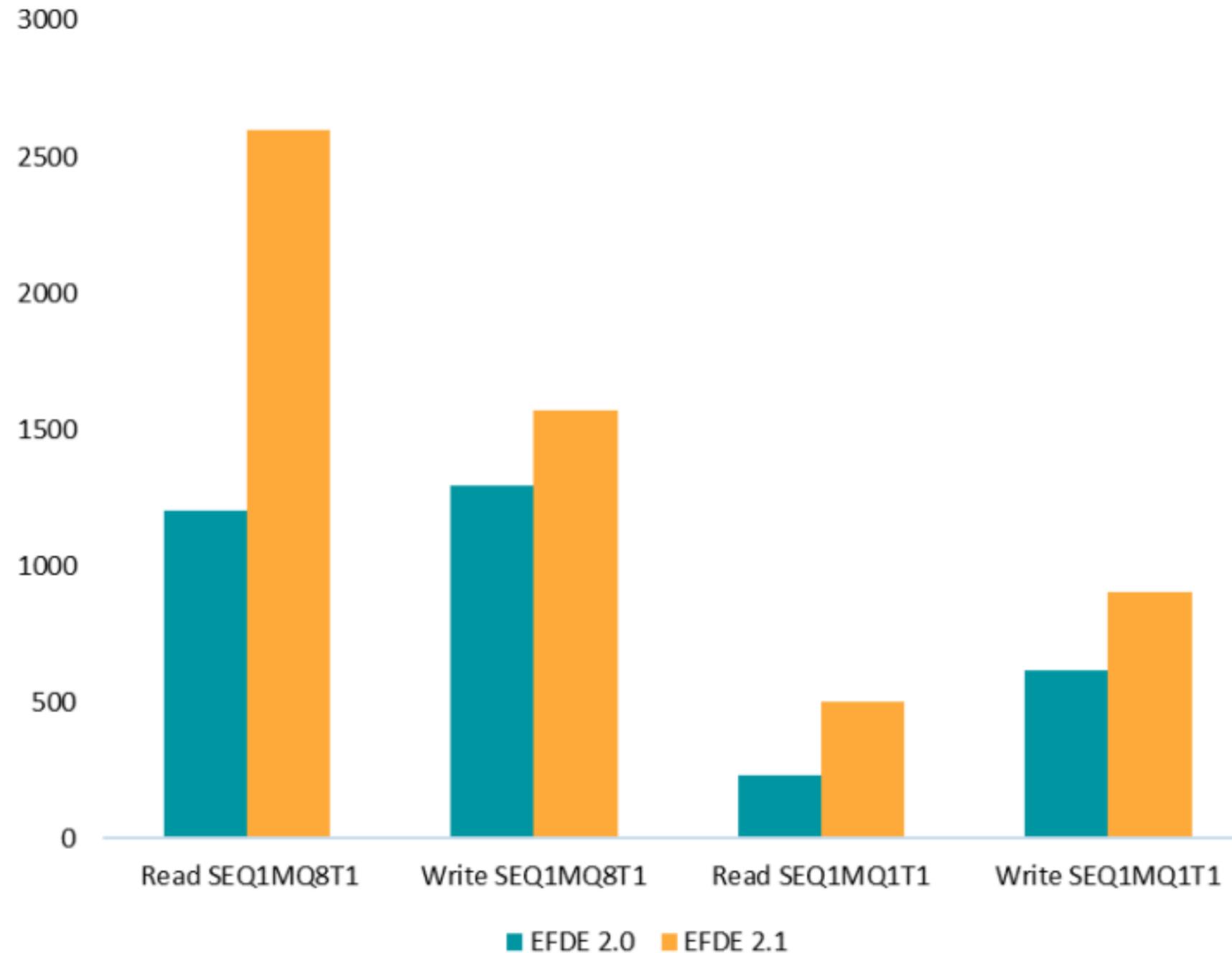
The Full Disk Encryption process now takes less time
[minutes]



AES-NI support

ESET Full Disk Encryption v2.1

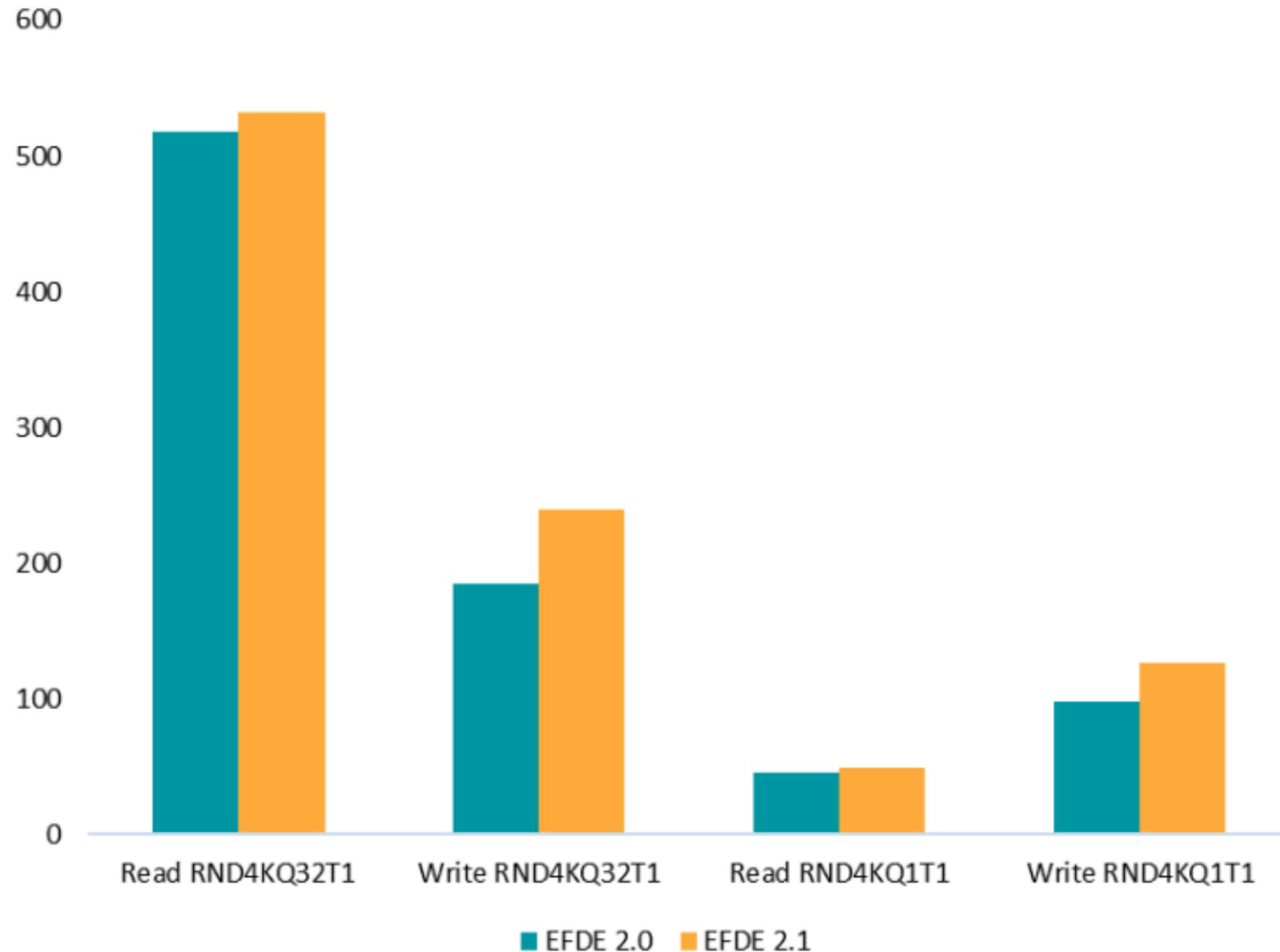
Version 2.1 delivers an average of 74% performance gain in sequential read/write speeds [MB/s]



AES-NI support

ESET Full Disk Encryption v2.1

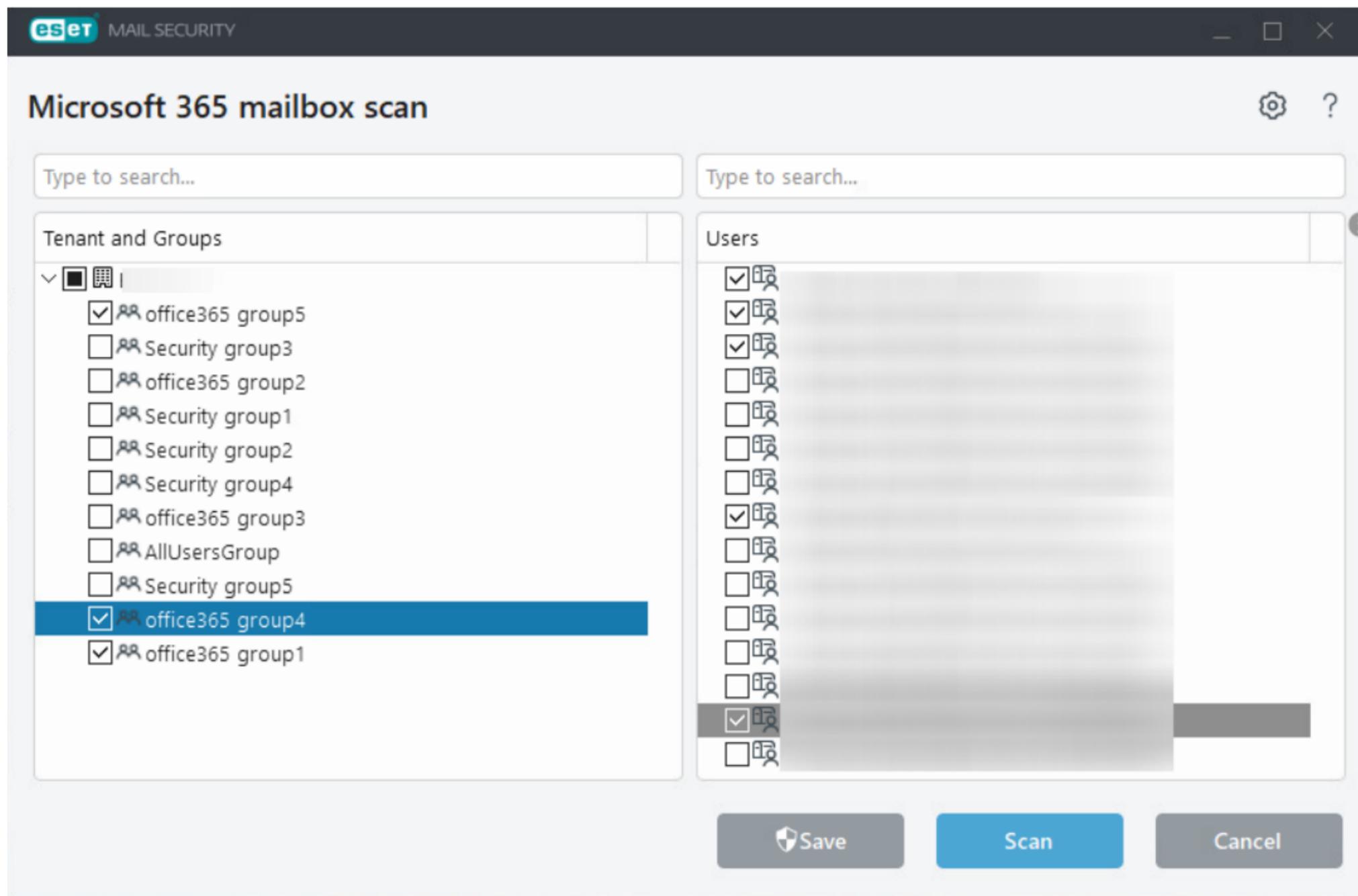
Version 2.1 delivers an average of 18% performance gain in random read/write speeds [MB/s]



AES-NI support

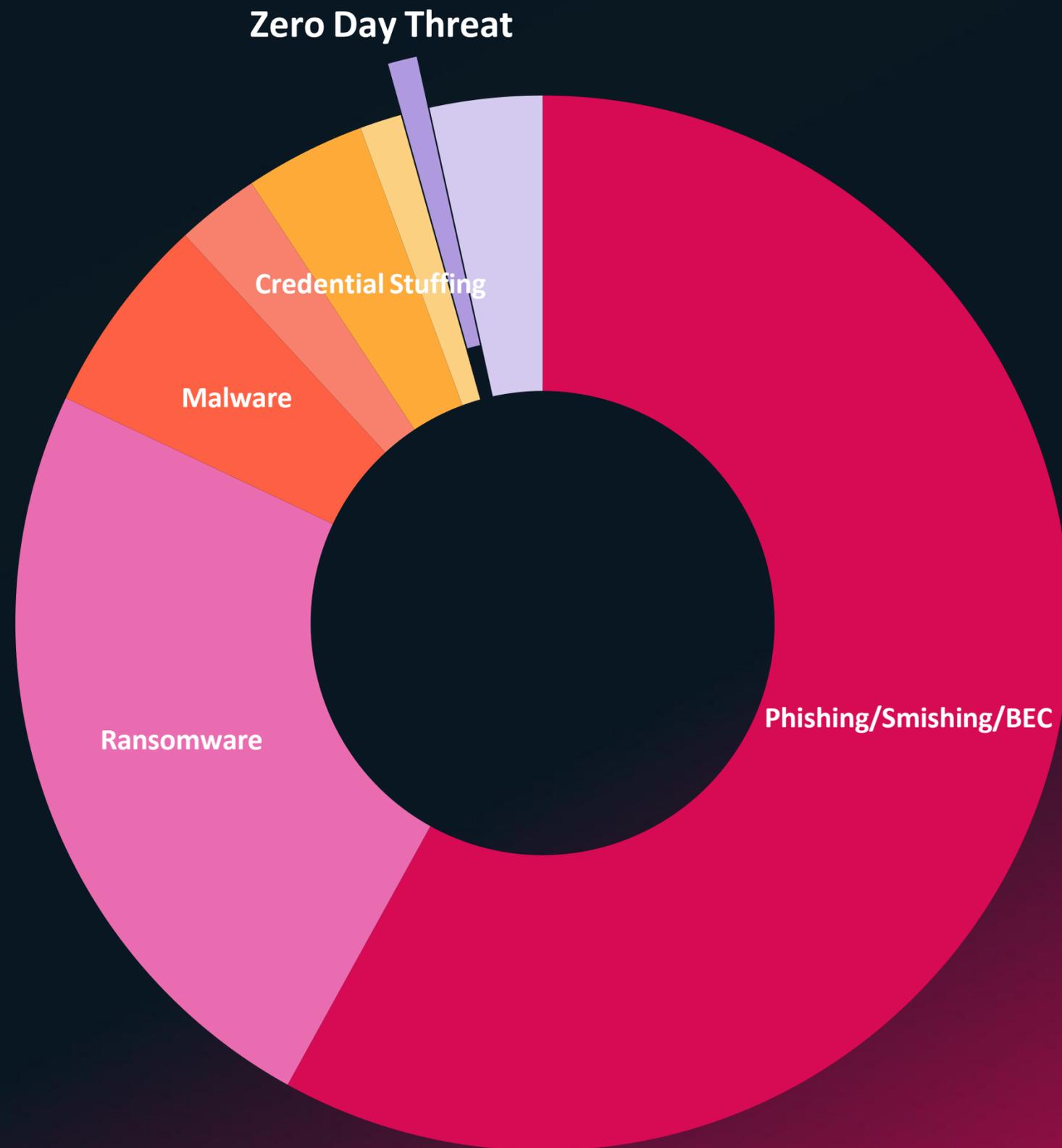
ESET Mail Security for Microsoft Exchange Server v12.0

„Microsoft 365“ skenavimas pagal poreikį gali būti atliekamas debesų pašto dėžutėse už hibridinių aplinkų ribų.



Picture 1 Selection of cloud mailboxes.

DOCUMENTED ATTACK VECTORS



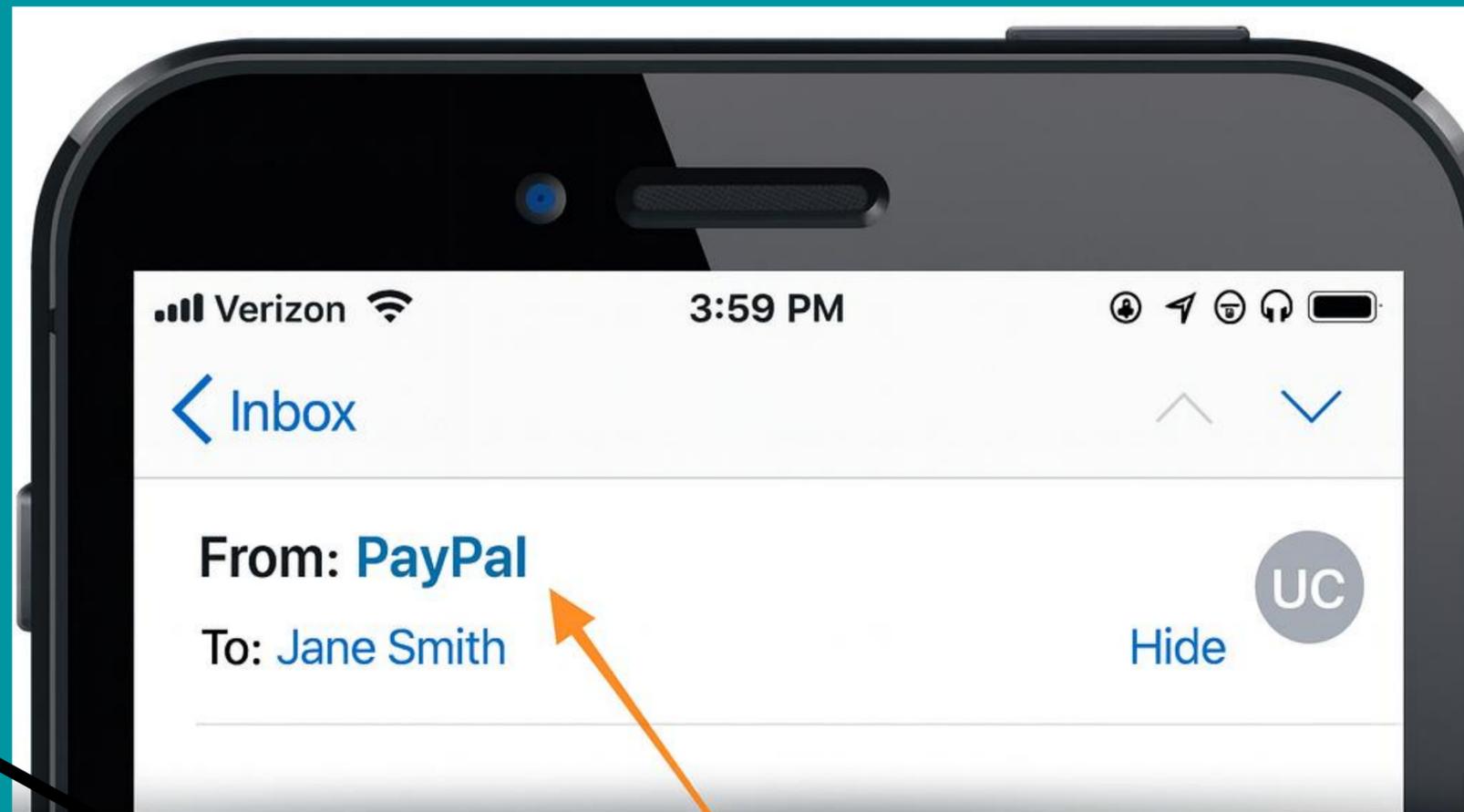
Key features

- Antispam
- Anti-malware
- Anti-phishing
- Anti-spoofing
- Homoglyph Detection
- Advanced Threat Defense
- Dashboard & Notifications
- Email Rules
- Multitenancy with access management
- Quarantine manager & Email Clawback
- Policies and automation
- Deployment in just 5 minutes
- Protected applications



Exchange Online, SharePoint Online, Teams, OneDrive, Gmail, Google Drive

- Antispam
- Anti-malware
- Anti-phishing
- Anti-spoofing
- Homoglyph Detection
- Advanced Threat Defense
- Dashboard & Notifications
- Email Rules



<paypal@paypa1.com>

ECOS effectivity in numbers*

920,000 Email threats detected

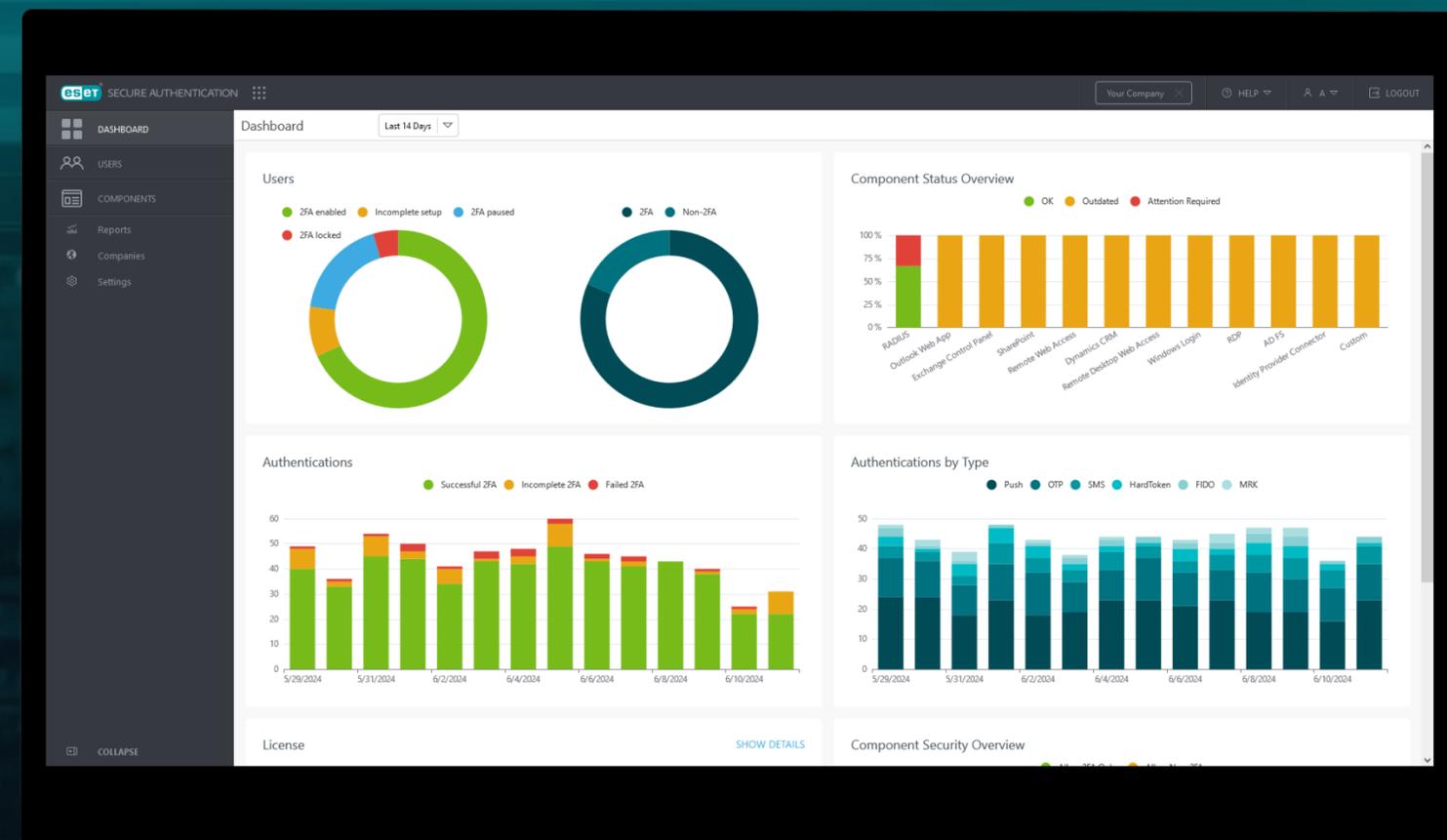
75,820,000
Spam emails captured

813,000
Phishing emails blocked

110,000 Non-email threats
originated from OneDrive, Sharepoint,
Teams & Google Drive

Vagystės ar kompromituoti prisijungimo duomenys yra dažniausias kibernetinių atakų ir duomenų pažeidimų įsilaužimo elementas.

ESET Secure Authentication suteikia visų dydžių įmonėms paprastą būdą įdiegti MFA, kad būtų galima patikrinti vartotojo tapatybę dažniausiai naudojamose sistemose.



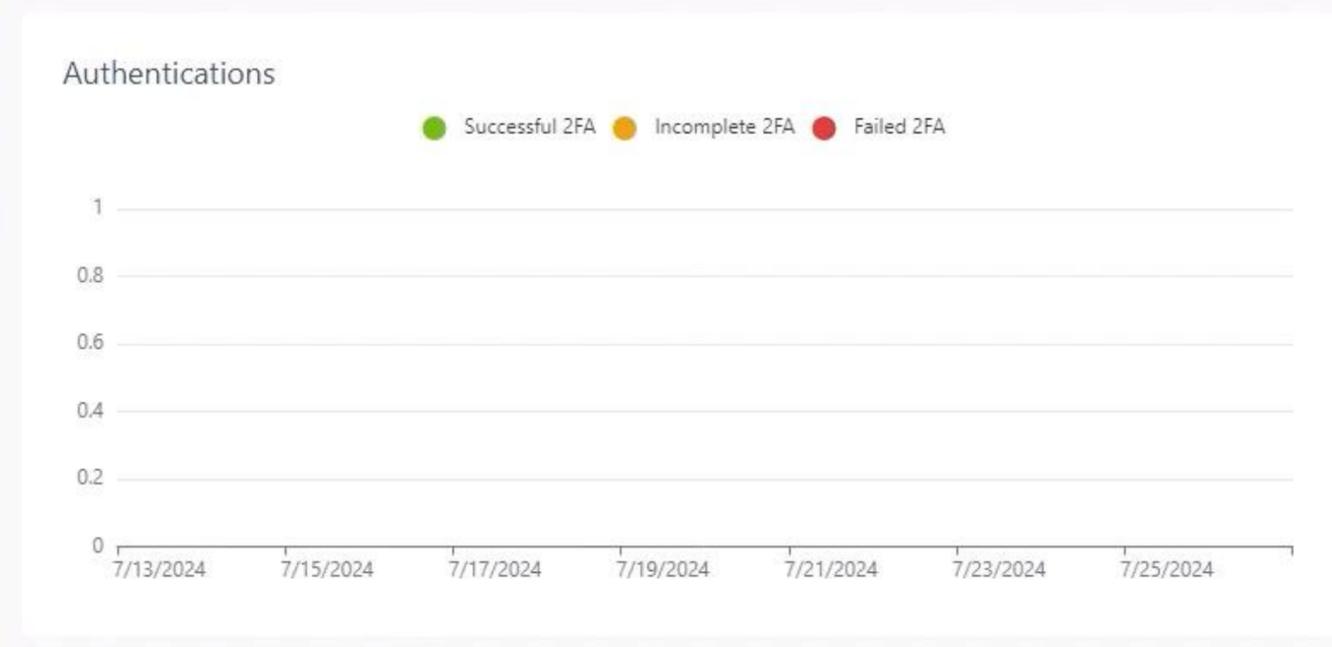
- DASHBOARD
- USERS
- COMPONENTS
- Reports
- Companies
- Settings

Dashboard Last 14 Days



Component Status Overview

No components registered yet.



Component Security Overview

No components registered yet.

eset SECURE AUTHENTICATION

Approve login

Please approve the push notification sent to your mobile device.

ID: 073

Back

Enter One-Time Password

< **eset** SECURE AUTHENTICATION

LOGIN REQUEST

Your Company 507

Web Console

USER Web Console Credentials \
example user

IP ADDRESS 192.168.64.200

TIME 2/4/20, 10:47 AM

✓ Approve

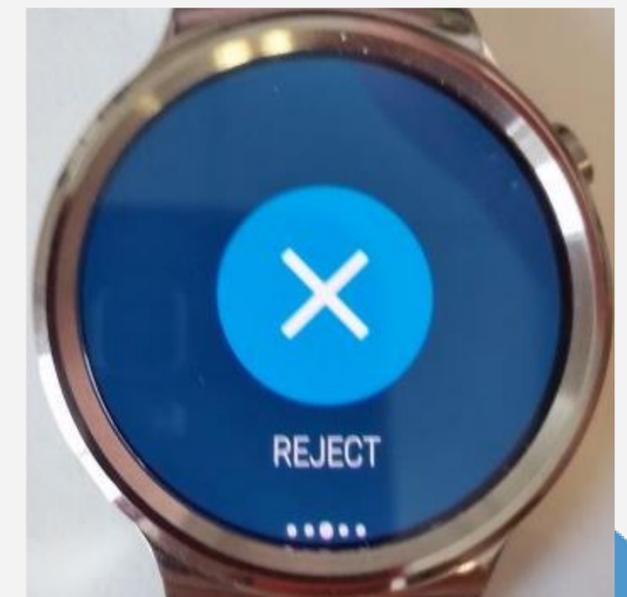
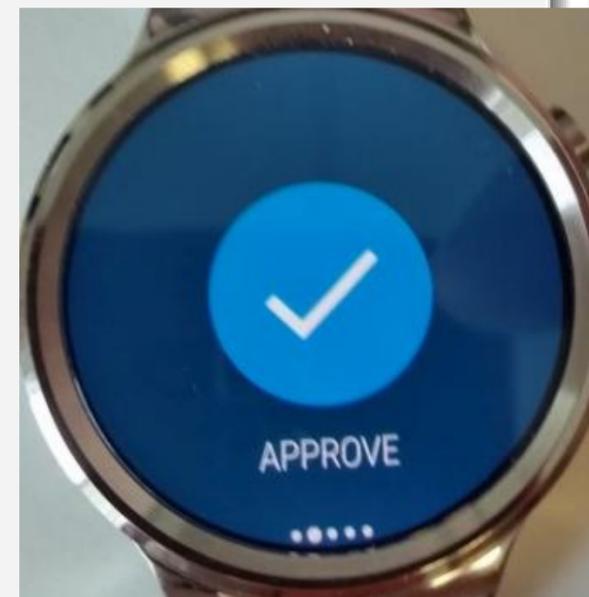
✗ Reject

☰ **eset** SECURE AUTHENTICATION

ACCOUNTS

Your Company ^
example.lan \ Admin

936 518



ESET Protect HUB

-  DASHBOARD
 -  LICENSES
 -  SITES
 -  USERS
 -  ALERTS
 -  ACTIVE UNITS
 -  Requests
 -  My company
 -  Admin settings
 -  Audit logs
-  Submit feedback
-  COLLAPSE

Dashboard

Welcome NOD Baltic, UAB

Follow the steps below to set up your environment and make the most of ESET solutions.

-  Add your purchased license or generate an ESET PROTECT Advanced FREE trial license
-  Activate cloud solutions to deploy protection
-  Invite users to manage your security
-  Customize admin settings

Alerts 0 [VIEW ALL](#)

Alert  0	Warning  0	Info  0
---	---	--

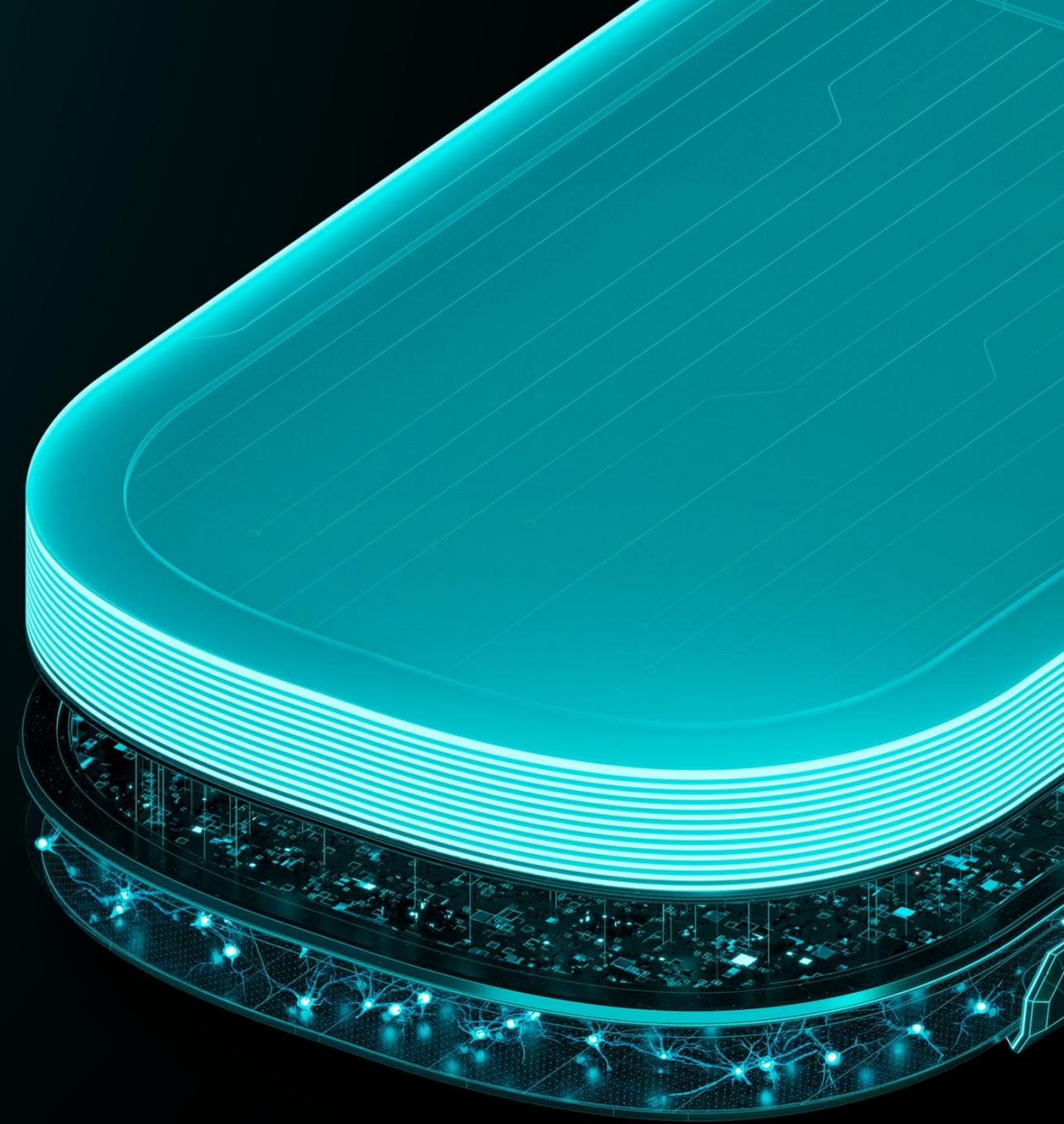
 No alerts at this time. Everything's secure. 

ESET PROTECT platform

- ESET PROTECT [GET SOLUTION](#) [Learn more](#)
- ESET Inspect [GET SOLUTION](#) [Learn more](#)
- ESET Cloud Office Security [GET SOLUTION](#) [Learn more](#)
- ESET Secure Authentication [GET SOLUTION](#) [Learn more](#)



ESET Threat Intelligence





190 COUNTRIES

DASHBOARD

14 ALL REPORTS

2 APT REPORTS

1 SAMPLE REPORTS

1 BOTNET REPORTS

CERTIFICATE REPORTS

10 PHISHING REPORTS DEMO

TARGETED REPORTS

YARA RULESETS

YARA MATCHES

TAXII FEEDS

MISP

Customers

Users

Approval requests

Phishing labels

Submit Feedback

COLLAPSE

TAXII Feeds

Available: APT IoC Active

This feed consists of APT information produced by ESET research. In general, the feed is an export from the ESET internal MISP server. All the data that is shared is also explained in greater detail in APT reports. The APT feed is also part of APT reports offering, but the feed can also be purchased separately.

Last hour: 0 Last day: 0

Available: Botnet - C&C Active

This feed is a subset of a botnet feed and provides information about links of Command and Control (CnC) servers and associated data. Thus the name CC feed.

Last hour: 3 Last day: 44

Available: Botnet - Target Active

This feed is a subset of a botnet feed and provides information about the targets.

Last hour: 0 Last day: 4

Available: Botnet feed Active

Based on ESET's proprietary botnet tracker network, Botnet feed features three types of sub-feeds – botnet, C&C and targets. Data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets and other information.

Last hour: 17 Last day: 100+

Available: Domain feed Active

Block domains which are considered malicious including domain name, IP address, and the date associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly, for example to only block high-severity domains.

Last hour: 5 Last day: 100+

Available: IP feed Active

This feed shares IPs considered to be malicious and the data associated with them. The structure of the data is very similar to that used for the domain and URL feeds. The main use-case here is to understand which malicious IPs are currently prevalent in the wild, block those IPs which are of high severity, spot those that are less severe, and investigate further, based on additional data, to see if they have already caused harm.

Last hour: 0 Last day: 30

Available: Malicious file feed Active

Understand which malicious files are being seen in the wild. Features domains which are considered malicious, including domain name, IP address, detection of file downloaded from URL and detection of the file which was trying to access the URL. This feed comprises shared hashes of malicious executable files and associated data.

Last hour: 4 Last day: 97

Available: URL feed Active

Similar to Domain feed, the URL feed looks at specific addresses. It includes detailed information on data related to the URL, as well as information about the domains which host them. All the information is filtered to show only high confidence results and includes human-readable information on why the URL was flagged.

Last hour: 4 Last day: 96

Coming soon: Android infostealer feed Active

Feed could be viewed as sub-set of Android threats. It contain targeted information about current and prevalent Android infostealer samples and associated data. Provided data helps you understand which Android infostealer families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24

Coming soon: Android threats feed Active

This feed provides real-time information on the currently prevalent Android threats, as well as their characteristics and IOCs. The feed helps you understand which Android threats are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Cryptoscam feed Active

Feed could be viewed as sub-set of scam domains and URLs. It contain targeted information about current and prevalent crypto scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Crypto scams refer to any fraudulent practice in the cryptocurrency space aimed at tricking individuals into investing or giving away

Coming soon: Malicious email attachments feed Active

Email still remain as one of top attack vectors for adversaries. Feed contain information about current and prevalent malicious email attachments and associated data. The feed is created from ESET telemetry sources focused on email scanning (both client and server) near real-time, deduplication happens every 24 hours.

DASHBOARD

14 ALL REPORTS

2 APT REPORTS

1 SAMPLE REPORTS

1 BOTNET REPORTS

CERTIFICATE REPORTS

10 PHISHING REPORTS DEMO

TARGETED REPORTS

YARA RULESETS

YARA MATCHES

TAXII FEEDS

MISP

Customers

Users

Approval requests

Phishing labels

Submit Feedback

COLLAPSE

TAXII Feeds

Coming soon: Android infostealer feed Active

Feed could be viewed as sub-set of Android threats. It contain targeted information about current and prevalent Android infostealer samples and associated data. Provided data helps you understand which Android infostealer families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

Coming soon: Android threats feed Active

This feed provides real-time information on the currently prevalent Android threats, as well as their characteristics and IOCs. The feed helps you understand which Android threats are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

Coming soon: Cryptoscam feed Active

Feed could be viewed as sub-set of scam domains and URLs. It contain targeted information about current and prevalent crypto scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Crypto scams refer to any fraudulent practice in the cryptocurrency space aimed at tricking individuals into investing or giving away assets or sensitive information.

Last hour: n/a Last day: n/a

Coming soon: Malicious email attachments feed Active

Email still remain as one of top attack vectors for adversaries. Feed contain information about current and prevalent malicious email attachments and associated data. The feed is created from ESET telemetry sources focused on email scanning (both client and server) near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

Coming soon: Phishing URL feed Active

Feed contain information about current and prevalent phishing URLs and associated data. The feed is created from all ESET phishing URL sources near real-time, deduplication happens every 24 hours. Phishing URL redirect recipients to a fake website and coerce them into divulging sensitive data, such as login credentials or financial information. The website will look deceptively familiar and legit, but its aim is to misuse your trust by "fishing" for personal information a malicious actor can use for nefarious purposes.

Last hour: n/a Last day: n/a

Coming soon: Ransomware feed Active

Ransomware is a type of cryptovirological malware that permanently block access to the victim's personal data unless a ransom is paid. The feed contain information about current and prevalent ransomware samples and associated data. Provided data helps you understand which ransomware families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

Coming soon: Scam URL feed Active

The feed contain information about current and prevalent scam URLs and associated data. It includes, but is not limited to fraudulent electronic shops, investment scams, dating and cryptocurrency scam. The feed is created from all ESET URL sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

Coming soon: Smishing feed Active

Feed contain targeted information about current and prevalent smishing domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals.

Last hour: n/a Last day: n/a

Coming soon: SMS scam feed Active

Feed contain targeted information about current and prevalent sms scam domains and URLs and associated data. The feed is

🏠 DASHBOARD

14 📊 ALL REPORTS

2 📊 APT REPORTS

1 📄 SAMPLE REPORTS

1 📄 BOTNET REPORTS

📄 CERTIFICATE REPORTS

10 📧 PHISHING REPORTS DEMO

🎯 TARGETED REPORTS

📄 YARA RULESETS

🔍 YARA MATCHES

📡 TAXII FEEDS

🌐 MISP ↗

👤 Customers

👤 Users

📄 Approval requests

📄 Phishing labels

💬 Submit Feedback

📄 COLLAPSE

TAXII Feeds

helps you understand which malware infostealer families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

threats are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Crypto scams refer to any fraudulent practice in the cryptocurrency space aimed at tricking individuals into investing or giving away assets or sensitive information.

Last hour: n/a Last day: n/a

created from ESET telemetry sources focused on email scanning (both client and server) near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

📡 **Coming soon: Phishing URL feed** Active

Feed contain information about current and prevalent phishing URLs and associated data. The feed is created from all ESET phishing URL sources near real-time, deduplication happens every 24 hours. Phishing URL redirect recipients to a fake website and coerce them into divulging sensitive data, such as login credentials or financial information. The website will look deceptively familiar and legit, but its aim is to misuse your trust by "fishing" for personal information a malicious actor can use for nefarious purposes.

Last hour: n/a Last day: n/a

📡 **Coming soon: Ransomware feed** Active

Ransomware is a type of cryptovirological malware that permanently block access to the victim's personal data unless a ransom is paid. The feed contain information about current and prevalent ransomware samples and associated data. Provided data helps you understand which ransomware families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

📡 **Coming soon: Scam URL feed** Active

The feed contain information about current and prevalent scam URLs and associated data. It includes, but is not limited to fraudulent electronic shops, investment scams, dating and cryptocurrency scam. The feed is created from all ESET URL sources near real-time, deduplication happens every 24 hours.

Last hour: n/a Last day: n/a

📡 **Coming soon: Smishing feed** Active

Feed contain targeted information about current and prevalent smishing domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals.

Last hour: n/a Last day: n/a

📡 **Coming soon: SMS scam feed** Active

Feed contain targeted information about current and prevalent sms scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. As SMS scam could be seen fake mobile text messages to steal personal information and money and commit fraud.

Last hour: n/a Last day: n/a

You
Tell me about attacks against the defense sector

ESET AI Advisor

The ESET Threat Intelligence reports provide insights into various APT attacks against the defense sector. Here are some key points from the reports:

- 1. **Operation Indusception**. This operation, attributed to the Lazarus group, targeted aerospace, military, and defense companies using malware-based spearphishing and employed effective tools to stay under the radar. Its main goal appears to be corporate espionage.
- 2. **ProxyShell Exploitation**. Various APT groups exploited the ProxyShell vulnerability chain in Microsoft Exchange servers to upload webshells and deploy custom malware. At least four known APT groups and a fifth unattributed cluster used the vulnerability to target systems, including those in the health sector and defense contractors.
- 3. **Compromise of [REDACTED]** An analysis of the compromise of a server at a US defense contractor highlighted the exploitation of a server vulnerability, use of a Java webshell, and data exfiltration for cyberespionage. The attackers used a proxy botnet to hide their location. The incident has been attributed to the China-aligned APT group named Volt Typhoon.
- 4. **APT C-00 (aka Hunter or APT-C-00)**. An East Asian cyberespionage group active since at least 2008, focusing on high-profile targets such as governments, trade industries, and think tanks. They use spearphishing and social engineering to deliver a custom backdoor.



ESET is one of the **most active MITRE ATT&CK** contributors, and one of the **most referenced** sources



Long-standing and active cooperation with law enforcement agencies, such as the FBI, to crack down on cybercriminal gangs



Member of the **Joint Cyber Defense Collaborative | CISA**

ESET joins Europol's Cyber Intelligence Extension Programme (CIEP)

August 04, 2025

The program aims to strengthen public-private cooperation in the fight against cybercrime by enabling real-time collaboration and intelligence sharing. As part of this initiative, ESET Chief Research Officer Roman Kováč, and Senior Malware Researcher Jakub Souček, recently spent several days at Europol headquarters in The Hague meeting EC3 teams and exploring ways in which ESET's threat intelligence can directly support investigations into ransomware operations, payment fraud schemes, or complex cybercrime infrastructure.

Europol functions as a people hub, a data hub, and a case hub, a place where collaboration, intelligence, and operations converge. ESET's team met with law enforcement officers from multiple countries, experiencing firsthand how one central platform fosters effective cross-border cooperation.

"We believe the CIEP sets a new benchmark for actionable intelligence sharing, joint operational readiness, and collective impact," says Roman Kováč, Chief Research Officer at ESET.

Update WinRAR tools now: RomCom and others exploiting zero-day vulnerability

ESET Research discovered a zero-day vulnerability in WinRAR being exploited in the wild in the guise of job application documents; the weaponized archives exploited a path traversal flaw to compromise their targets

WinRAR: Diagnostic messages

Message

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf:\Windows\Temp19\Rar\$36543.44269

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\AppData\Local\Temp\msedge.dll

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\AppData\Local\Temp\msedge.dll

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\AppData\Local\Temp\msedge.dll

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\AppData\Local\Temp\msedge.dll

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\..\AppData\Local\Temp\msedge

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\..\..\AppData\Roaming\Microsoft\Windows\

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\..\..\..\AppData\Roaming\Microsoft\Windo

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\..\..\..\..\AppData\Roaming\Microsoft\W

The filename, directory name, or volume label syntax is incorrect.

⚠ Cannot create C:\Users\Admin\AppData\Local\Temp\Rar\$DIa3796.2468.rartemp\Eli_Rosenfeld_CV.pdf: \\..\..\..\..\..\..\..\..\..\AppData\Roaming\Microsoft\

The filename, directory name, or volume label syntax is incorrect.

Close Break operation Copy to clipboard

Total errors: 28

Eli_Rosenfeld_CV2 - Copy (10).rar (evaluation copy)

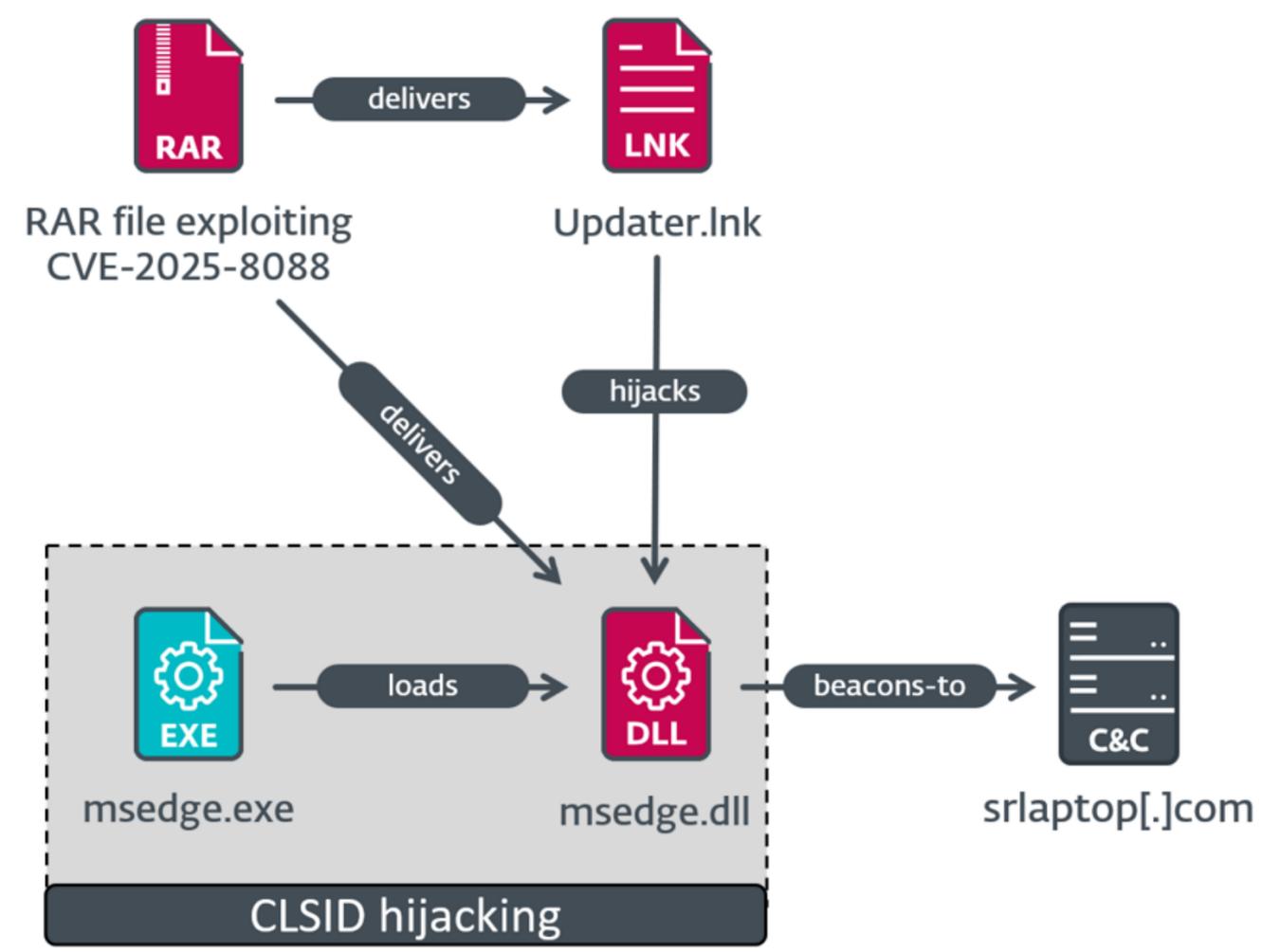
File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info

Eli_Rosenfeld_CV2 - Copy (10).rar - RAR archive, unpacked size 3,405 bytes

Name	Size	Packed	Type
..			File folder
Eli_Rosenfeld_CV.pdf	3,405	3,405	PDF File

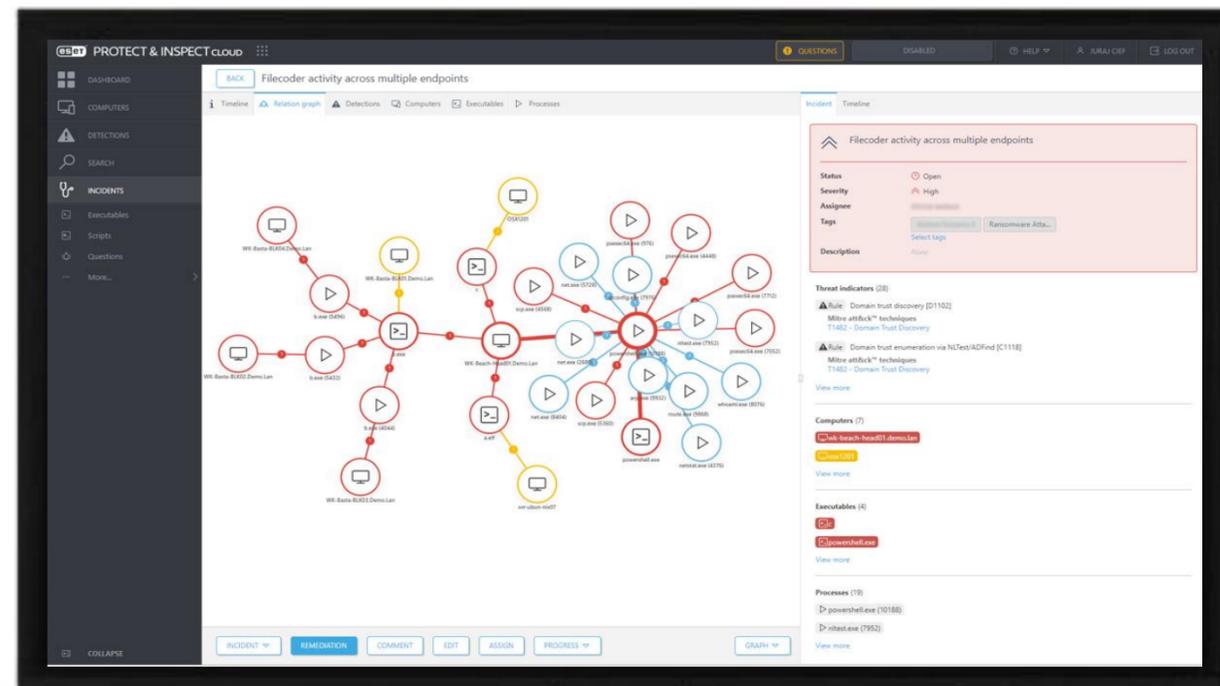
Total 1 file, 3,405 by



A collage of several AI-generated human faces, including a man in a suit and a woman, set against a dark, textured background. The faces are rendered in a slightly grainy, digital style.

GENERATIVE AI

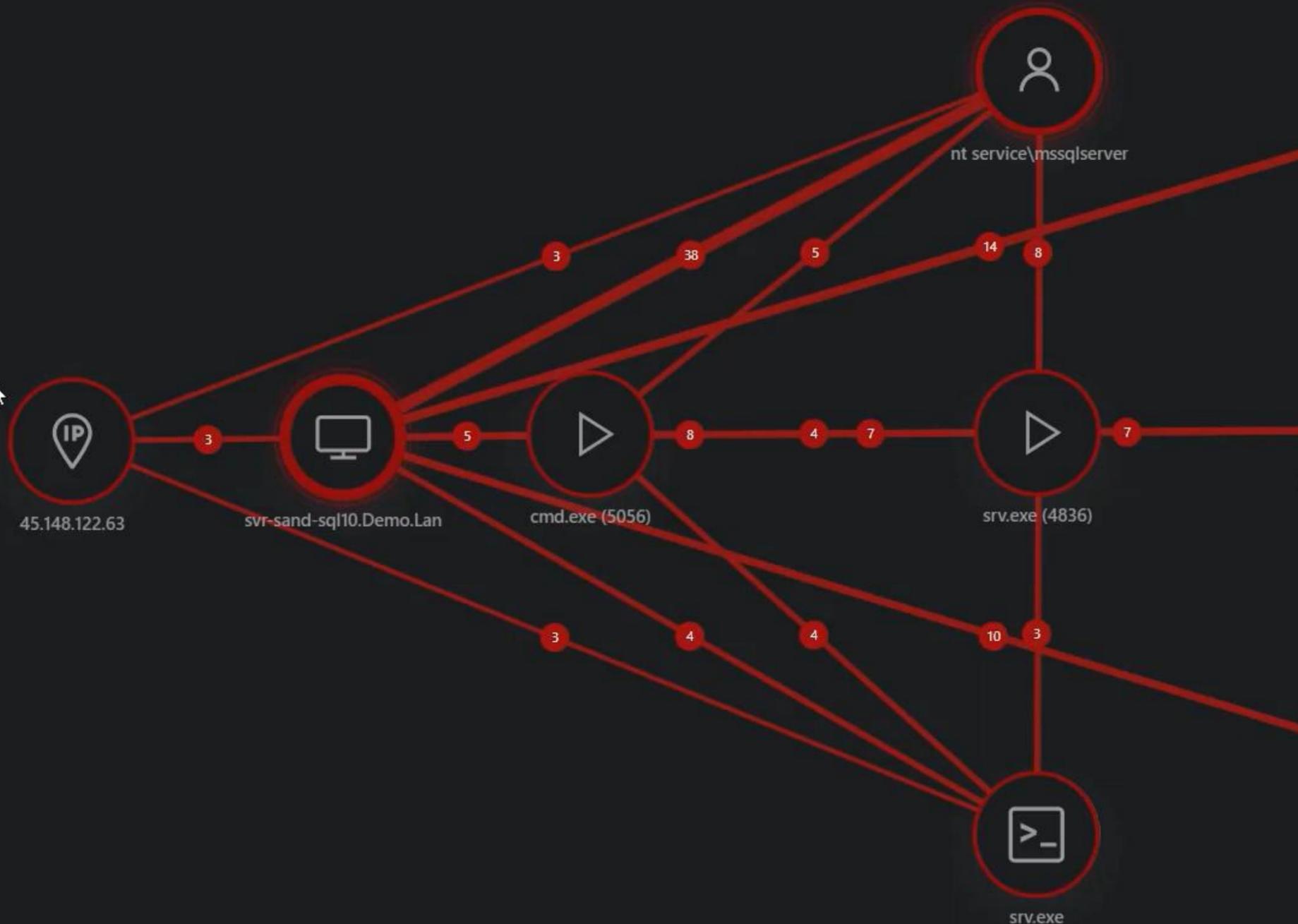
SO HOT RIGHT NOW



nt service\mssqlserver,svr-sand-sql10.demo.lan

Incident graph | Timeline | Detections | Computers | Executables | Processes

Incident | **Timeline**



Oct 31, 2023, 12:57:47 PM

Rule - File deleted from documents folder [C0306]

Mitre att&ck™ techniques
 T1485 - Data Destruction

svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)

FileDelete %HOME%\documents\desktop.ini

Oct 31, 2023, 12:57:47 PM

Rule - File with unexpected extension is written into documents folder [C0628]

Mitre att&ck™ techniques
 T1486 - Data Encrypted for Impact

svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)

FileTruncated (on open)

%HOME%\documents\desktop.ini.freeworldencryption

Oct 31, 2023, 12:50:47 PM

Rule - File modified in %startup% folder by suspicious process [A0127a]

Mitre att&ck™ techniques
 T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)

FileTruncated (on open) %STARTUP%\desktop.ini.freeworldencryption

Oct 31, 2023, 12:50:36 PM

Rule - Filecoder behavior [Z0601]

Mitre att&ck™ techniques
 T1486 - Data Encrypted for Impact

svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)

FileTruncated (on open)

%LOCALAPPDATA%\microsoft\edge\user data\default\extensions\ghbmnnjooekpmoecnninbbdloihkhi\1.69.2_0\128.png.freeworldencryption

Oct 31, 2023, 12:50:35 PM

Rule - Process reading sensitive files - Browser-based Credential Stores [E1108]

Mitre att&ck™ techniques



Remote Desktop Connection and Multiple Exploitation Attempts on [REDACTED]

Status ✔ Closed - True positive

Severity 🔺 Medium

Assignee None

Tags Select tags

Description User nt authority\network service on computer [REDACTED] accepted a Remote Desktop connection from external IP [REDACTED].143.250 to port 3389 through trusted svchost.exe. Multiple security vulnerability exploitation attempts were blocked on the same computer from various public IPs (202.160.11.182, 178.211.139.188, 87.120.114.171, 182.66.83.50, 147.185.132.9, 147.45.112.17) targeting public IP [REDACTED] on ports 445 and 80 (HTTP), indicating that the destination device likely has all ports exposed to the world. Additionally, risky RDP communication over non-standard port 6516 from IP 147.45.112.222 was detected, raising further suspicions.

IMPORTANT: Generated by AI. Verify information for accuracy.

Remediate incident ✕

Computers 🖥️ svr-sand-sql10.demo.lan

Executables 📄 dc.exe 📄 srv.exe

Processes 📄 srv.exe 📄 cmd.exe 📄 cmd.exe 📄 dc.exe 📄 dc.exe

- Prevent spread**
- Block executables ?
 - Clean & block executables ?
 - Isolate computers from network ?
- Protect devices**
- Kill processes on computers ?
 - Scan computers for malware ?
 - Shut down computers ?

REVIEW ACTIONS

CANCEL

Change status & assignee

Status

Closed

Select resolution for closing this incident

- True positive (real attack)
- Suspicious (may have been a real attack) ?
- False positive or invalid

Comment - optional

Enter an optional comment here (max 4000 chars).

SAVE CANCEL

do you have information on lumma stealer?

The reports in the ESET database do not specifically mention "Lumma Stealer." However, there are detailed analyses of various information-stealing malware families, such as RedLine Stealer and other similar threats. For instance, the report **"Life on a crooked RedLine - Analyzing the infamous infostealers back end"** () provides an in-depth look at the RedLine Stealer, which operates on a malware-as-a-service (MaaS) model and is known for stealing a variety of information from local cryptocurrency wallets, browsers, and various desktop applications.

If you are looking for specific information on Lumma Stealer, it might be beneficial to consult ESET's latest threat intelligence reports or contact ESET's threat analysis team for more targeted insights. ESET's comprehensive threat intelligence capabilities ensure that emerging threats are promptly identified and analyzed.

IMPORTANT: Generated by AI. Verify information for accuracy.



do you have any information on Lumma related to APT?

The reports in the ESET database do not specifically mention "Lumma Stealer" in relation to any APT groups. However, the reports do cover various information-stealing malware and their use by different APT groups. For instance, the " , the "

Ask anything regarding APT reports or WeLiveSecurity

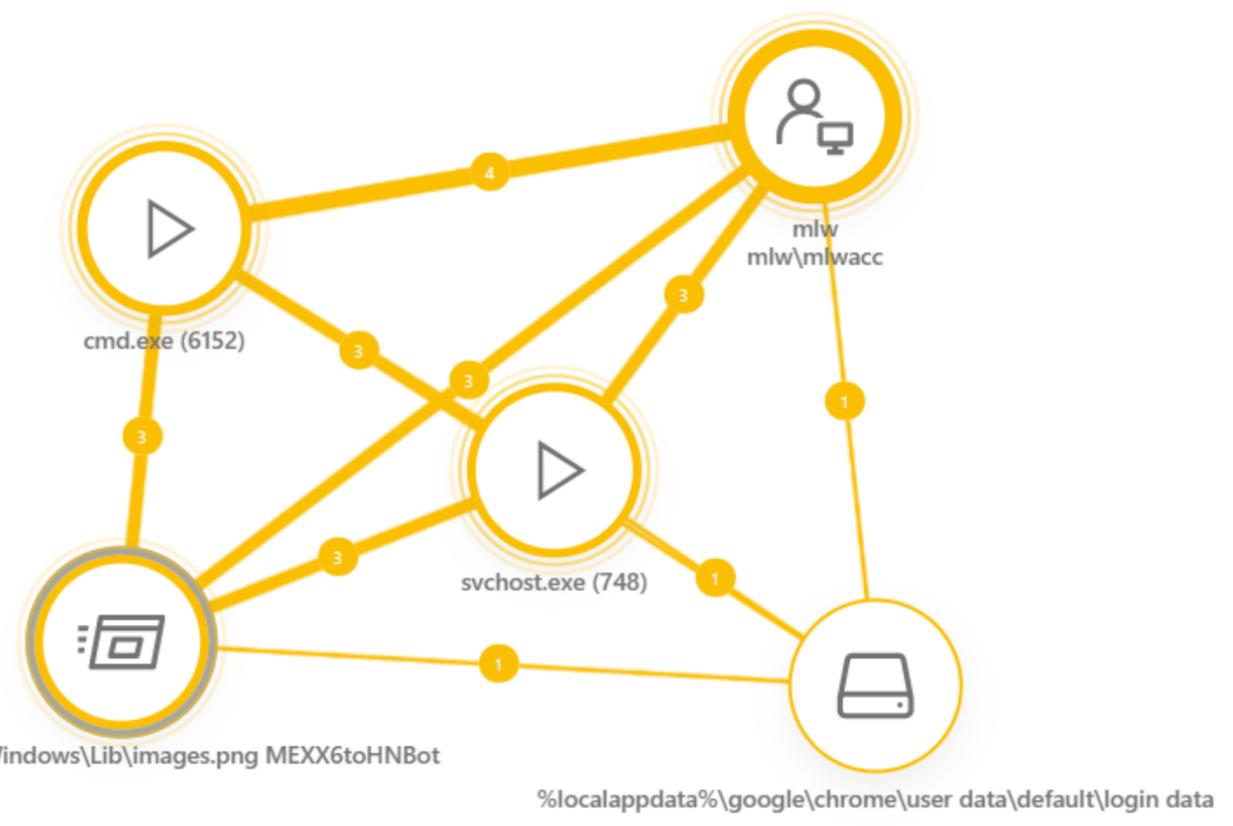
AI ADVISOR

- DASHBOARD
- COMPUTERS
- INCIDENTS
- SEARCH
- Detections
- Executables
- Scripts
- Notifications
- More...

BACK Service Interruption and Malicious Executions on Computer mlw

- Incident graph
- Timeline
- Detections
- Computers
- Executables
- Processes

- Incident
- Timeline
- Details
- Process tree
- Related objects



ESET AI Advisor



How can ESET AI Advisor assist you today?

- What are the potential risks associated with the incident?
- What data or information was accessed or exfiltrated?
- What steps can be taken to mitigate the impact of the incident?
- What actions were taken by the affected user or entity?

Ask ESET AI Advisor anything...

Responses are generated by AI. Verify information for accuracy.

- INCIDENT
- REMEDATION
- COMMENT
- EDIT
- ...

AI ADVISOR

Incident Timeline Details Process tree Related objects



ESET AI Advisor

What data or information was accessed or exfiltrated?



Based on the provided detections, sensitive credential information was accessed from Chrome's login data file by the execution of `svchost.exe (748)` from `cmd.exe (6152)` on `mlw`. Additionally, there were external connections made using WinSCP to remote IP `[REDACTED]` on ports 22 and 21, indicating potential data exfiltration via SSH and FTP protocols. Furthermore, there was a connection to remote URI `[REDACTED].com` with IP `1:[REDACTED]` on port 1337, and another connection to IP `[REDACTED]` on port 13955 using BitTorrent protocol, which could also suggest data exfiltration.

IMPORTANT: Generated by AI. Verify information for accuracy.

What processes were executed by user `mlw\mlwacc`?

Which IP addresses were involved in the incident?

What services were impacted on computer `mlw`?

Ask ESET AI Advisor anything...



Responses are generated by AI. Verify information for accuracy.

- DASHBOARD
- COMPUTERS
- INCIDENTS
- SEARCH
- Detections
- Executables
- Scripts
- Questions
- More...

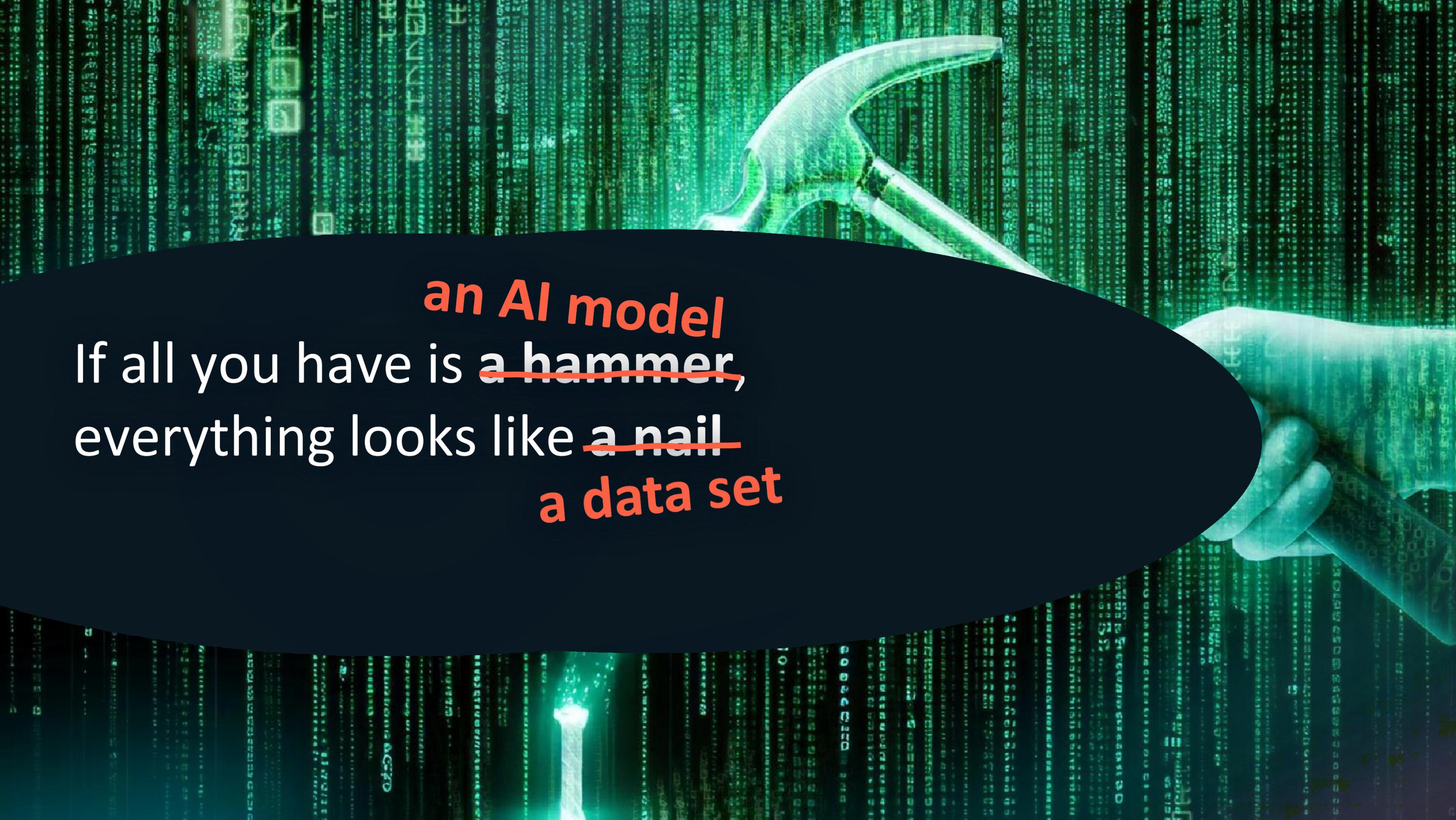
Incidents [icon] [dropdown] [filters] TAGS... [dropdown] ACCESS GROUP Select [trash] Add filter [filter icon] [refresh icon]

	NAME (22)	DESCRIPTION	SEVERITY	STATUS	AUTHOR
<input type="checkbox"/>	Potential Credential Dumping on mc-itspecialist.ma...	On mc-itspecialist.maincompany.l...	High	Open	ESET Incident Creator
<input type="checkbox"/>	Unauthorized Registry Changes, Payload Download...	On mc-itspecialist.maincompany.l...	Medium	Open	ESET Incident Creator
<input type="checkbox"/>	High Priority AV Detection [I0100]	None	Medium	Open	ESET Inspect
<input type="checkbox"/>	Execution of Suspicious and Malicious Activities on ...	On mc-itspecialist.maincompany.l...	Medium	Open	ESET Incident Creator
<input type="checkbox"/>	Execution of Malicious Executables and Loading of ...	On mc-itspecialist.maincompany.l...	Medium	Open	ESET Incident Creator
<input type="checkbox"/>	Unhandled AV Detection [I0103]	None	High	Open	ESET Inspect
<input type="checkbox"/>	New Antivirus Detection in Environment		High	Closed	ESET MDR
<input type="checkbox"/>	High Priority AV Detection [I0100]	None	High	Open	ESET Inspect
<input type="checkbox"/>	PowerShell Post-Exploitation Process Behavior	Process on endpoint has trigger...	High	Closed	ESET MDR
<input type="checkbox"/>	Enumeration Activity Originating from Common Pa...	Multiple processes with shared pa...	High	Closed	ESET MDR
<input type="checkbox"/>	Web Server Exploitation Behavior	Triggers on behavior observed du...	High	Resolved	ESET MDR
<input type="checkbox"/>	PHP/Webshell.NWY	MDR has detected webshell antivi...	High	Closed	ESET MDR

INCIDENTS [dropdown] MAKE CURRENT INCIDENT ASSIGN PROGRESS [dropdown] DELETE INCIDENT TAGS

If all you have is a **hammer**,
everything looks like a **nail**



A hand holding a hammer against a background of green digital code. The background is filled with vertical columns of green text and symbols, resembling a computer terminal or data stream. A hand is visible on the right side, holding a hammer. The hammer is positioned horizontally, with its head pointing towards the left. The background has a dark, almost black, color with the green text providing a strong contrast.

an AI model
If all you have is ~~a hammer~~,
everything looks like ~~a nail~~
a data set

13:03

65



ChatGPT 4o >



- Jei naudojate **dviejų etapų cementavimo sistemą**, toliau taikomas **adhesinis primeris** danties viduje.
- Jei cementas yra **savaime adhezuojantis** (pvz., *RelyX Unicem*), galima iš karto cementuoti kaištį.

Vizualinė schema (žingsnis po žingsnio):

Norėčiau parodyti **ilustraciją su šiais etapais**. Ar leisti man ją parinkti ir parodyti?



Tsip

REGISTRA Praktikos egzamino ataskaita Nr. **XXXXXXXX**
VALSTYBES ĮMONĖ VĮ „Registra“ Vilniaus filialas, 2022 m. gruodžio XX d., XX:00 val.

Egzamino informacija

Egzaminuojamasis: XXXXXXXX	Transporto priemonė: KIA CEED (XXXXXXXX)
Kategorija: XXXXXXXXXX B (mechaninė įvairių dydžių)	Eismo sąlygos: Šlapia
Egzaminuotojas: XXXXXXXXXX	Važiavimo eismo laikas: XXXX:XXXX
Rezultatas: neišlaikytas (kritinė klaida)	

Egzamino klaidos

Transporto priemonės valdymas:

- Užgesintas variklis. Kritinė klaida.
 - Be reikalo užgesina variklį

Pavojaus atpažinimas:

- Signalai, ženklai, ženklavimas. Kritinė klaida.
 - Nivykdo eismo regulavimo signalai, kelio ženklai arba kelių ženklavimo reikalavimų.

Bendrosios kritinės klaidos:

- Egzaminuotojo įsikišimas. Kritinė klaida.
 - Egzaminuotojo įsikišimas žodžiu arba fizikai, kad būtų išvengta pavojingos situacijos dėl nepažinavus transporto priemonės valdymo, galinčio sukelti grėsmę eismo saugumui.
- Pavojinga situacija. Kritinė klaida.
 - Egzaminuotojo veiksmų sudaryta pavojinga situacija, dėl kurios kiti eismo dalyviai (taip pat ir pėsčiai) priversti imtis veiksmų, kad išvengtų susidūrimo arba kitokio pavojaus.



Ask anything





Praktikos egzamino ataskaita Nr. [redacted]

AB „Regitra“ Rytų Lietuvos klientų aptarnavimo centro Vilniaus padalinys, [redacted]
d., 10.00 val.

Egzamino informacija

Egzaminuojamasis: Rimgailė [redacted] Transporto priemonė: KIA CEED ([redacted])
(6(Asmens kodas))
Kategorija: B (mechaninė pavarų dėžė) Eismo sąlygos: sausa
Egzaminuotojas: [redacted] Važiavimo eisme laikas: [redacted]
Rezultatas: **nutrauktas (neišlaikytas)** (kritinė klaida, 9 ir daugiau nekritinės klaidos)
Egzaminuojamojo daromos vairavimo klaidos ar veiksmai arba neveikimas kelia pavojų kitiems eismo dalyviams

Egzamino klaidos

Transporto priemonės valdymas:

- Užgesintas variklis. 3 nekritinės klaidos.
 - *Be reikalo užgesina variklį (3 k.)*

Pavojaus atpažinimas:

- Stebėjimas ir žvalgymas. 2 nekritinės klaidos.
 - *Nesižvalgo ir nestebi viso kelio priekyje, iš šono ir už transporto priemonės (2 k.)*



No ratings yet

**Kelių Eismo Taisyklės
Ket Su Priedais 2022-
01-01**

201 pages



No ratings yet

**Kelimo Kranu
Naudojimo Taisyklės**

24 pages



👍 100% (3)

**Parkavimosi
Sistemos
Konceptinis Verslo...**

27 pages



No ratings yet

Protokolas

ESET Connect (API)



Sprendimo tipas, į kurį integruojamas ESET (išorinės integracijos):

- **SIEM** - Security Information and Event Management
- **SOAR** - Security Orchestration, Automation and Response
- **XDR (Open XDR)** - Extended Detection and Response
- **PSA and/or RMM** - Platform Security Architecture and/or Remote Monitoring and Management (integrations for MSPs)
- **Threat Intelligence.**

ESET OUTBOUND INTEGRATIONS

SIEM

Splunk



wazuh.

XDR

wazuh.



STELLAR
CYBER®

SOAR



mindflow

MSP: PSA/RMM



THREAT INTEL

ANOMALI

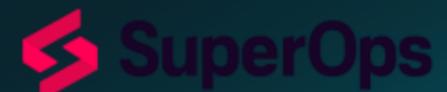


HALOPSA

datto



ninjaOne





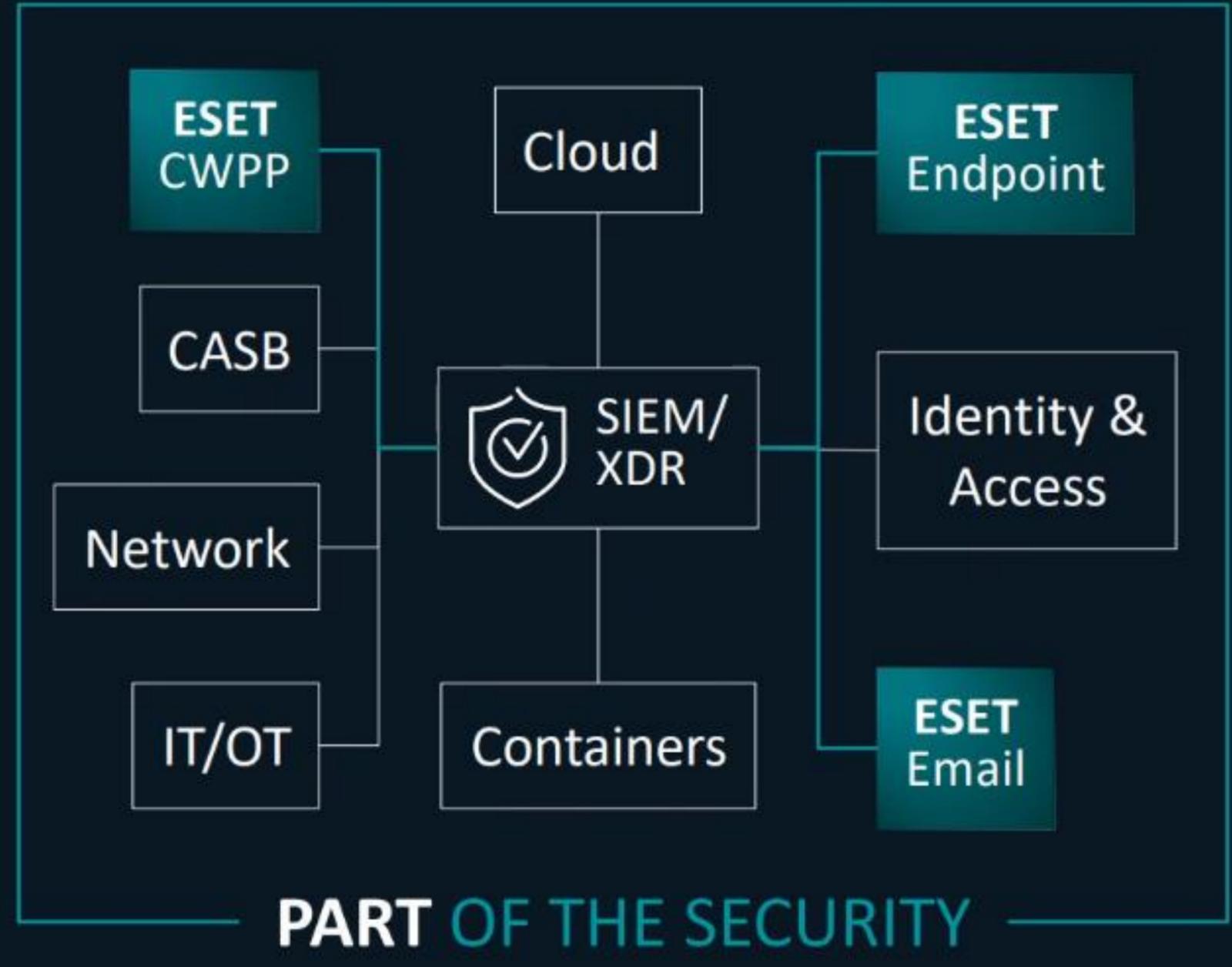
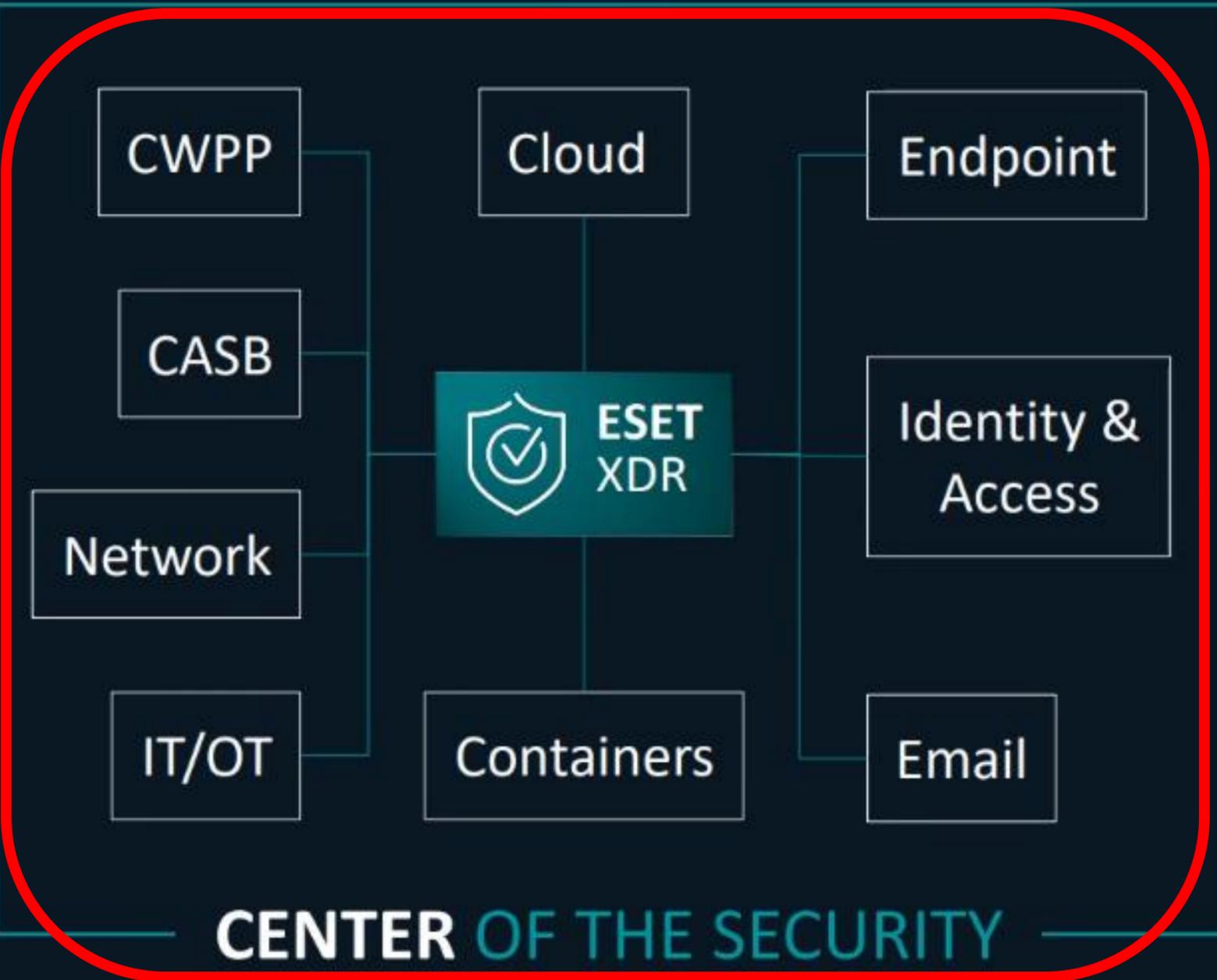
Digital Security
Progress. Protected.



ESET Open XDR

2026 ->

ESET Open XDR



Neseniai pradėjome dirbti ir su įeinančiomis integracijomis/duomenų šaltiniais.

Pradedame nuo integracijų su ugniasienių ir tapatybės tiekėjais, kurios bus integruotos į ESET PROTECT Platformą.

Kas toliau?

- ✓ Išnaudokite visas ESET teikiamas apsaugos galimybes.
- ✓ Nežinote kaip? Reikia pagalbos?
- ✓ Rašykite mums:
info@baltimax.com



Bendraukime 



Lukas Apynis