SECURITY DAYS

ESET PROTECT v praxi: Evolúcia bezpečnostnej platformy

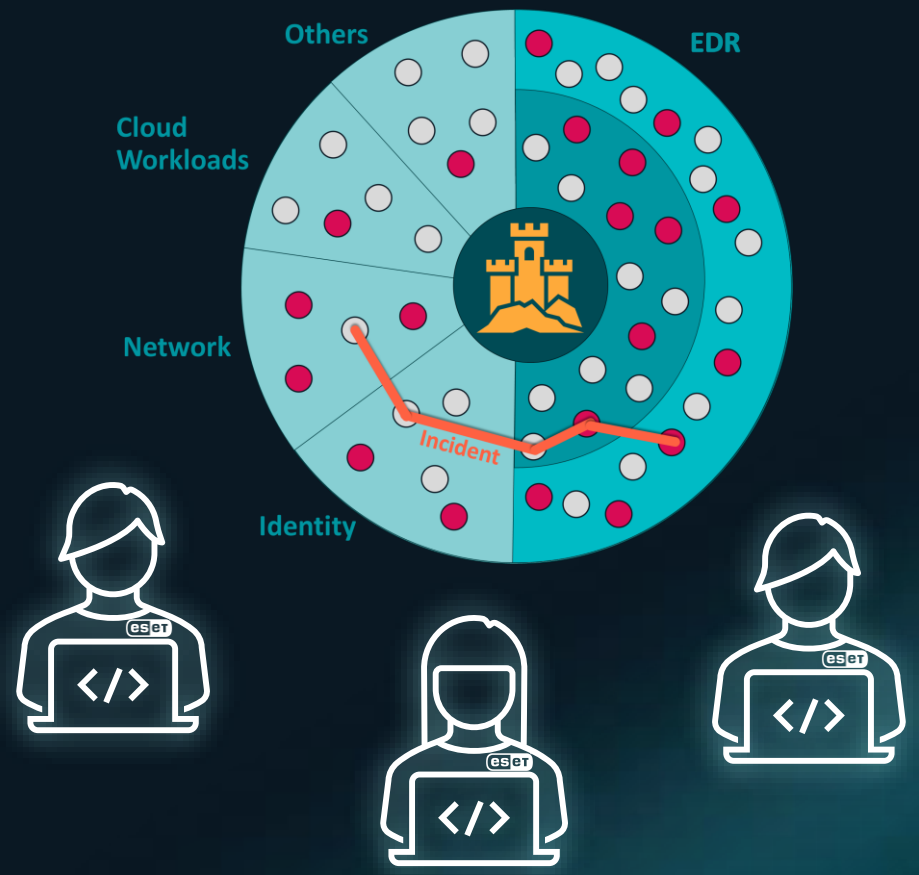
Igor Hula
Principal Product Manager

14. apríl 2026 / hotel NH Bratislava Gate One

Cybersecurity Progress. Protected. & SME KONFERENCIE

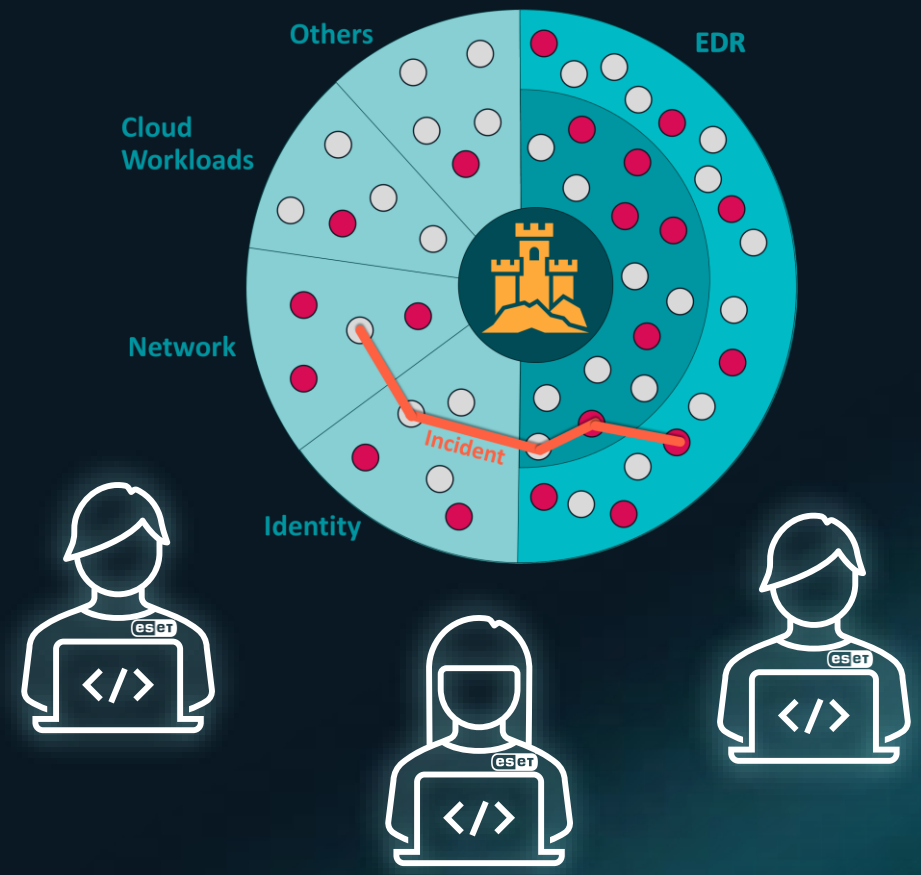
Vízia

MENEJ SPRAVOVAŤ
VIAC CHRÁNIŤ
DÔVEROVAŤ ESETU



Vision

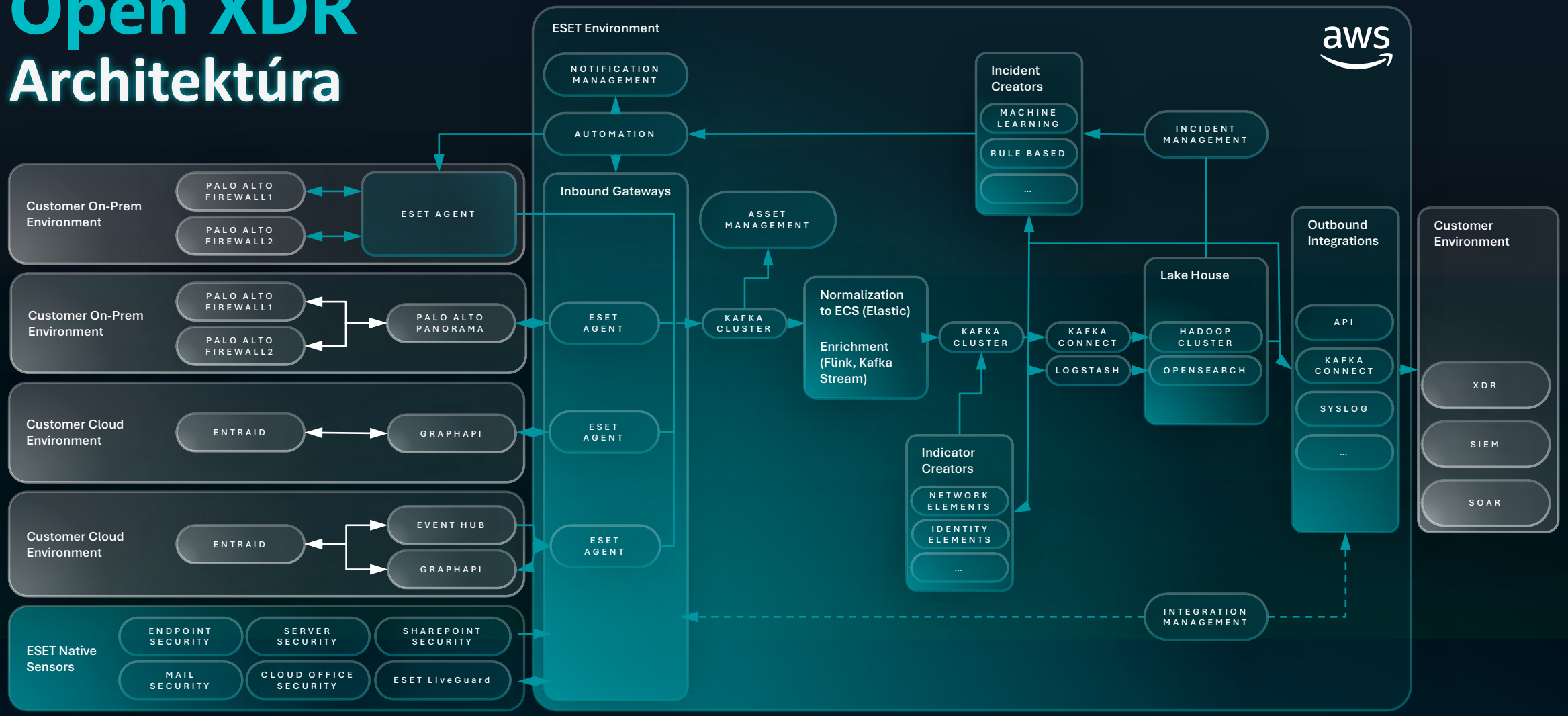
MANAGE LESS
PROTECT MORE
TRUST ESET



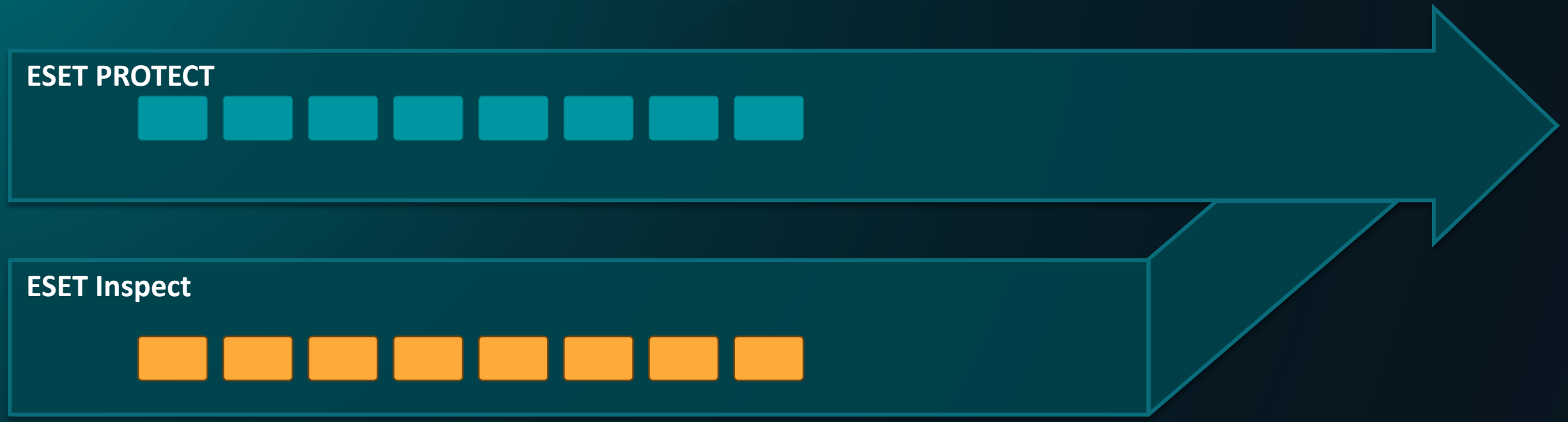
ESET PROTECT Transformácia

Nová architektúra & Lepší používateľský zážitok

Open XDR Architektúra



ESET PROTECT – konsolidácia rozhraní



EP 7.0
Január 2026

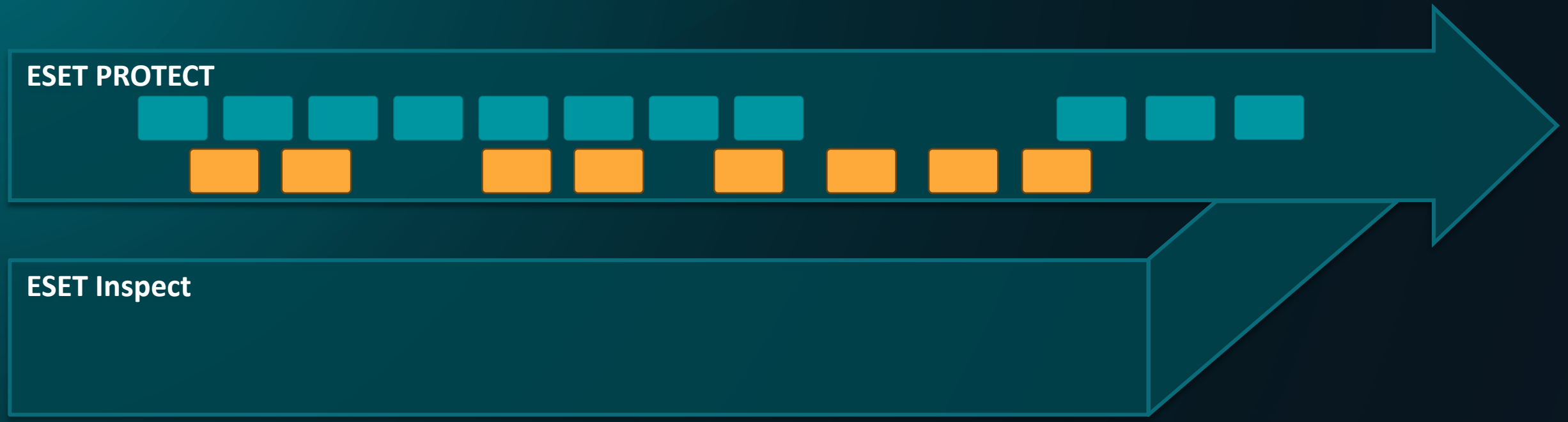
EP 7.1
Marec 2026

EP 7.2
Jún 2026

EP 7.3
September 2026

EP NEXT
Q4 2026 → Budúcnosť

ESET PROTECT – konsolidácia rozhraní



EP 7.0
Január 2026

EP 7.1
Marec 2026

EP 7.2
Jún 2026

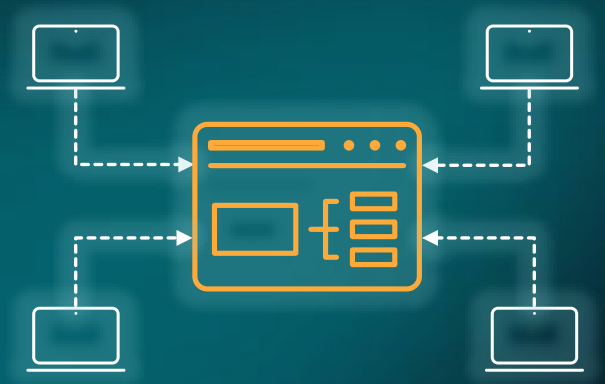
EP 7.3
September 2026

EP NEXT
Q4 2026 → Budúcnosť

Open XDR Integrácie

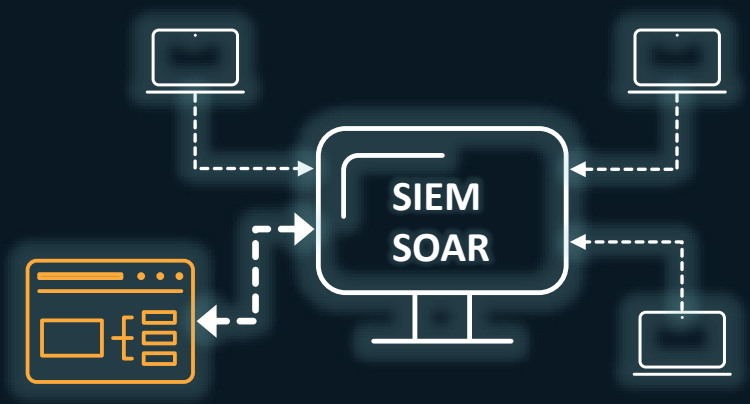
Čo sa snažíme robiť inak?

Dva hlavné režimy fungovania



CENTRUM BEZPEČNOSTI

Zameranie na XDR integrácie pre lepšiu viditeľnosť a vyššiu úroveň bezpečnosti



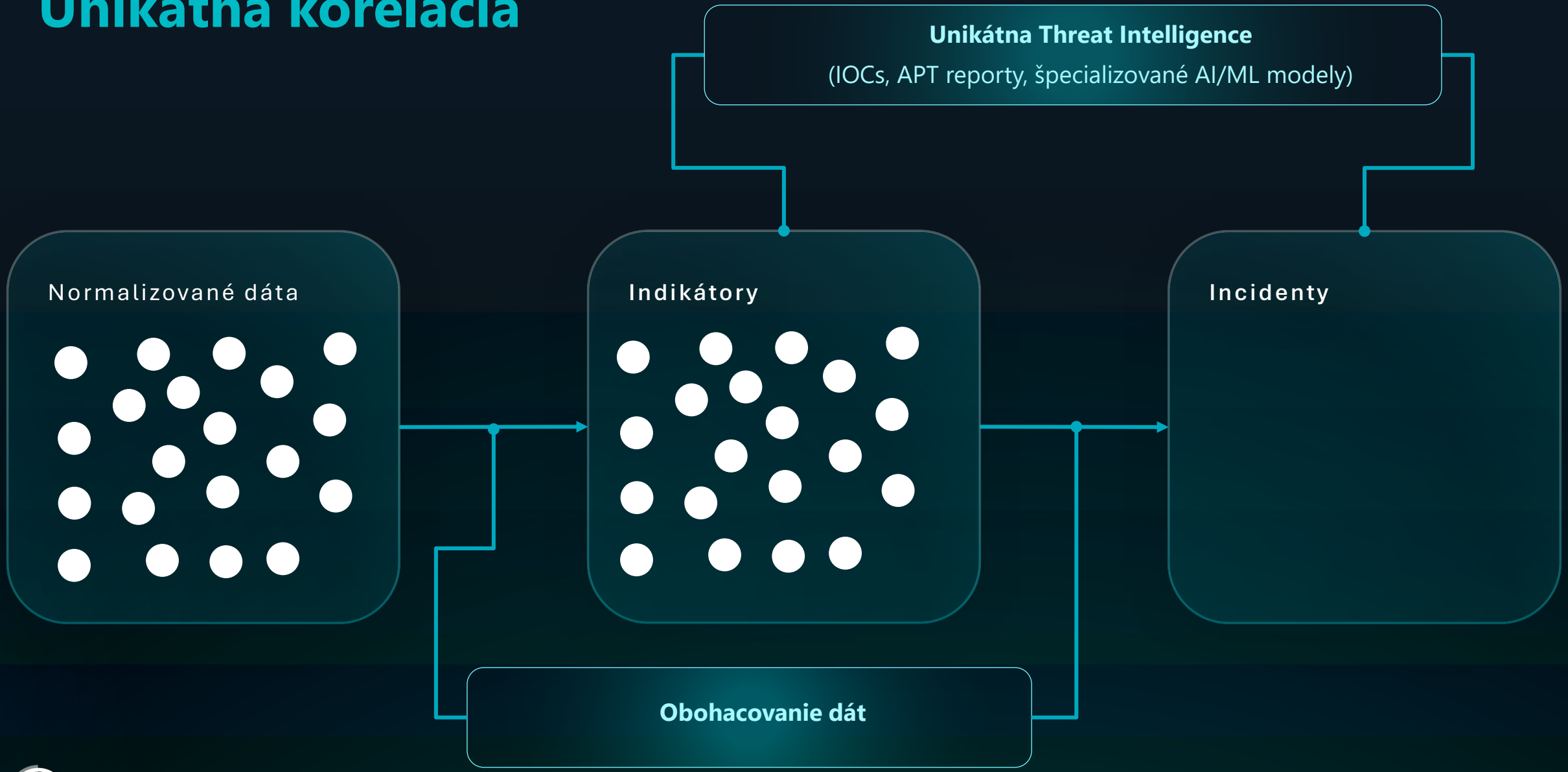
SÚČASŤ BEZPEČNOSTI

Poskytovanie kvalitných dát (napr. incidentov) prostredníctvom streamovania alebo cez API

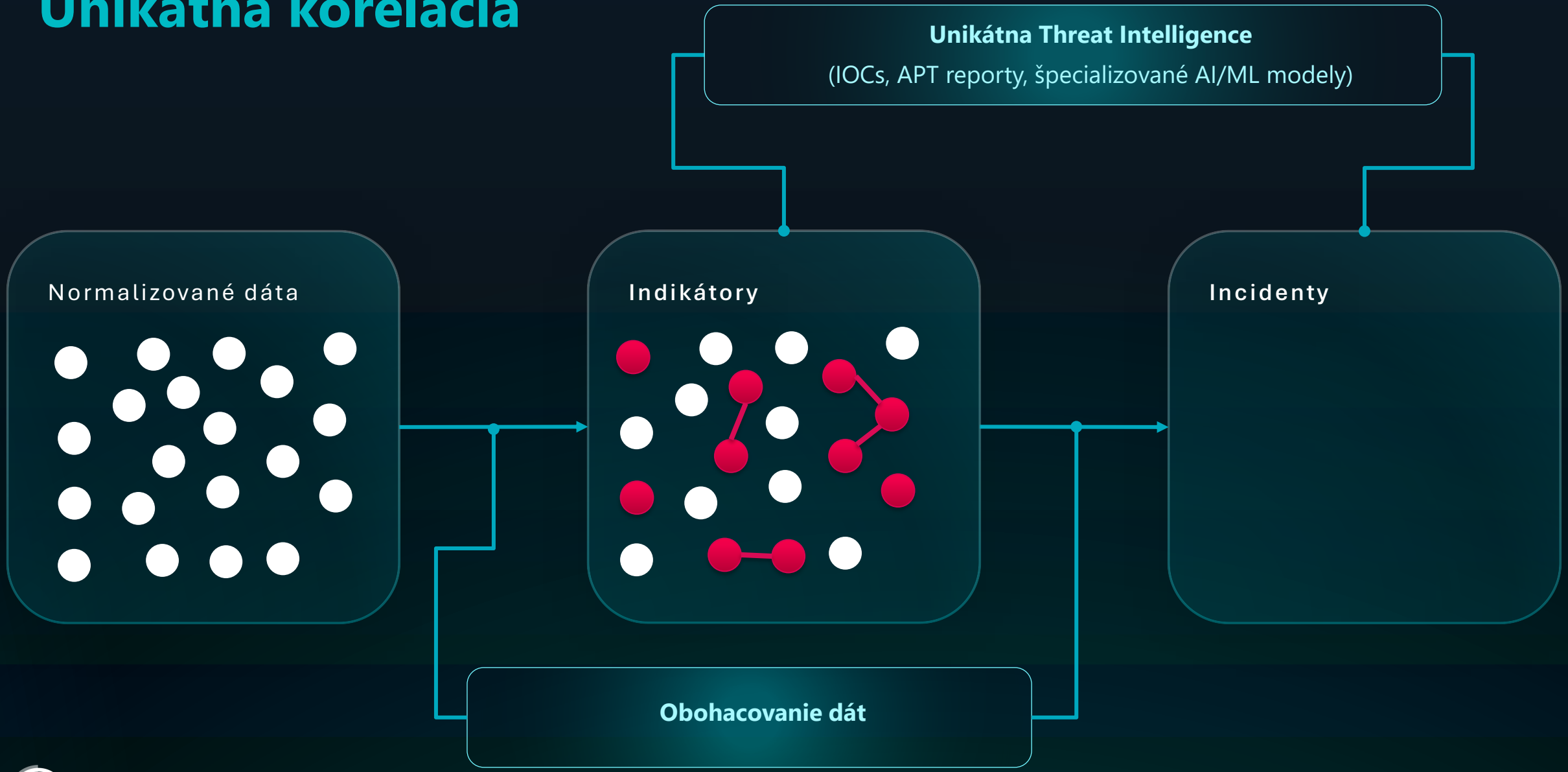

ESET PROTECT – Open XDR Integrácie
Šírka Integrácie
INTEGRÁCIA XY
Aktivácia Integrácie
Zber dát
Korelácia
Synchronizácia Assetov
Akcie (Reakcie)
Hĺbka Integrácie
Verzia 1
Rozširovanie pokrytia
Verzia 1
Rozširovanie schémy
Verzia 1
Verzia 2
Verzia 3
Verzia 4
Verzia 5
Verzia 6
...
Verzia 1
Verzia 2
...
Verzia 1
Verzia 2
Verzia 3
Verzia 4
...

Unikátna korelácia

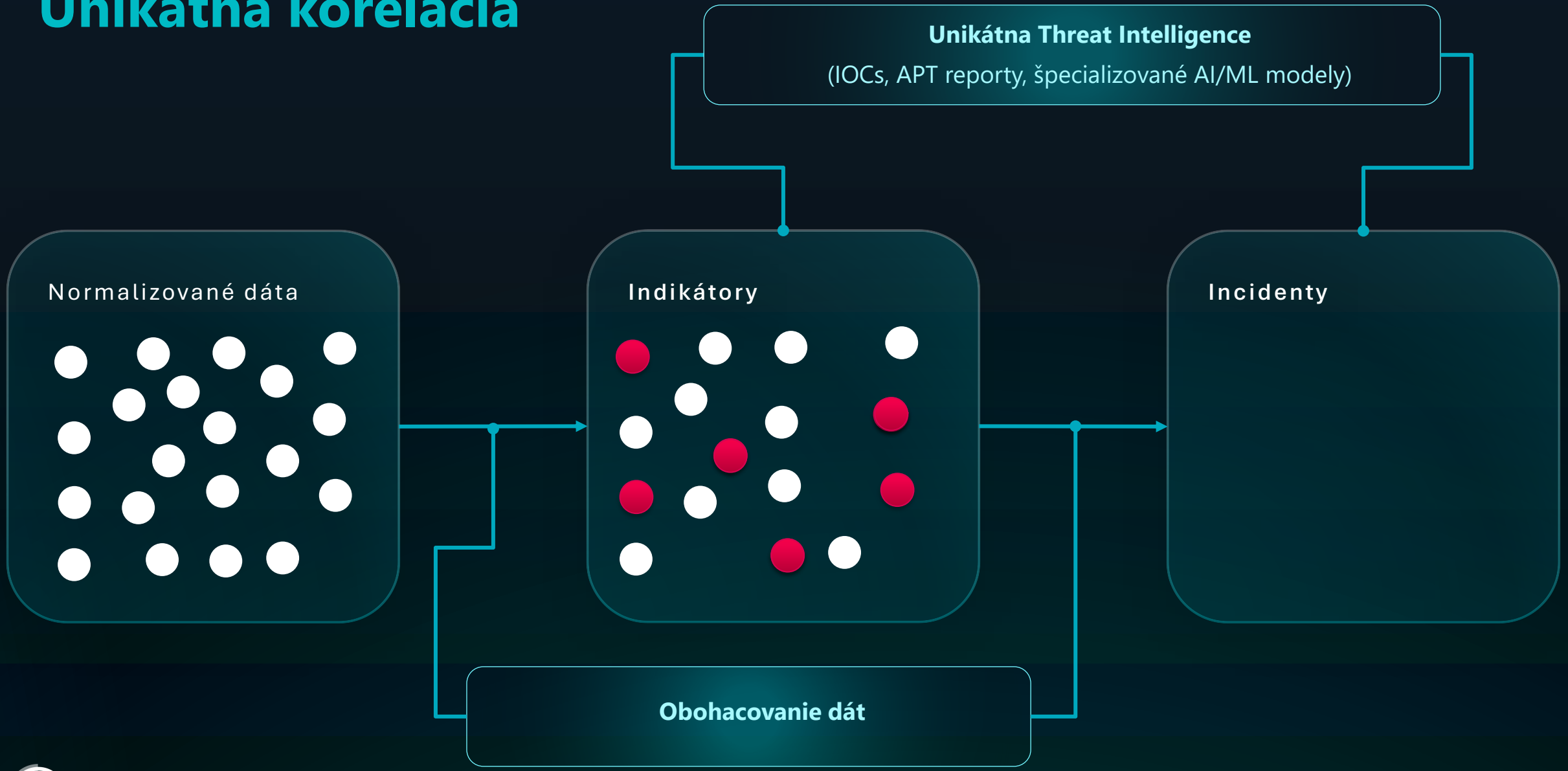
Unikátna korelácia



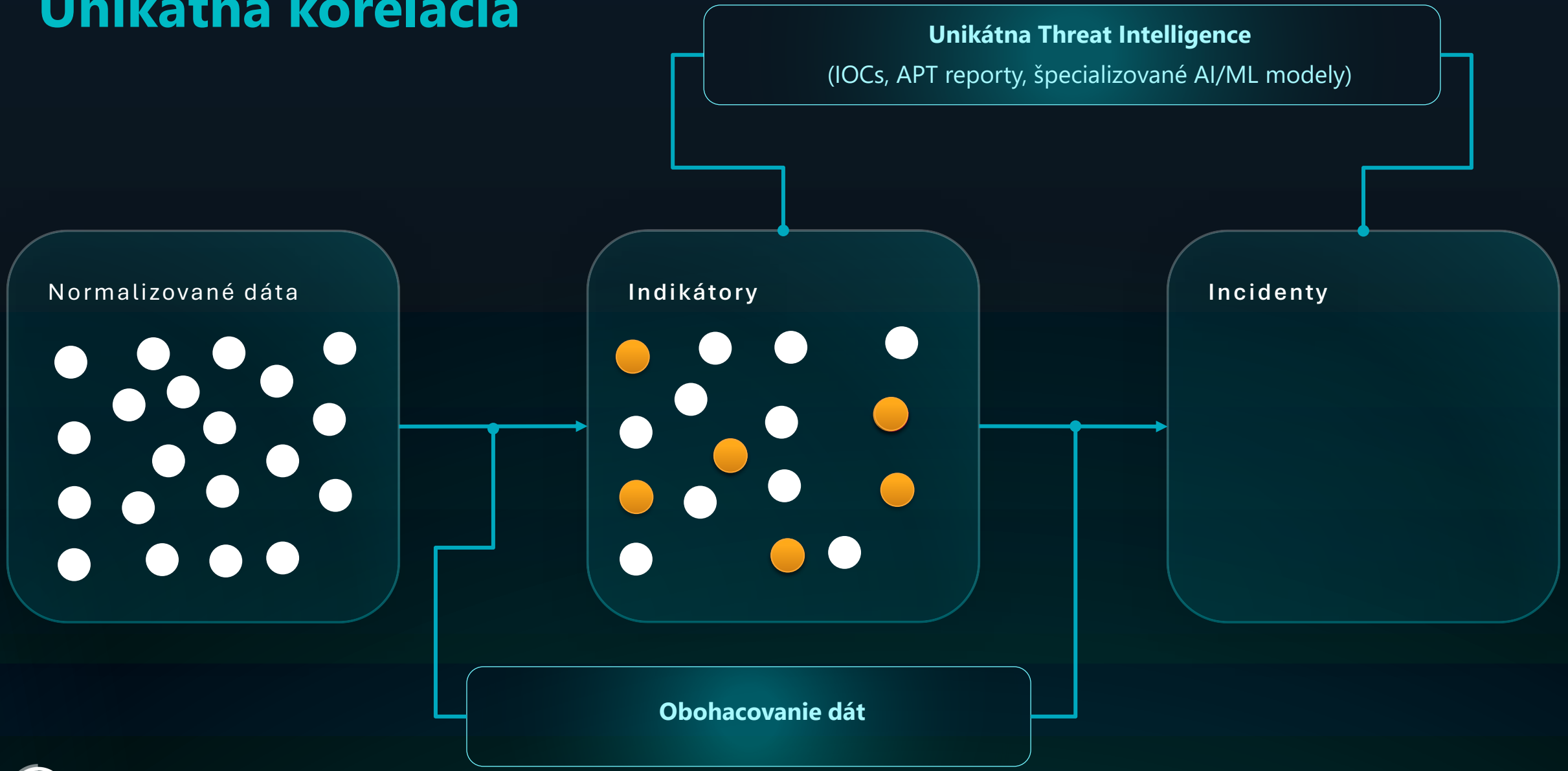
Unikátna korelácia



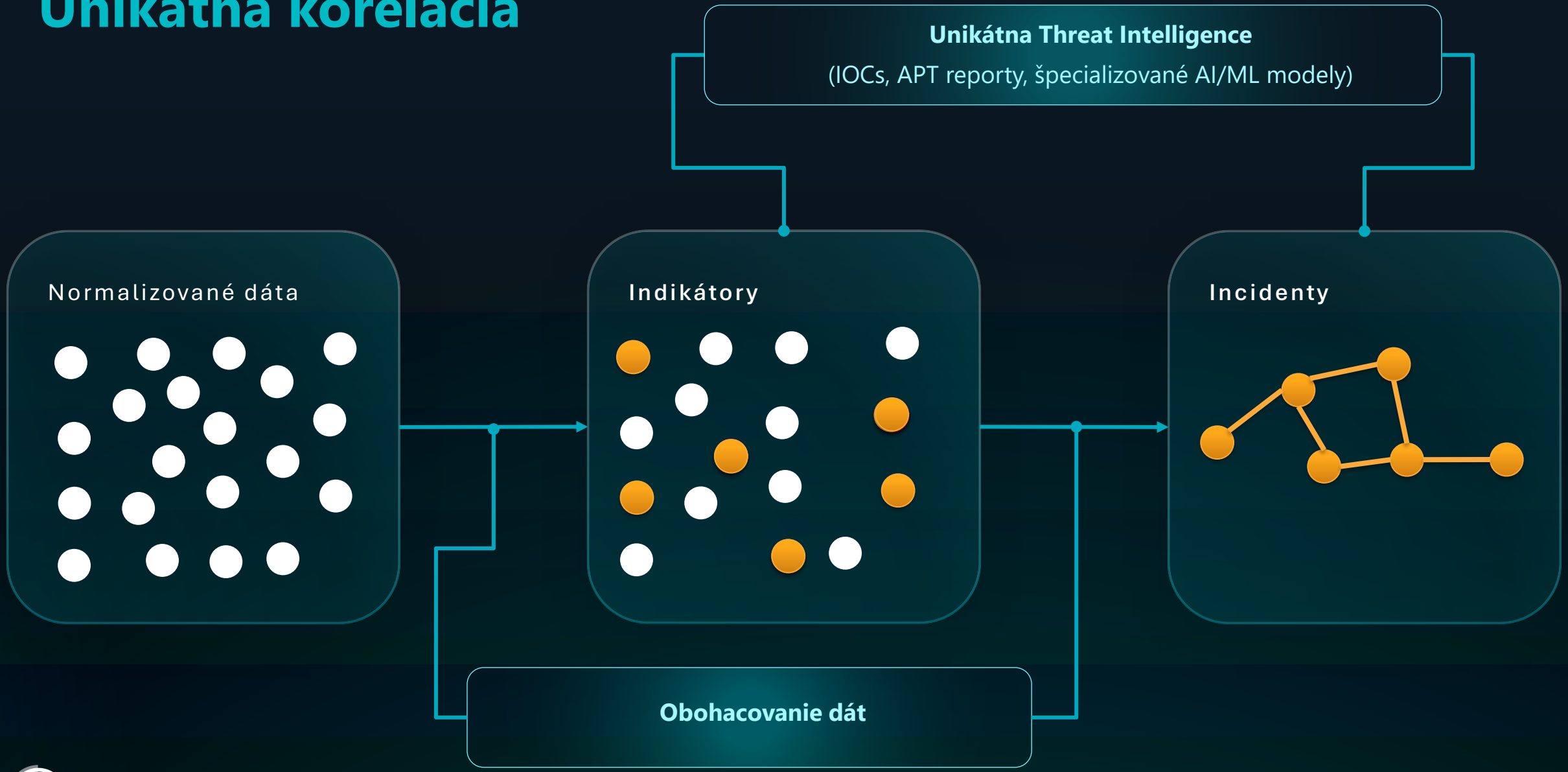
Unikátna korelácia



Unikátna korelácia



Unikátna korelácia



Zoznam Open XDR Integrácií

DOSTUPNÉ

Microsoft Entra ID

Active Directory

Azure

aws

Google Cloud

paloalto NETWORKS

PLÁNOVANÉ

FORTINET

proofpoint. Targeted Attack Protection

mimecast

Amazon GuardDuty

CHECK POINT

okta

Defender for Cloud

WIZ

STORMSHIELD

mimecast

DARKTRACE

Roadmapa a smerovanie

Prehľad kľúčových iniciatív, plánov a praktických ukážok toho, čo prinášame zákazníkom.

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

EP 7.0
Január 2026

- **Počiatočná verzia ESET Open XDR**
- **Vylepšené incidenty** (Graf, Affected identities)
- **AI asistent**
- **Pokročilé vyhľadávanie**
- **Vylepšenia MDR** (Kvartáne TI reporty, Dashboard,...)
- **Sekcia integrácií** (Entra ID, MS AD)

EP 7.1
Marec 2026

- **Cloud Workload Protection** (Azure, AWS, GCP)
- **Viac XDR integrácií** (Palo Alto Firewall)
- **Reakčné akcie XDR**
- **Vylepšené pokročilé vyhľadávanie**
- **Vylepšené incidenty** (Reporty)

EP 7.2
Jún 2026

- Vylepšená **sekcia integrácií** (Monitoring objemu dát)
- **Vylepšené incidenty** (Odporúčané akcie, Zoznam procesov and spustiteľných súborov)
- **Rozšírený AI asistent** (Širší kontext, Reakčné akcie)
- **Nový vzdialený prístup**

EP 7.3
September 2026

- **Dlhodobé ukladanie indikátorov**
- **Viac XDR integrácií** (Fortinet Firewall)
- **Počiatočná integrácia s ECOS**
- **Správa EDR pravidiel**
- **Správa výnimiek**
- **Správa blokovaných entít**
- **Multitenantné outbound integrácie**

EP NEXT
Q4 2026 → Budúcnosť

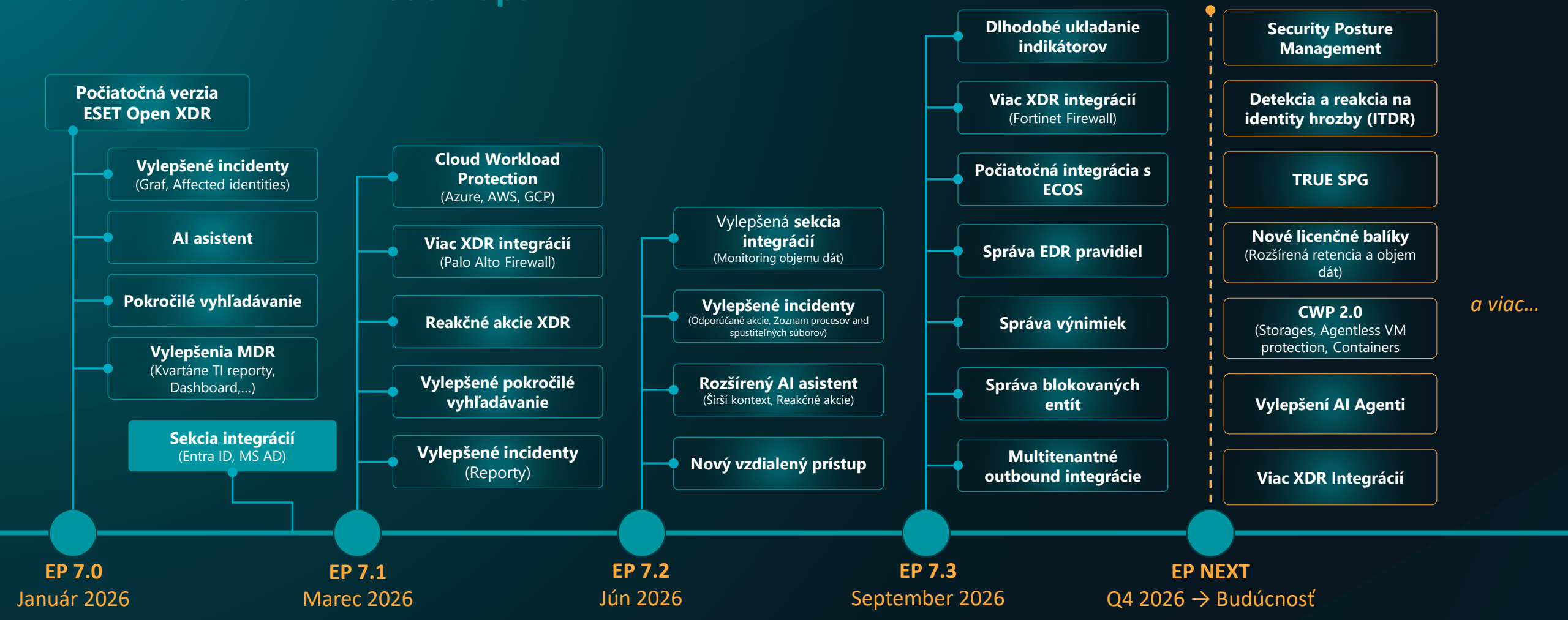
- **Security Posture Management**
- **Detekcia a reakcia na identity hrozby (ITDR)**
- **TRUE SPG**
- **Nové licenčné balíky** (Rozšírená retencia a objem dát)
- **CWP 2.0** (Storages, Agentless VM protection, Containers
- **Vylepšení AI Agenti**
- **Viac XDR Integrácií**

a viac...

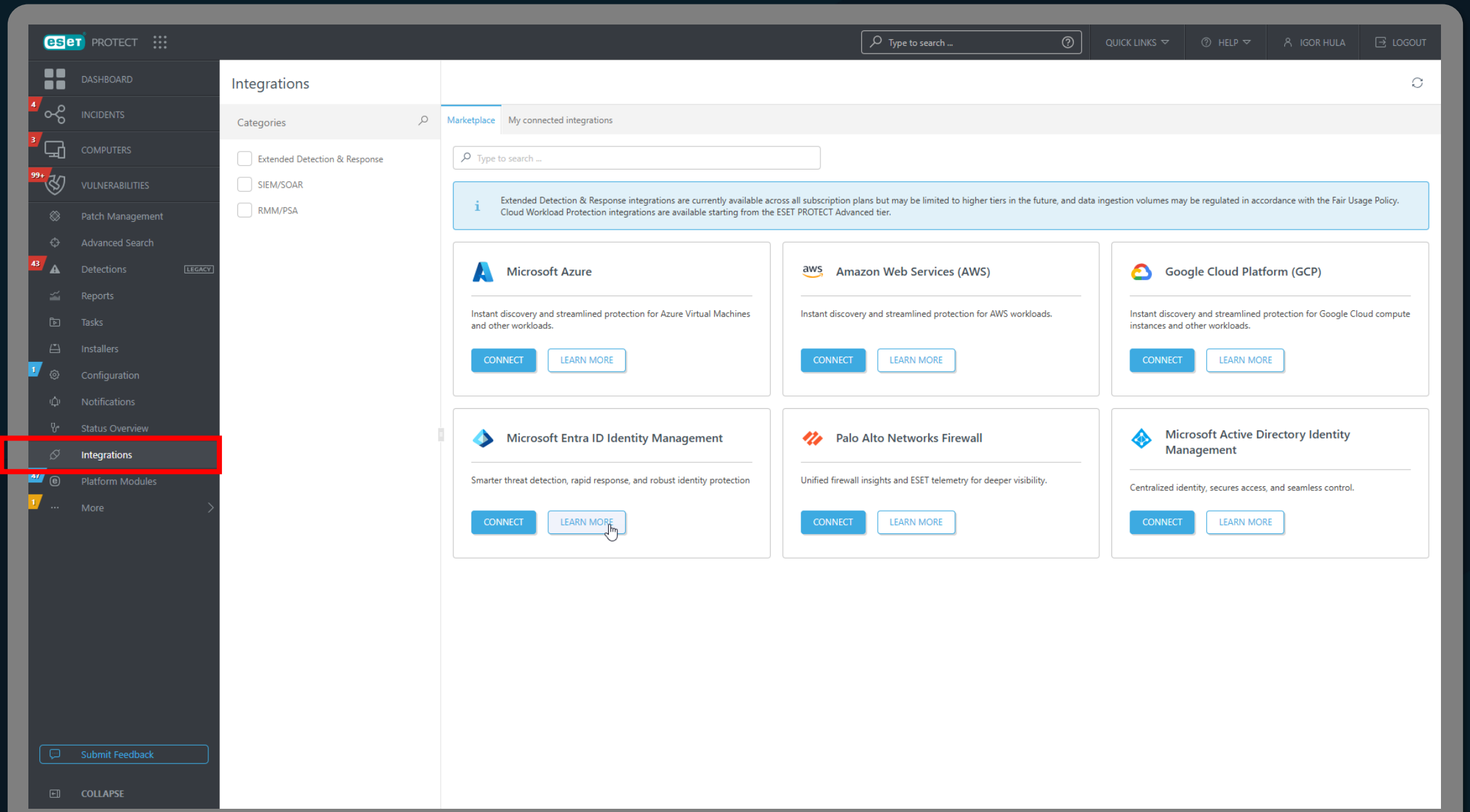
Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

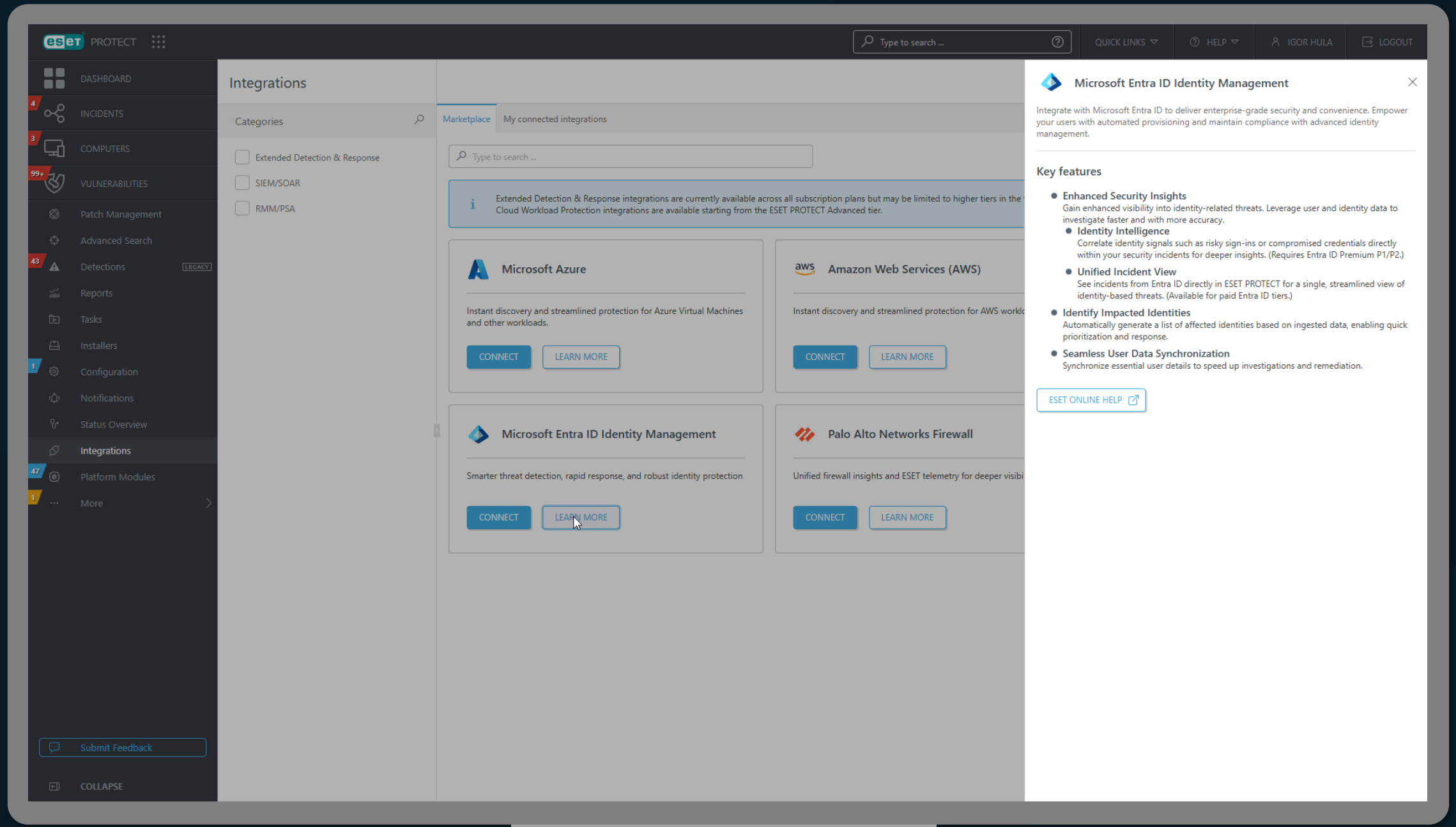
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

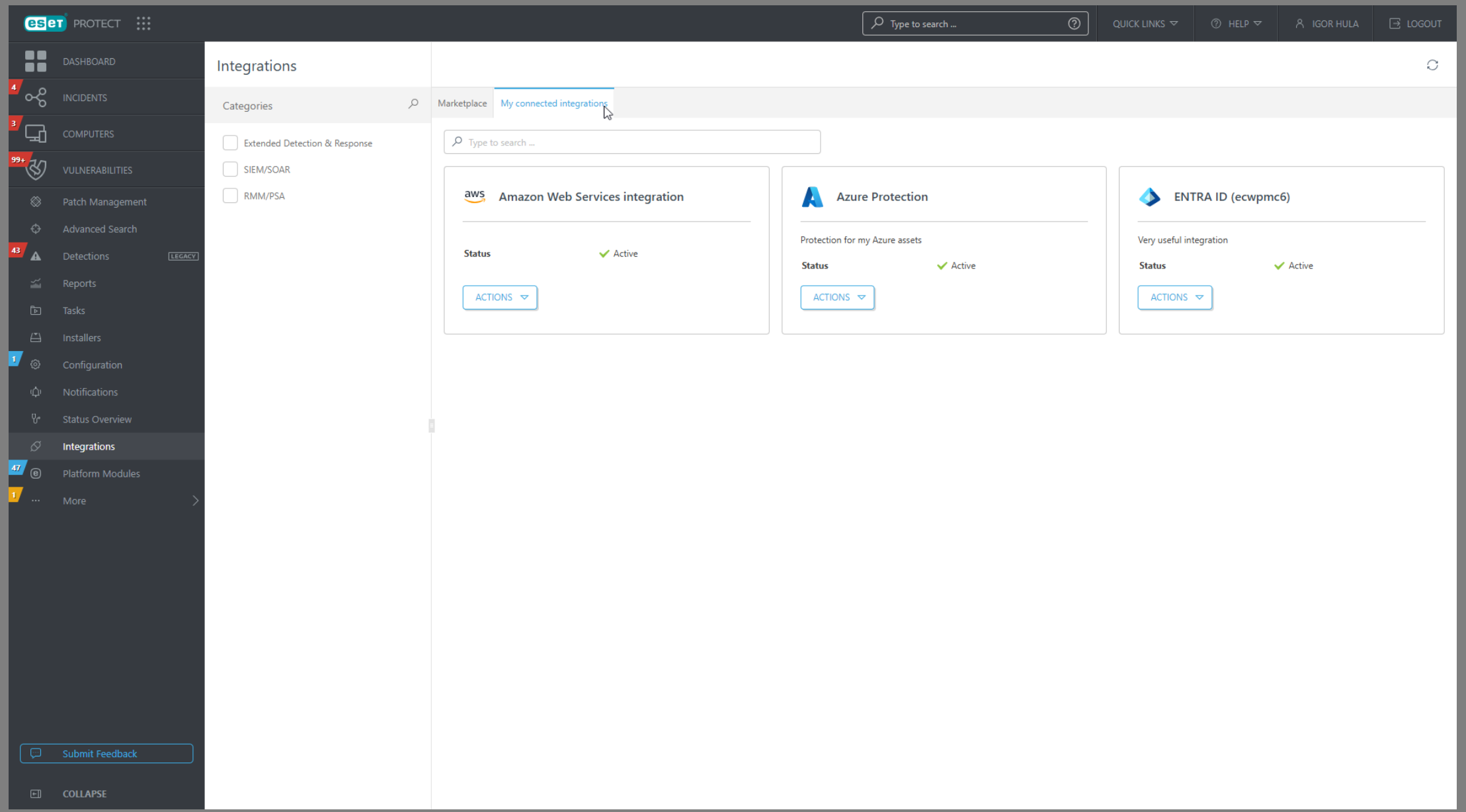
ESET PROTECT – HL Roadmapa



Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

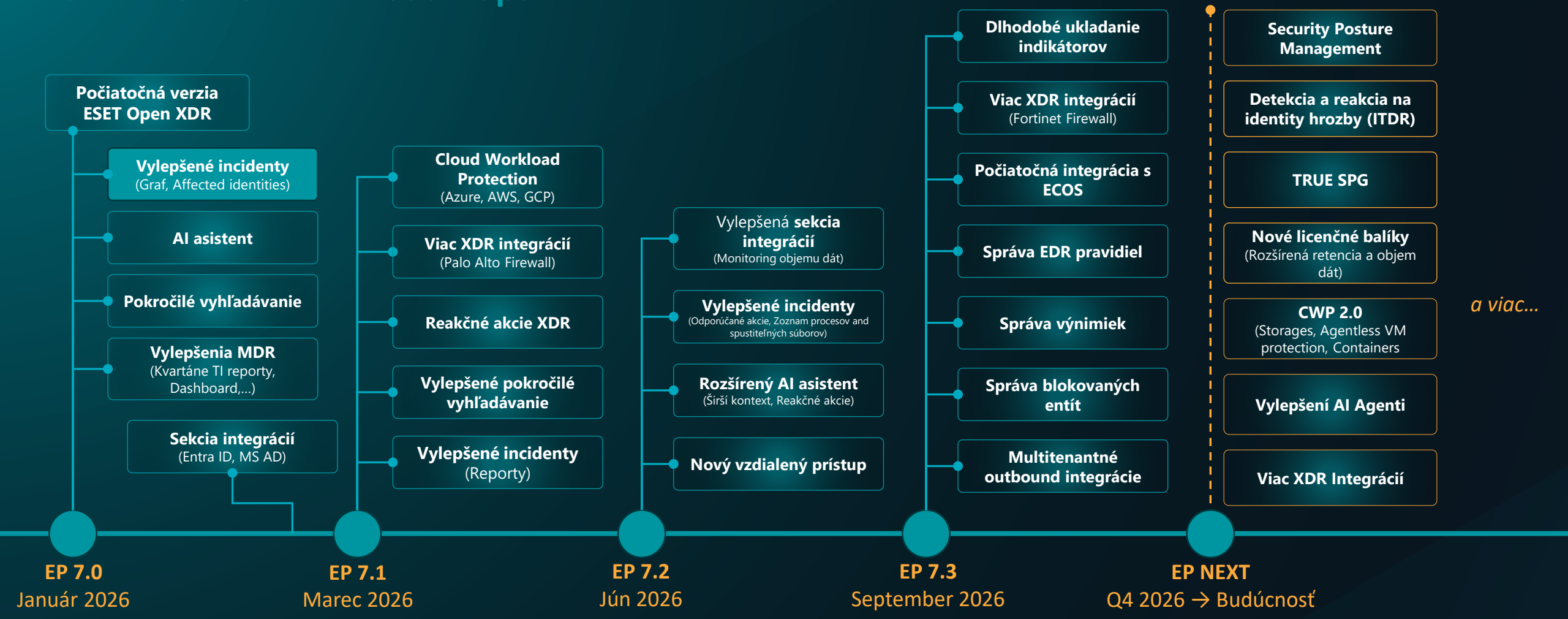

ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Integrations
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Type to search ...
Extended Detection & Response integrations are currently available across all subscription plans but may be limited to higher tiers in the future, and data ingestion volumes may be regulated in accordance with the Fair Usage Policy.
Cloud Workload Protection integrations are available starting from the ESET PROTECT Advanced tier.
Microsoft Azure
Instant discovery and streamlined protection for Azure Virtual Machines and other workloads.
CONNECT
LEARN MORE
Amazon Web Services (AWS)
Instant discovery and streamlined protection for AWS workloads.
CONNECT
LEARN MORE
Google Cloud Platform (GCP)
Instant discovery and streamlined protection for Google Cloud compute instances and other workloads.
CONNECT
LEARN MORE
Microsoft Entra ID Identity Management
Smarter threat detection, rapid response, and robust identity protection
CONNECT
LEARN MORE
Palo Alto Networks Firewall
Unified firewall insights and ESET telemetry for deeper visibility.
CONNECT
LEARN MORE
Microsoft Active Directory Identity Management
Centralized identity, secures access, and seamless control.
CONNECT
LEARN MORE


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Integrations
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Type to search ...
Extended Detection & Response integrations are currently available across all subscription plans but may be limited to higher tiers in the
Cloud Workload Protection integrations are available starting from the ESET PROTECT Advanced tier.
Microsoft Azure
Instant discovery and streamlined protection for Azure Virtual Machines and other workloads.
CONNECT
LEARN MORE
Amazon Web Services (AWS)
Instant discovery and streamlined protection for AWS workl
CONNECT
LEARN MORE
Microsoft Entra ID Identity Management
Smarter threat detection, rapid response, and robust identity protection
CONNECT
LEARN MORE
Palo Alto Networks Firewall
Unified firewall insights and ESET telemetry for deeper visibi
CONNECT
LEARN MORE
Microsoft Entra ID Identity Management
Integrate with Microsoft Entra ID to deliver enterprise-grade security and convenience. Empower your users with automated provisioning and maintain compliance with advanced identity management.
Key features
Enhanced Security Insights
Gain enhanced visibility into identity-related threats. Leverage user and identity data to investigate faster and with more accuracy.
Identity Intelligence
Correlate identity signals such as risky sign-ins or compromised credentials directly within your security incidents for deeper insights. (Requires Entra ID Premium P1/P2.)
Unified Incident View
See incidents from Entra ID directly in ESET PROTECT for a single, streamlined view of identity-based threats. (Available for paid Entra ID tiers.)
Identify Impacted Identities
Automatically generate a list of affected identities based on ingested data, enabling quick prioritization and response.
Seamless User Data Synchronization
Synchronize essential user details to speed up investigations and remediation.
ESET ONLINE HELP

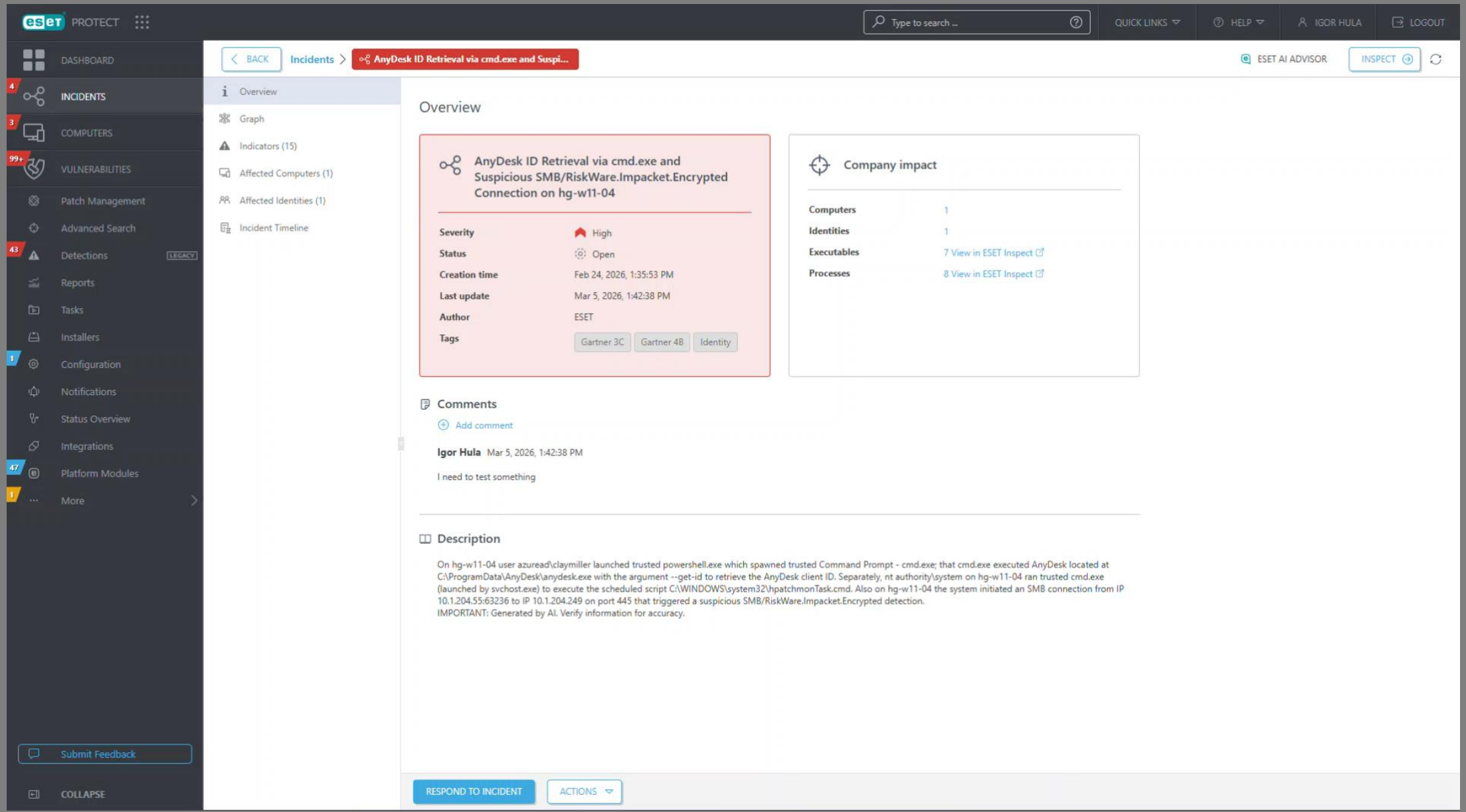

ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Integrations
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Type to search ...
Amazon Web Services integration
Status
Active
ACTIONS
Azure Protection
Protection for my Azure assets
Status
Active
ACTIONS
ENTRA ID (ecwpmc6)
Very useful integration
Status
Active
ACTIONS

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

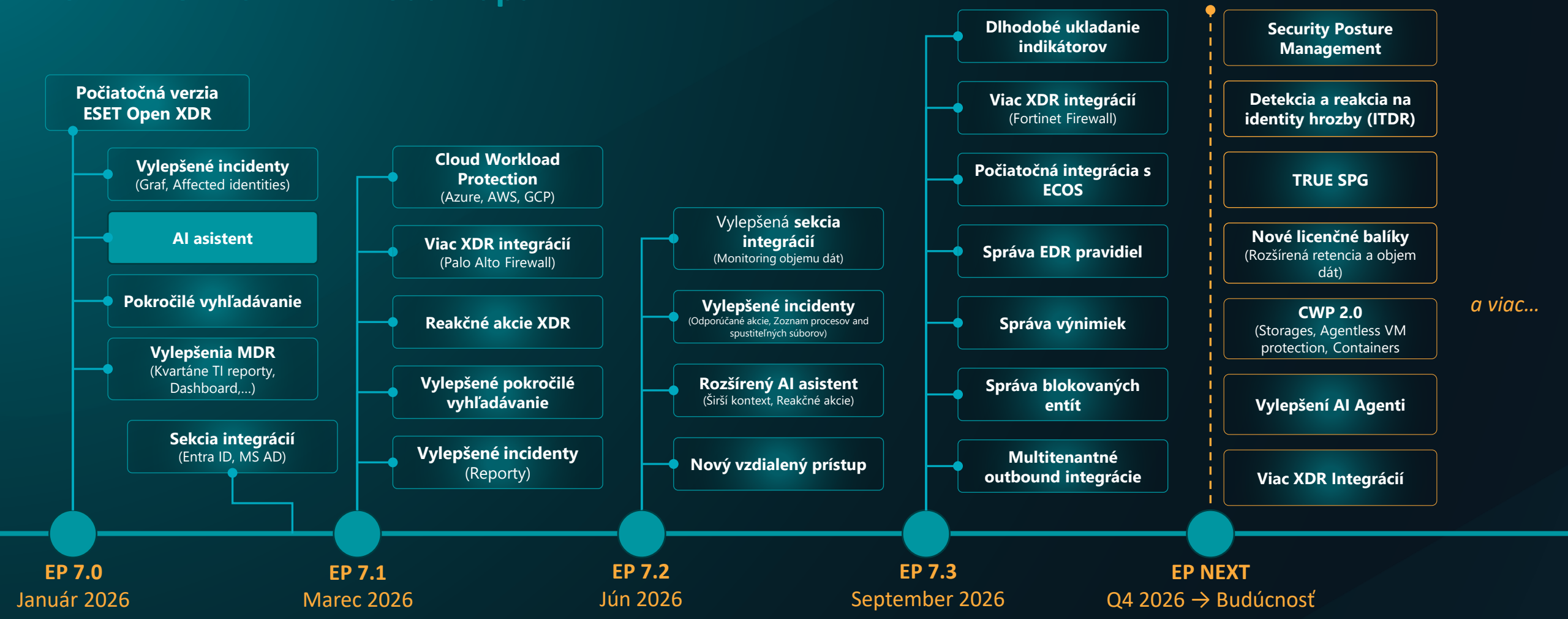


Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

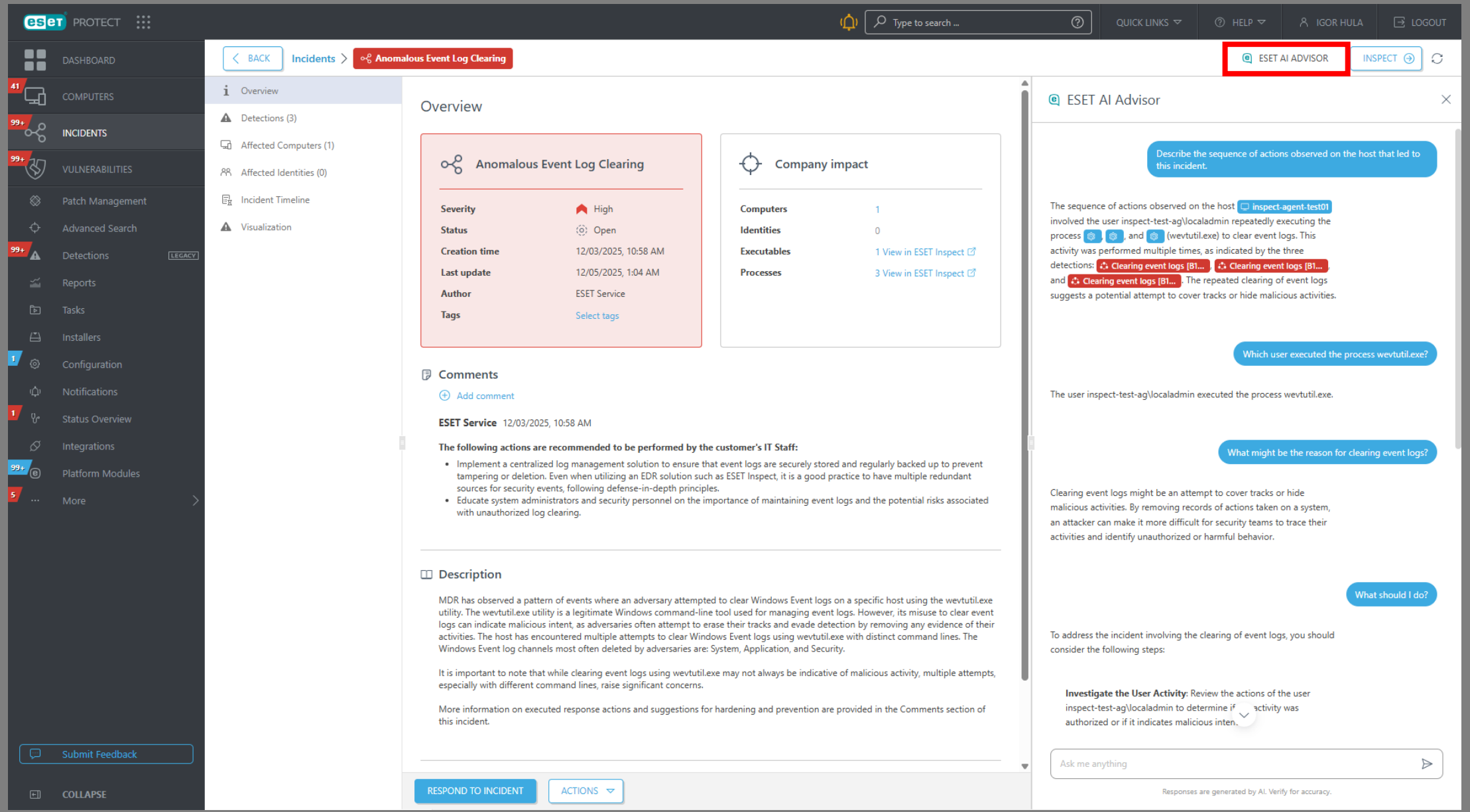

PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
AnyDesk ID Retrieval via cmd.exe and Suspi...
ESET AI ADVISOR
INSPECT
Overview
Graph
Indicators (15)
Affected Computers (1)
Affected Identities (1)
Incident Timeline
Overview
AnyDesk ID Retrieval via cmd.exe and Suspicious SMB/RiskWare.Impacket.Encrypted Connection on hg-w11-04
Severity
High
Status
Open
Creation time
Feb 24, 2026, 1:35:53 PM
Last update
Mar 5, 2026, 1:42:38 PM
Author
ESET
Tags
Gartner 3C
Gartner 4B
Identity
Company impact
Computers
1
Identities
1
Executables
7 View in ESET Inspect
Processes
8 View in ESET Inspect
Comments
Add comment
Igor Hula Mar 5, 2026, 1:42:38 PM
I need to test something
Description
On hg-w11-04 user azuread\claymiller launched trusted powershell.exe which spawned trusted Command Prompt - cmd.exe; that cmd.exe executed AnyDesk located at C:\ProgramData\AnyDesk\anydesk.exe with the argument --get-id to retrieve the AnyDesk client ID. Separately, nt authority\system on hg-w11-04 ran trusted cmd.exe (launched by svchost.exe) to execute the scheduled script C:\WINDOWS\system32\hpatchmonTask.cmd. Also on hg-w11-04 the system initiated an SMB connection from IP 10.1.204.55:63236 to IP 10.1.204.249 on port 445 that triggered a suspicious SMB/RiskWare.Impacket.Encrypted detection.
IMPORTANT: Generated by AI. Verify information for accuracy.
RESPOND TO INCIDENT
ACTIONS

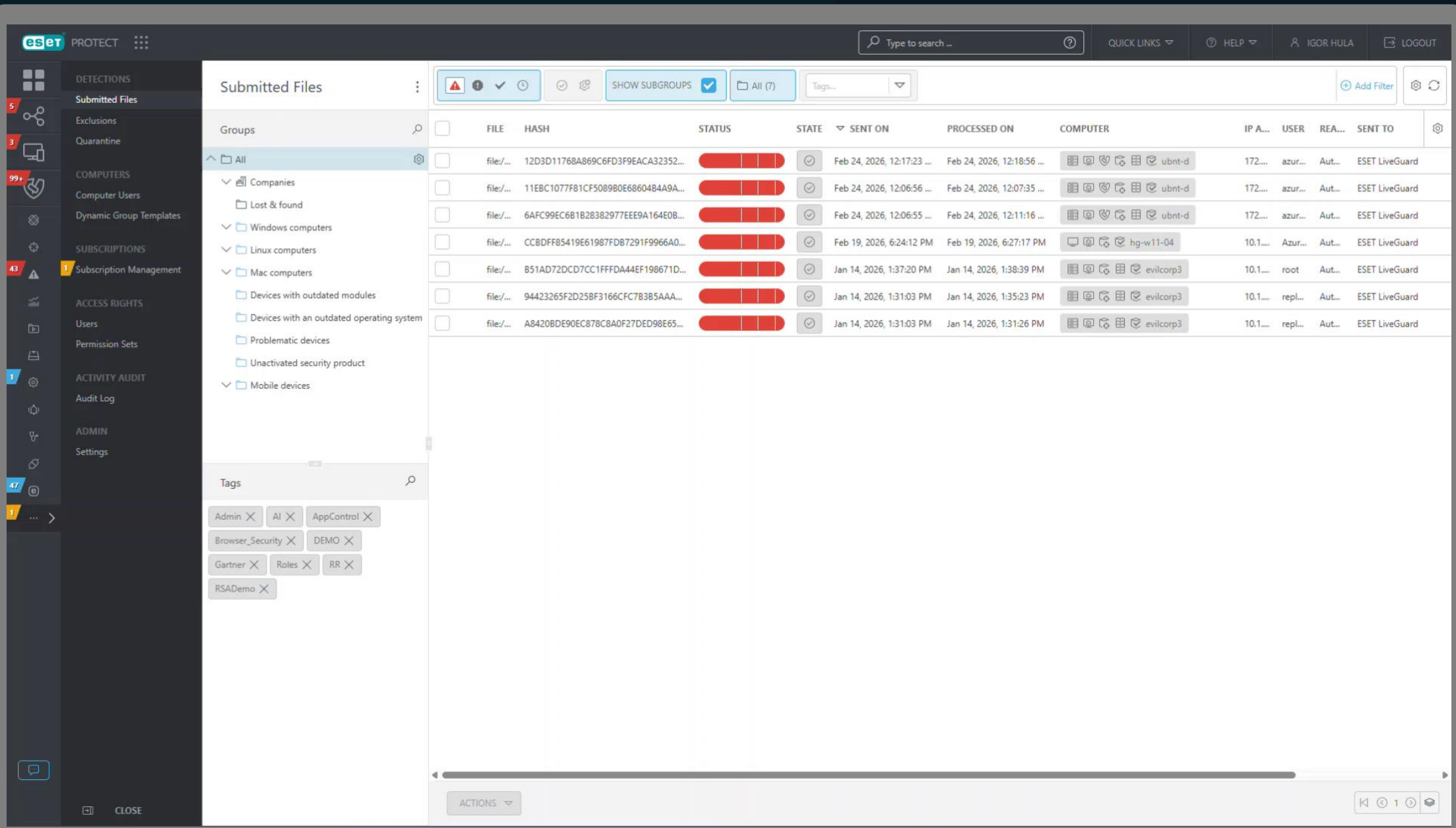
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa



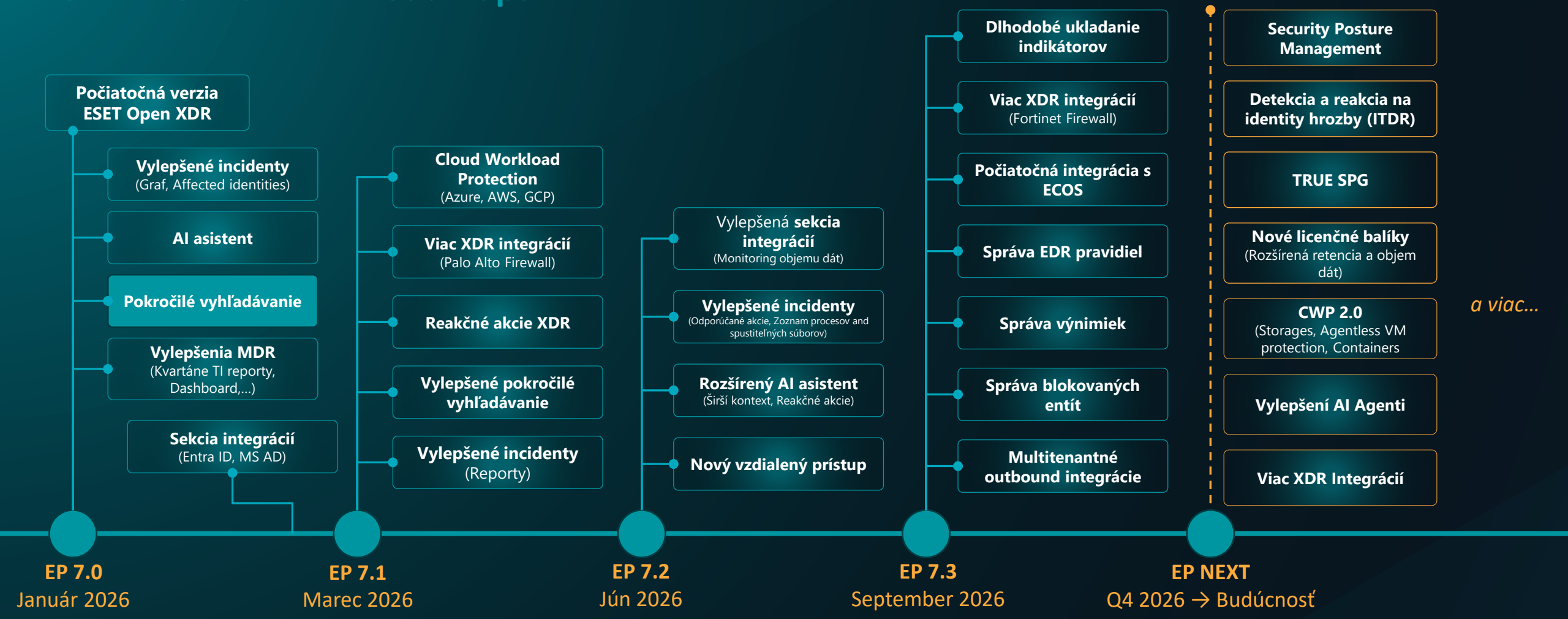
Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
Anomalous Event Log Clearing
ESET AI ADVISOR
INSPECT
Overview
Detections (3)
Affected Computers (1)
Affected Identities (0)
Incident Timeline
Visualization
Overview
Anomalous Event Log Clearing
Severity
High
Status
Open
Creation time
12/03/2025, 10:58 AM
Last update
12/05/2025, 1:04 AM
Author
ESET Service
Tags
Select tags
Company impact
Computers
1
Identities
0
Executables
1 View in ESET Inspect
Processes
3 View in ESET Inspect
Comments
Add comment
ESET Service 12/03/2025, 10:58 AM
The following actions are recommended to be performed by the customer's IT Staff:
Implement a centralized log management solution to ensure that event logs are securely stored and regularly backed up to prevent tampering or deletion. Even when utilizing an EDR solution such as ESET Inspect, it is a good practice to have multiple redundant sources for security events, following defense-in-depth principles.
Educate system administrators and security personnel on the importance of maintaining event logs and the potential risks associated with unauthorized log clearing.
Description
MDR has observed a pattern of events where an adversary attempted to clear Windows Event logs on a specific host using the wevtutil.exe utility. The wevtutil.exe utility is a legitimate Windows command-line tool used for managing event logs. However, its misuse to clear event logs can indicate malicious intent, as adversaries often attempt to erase their tracks and evade detection by removing any evidence of their activities. The host has encountered multiple attempts to clear Windows Event logs using wevtutil.exe with distinct command lines. The Windows Event log channels most often deleted by adversaries are: System, Application, and Security.
It is important to note that while clearing event logs using wevtutil.exe may not always be indicative of malicious activity, multiple attempts, especially with different command lines, raise significant concerns.
More information on executed response actions and suggestions for hardening and prevention are provided in the Comments section of this incident.
RESPOND TO INCIDENT
ACTIONS
ESET AI Advisor
Describe the sequence of actions observed on the host that led to this incident.
The sequence of actions observed on the host inspect-agent-test01 involved the user inspect-test-ag\localadmin repeatedly executing the process , , and (wevtutil.exe) to clear event logs. This activity was performed multiple times, as indicated by the three detections: Clearing event logs [B1... Clearing event logs [B1... and Clearing event logs [B1... The repeated clearing of event logs suggests a potential attempt to cover tracks or hide malicious activities.
Which user executed the process wevtutil.exe?
The user inspect-test-ag\localadmin executed the process wevtutil.exe.
What might be the reason for clearing event logs?
Clearing event logs might be an attempt to cover tracks or hide malicious activities. By removing records of actions taken on a system, an attacker can make it more difficult for security teams to trace their activities and identify unauthorized or harmful behavior.
What should I do?
To address the incident involving the clearing of event logs, you should consider the following steps:
Investigate the User Activity: Review the actions of the user inspect-test-ag\localadmin to determine if activity was authorized or if it indicates malicious inten
Ask me anything
Responses are generated by AI. Verify for accuracy.

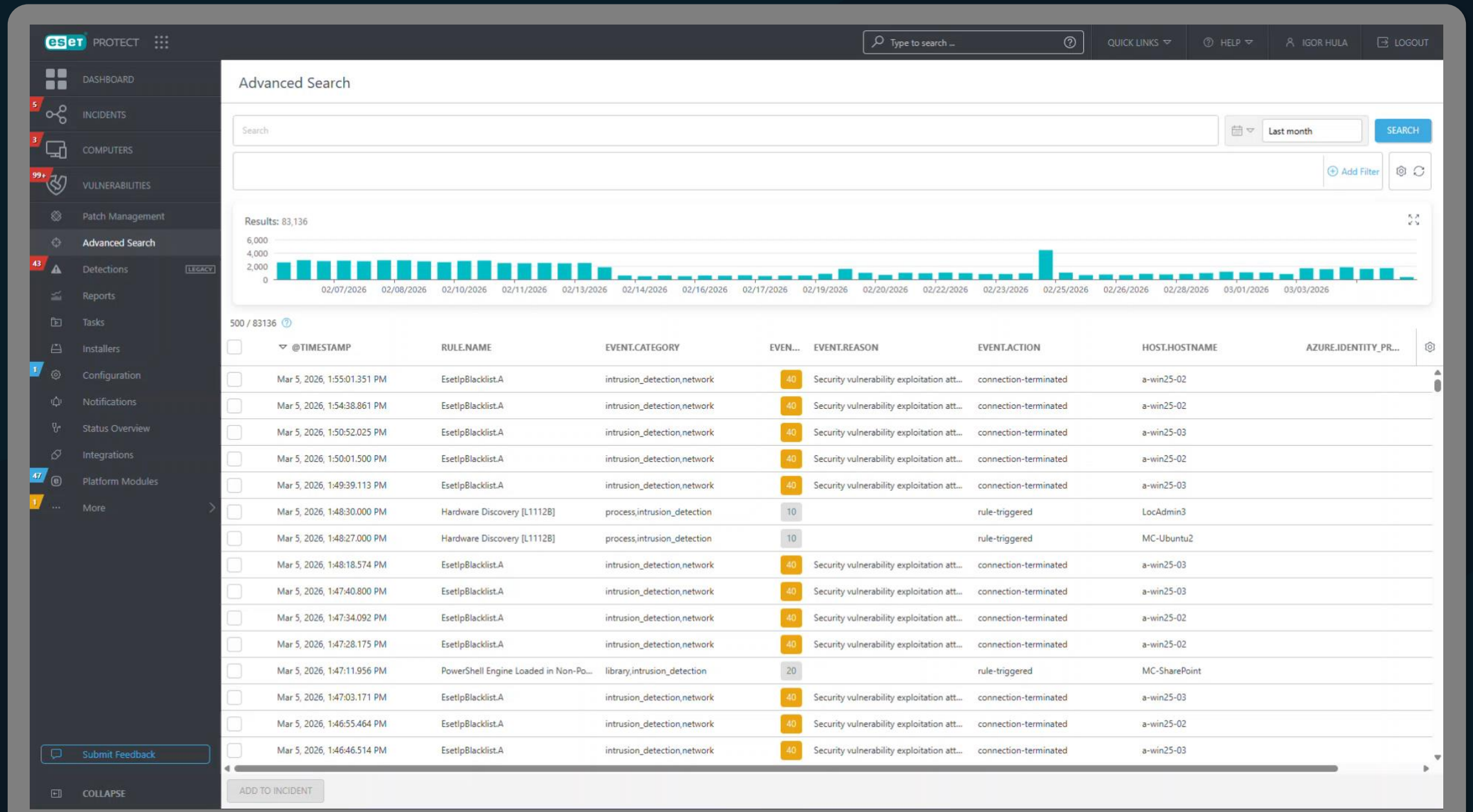

PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DETECTIONS
Submitted Files
Exclusions
Quarantine
COMPUTERS
Computer Users
Dynamic Group Templates
SUBSCRIPTIONS
Subscription Management
ACCESS RIGHTS
Users
Permission Sets
ACTIVITY AUDIT
Audit Log
ADMIN
Settings
CLOSE
Submitted Files
Groups
All
Companies
Lost & found
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Devices with an outdated operating system
Problematic devices
Unactivated security product
Mobile devices
Tags
Admin
AI
AppControl
Browser_Security
DEMO
Gartner
Roles
RR
RSADemo
SHOW SUBGROUPS
All (7)
Tags...
Add Filter
FILE
HASH
STATUS
STATE
SENT ON
PROCESSED ON
COMPUTER
IP A...
USER
REA...
SENT TO
file:/...
12D3D11768A869C6FD3F9EACA32352...
Feb 24, 2026, 12:17:23 ...
Feb 24, 2026, 12:18:56 ...
ubnt-d
172....
azur...
Aut...
ESET LiveGuard
file:/...
11EBC1077F81CF5089B0E68604B4A9A...
Feb 24, 2026, 12:06:56 ...
Feb 24, 2026, 12:07:35 ...
ubnt-d
172....
azur...
Aut...
ESET LiveGuard
file:/...
6AFC99EC6B1B28382977EEE9A164E0B...
Feb 24, 2026, 12:06:55 ...
Feb 24, 2026, 12:11:16 ...
ubnt-d
172....
azur...
Aut...
ESET LiveGuard
file:/...
CCBDFF85419E61987FDB7291F9966A0...
Feb 19, 2026, 6:24:12 PM
Feb 19, 2026, 6:27:17 PM
hg-w11-04
10.1....
Azur...
Aut...
ESET LiveGuard
file:/...
B51AD72DCD7CC1FFFDA44EF198671D...
Jan 14, 2026, 1:37:20 PM
Jan 14, 2026, 1:38:39 PM
evilcorp3
10.1....
root
Aut...
ESET LiveGuard
file:/...
94423265F2D25BF3166CFC7B3B5AAA...
Jan 14, 2026, 1:31:03 PM
Jan 14, 2026, 1:35:23 PM
evilcorp3
10.1....
repl...
Aut...
ESET LiveGuard
file:/...
A8420BDE90EC878C8A0F27DED98E65...
Jan 14, 2026, 1:31:03 PM
Jan 14, 2026, 1:31:26 PM
evilcorp3
10.1....
repl...
Aut...
ESET LiveGuard
ACTIONS
1

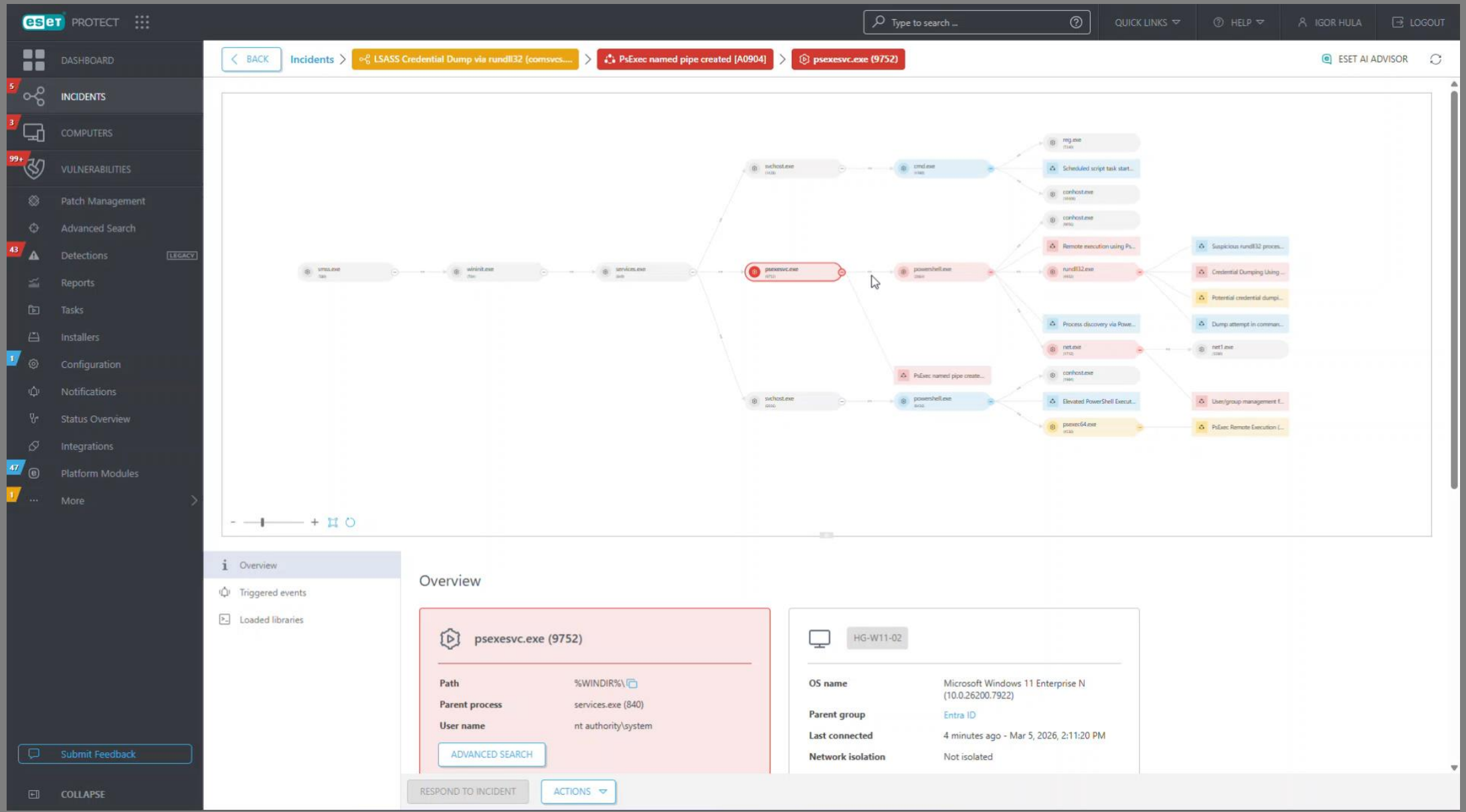
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa



Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Advanced Search
Search
Last month
SEARCH
Add Filter
Results: 83,136
6,000
4,000
2,000
0
02/07/2026
02/08/2026
02/10/2026
02/11/2026
02/13/2026
02/14/2026
02/16/2026
02/17/2026
02/19/2026
02/20/2026
02/22/2026
02/23/2026
02/25/2026
02/26/2026
02/28/2026
03/01/2026
03/03/2026
500 / 83136
@TIMESTAMP
RULE.NAME
EVENT.CATEGORY
EVEN...
EVENT.REASON
EVENT.ACTION
HOST.HOSTNAME
AZURE.IDENTITY_PR...
Mar 5, 2026, 1:55:01.351 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:54:38.861 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:50:52.025 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
Mar 5, 2026, 1:50:01.500 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:49:39.113 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
Mar 5, 2026, 1:48:30.000 PM Hardware Discovery [L1112B] process,intrusion_detection 10 rule-triggered LocAdmin3
Mar 5, 2026, 1:48:27.000 PM Hardware Discovery [L1112B] process,intrusion_detection 10 rule-triggered MC-Ubuntu2
Mar 5, 2026, 1:48:18.574 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
Mar 5, 2026, 1:47:40.800 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
Mar 5, 2026, 1:47:34.092 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:47:28.175 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:47:11.956 PM PowerShell Engine Loaded in Non-Po... library,intrusion_detection 20 rule-triggered MC-SharePoint
Mar 5, 2026, 1:47:03.171 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
Mar 5, 2026, 1:46:55.464 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-02
Mar 5, 2026, 1:46:46.514 PM EsetIpBlacklist.A intrusion_detection,network 40 Security vulnerability exploitation att... connection-terminated a-win25-03
ADD TO INCIDENT


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
LSASS Credential Dump via rundll32 (comsvcs....
PsExec named pipe created [A0904]
psexesvc.exe (9752)
ESET AI ADVISOR
Overview
Triggered events
Loaded libraries
Overview
psexesvc.exe (9752)
Path
%WINDIR%\
Parent process
services.exe (840)
User name
nt authority\system
ADVANCED SEARCH
HG-W11-02
OS name
Microsoft Windows 11 Enterprise N (10.0.26200.7922)
Parent group
Entra ID
Last connected
4 minutes ago - Mar 5, 2026, 2:11:20 PM
Network isolation
Not isolated
RESPOND TO INCIDENT
ACTIONS

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

EP 7.0
Január 2026

- **Počiatočná verzia ESET Open XDR**
- **Vylepšené incidenty** (Graf, Affected identities)
- **AI asistent**
- **Pokročilé vyhľadávanie**
- **Vylepšenia MDR** (Kvartáne TI reporty, Dashboard,...)
- **Sekcia integrácií** (Entra ID, MS AD)

EP 7.1
Marec 2026

- **Cloud Workload Protection** (Azure, AWS, GCP)
- **Viac XDR integrácií** (Palo Alto Firewall)
- **Reakčné akcie XDR**
- **Vylepšené pokročilé vyhľadávanie**
- **Vylepšené incidenty** (Reporty)

EP 7.2
Jún 2026

- Vylepšená **sekcia integrácií** (Monitoring objemu dát)
- **Vylepšené incidenty** (Odporúčané akcie, Zoznam procesov and spustiteľných súborov)
- **Rozšírený AI asistent** (Širší kontext, Reakčné akcie)
- **Nový vzdialený prístup**

EP 7.3
September 2026

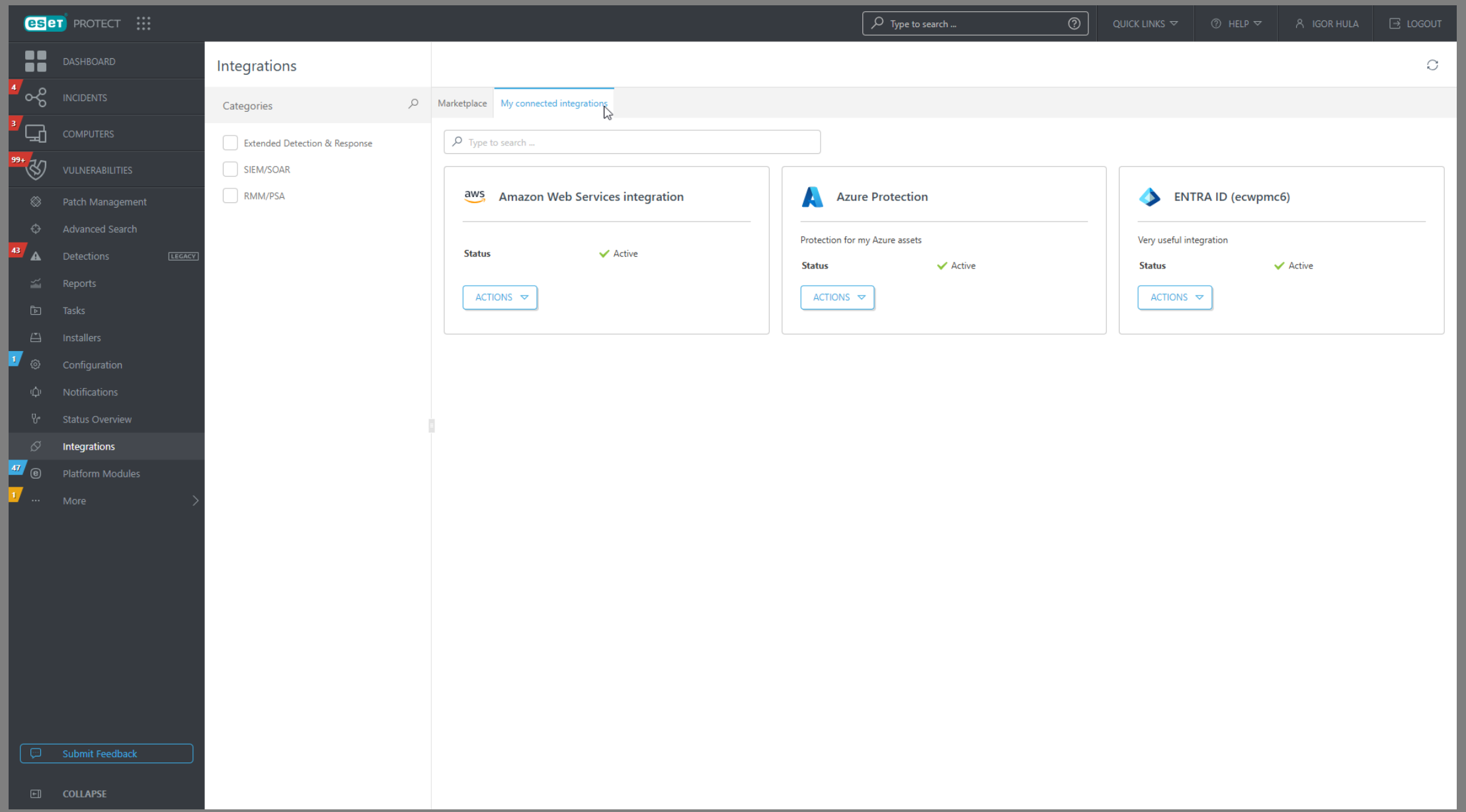
- **Dlhodobé ukladanie indikátorov**
- **Viac XDR integrácií** (Fortinet Firewall)
- **Počiatočná integrácia s ECOS**
- **Správa EDR pravidiel**
- **Správa výnimiek**
- **Správa blokovaných entít**
- **Multitenantné outbound integrácie**

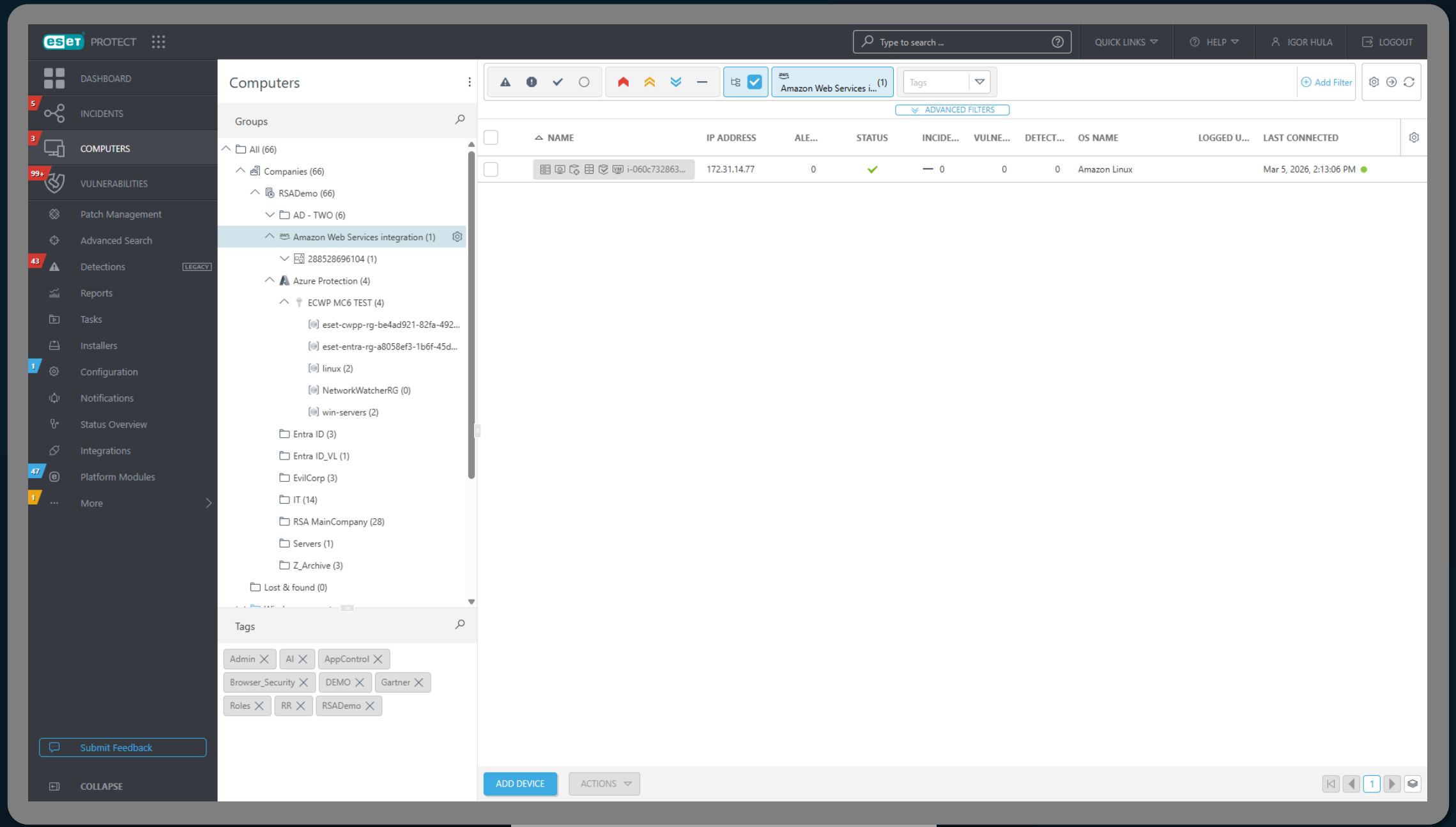
EP NEXT
Q4 2026 → Budúcnosť

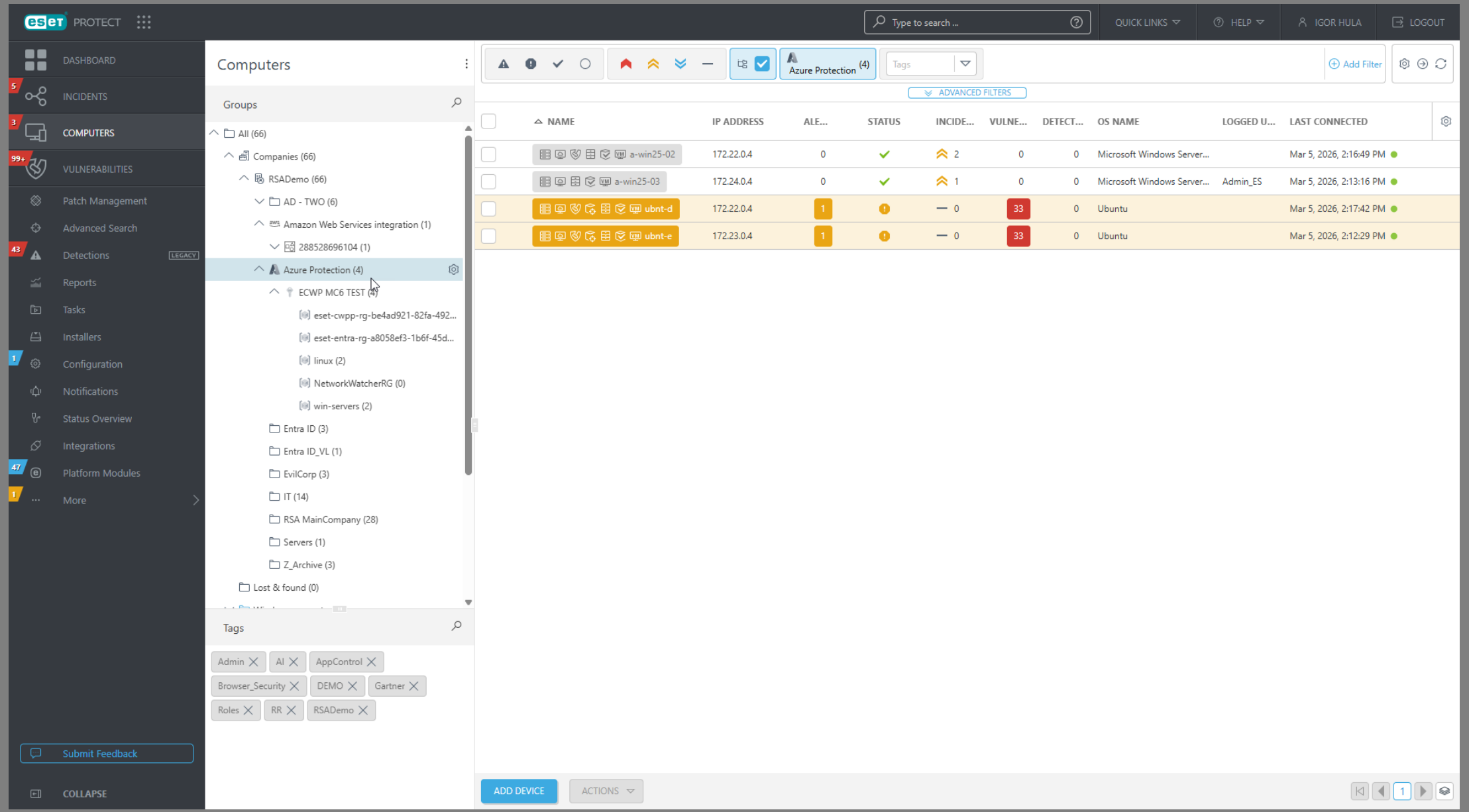
- **Security Posture Management**
- **Detekcia a reakcia na identity hrozby (ITDR)**
- **TRUE SPG**
- **Nové licenčné balíky** (Rozšírená retencia a objem dát)
- **CWP 2.0** (Storages, Agentless VM protection, Containers
- **Vylepšení AI Agenti**
- **Viac XDR Integrácií**

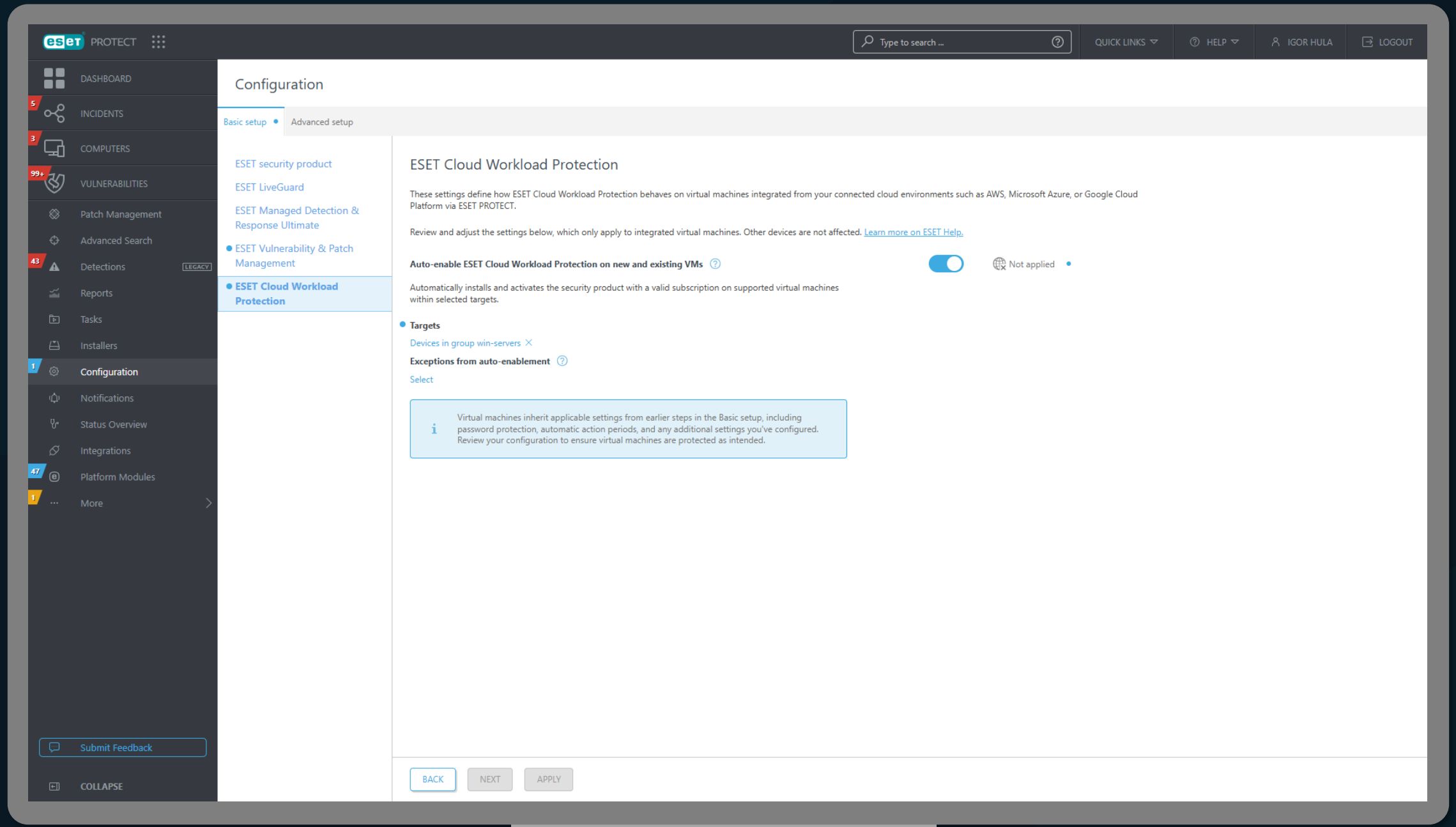
a viac...

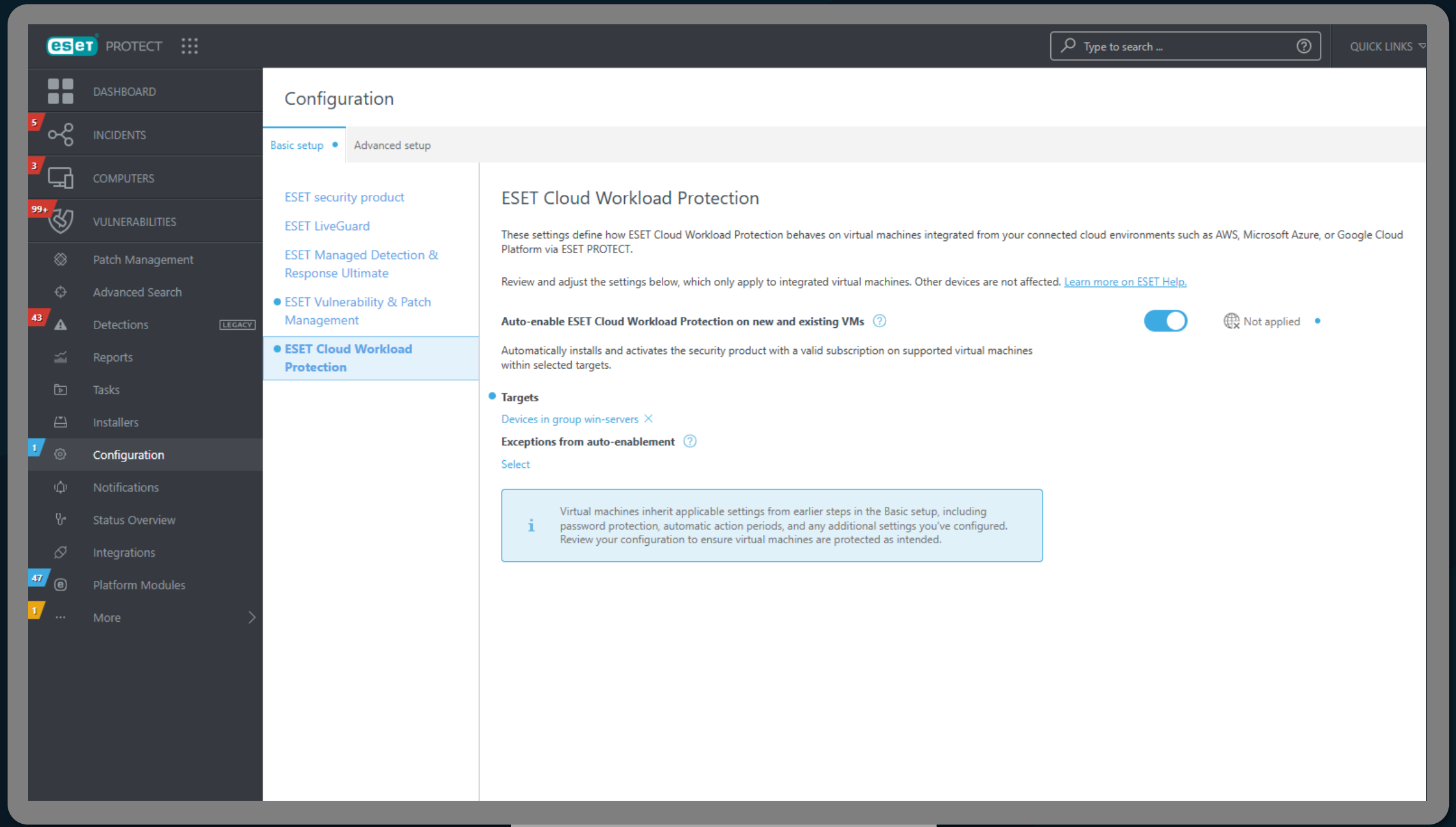
Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Integrations
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Type to search ...
Amazon Web Services integration
Status
Active
ACTIONS
Azure Protection
Protection for my Azure assets
Status
Active
ACTIONS
ENTRA ID (ecwpmc6)
Very useful integration
Status
Active
ACTIONS


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Computers
Groups
All (66)
Companies (66)
RSADemo (66)
AD - TWO (6)
Amazon Web Services integration (1)
288528696104 (1)
Azure Protection (4)
ECWP MC6 TEST (4)
eset-cwpp-rg-be4ad921-82fa-492...
eset-entra-rg-a8058ef3-1b6f-45d...
linux (2)
NetworkWatcherRG (0)
win-servers (2)
Entra ID (3)
Entra ID_VL (1)
EvilCorp (3)
IT (14)
RSA MainCompany (28)
Servers (1)
Z_Archive (3)
Lost & found (0)
Tags
Admin
AI
AppControl
Browser_Security
DEMO
Gartner
Roles
RR
RSADemo
Amazon Web Services i... (1)
Tags
Add Filter
ADVANCED FILTERS
NAME
IP ADDRESS
ALE...
STATUS
INCIDE...
VULNE...
DETECT...
OS NAME
LOGGED U...
LAST CONNECTED
i-060c732863...
172.31.14.77
0
0
0
0
Amazon Linux
Mar 5, 2026, 2:13:06 PM
ADD DEVICE
ACTIONS
1

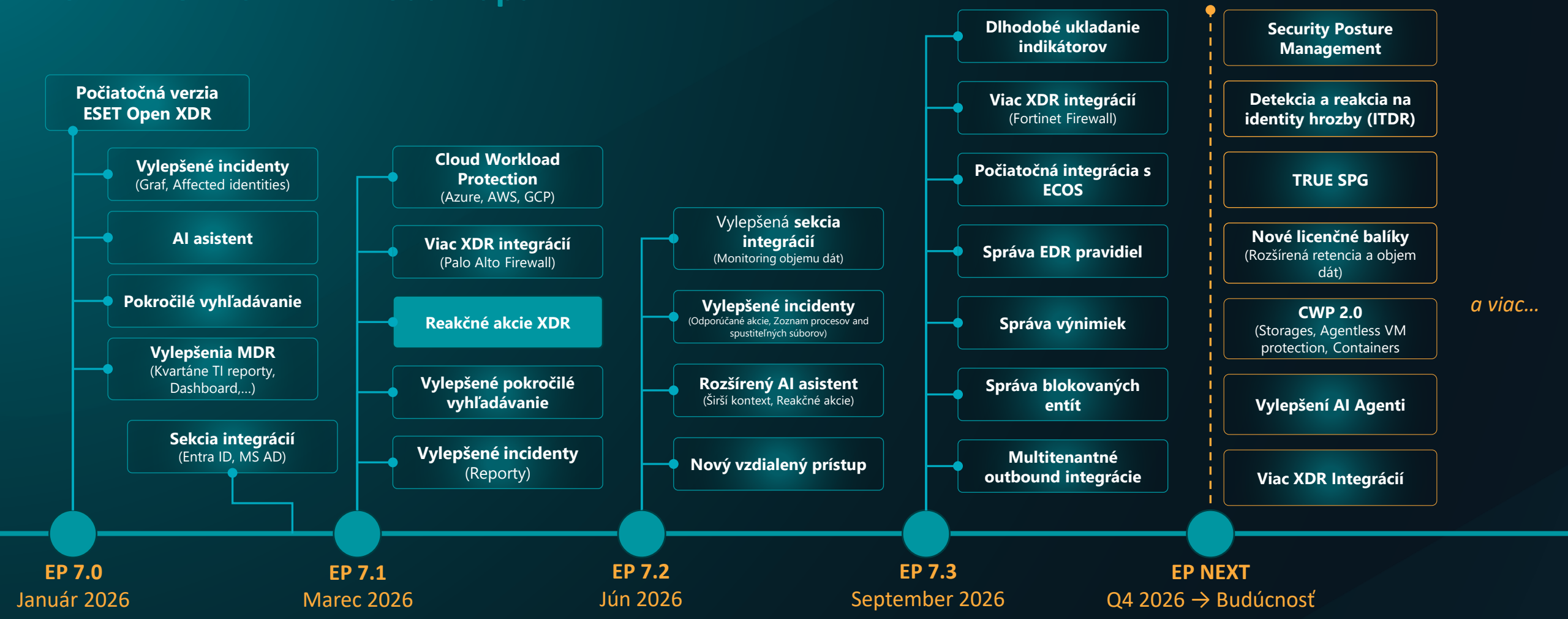

ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Computers
Groups
All (66)
Companies (66)
RSADemo (66)
AD - TWO (6)
Amazon Web Services integration (1)
288528696104 (1)
Azure Protection (4)
ECWP MC6 TEST (4)
eset-cwpp-rg-be4ad921-82fa-492...
eset-entra-rg-a8058ef3-1b6f-45d...
linux (2)
NetworkWatcherRG (0)
win-servers (2)
Entra ID (3)
Entra ID_VL (1)
EvilCorp (3)
IT (14)
RSA MainCompany (28)
Servers (1)
Z_Archive (3)
Lost & found (0)
Tags
Admin
AI
AppControl
Browser_Security
DEMO
Gartner
Roles
RR
RSADemo
Azure Protection (4)
Tags
Add Filter
ADVANCED FILTERS
NAME
IP ADDRESS
ALE...
STATUS
INCIDE...
VULNE...
DETECT...
OS NAME
LOGGED U...
LAST CONNECTED
a-win25-02
172.22.0.4
0
2
0
0
Microsoft Windows Server...
Mar 5, 2026, 2:16:49 PM
a-win25-03
172.24.0.4
0
1
0
0
Microsoft Windows Server...
Admin_ES
Mar 5, 2026, 2:13:16 PM
ubnt-d
172.22.0.4
1
0
33
0
Ubuntu
Mar 5, 2026, 2:17:42 PM
ubnt-e
172.23.0.4
1
0
33
0
Ubuntu
Mar 5, 2026, 2:12:29 PM
ADD DEVICE
ACTIONS
1


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Configuration
Basic setup
Advanced setup
ESET security product
ESET LiveGuard
ESET Managed Detection & Response Ultimate
ESET Vulnerability & Patch Management
ESET Cloud Workload Protection
ESET Cloud Workload Protection
These settings define how ESET Cloud Workload Protection behaves on virtual machines integrated from your connected cloud environments such as AWS, Microsoft Azure, or Google Cloud Platform via ESET PROTECT.
Review and adjust the settings below, which only apply to integrated virtual machines. Other devices are not affected. Learn more on ESET Help.
Auto-enable ESET Cloud Workload Protection on new and existing VMs
Not applied
Automatically installs and activates the security product with a valid subscription on supported virtual machines within selected targets.
Targets
Devices in group win-servers
Exceptions from auto-enablement
Select
Virtual machines inherit applicable settings from earlier steps in the Basic setup, including password protection, automatic action periods, and any additional settings you've configured. Review your configuration to ensure virtual machines are protected as intended.
BACK
NEXT
APPLY

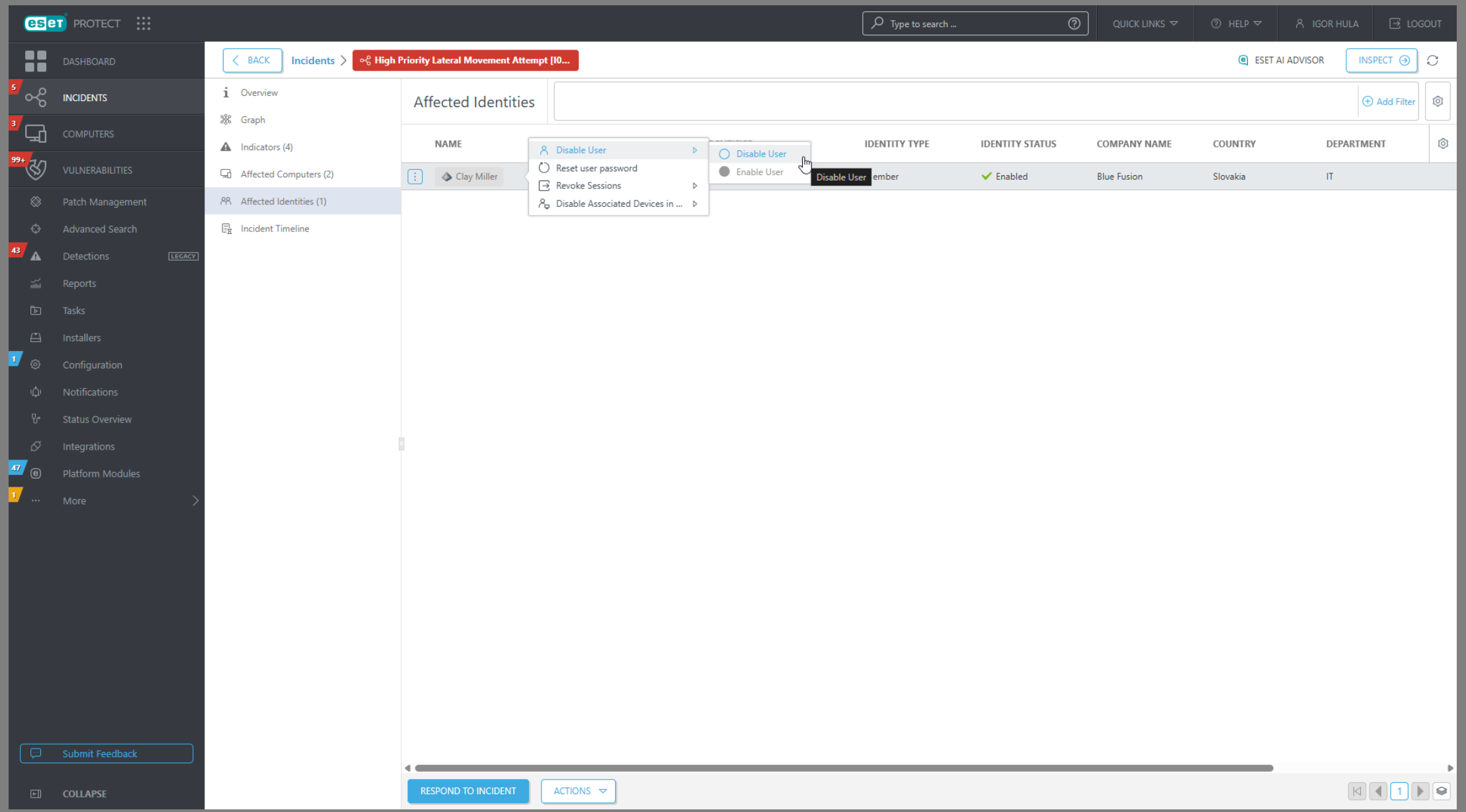

eset PROTECT
Type to search ...
QUICK LINKS
DASHBOARD
5 INCIDENTS
3 COMPUTERS
99+ VULNERABILITIES
Patch Management
Advanced Search
43 Detections LEGACY
Reports
Tasks
Installers
1 Configuration
Notifications
Status Overview
Integrations
47 Platform Modules
1 More
Configuration
Basic setup
Advanced setup
ESET security product
ESET LiveGuard
ESET Managed Detection & Response Ultimate
ESET Vulnerability & Patch Management
ESET Cloud Workload Protection
ESET Cloud Workload Protection
These settings define how ESET Cloud Workload Protection behaves on virtual machines integrated from your connected cloud environments such as AWS, Microsoft Azure, or Google Cloud Platform via ESET PROTECT.
Review and adjust the settings below, which only apply to integrated virtual machines. Other devices are not affected. Learn more on ESET Help.
Auto-enable ESET Cloud Workload Protection on new and existing VMs
Not applied
Automatically installs and activates the security product with a valid subscription on supported virtual machines within selected targets.
Targets
Devices in group win-servers
Exceptions from auto-enablement
Select
Virtual machines inherit applicable settings from earlier steps in the Basic setup, including password protection, automatic action periods, and any additional settings you've configured. Review your configuration to ensure virtual machines are protected as intended.

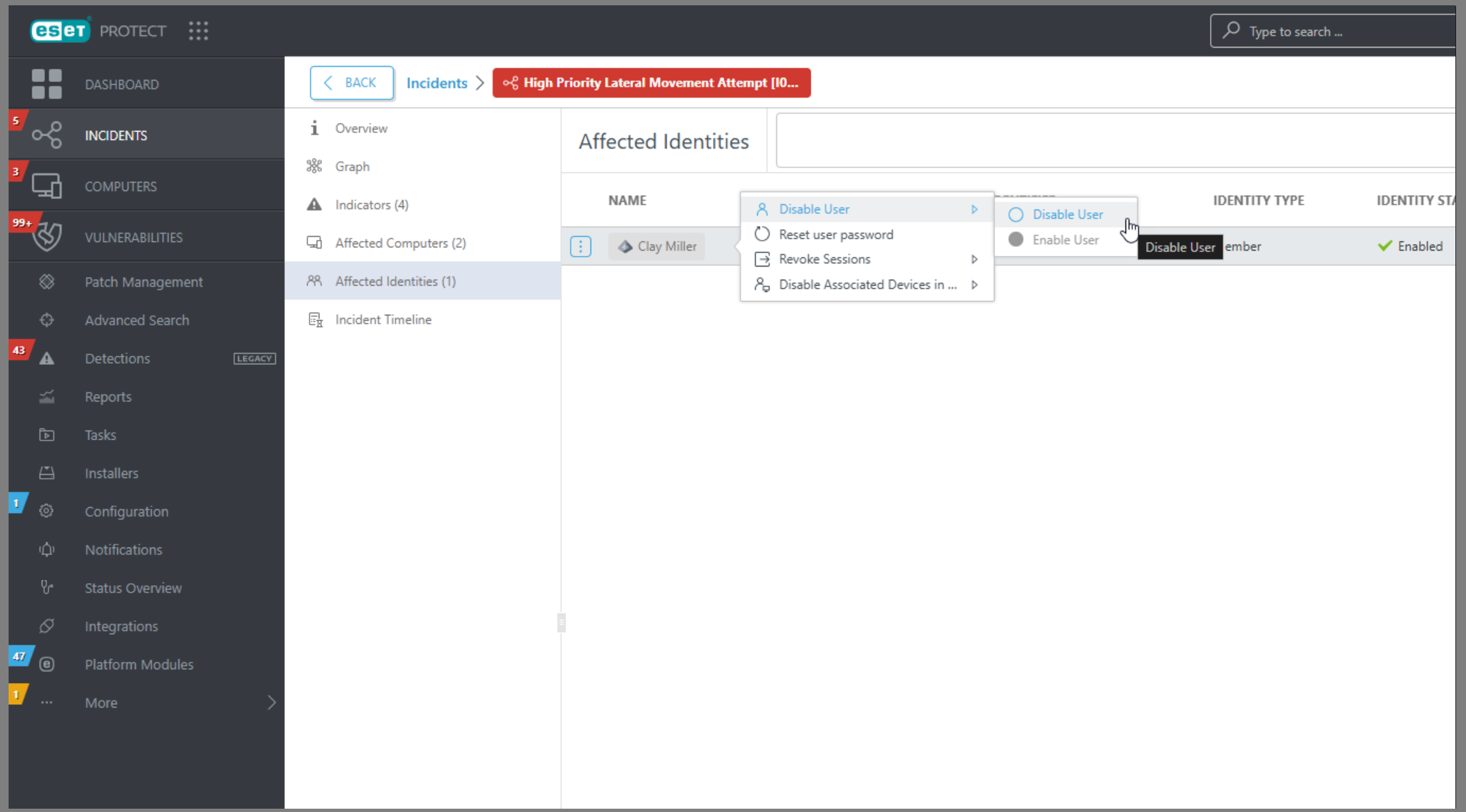
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

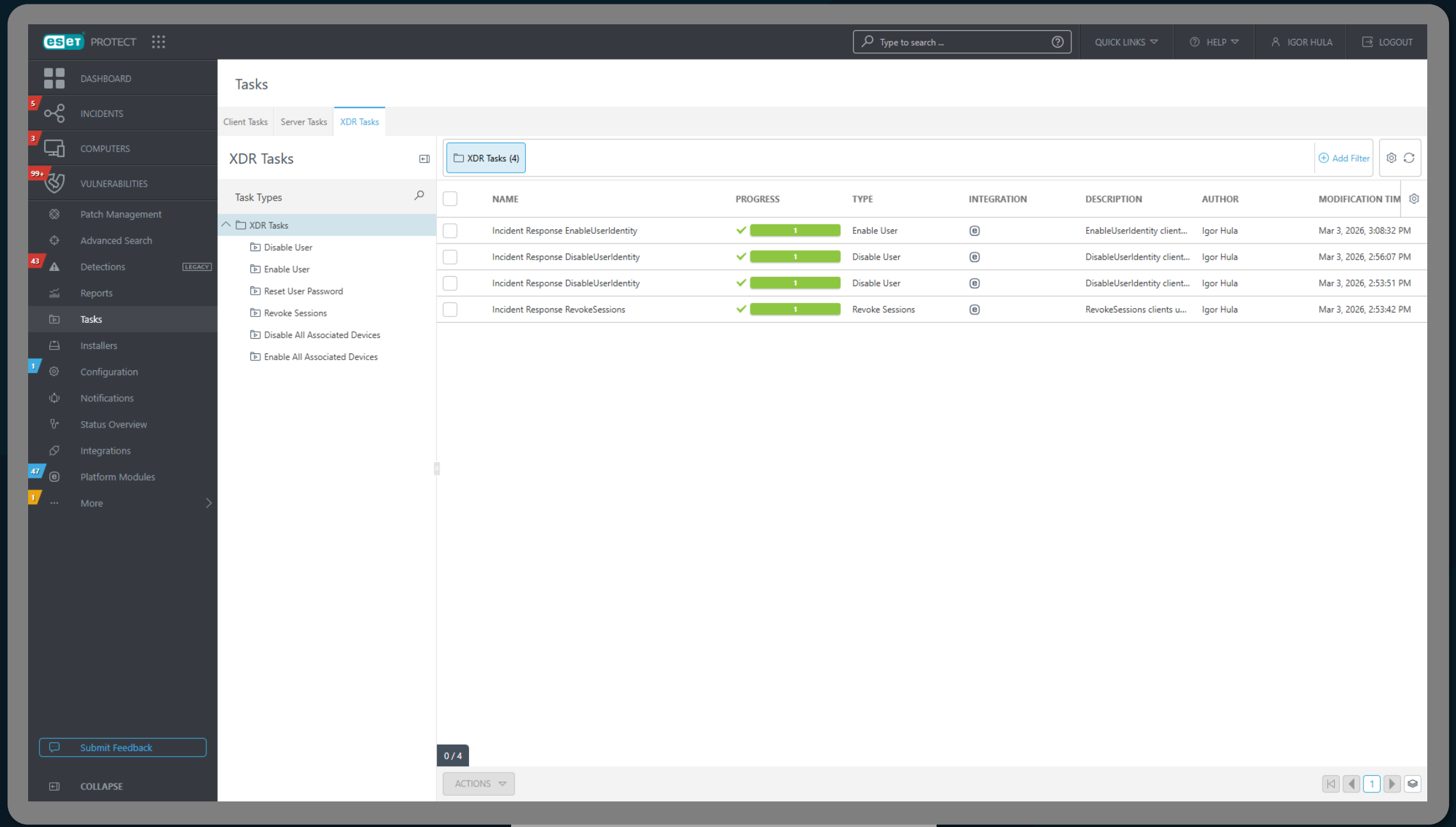
ESET PROTECT – HL Roadmapa

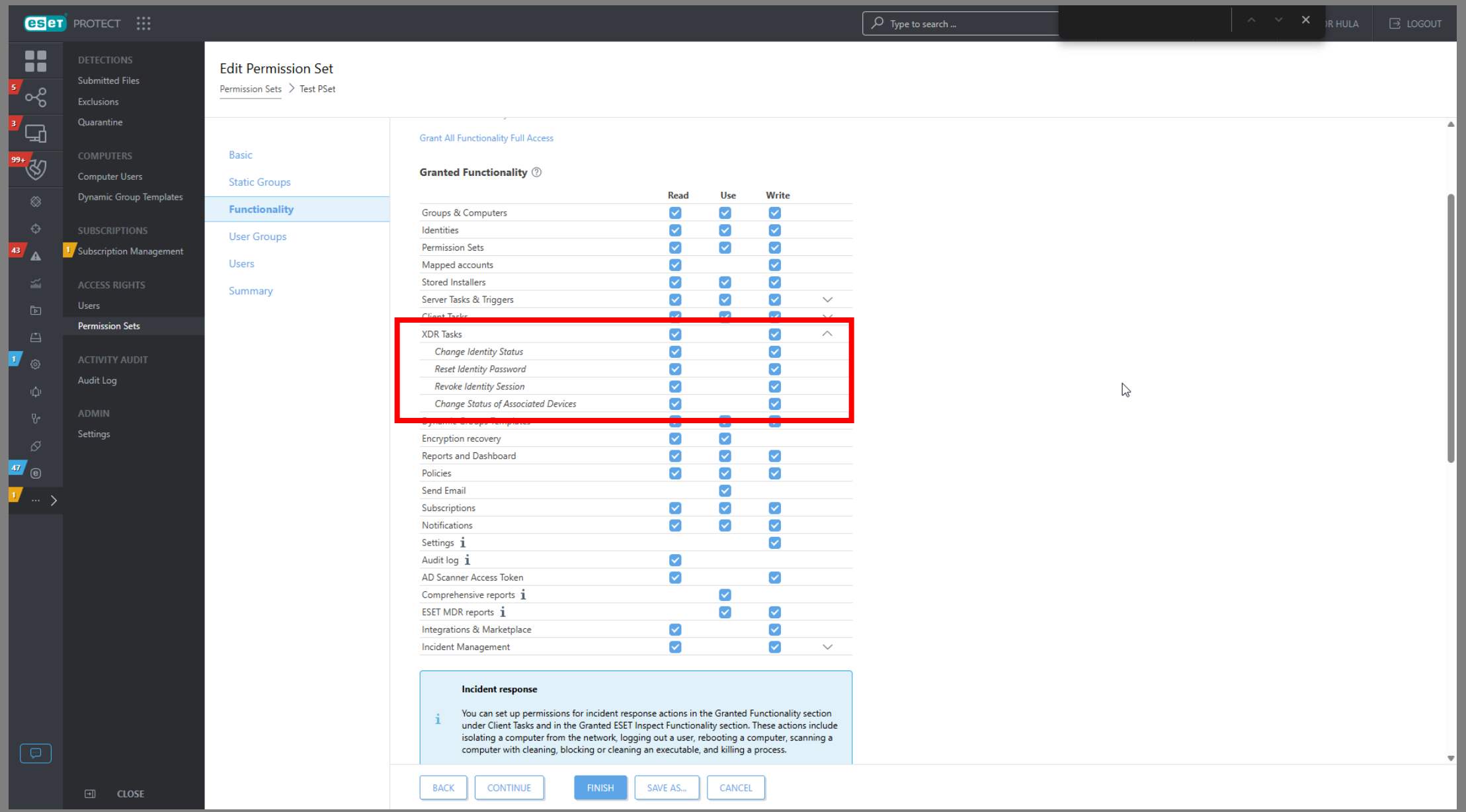


Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
High Priority Lateral Movement Attempt [I0...
ESET AI ADVISOR
INSPECT
Overview
Graph
Indicators (4)
Affected Computers (2)
Affected Identities (1)
Incident Timeline
Affected Identities
Add Filter
NAME
IDENTITY TYPE
IDENTITY STATUS
COMPANY NAME
COUNTRY
DEPARTMENT
Clay Miller
Disable User
Reset user password
Revoke Sessions
Disable Associated Devices in ...
Disable User
Enable User
Disable User
ember
Enabled
Blue Fusion
Slovakia
IT
RESPOND TO INCIDENT
ACTIONS
1

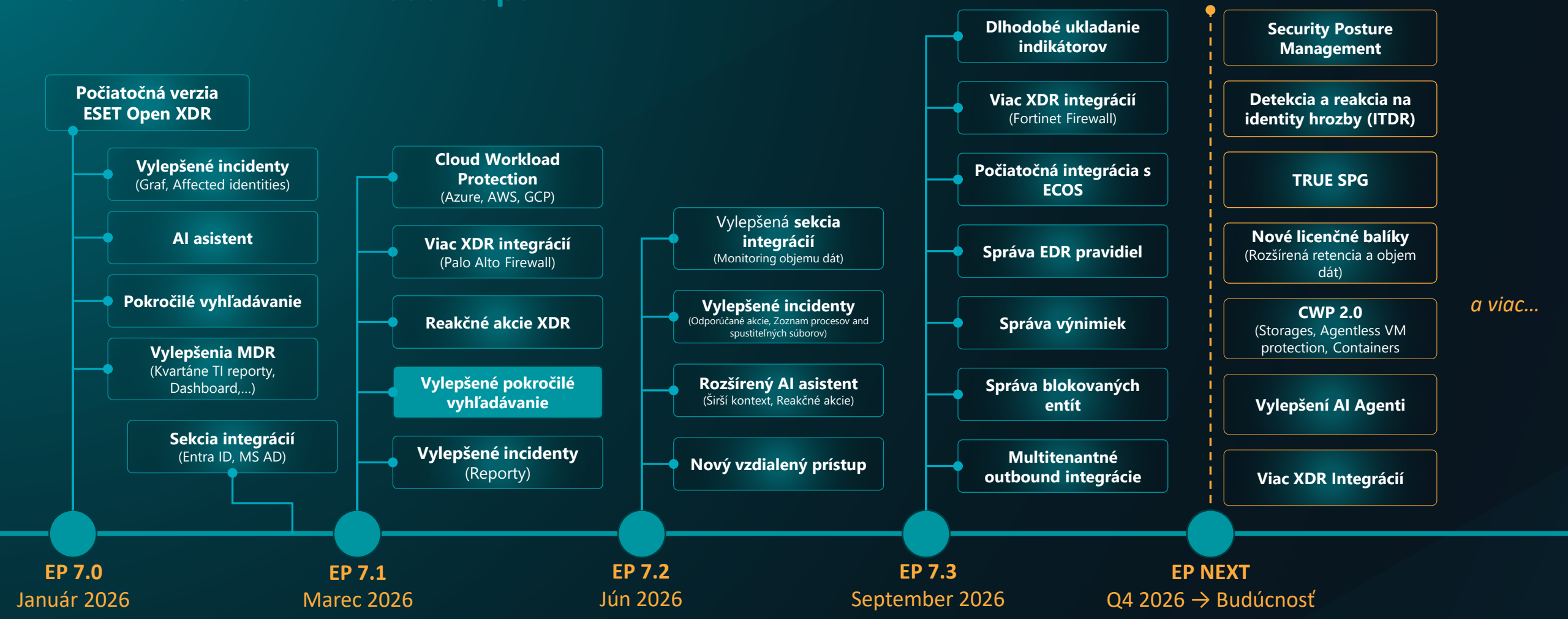

eset PROTECT
Type to search ...
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
BACK
Incidents
High Priority Lateral Movement Attempt [I0...
Overview
Graph
Indicators (4)
Affected Computers (2)
Affected Identities (1)
Incident Timeline
Affected Identities
NAME
IDENTITY TYPE
Clay Miller
Disable User
Reset user password
Revoke Sessions
Disable Associated Devices in ...
Disable User
Enable User
Disable User
ember
Enabled


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Tasks
Client Tasks
Server Tasks
XDR Tasks
XDR Tasks
Task Types
XDR Tasks
Disable User
Enable User
Reset User Password
Revoke Sessions
Disable All Associated Devices
Enable All Associated Devices
XDR Tasks (4)
Add Filter
NAME
PROGRESS
TYPE
INTEGRATION
DESCRIPTION
AUTHOR
MODIFICATION TIM
Incident Response EnableUserIdentity
Enable User
EnableUserIdentity client...
Igor Hula
Mar 3, 2026, 3:08:32 PM
Incident Response DisableUserIdentity
Disable User
DisableUserIdentity client...
Igor Hula
Mar 3, 2026, 2:56:07 PM
Incident Response DisableUserIdentity
Disable User
DisableUserIdentity client...
Igor Hula
Mar 3, 2026, 2:53:51 PM
Incident Response RevokeSessions
Revoke Sessions
RevokeSessions clients u...
Igor Hula
Mar 3, 2026, 2:53:42 PM
0 / 4
ACTIONS

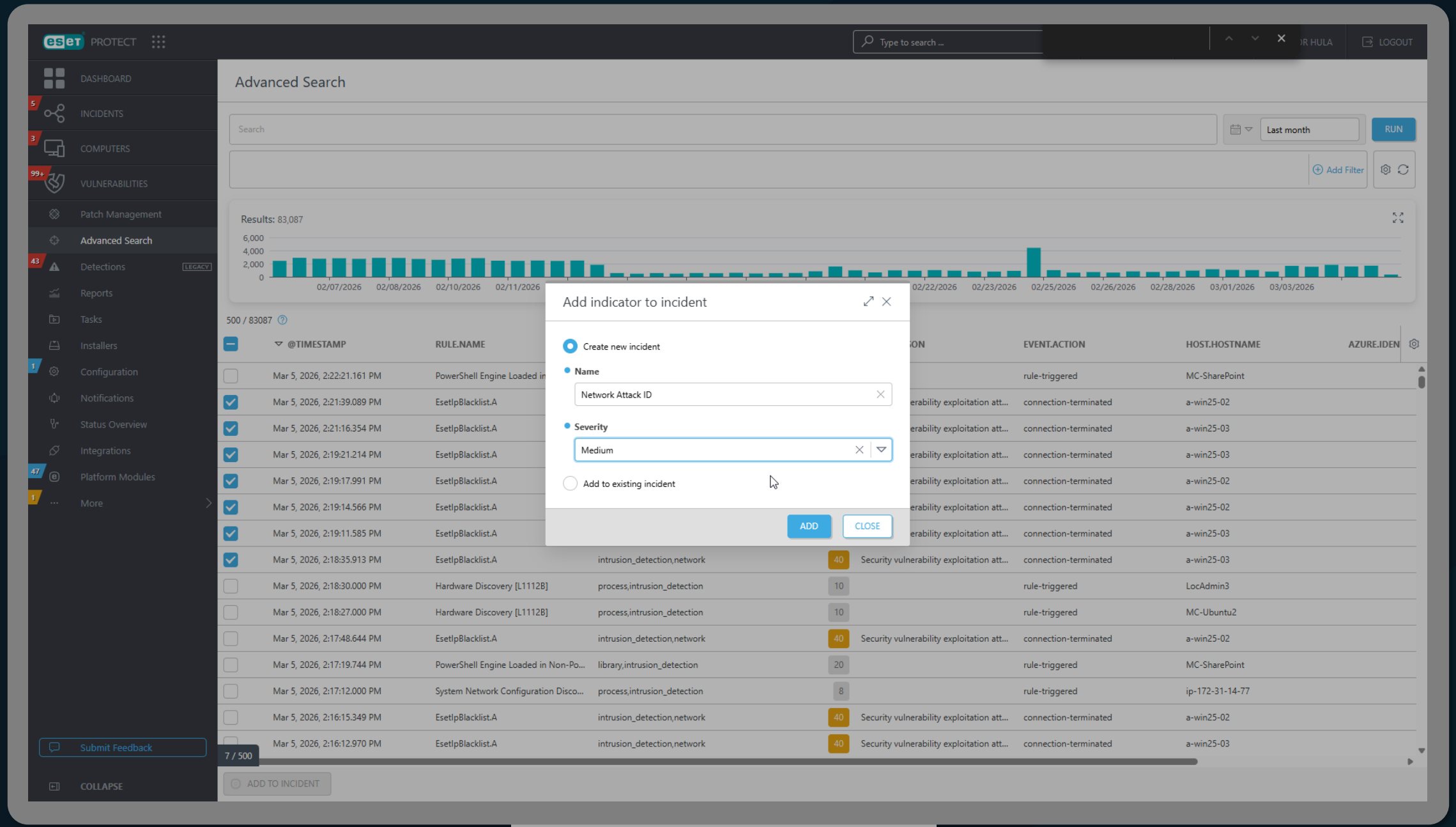

PROTECT
Type to search ...
LOGOUT
DETECTIONS
Submitted Files
Exclusions
Quarantine
COMPUTERS
Computer Users
Dynamic Group Templates
SUBSCRIPTIONS
Subscription Management
ACCESS RIGHTS
Users
Permission Sets
ACTIVITY AUDIT
Audit Log
ADMIN
Settings
CLOSE
Edit Permission Set
Permission Sets > Test PSet
Basic
Static Groups
Functionality
User Groups
Users
Summary
Grant All Functionality Full Access
Granted Functionality
Read
Use
Write
Groups & Computers
Identities
Permission Sets
Mapped accounts
Stored Installers
Server Tasks & Triggers
XDR Tasks
Change Identity Status
Reset Identity Password
Revoke Identity Session
Change Status of Associated Devices
Encryption recovery
Reports and Dashboard
Policies
Send Email
Subscriptions
Notifications
Settings
Audit log
AD Scanner Access Token
Comprehensive reports
ESET MDR reports
Integrations & Marketplace
Incident Management
Incident response
You can set up permissions for incident response actions in the Granted Functionality section under Client Tasks and in the Granted ESET Inspect Functionality section. These actions include isolating a computer from the network, logging out a user, rebooting a computer, scanning a computer with cleaning, blocking or cleaning an executable, and killing a process.
BACK
CONTINUE
FINISH
SAVE AS...
CANCEL

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa



Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


PROTECT
Type to search ...
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Advanced Search
Search
Last month
RUN
Add Filter
Results: 83,087
6,000
4,000
2,000
0
02/07/2026
02/08/2026
02/10/2026
02/11/2026
02/22/2026
02/23/2026
02/25/2026
02/26/2026
02/28/2026
03/01/2026
03/03/2026
500 / 83087
@TIMESTAMP
RULE.NAME
EVENT.ACTION
HOST.HOSTNAME
AZURE.IDEN
Mar 5, 2026, 2:22:21.161 PM
PowerShell Engine Loaded in
rule-triggered
MC-SharePoint
Mar 5, 2026, 2:21:39.089 PM
EsetIpBlacklist.A
connection-terminated
a-win25-02
Mar 5, 2026, 2:21:16.354 PM
EsetIpBlacklist.A
connection-terminated
a-win25-03
Mar 5, 2026, 2:19:21.214 PM
EsetIpBlacklist.A
connection-terminated
a-win25-03
Mar 5, 2026, 2:19:17.991 PM
EsetIpBlacklist.A
connection-terminated
a-win25-02
Mar 5, 2026, 2:19:14.566 PM
EsetIpBlacklist.A
connection-terminated
a-win25-02
Mar 5, 2026, 2:19:11.585 PM
EsetIpBlacklist.A
connection-terminated
a-win25-03
Mar 5, 2026, 2:18:35.913 PM
EsetIpBlacklist.A
intrusion_detection,network
40
Security vulnerability exploitation att...
connection-terminated
a-win25-03
Mar 5, 2026, 2:18:30.000 PM
Hardware Discovery [L1112B]
process,intrusion_detection
10
rule-triggered
LocAdmin3
Mar 5, 2026, 2:18:27.000 PM
Hardware Discovery [L1112B]
process,intrusion_detection
10
rule-triggered
MC-Ubuntu2
Mar 5, 2026, 2:17:48.644 PM
EsetIpBlacklist.A
intrusion_detection,network
40
Security vulnerability exploitation att...
connection-terminated
a-win25-02
Mar 5, 2026, 2:17:19.744 PM
PowerShell Engine Loaded in Non-Po...
library,intrusion_detection
20
rule-triggered
MC-SharePoint
Mar 5, 2026, 2:17:12.000 PM
System Network Configuration Disco...
process,intrusion_detection
8
rule-triggered
ip-172-31-14-77
Mar 5, 2026, 2:16:15.349 PM
EsetIpBlacklist.A
intrusion_detection,network
40
Security vulnerability exploitation att...
connection-terminated
a-win25-02
Mar 5, 2026, 2:16:12.970 PM
EsetIpBlacklist.A
intrusion_detection,network
40
Security vulnerability exploitation att...
connection-terminated
a-win25-03
7 / 500
ADD TO INCIDENT
Add indicator to incident
Create new incident
Name
Network Attack ID
Severity
Medium
Add to existing incident
ADD
CLOSE

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

EP 7.0
Január 2026

- **Počiatočná verzia ESET Open XDR**
- **Vylepšené incidenty** (Graf, Affected identities)
- **AI asistent**
- **Pokročilé vyhľadávanie**
- **Vylepšenia MDR** (Kvartáne TI reporty, Dashboard,...)
- **Sekcia integrácií** (Entra ID, MS AD)

EP 7.1
Marec 2026

- **Cloud Workload Protection** (Azure, AWS, GCP)
- **Viac XDR integrácií** (Palo Alto Firewall)
- **Reakčné akcie XDR**
- **Vylepšené pokročilé vyhľadávanie**
- **Vylepšené incidenty** (Reporty)

EP 7.2
Jún 2026

- Vylepšená **sekcia integrácií** (Monitoring objemu dát)
- **Vylepšené incidenty** (Odporúčané akcie, Zoznam procesov and spustiteľných súborov)
- **Rozšírený AI asistent** (Širší kontext, Reakčné akcie)
- **Nový vzdialený prístup**

EP 7.3
September 2026

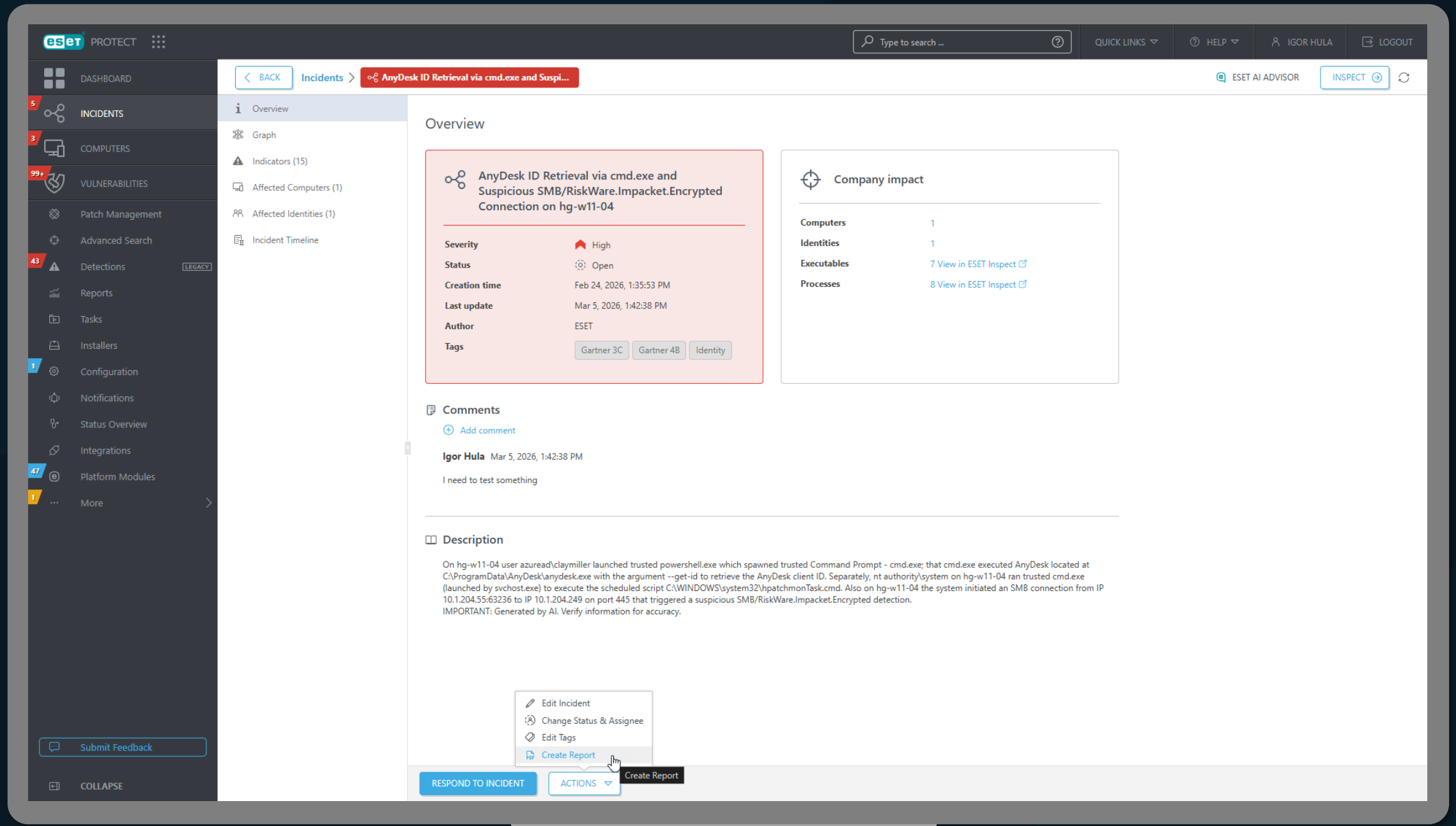
- **Dlhodobé ukladanie indikátorov**
- **Viac XDR integrácií** (Fortinet Firewall)
- **Počiatočná integrácia s ECOS**
- **Správa EDR pravidiel**
- **Správa výnimiek**
- **Správa blokovaných entít**
- **Multitenantné outbound integrácie**

EP NEXT
Q4 2026 → Budúcnosť

- **Security Posture Management**
- **Detekcia a reakcia na identity hrozby (ITDR)**
- **TRUE SPG**
- **Nové licenčné balíky** (Rozšírená retencia a objem dát)
- **CWP 2.0** (Storages, Agentless VM protection, Containers
- **Vylepšení AI Agenti**
- **Viac XDR Integrácií**

a viac...

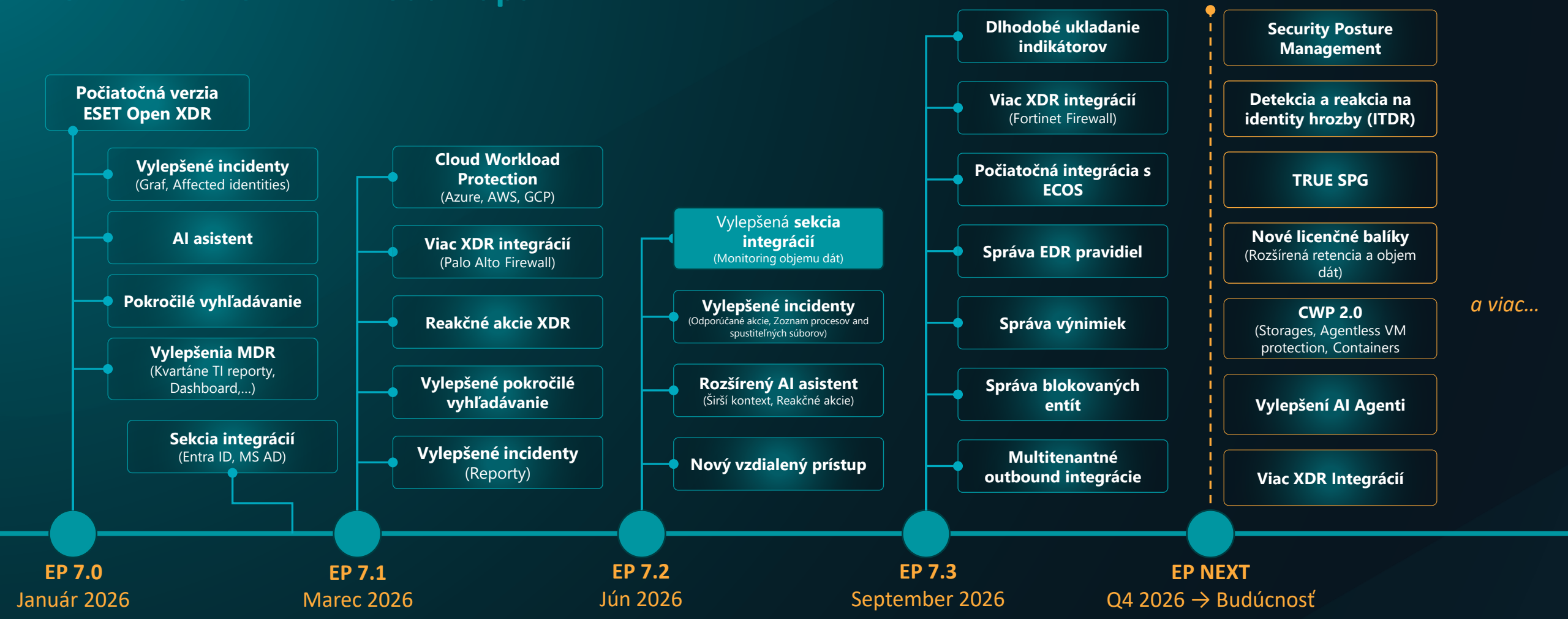
Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
AnyDesk ID Retrieval via cmd.exe and Suspi...
ESET AI ADVISOR
INSPECT
Overview
Graph
Indicators (15)
Affected Computers (1)
Affected Identities (1)
Incident Timeline
Overview
AnyDesk ID Retrieval via cmd.exe and Suspicious SMB/RiskWare.Impacket.Encrypted Connection on hg-w11-04
Severity
High
Status
Open
Creation time
Feb 24, 2026, 1:35:53 PM
Last update
Mar 5, 2026, 1:42:38 PM
Author
ESET
Tags
Gartner 3C
Gartner 4B
Identity
Company impact
Computers
1
Identities
1
Executables
7 View in ESET Inspect
Processes
8 View in ESET Inspect
Comments
Add comment
Igor Hula Mar 5, 2026, 1:42:38 PM
I need to test something
Description
On hg-w11-04 user azuread\claymiller launched trusted powershell.exe which spawned trusted Command Prompt - cmd.exe; that cmd.exe executed AnyDesk located at C:\ProgramData\AnyDesk\anydesk.exe with the argument --get-id to retrieve the AnyDesk client ID. Separately, nt authority\system on hg-w11-04 ran trusted cmd.exe (launched by svchost.exe) to execute the scheduled script C:\WINDOWS\system32\hpatchmonTask.cmd. Also on hg-w11-04 the system initiated an SMB connection from IP 10.1.204.55:63236 to IP 10.1.204.249 on port 445 that triggered a suspicious SMB/RiskWare.Impacket.Encrypted detection.
IMPORTANT: Generated by AI. Verify information for accuracy.
Edit Incident
Change Status & Assignee
Edit Tags
Create Report
RESPOND TO INCIDENT
ACTIONS
Create Report

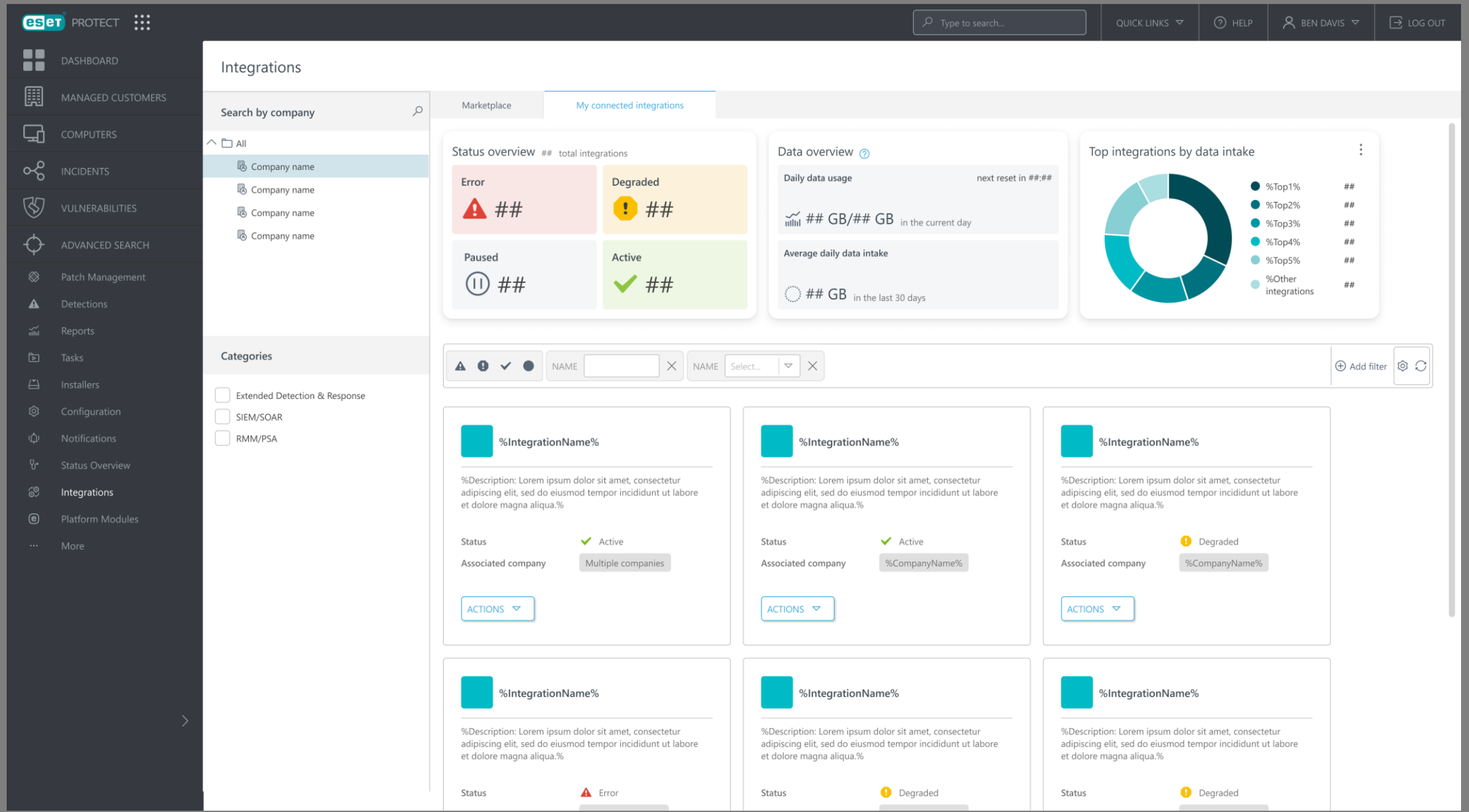

ESET Incident Report
1 / 49
100%
1
2
3
4
5
Cybersecurity
Progress. Protected.
ESET Incident Report
AnyDesk ID Retrieval via cmd.exe and Suspicious
SMB/RiskWare.Impacket.Encrypted Connection on hg-w11-04

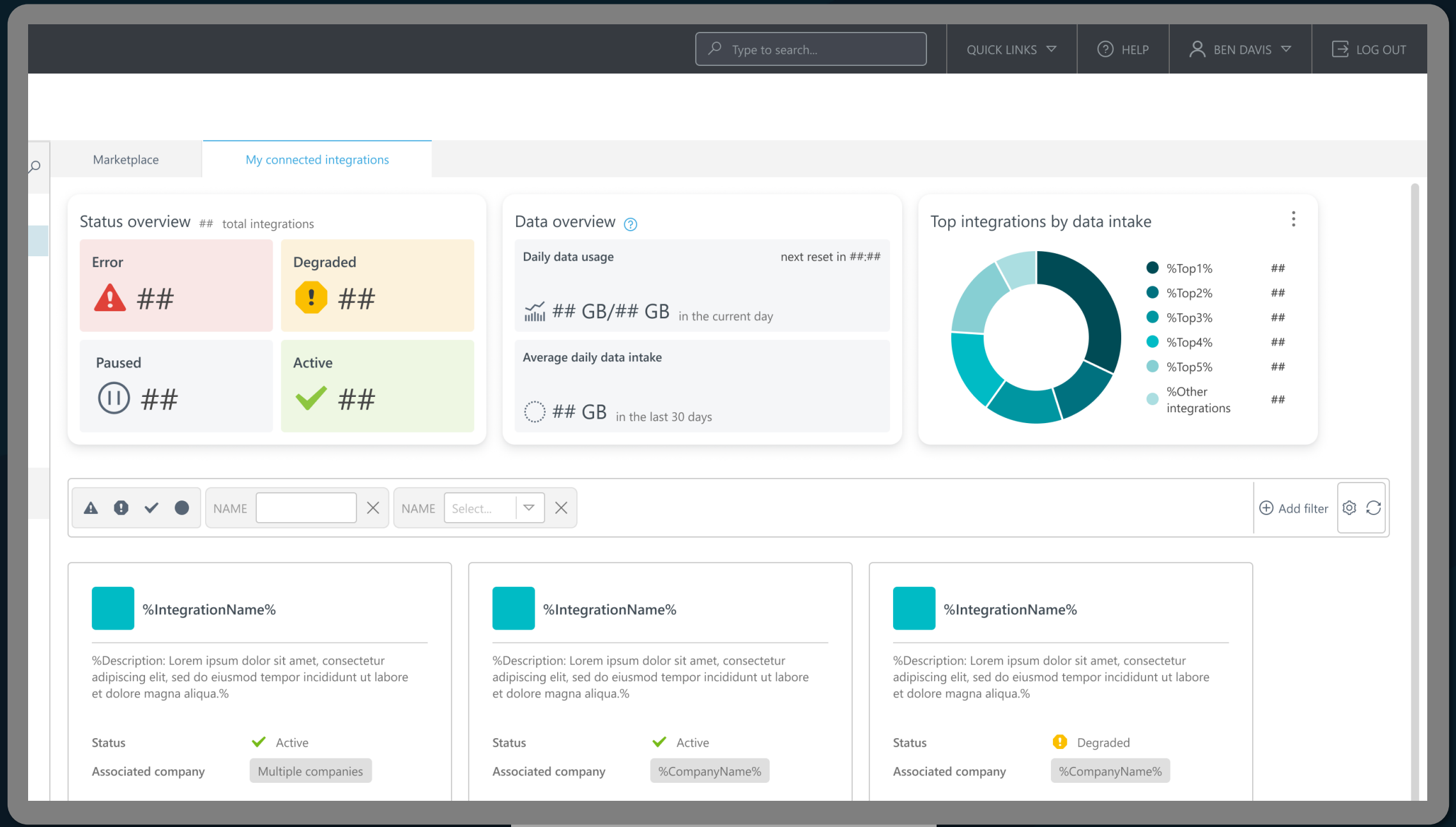
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa



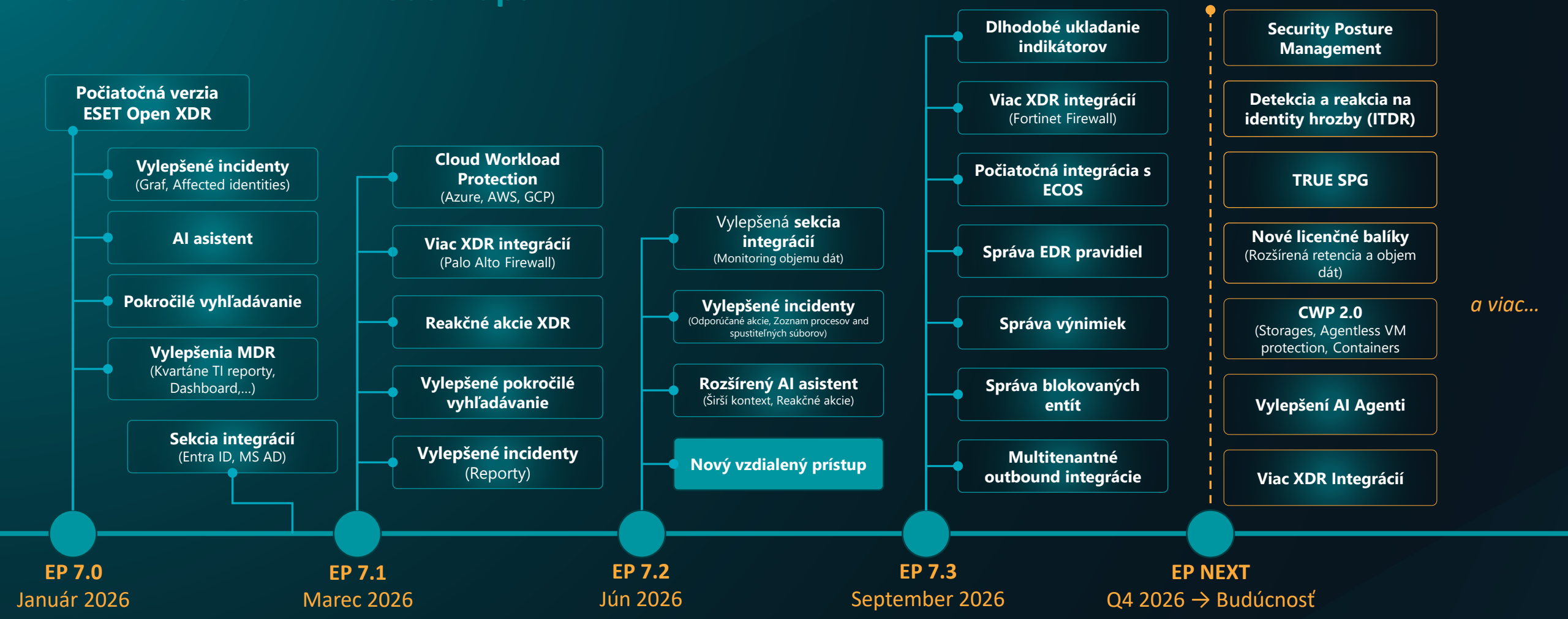
Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


PROTECT
Type to search...
QUICK LINKS
HELP
BEN DAVIS
LOG OUT
DASHBOARD
MANAGED CUSTOMERS
COMPUTERS
INCIDENTS
VULNERABILITIES
ADVANCED SEARCH
Patch Management
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Integrations
Search by company
All
Company name
Company name
Company name
Company name
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Status overview ## total integrations
Error
##
Degraded
##
Paused
##
Active
##
Data overview
Daily data usage
next reset in ##:##
GB/## GB in the current day
Average daily data intake
GB in the last 30 days
Top integrations by data intake
%Top1% ##
%Top2% ##
%Top3% ##
%Top4% ##
%Top5% ##
%Other integrations ##
NAME
NAME
Select...
Add filter
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Active
Associated company
Multiple companies
ACTIONS
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Active
Associated company
%CompanyName%
ACTIONS
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Degraded
Associated company
%CompanyName%
ACTIONS
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Error
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Degraded
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Degraded

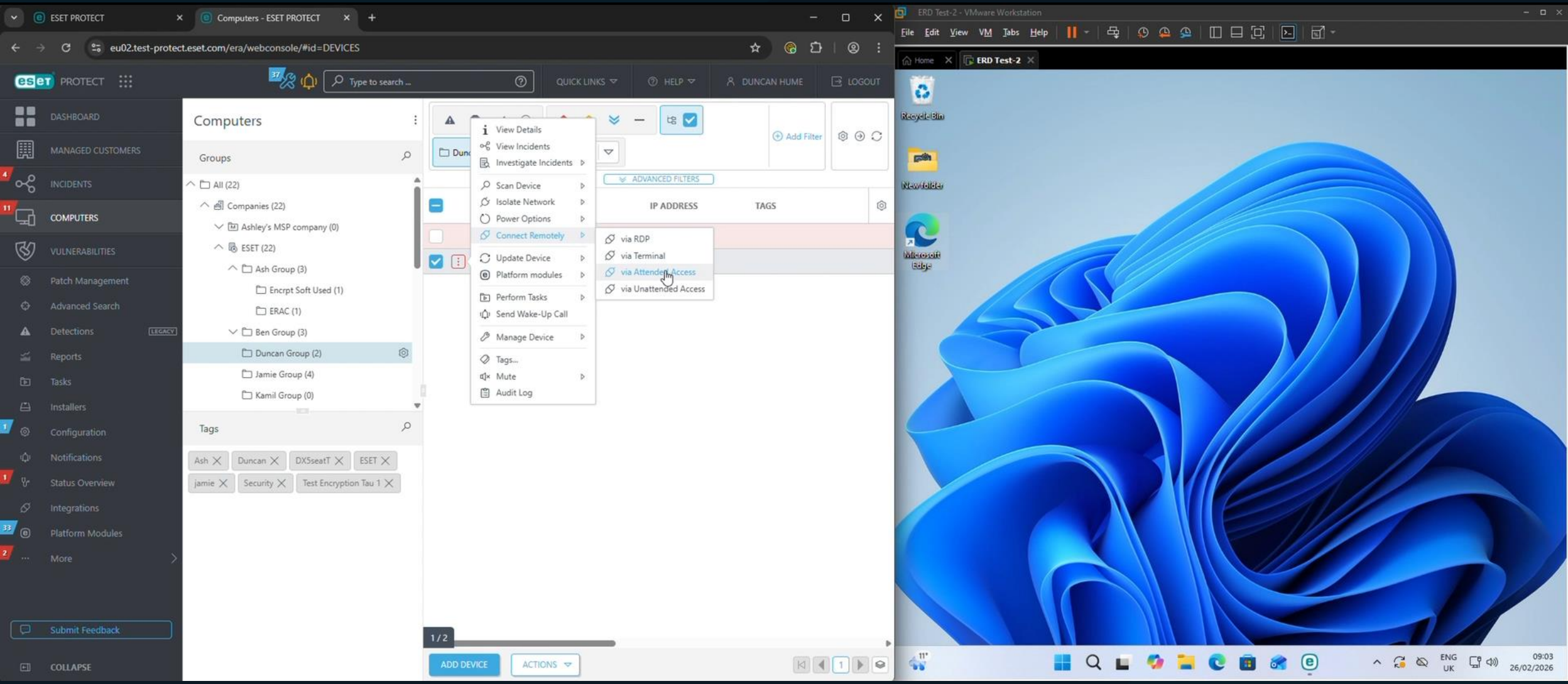

Type to search...
QUICK LINKS
HELP
BEN DAVIS
LOG OUT
Marketplace
My connected integrations
Status overview ## total integrations
Error
##
Degraded
##
Paused
##
Active
##
Data overview
Daily data usage
next reset in ##:##
GB/## GB in the current day
Average daily data intake
GB in the last 30 days
Top integrations by data intake
%Top1% ##
%Top2% ##
%Top3% ##
%Top4% ##
%Top5% ##
%Other integrations ##
NAME
NAME
Select...
Add filter
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Active
Associated company
Multiple companies
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Active
Associated company
%CompanyName%
%IntegrationName%
%Description: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.%
Status
Degraded
Associated company
%CompanyName%

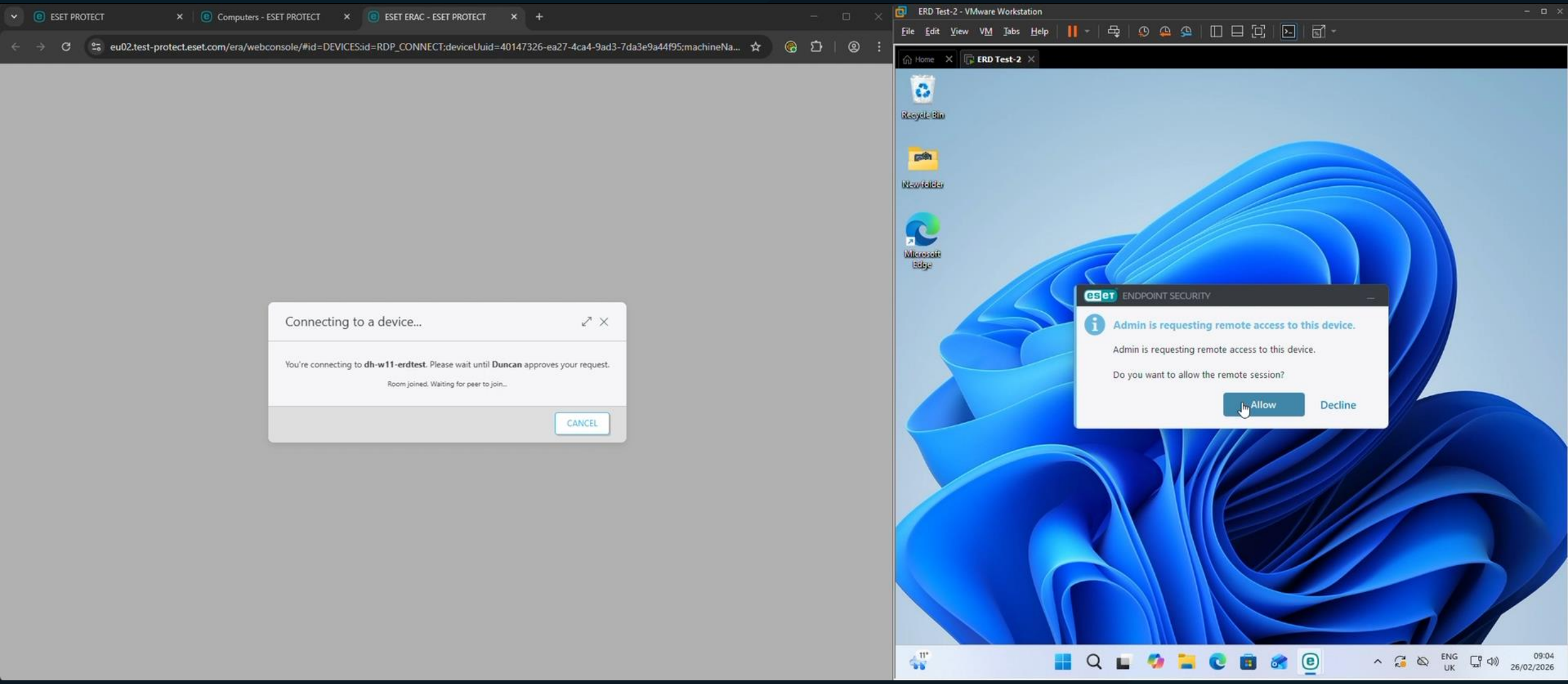
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

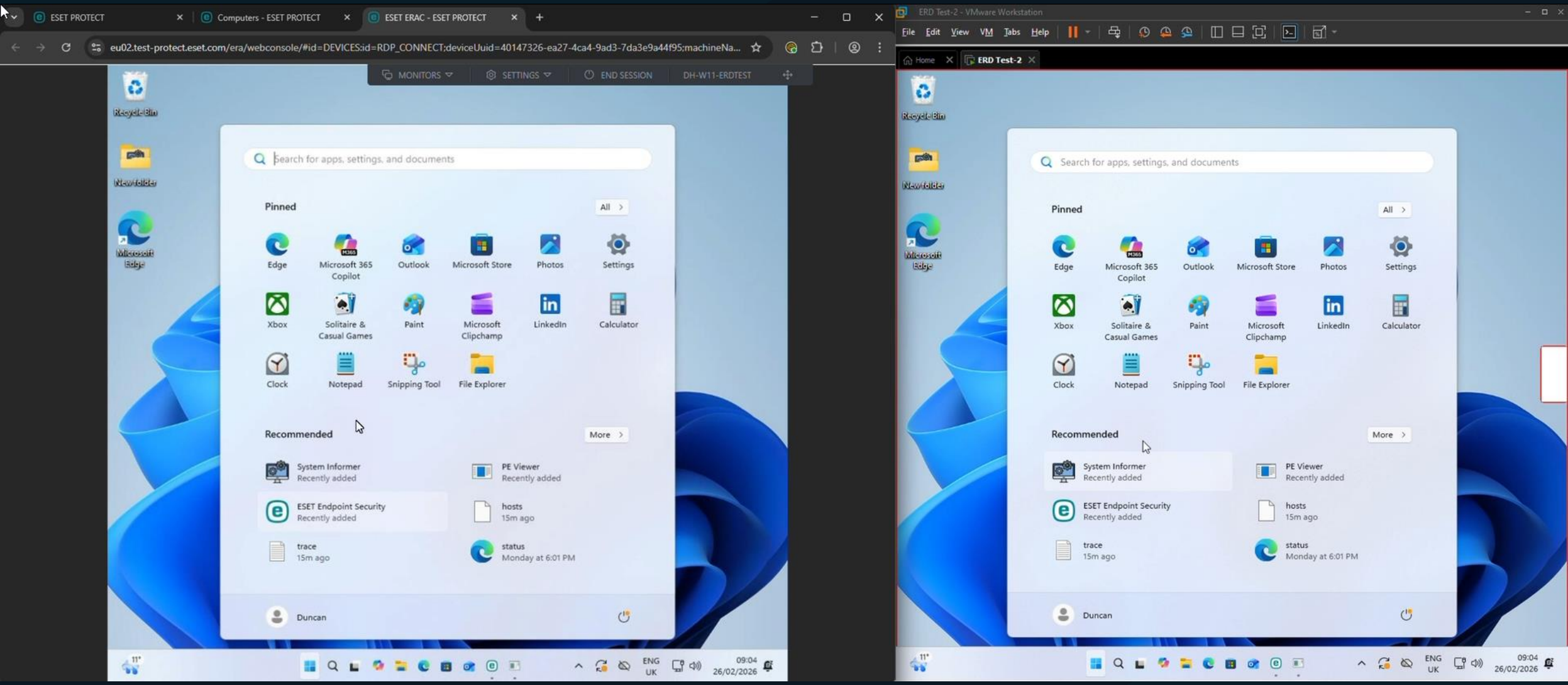
ESET PROTECT – HL Roadmapa



Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

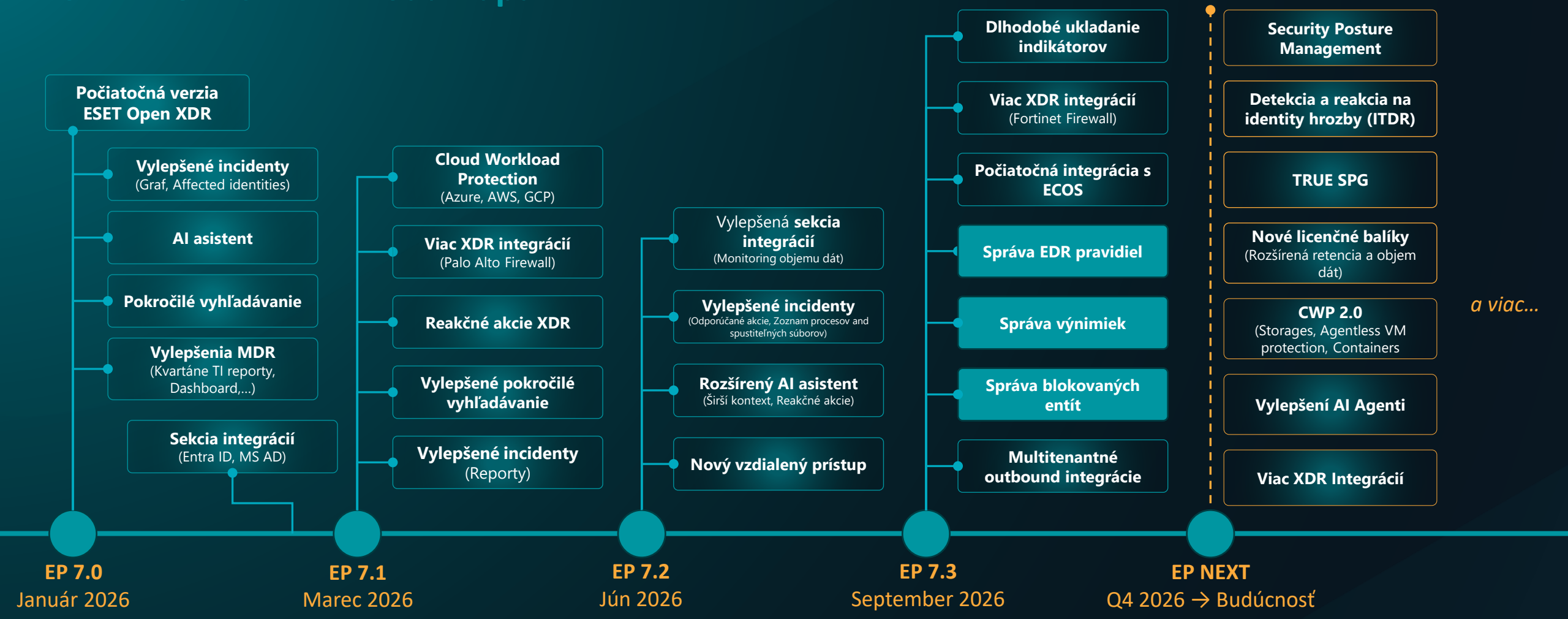

ESET PROTECT
Computers - ESET PROTECT
eu02.test-protect.eset.com/era/webconsole/#id=DEVICES
PROTECT
Type to search ...
QUICK LINKS
HELP
DUNCAN HUME
LOGOUT
DASHBOARD
MANAGED CUSTOMERS
INCIDENTS
COMPUTERS
VULNERABILITIES
Patch Management
Advanced Search
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Computers
Groups
All (22)
Companies (22)
Ashley's MSP company (0)
ESET (22)
Ash Group (3)
Encrpt Soft Used (1)
ERAC (1)
Ben Group (3)
Duncan Group (2)
Jamie Group (4)
Kamil Group (0)
Tags
Ash
Duncan
DXSseatT
ESET
jamie
Security
Test Encryption Tau 1
View Details
View Incidents
Investigate Incidents
Scan Device
Isolate Network
Power Options
Connect Remotely
Update Device
Platform modules
Perform Tasks
Send Wake-Up Call
Manage Device
Tags...
Mute
Audit Log
via RDP
via Terminal
via Attended Access
via Unattended Access
Add Filter
ADVANCED FILTERS
IP ADDRESS
TAGS
1 / 2
ADD DEVICE
ACTIONS
ERD Test-2 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
ERD Test-2
Recycle Bin
New folder
Microsoft Edge
ENG
UK
09:03
26/02/2026


ESET PROTECT
Computers - ESET PROTECT
ESET ERAC - ESET PROTECT
eu02.test-protect.eset.com/era/webconsole/#id=DEVICES:id=RDP_CONNECT;deviceUuid=40147326-ea27-4ca4-9ad3-7da3e9a44f95;machineNa...
Connecting to a device...
You're connecting to dh-w11-erdtest. Please wait until Duncan approves your request.
Room joined. Waiting for peer to join...
CANCEL
ERD Test-2 - VMware Workstation
File Edit View VM Tabs Help
Home
ERD Test-2
Recycle Bin
New folder
Microsoft Edge
ESET ENDPOINT SECURITY
Admin is requesting remote access to this device.
Admin is requesting remote access to this device.
Do you want to allow the remote session?
Allow
Decline
ENG UK
09:04 26/02/2026

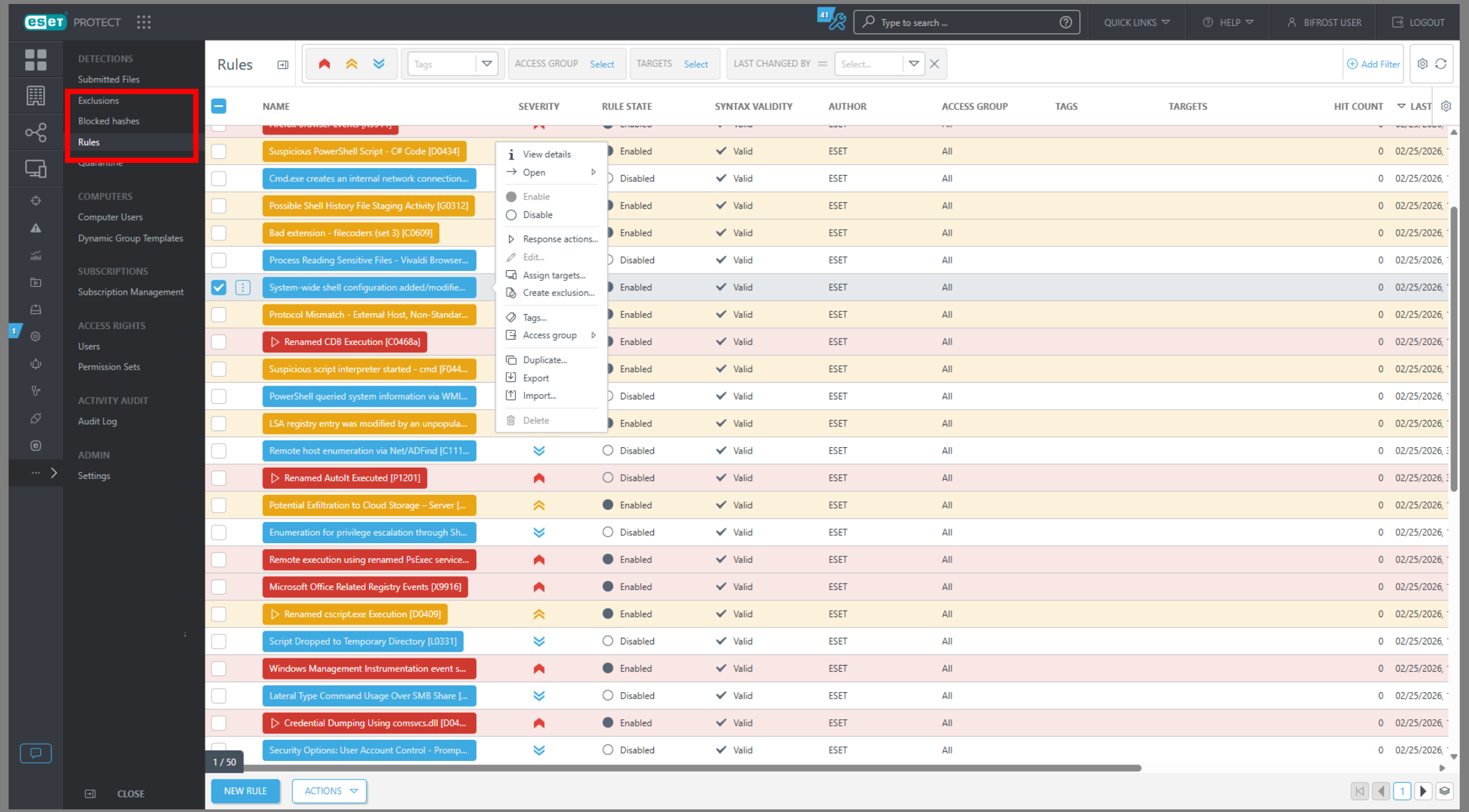

ESET PROTECT
Computers - ESET PROTECT
ESET ERAC - ESET PROTECT
eu02.test-protect.eset.com/era/webconsole/#id=DEVICES;id=RDP_CONNECT;deviceUuid=40147326-ea27-4ca4-9ad3-7da3e9a44f95;machineNa...
MONITORS
SETTINGS
END SESSION
DH-W11-ERDTEST
Recycle Bin
New folder
Microsoft Edge
Search for apps, settings, and documents
Pinned
All
Edge
Microsoft 365 Copilot
Outlook
Microsoft Store
Photos
Settings
Xbox
Solitaire & Casual Games
Paint
Microsoft Clipchamp
LinkedIn
Calculator
Clock
Notepad
Snipping Tool
File Explorer
Recommended
More
System Informer
Recently added
PE Viewer
Recently added
ESET Endpoint Security
Recently added
hosts
15m ago
trace
15m ago
status
Monday at 6:01 PM
Duncan
ENG
UK
09:04
26/02/2026
ERD Test-2 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
ERD Test-2
Recycle Bin
New folder
Microsoft Edge
Search for apps, settings, and documents
Pinned
All
Edge
Microsoft 365 Copilot
Outlook
Microsoft Store
Photos
Settings
Xbox
Solitaire & Casual Games
Paint
Microsoft Clipchamp
LinkedIn
Calculator
Clock
Notepad
Snipping Tool
File Explorer
Recommended
More
System Informer
Recently added
PE Viewer
Recently added
ESET Endpoint Security
Recently added
hosts
15m ago
trace
15m ago
status
Monday at 6:01 PM
Duncan
ENG
UK
09:04
26/02/2026

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

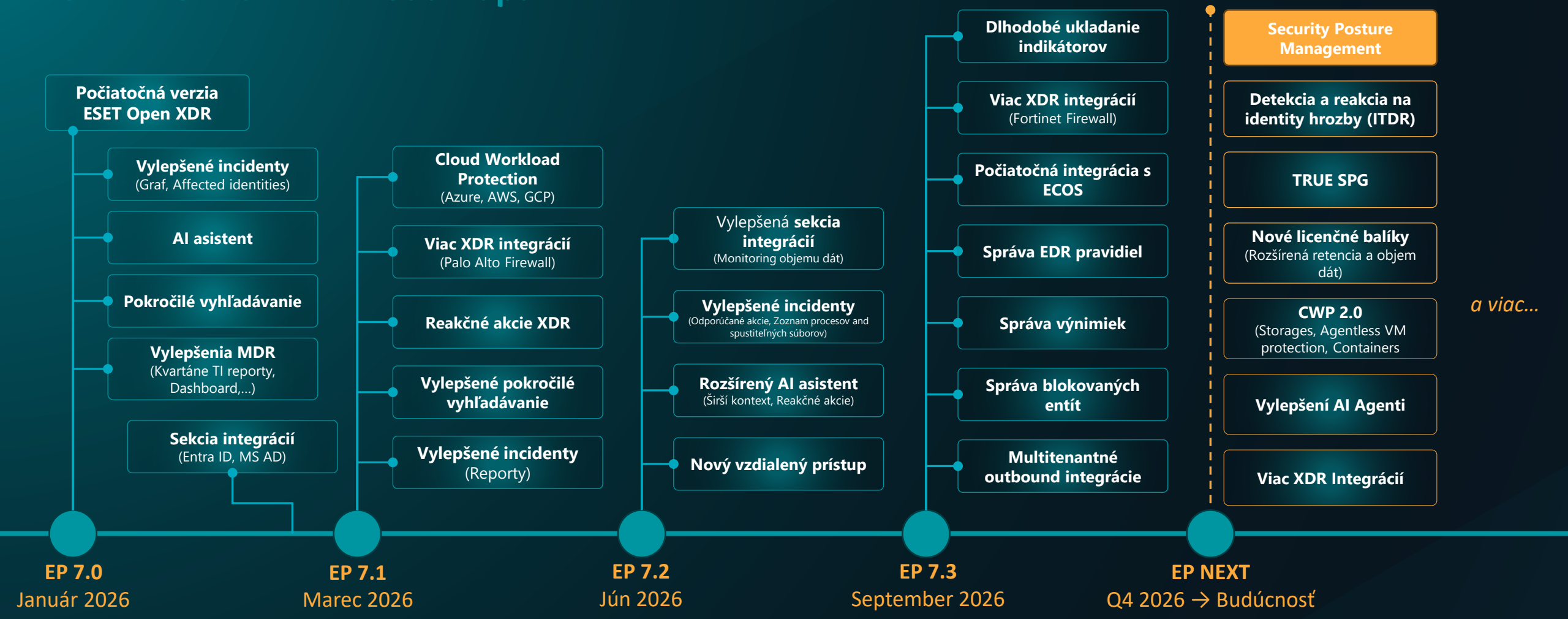


Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

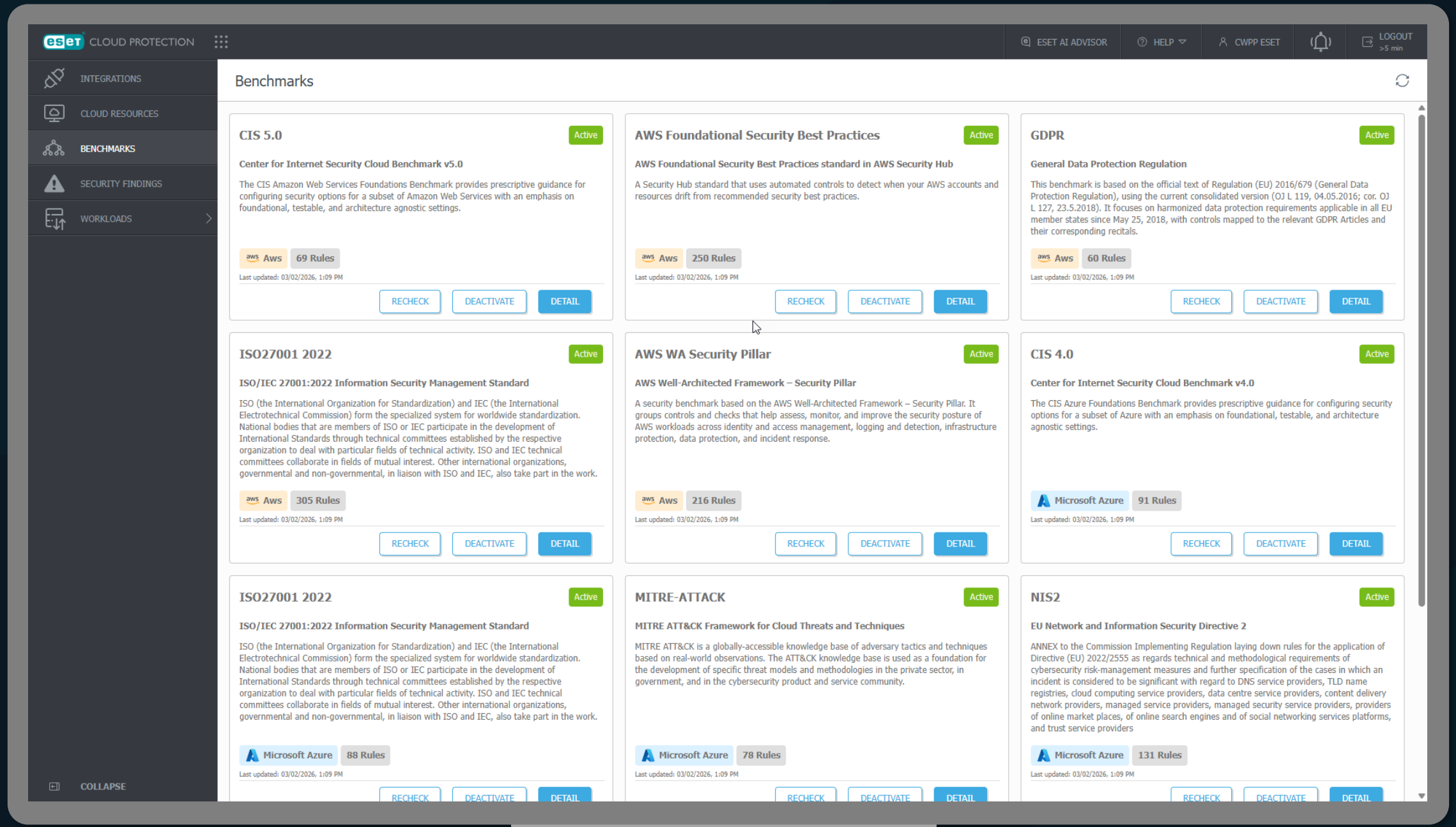

PROTECT
Type to search ...
QUICK LINKS
HELP
BIFROST USER
LOGOUT
DETECTIONS
Submitted Files
Exclusions
Blocked hashes
Rules
COMPUTERS
Computer Users
Dynamic Group Templates
SUBSCRIPTIONS
Subscription Management
ACCESS RIGHTS
Users
Permission Sets
ACTIVITY AUDIT
Audit Log
ADMIN
Settings
CLOSE
Rules
Tags
ACCESS GROUP Select
TARGETS Select
LAST CHANGED BY
Select...
Add Filter
NAME
SEVERITY
RULE STATE
SYNTAX VALIDITY
AUTHOR
ACCESS GROUP
TAGS
TARGETS
HIT COUNT
LAST
Suspicious PowerShell Script - C# Code [D0434]
Cmd.exe creates an internal network connection...
Possible Shell History File Staging Activity [G0312]
Bad extension - filecoders (set 3) [C0609]
Process Reading Sensitive Files - Vivaldi Browser...
System-wide shell configuration added/modifie...
Protocol Mismatch - External Host, Non-Standar...
Renamed CDB Execution [C0468a]
Suspicious script interpreter started - cmd [F044...
PowerShell queried system information via WMI...
LSA registry entry was modified by an unpopula...
Remote host enumeration via Net/ADFind [C111...
Renamed AutoIt Executed [P1201]
Potential Exfiltration to Cloud Storage – Server [...
Enumeration for privilege escalation through Sh...
Remote execution using renamed PsExec service...
Microsoft Office Related Registry Events [X9916]
Renamed cscript.exe Execution [D0409]
Script Dropped to Temporary Directory [L0331]
Windows Management Instrumentation event s...
Lateral Type Command Usage Over SMB Share [...
Credential Dumping Using comsvcs.dll [D04...
Security Options: User Account Control - Promp...
Enabled
Disabled
Valid
ESET
All
0
02/25/2026,
View details
Open
Enable
Disable
Response actions...
Edit...
Assign targets...
Create exclusion...
Tags...
Access group
Duplicate...
Export
Import...
Delete
1 / 50
NEW RULE
ACTIONS

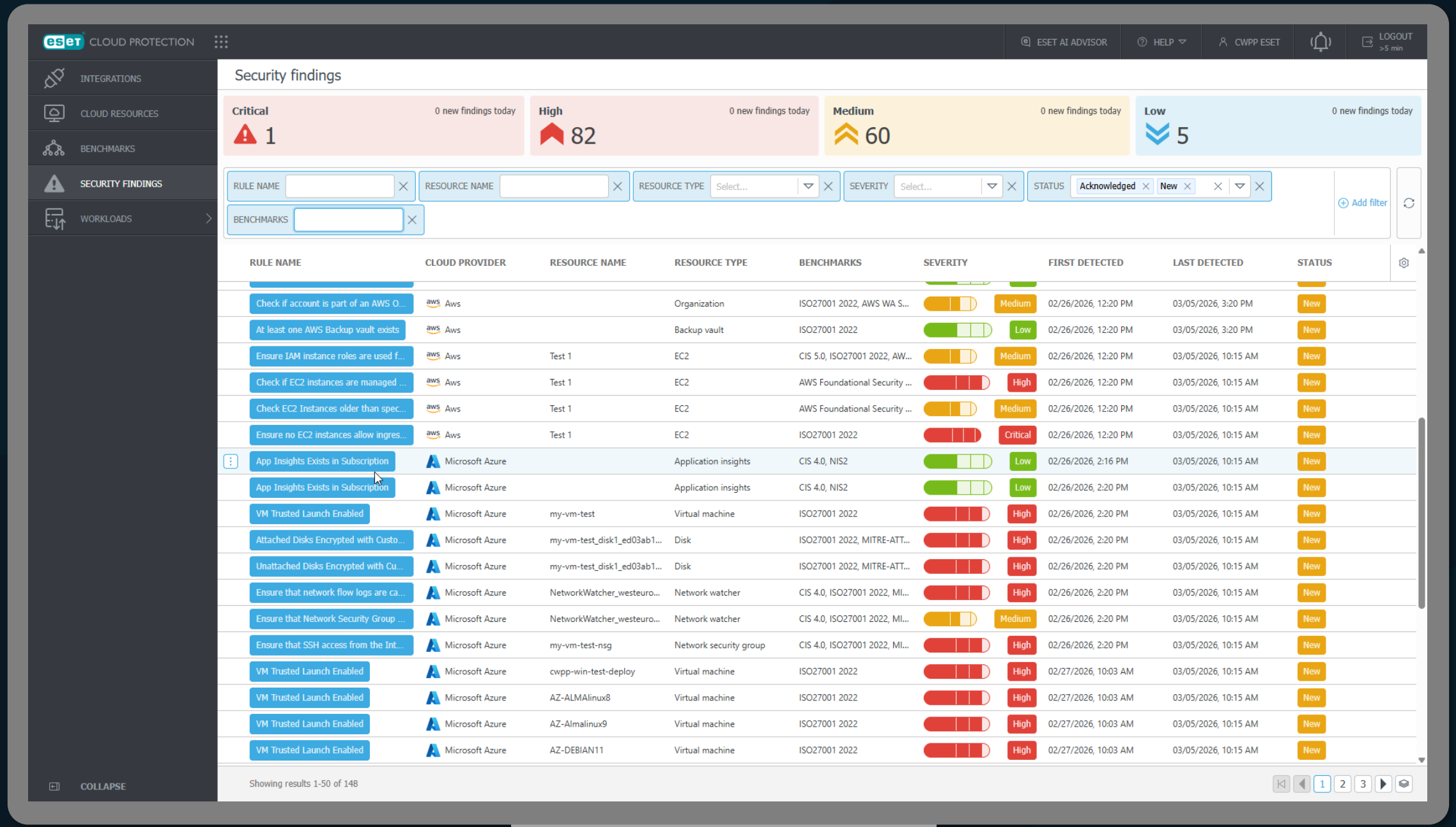
Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa



Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)


ESET CLOUD PROTECTION
ESET AI ADVISOR
HELP
CWPP ESET
LOGOUT
>5 min
INTEGRATIONS
CLOUD RESOURCES
BENCHMARKS
SECURITY FINDINGS
WORKLOADS
COLLAPSE
Benchmarks
CIS 5.0
Active
Center for Internet Security Cloud Benchmark v5.0
The CIS Amazon Web Services Foundations Benchmark provides prescriptive guidance for configuring security options for a subset of Amazon Web Services with an emphasis on foundational, testable, and architecture agnostic settings.
Aws
69 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
AWS Foundational Security Best Practices
Active
AWS Foundational Security Best Practices standard in AWS Security Hub
A Security Hub standard that uses automated controls to detect when your AWS accounts and resources drift from recommended security best practices.
Aws
250 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
GDPR
Active
General Data Protection Regulation
This benchmark is based on the official text of Regulation (EU) 2016/679 (General Data Protection Regulation), using the current consolidated version (OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018). It focuses on harmonized data protection requirements applicable in all EU member states since May 25, 2018, with controls mapped to the relevant GDPR Articles and their corresponding recitals.
Aws
60 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
ISO27001 2022
Active
ISO/IEC 27001:2022 Information Security Management Standard
ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
Aws
305 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
AWS WA Security Pillar
Active
AWS Well-Architected Framework – Security Pillar
A security benchmark based on the AWS Well-Architected Framework – Security Pillar. It groups controls and checks that help assess, monitor, and improve the security posture of AWS workloads across identity and access management, logging and detection, infrastructure protection, data protection, and incident response.
Aws
216 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
CIS 4.0
Active
Center for Internet Security Cloud Benchmark v4.0
The CIS Azure Foundations Benchmark provides prescriptive guidance for configuring security options for a subset of Azure with an emphasis on foundational, testable, and architecture agnostic settings.
Microsoft Azure
91 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
ISO27001 2022
Active
ISO/IEC 27001:2022 Information Security Management Standard
ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
Microsoft Azure
88 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
MITRE-ATTACK
Active
MITRE ATT&CK Framework for Cloud Threats and Techniques
MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Microsoft Azure
78 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL
NIS2
Active
EU Network and Information Security Directive 2
ANNEX to the Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers
Microsoft Azure
131 Rules
Last updated: 03/02/2026, 1:09 PM
RECHECK
DEACTIVATE
DETAIL


ESET CLOUD PROTECTION
ESET AI ADVISOR
HELP
CWPP ESET
LOGOUT
>5 min
INTEGRATIONS
CLOUD RESOURCES
BENCHMARKS
SECURITY FINDINGS
WORKLOADS
COLLAPSE
Security findings
Critical
0 new findings today
1
High
0 new findings today
82
Medium
0 new findings today
60
Low
0 new findings today
5
RULE NAME
RESOURCE NAME
RESOURCE TYPE
Select...
SEVERITY
Select...
STATUS
Acknowledged
New
BENCHMARKS
Add filter
RULE NAME
CLOUD PROVIDER
RESOURCE NAME
RESOURCE TYPE
BENCHMARKS
SEVERITY
FIRST DETECTED
LAST DETECTED
STATUS
Check if account is part of an AWS O... | Aws | | Organization | ISO27001 2022, AWS WA S... | Medium | 02/26/2026, 12:20 PM | 03/05/2026, 3:20 PM | New
At least one AWS Backup vault exists | Aws | | Backup vault | ISO27001 2022 | Low | 02/26/2026, 12:20 PM | 03/05/2026, 3:20 PM | New
Ensure IAM instance roles are used f... | Aws | Test 1 | EC2 | CIS 5.0, ISO27001 2022, AW... | Medium | 02/26/2026, 12:20 PM | 03/05/2026, 10:15 AM | New
Check if EC2 instances are managed ... | Aws | Test 1 | EC2 | AWS Foundational Security ... | High | 02/26/2026, 12:20 PM | 03/05/2026, 10:15 AM | New
Check EC2 Instances older than spec... | Aws | Test 1 | EC2 | AWS Foundational Security ... | Medium | 02/26/2026, 12:20 PM | 03/05/2026, 10:15 AM | New
Ensure no EC2 instances allow ingres... | Aws | Test 1 | EC2 | ISO27001 2022 | Critical | 02/26/2026, 12:20 PM | 03/05/2026, 10:15 AM | New
App Insights Exists in Subscription | Microsoft Azure | | Application insights | CIS 4.0, NIS2 | Low | 02/26/2026, 2:16 PM | 03/05/2026, 10:15 AM | New
App Insights Exists in Subscription | Microsoft Azure | | Application insights | CIS 4.0, NIS2 | Low | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
VM Trusted Launch Enabled | Microsoft Azure | my-vm-test | Virtual machine | ISO27001 2022 | High | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
Attached Disks Encrypted with Custo... | Microsoft Azure | my-vm-test_disk1_ed03ab1... | Disk | ISO27001 2022, MITRE-ATT... | High | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
Unattached Disks Encrypted with Cu... | Microsoft Azure | my-vm-test_disk1_ed03ab1... | Disk | ISO27001 2022, MITRE-ATT... | High | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
Ensure that network flow logs are ca... | Microsoft Azure | NetworkWatcher_westeuro... | Network watcher | CIS 4.0, ISO27001 2022, MI... | High | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
Ensure that Network Security Group ... | Microsoft Azure | NetworkWatcher_westeuro... | Network watcher | CIS 4.0, ISO27001 2022, MI... | Medium | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
Ensure that SSH access from the Int... | Microsoft Azure | my-vm-test-nsg | Network security group | CIS 4.0, ISO27001 2022, MI... | High | 02/26/2026, 2:20 PM | 03/05/2026, 10:15 AM | New
VM Trusted Launch Enabled | Microsoft Azure | cwpp-win-test-deploy | Virtual machine | ISO27001 2022 | High | 02/27/2026, 10:03 AM | 03/05/2026, 10:15 AM | New
VM Trusted Launch Enabled | Microsoft Azure | AZ-ALMAlinux8 | Virtual machine | ISO27001 2022 | High | 02/27/2026, 10:03 AM | 03/05/2026, 10:15 AM | New
VM Trusted Launch Enabled | Microsoft Azure | AZ-Almalinux9 | Virtual machine | ISO27001 2022 | High | 02/27/2026, 10:03 AM | 03/05/2026, 10:15 AM | New
VM Trusted Launch Enabled | Microsoft Azure | AZ-DEBIAN11 | Virtual machine | ISO27001 2022 | High | 02/27/2026, 10:03 AM | 03/05/2026, 10:15 AM | New
Showing results 1-50 of 148
1
2
3

Dôležité: *Predbežný plan, ktorý sa môže meniť.*

ESET PROTECT – HL Roadmapa

EP 7.0
Január 2026

- **Počiatočná verzia ESET Open XDR**
- **Vylepšené incidenty** (Graf, Affected identities)
- **AI asistent**
- **Pokročilé vyhľadávanie**
- **Vylepšenia MDR** (Kvartáne TI reporty, Dashboard,...)
- **Sekcia integrácií** (Entra ID, MS AD)

EP 7.1
Marec 2026

- **Cloud Workload Protection** (Azure, AWS, GCP)
- **Viac XDR integrácií** (Palo Alto Firewall)
- **Reakčné akcie XDR**
- **Vylepšené pokročilé vyhľadávanie**
- **Vylepšené incidenty** (Reporty)

EP 7.2
Jún 2026

- Vylepšená **sekcia integrácií** (Monitoring objemu dát)
- **Vylepšené incidenty** (Odporúčané akcie, Zoznam procesov and spustiteľných súborov)
- **Rozšírený AI asistent** (Širší kontext, Reakčné akcie)
- **Nový vzdialený prístup**

EP 7.3
September 2026

- **Dlhodobé ukladanie indikátorov**
- **Viac XDR integrácií** (Fortinet Firewall)
- **Počiatočná integrácia s ECOS**
- **Správa EDR pravidiel**
- **Správa výnimiek**
- **Správa blokovaných entít**
- **Multitenantné outbound integrácie**

EP NEXT
Q4 2026 → Budúcnosť

- **Security Posture Management**
- **Detekcia a reakcia na identity hrozby (ITDR)**
- **TRUE SPG**
- **Nové licenčné balíky** (Rozšírená retencia a objem dát)
- **CWP 2.0** (Storages, Agentless VM protection, Containers
- **Vylepšení AI Agenti**
- **Viac XDR Integrácií**

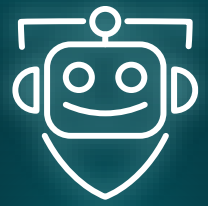
a viac...

Neustále zlepšovanie detekčných technológií (lepšia korelácia indikátorov a incidentov)

V skratke

Špičková detekcia naprieč perimetrami

Prevencia a detekcia hrozieb na úrovni best-in-class



Maximalizácia automatizácie

AI riadená automatizácia pre rýchlu reakciu

Pokrytie medzier pomocou MDR

SOC služby formou outsourcingu

Vaša spätná väzba je pre nás dôležitá a vždy ju berieme do úvahy

In-Product Feedback

Každú spätnú väzbu čítame a vyhodnocujeme

Požiadavky trhu

Prioritizujeme podľa reálnych potrieb trhu

Zákaznícky výskum

Chcete sa zapojiť do nášho výskumu?

feedback-protect@eset.com