Нові рішення з кібербезпеки: як захистити бізнес у 2026 році

Cybersecurity
Progress. Protected.

Нікіта Веселков

Керівник відділу
з технічного супроводження проєктів

nikita.v@eset.ua

ПІДСУМКИ 2025 РОКУ

СТАТИСТИКА ЗА РЕЗУЛЬТАТАМИ РОБОТИ СПЕЦІАЛІСТІВ ESET В УКРАЇНІ

Більше 80 розслідувань кібератак

Надано **понад 500** безкоштовних **ліцензій** для об’єктів критичної інфраструктури

6000 годин побудови/модернізації систем захисту

2 000 годин проведення розслідувань

Energetic Bear

The Dukes
Cozy Bear/APT29

Sandworm
Telebots
/Voodoo Bear

Turla

InvisiMole

Sednit
Fancy Bear/APT28

Gamaredon

Buhtrap

Buhtrap

InvisiMole

Energetic Bear

Turla

Gamaredon

ФСБ

The Dukes

Cozy Bear/APT29

СЗР

Sandworm

Telebots
/Voodoo Bear

Sednit

Fancy
Bear/APT28

ГРУ

Джерела:

FBI

National Cyber Security Centre

Militaire Inlichtingen en Veiligheidsdienst

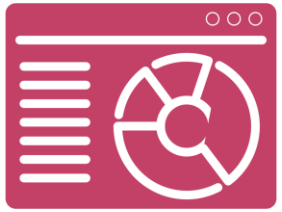
SECURITY SERVICE OF UKRAINE

Microsoft

МИ НАДАЄМО ДОПОМОГУ З РОЗСЛІДУВАННЯМ БУДЬ-ЯКИМ УКРАЇНСЬКИМ ОРГАНІЗАЦІЯМ У ВИПАДКАХ КІБЕРАТАК ТА ІНШОЇ АНОМАЛЬНОЇ АКТИВНОСТІ

ОДИН ІЗ НАЙЦІКАВІШИХ ІНЦИДЕНТІВ 2025 РОКУ

Зловмисники з рф отримують дані одного з адміністраторів компанії



Зловмисники використовують системи захисту та інші рішення для знищення інфраструктури

Активність продовжується впродовж всього розслідування, зловмисники маскуються під співробітників компанії

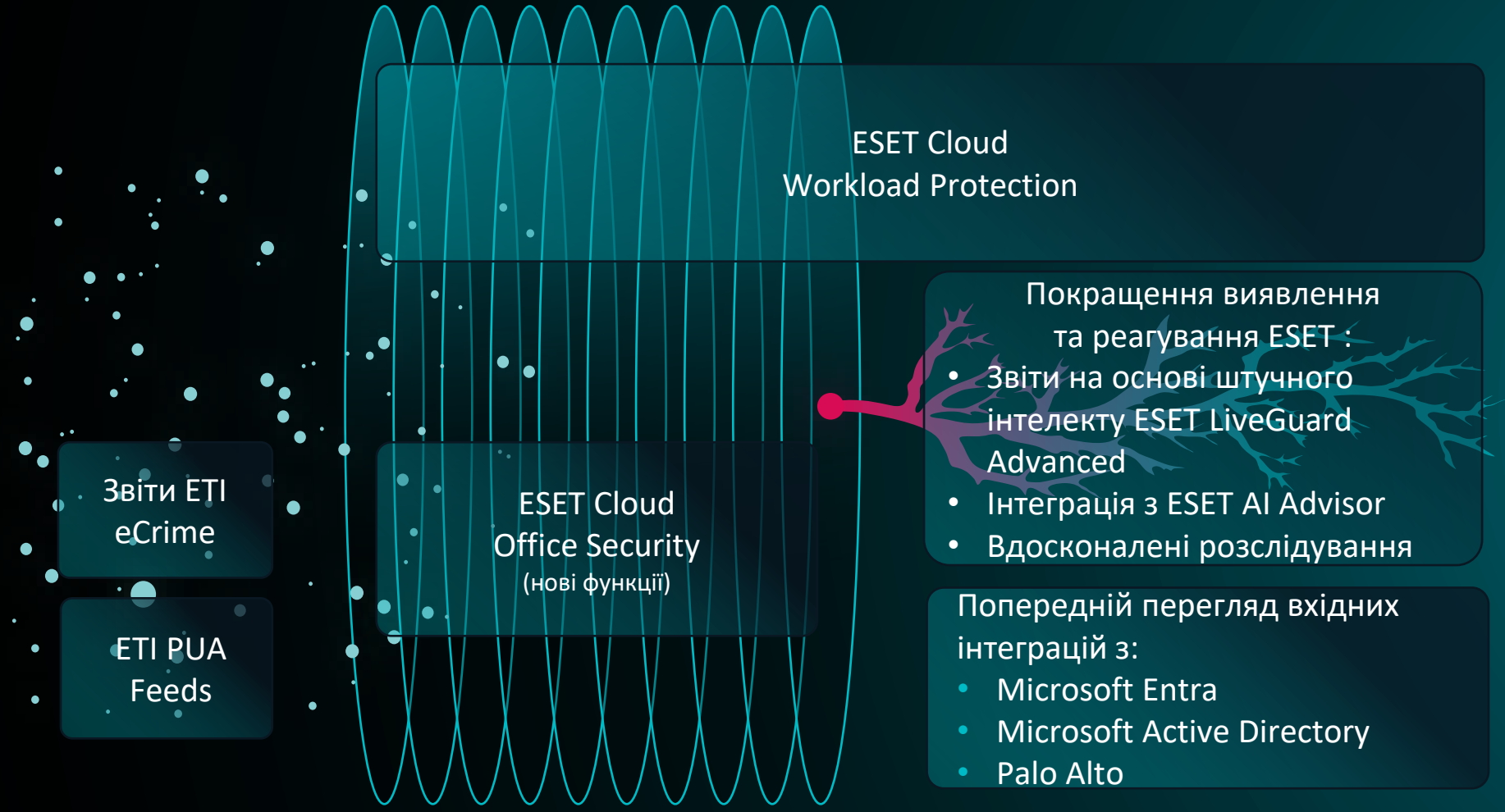
ВСЕБІЧНИЙ ПІДХІД ДО ЗАХИСТУ

- Консоль управління
- Захист робочих станцій
- Захист файлових серверів
- Розширений аналіз у хмарі (хмарна пісочниця)
- Повнодискове шифрування
- Виявлення та реагування (XDR)
- Захист хмарних додатків
- Захист поштових серверів
- Управління уразливостями та виправленнями
- Багатофакторна автентифікація

ПРОГНОЗУВАННЯ

ЗАПОБІГАННЯ ТА ЗАХИСТ

ВИЯВЛЕННЯ ТА РЕАГУВАННЯ



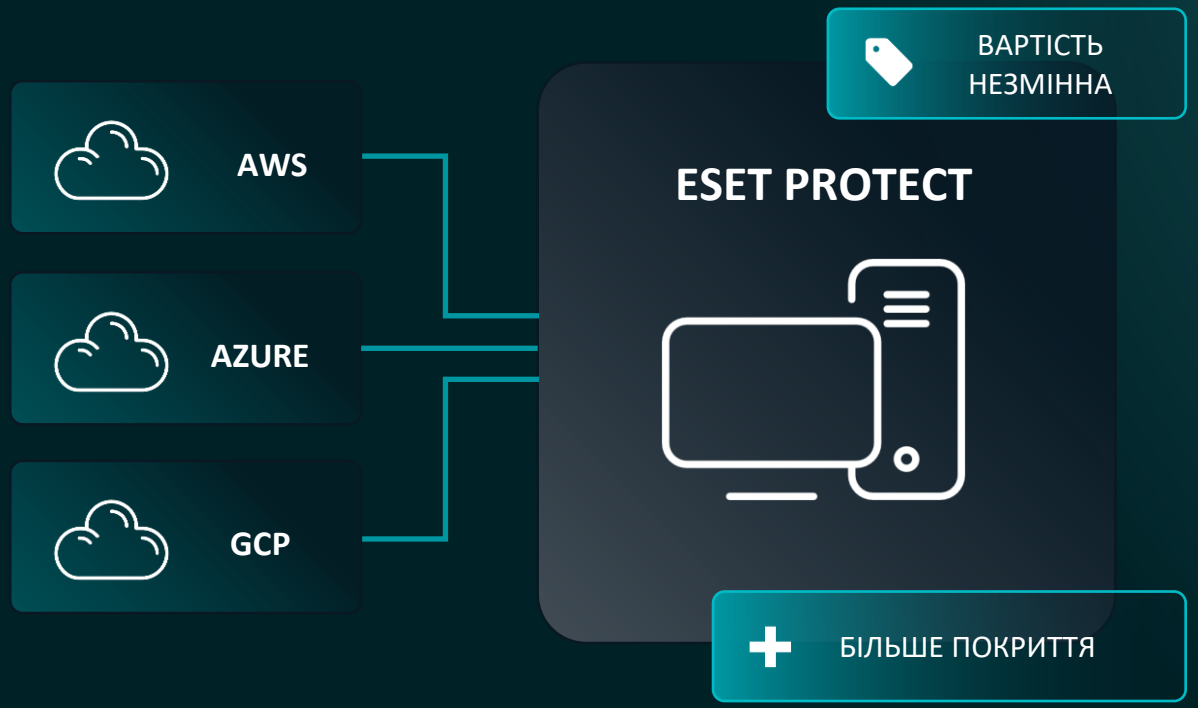
Захист робочих навантажень у хмарі

- Легкий агентний захист для хмарних віртуальних машин
- Виявлення та запобігання загрозам у режимі реального часу
- Централізоване управління через платформу ESET PROTECT
- Проста інтеграція з постачальниками публічних хмарних послуг (AWS, Azure, GCP)

На відміну від інших конкурентів, ESET **пропонує:**

- Функціонал на рівні ядра ESET Endpoint Protection.
- Захист віртуальних машин у рамках комплексних рішень, починаючи з ESET PROTECT Advanced.

Ключові моменти

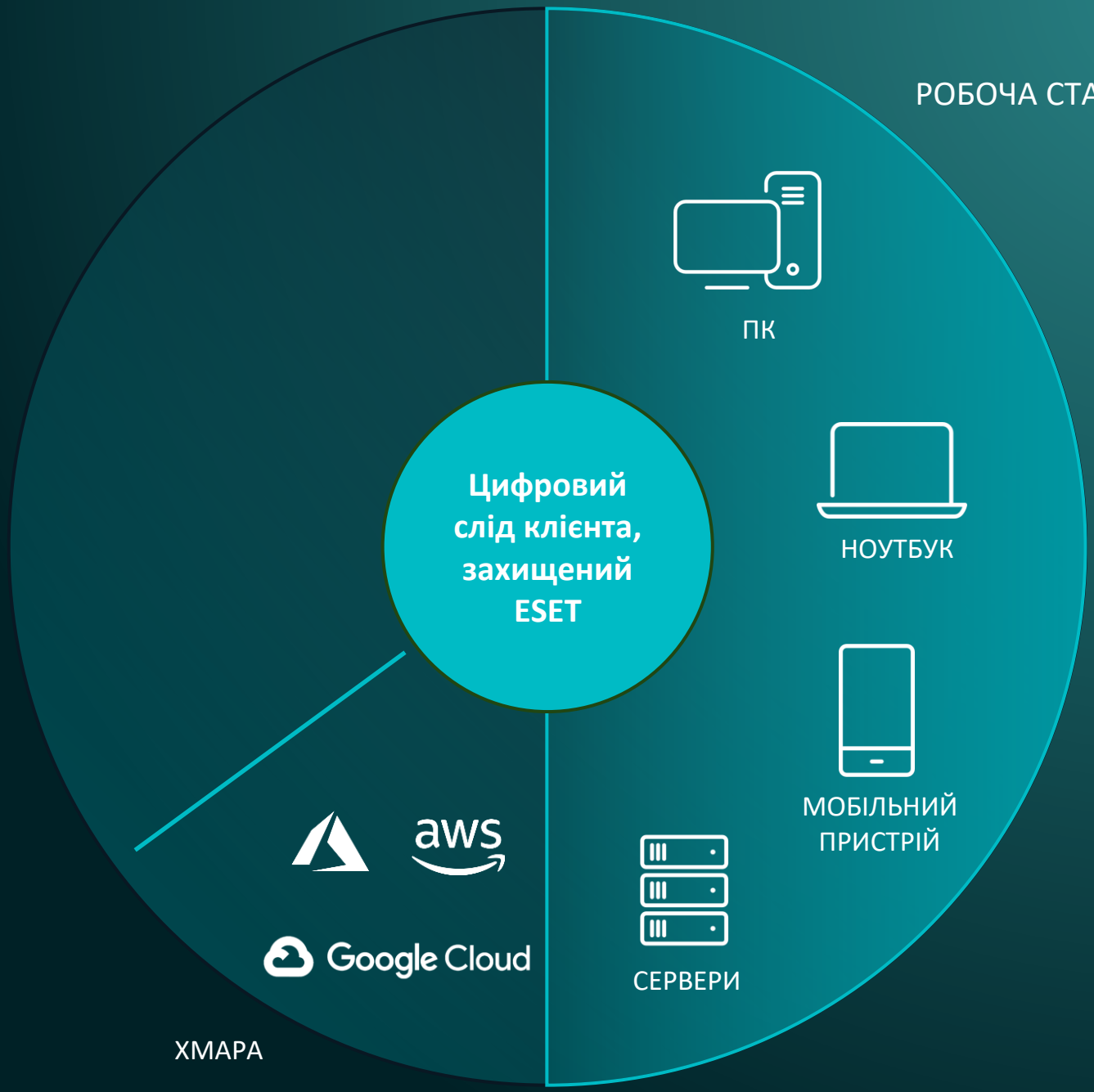


- Легкий агентний захист для хмарних віртуальних машин
- Інтегрується з AWS, Azure, GCP
- Виявлення та запобігання загрозам у режимі реального часу
- Централізоване управління в ESET PROTECT
- Ціна комплексного рішення, до якого входить захист, не змінюється

Зміна фокусу з поточної робочої станції

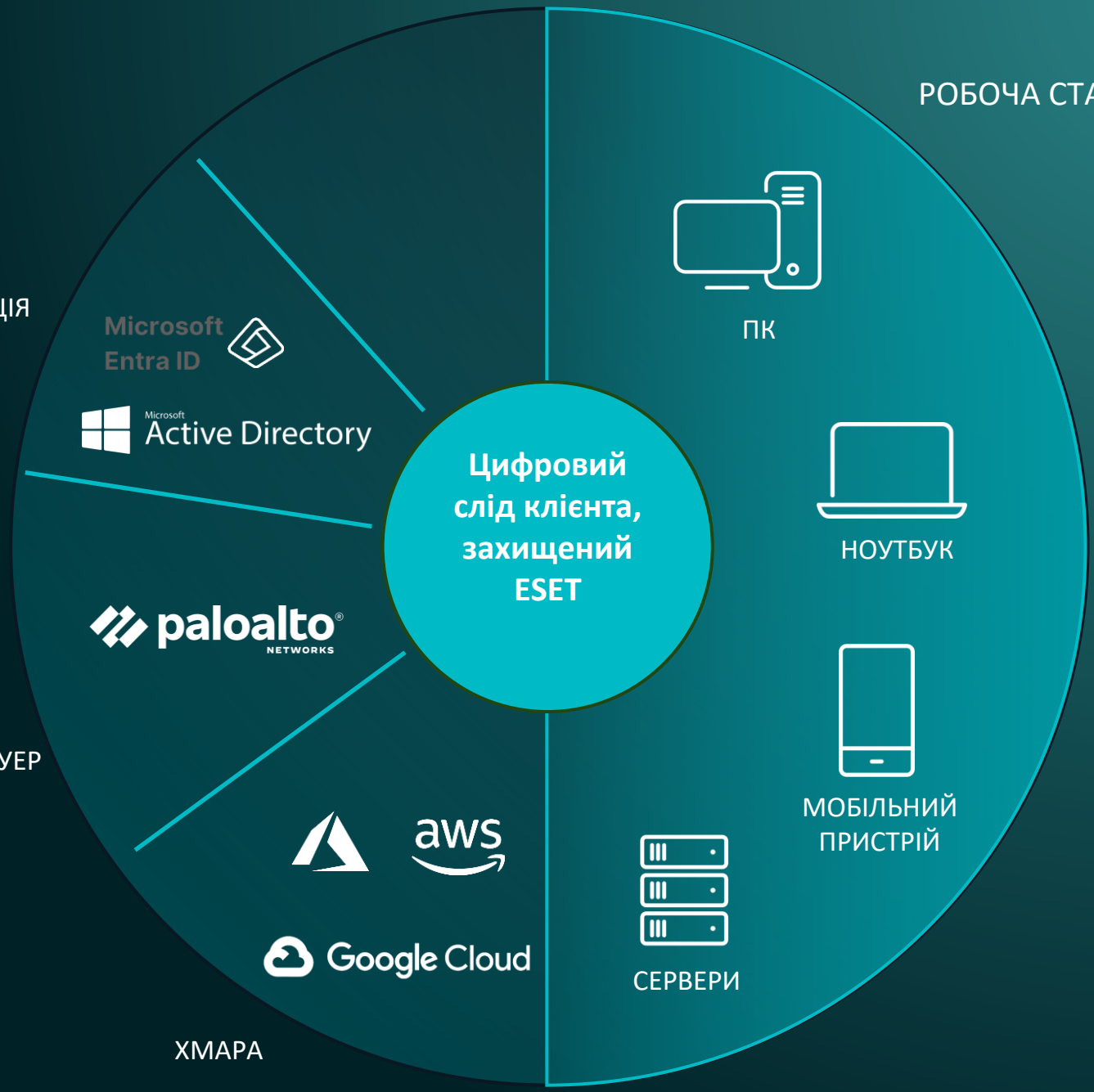
Починаючи з 2026 року

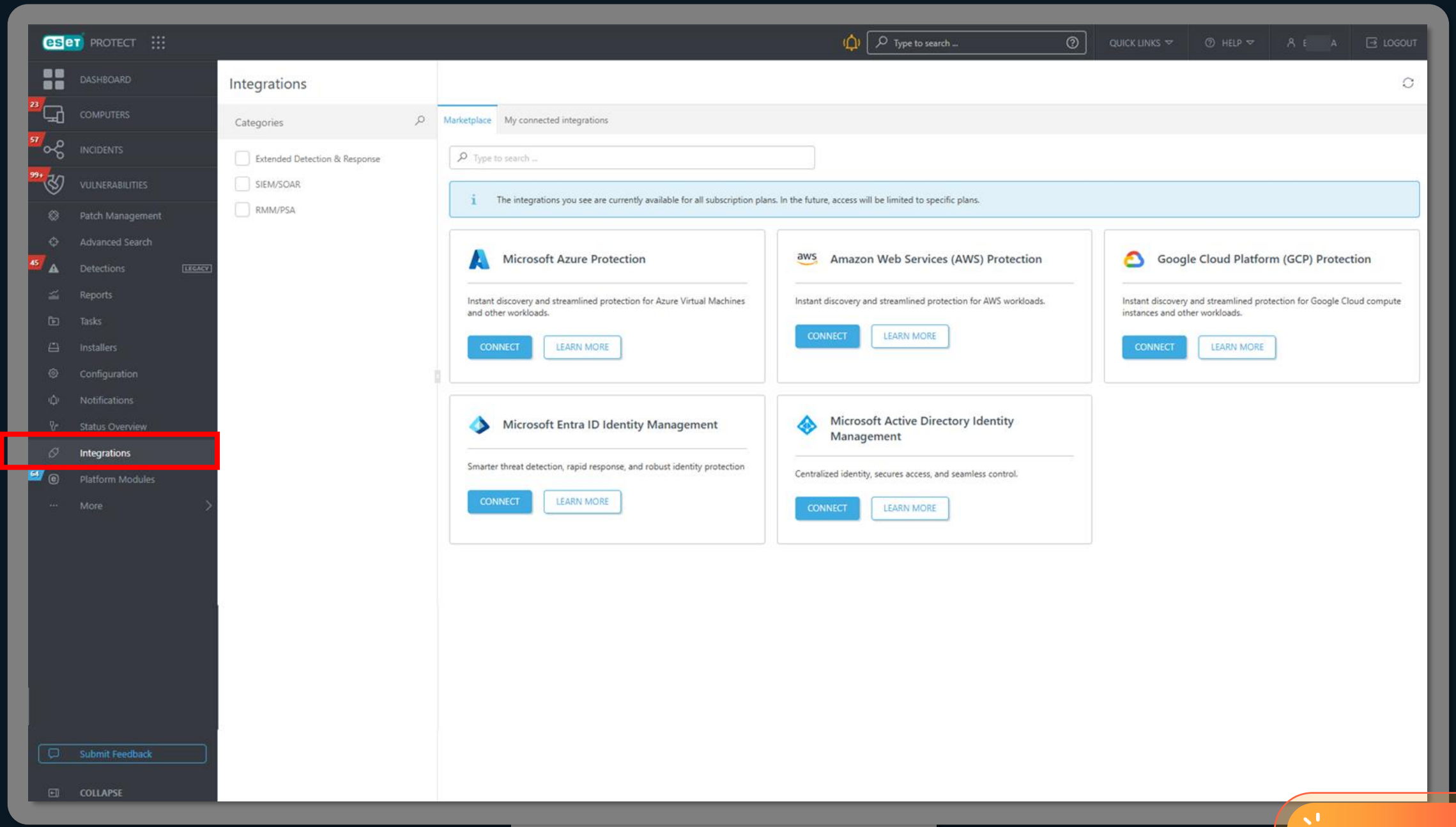
Розширена безпека із захистом хмарних робочих сервісів



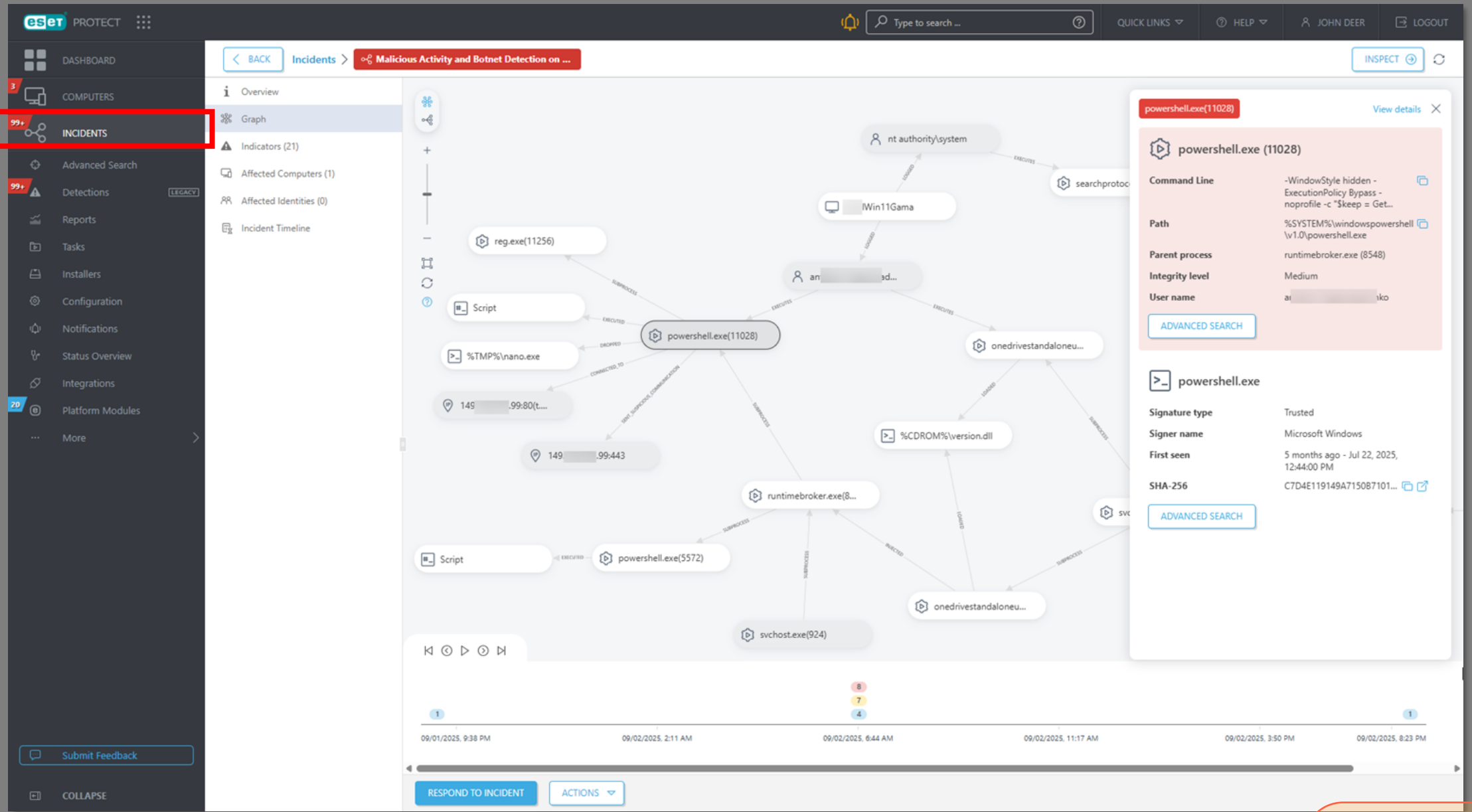
Починаючи з 2026 року

Багаторівнева безпека із захистом хмарних сервісів та з розширенням інтеграцій ESET PROTECT

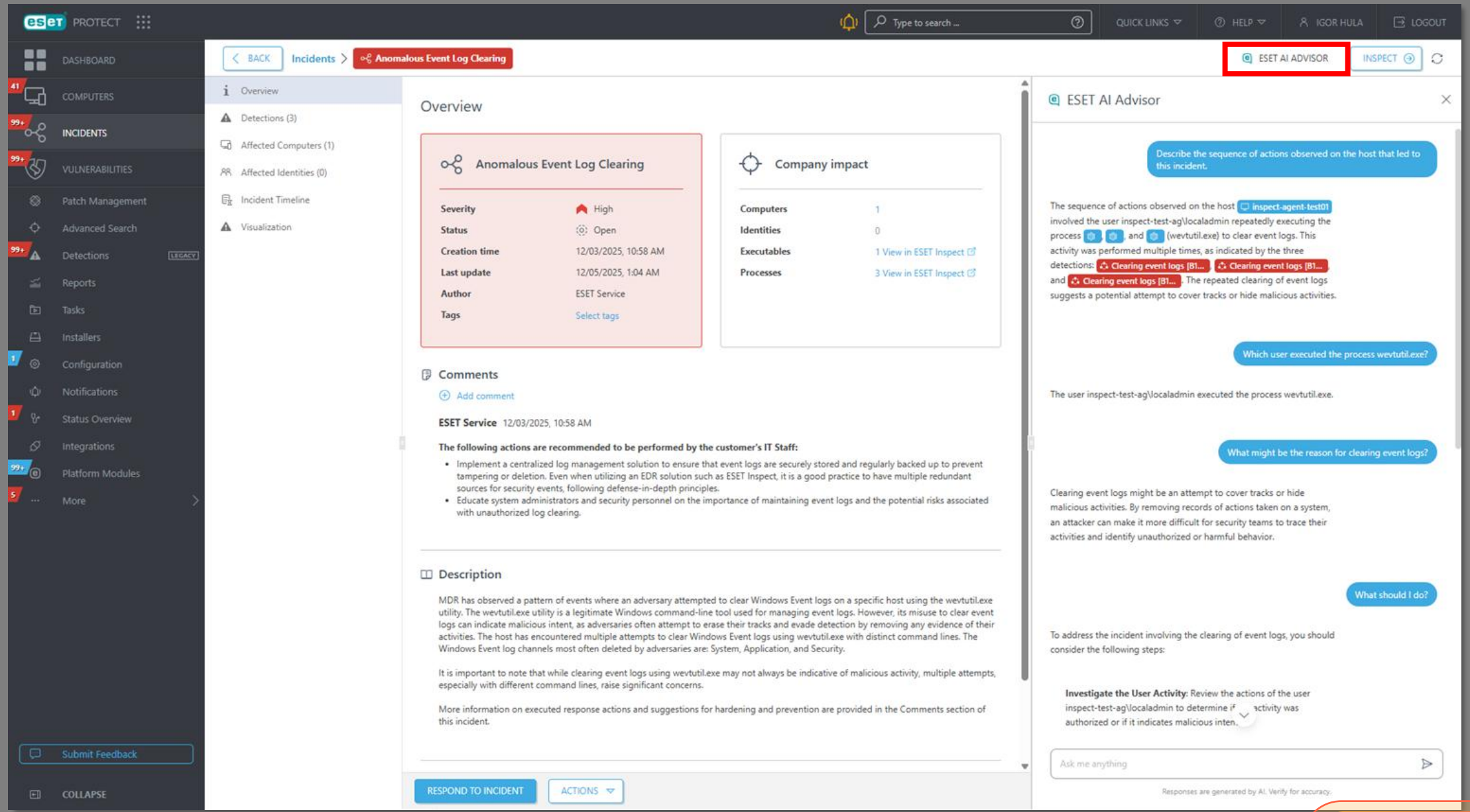



PROTECT
Type to search ...
QUICK LINKS
HELP
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Integrations
Categories
Extended Detection & Response
SIEM/SOAR
RMM/PSA
Marketplace
My connected integrations
Type to search ...
The integrations you see are currently available for all subscription plans. In the future, access will be limited to specific plans.
Microsoft Azure Protection
Instant discovery and streamlined protection for Azure Virtual Machines and other workloads.
CONNECT
LEARN MORE
Amazon Web Services (AWS) Protection
Instant discovery and streamlined protection for AWS workloads.
CONNECT
LEARN MORE
Google Cloud Platform (GCP) Protection
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
Microsoft Active Directory Identity Management
Centralized identity, secures access, and seamless control.
CONNECT
LEARN MORE

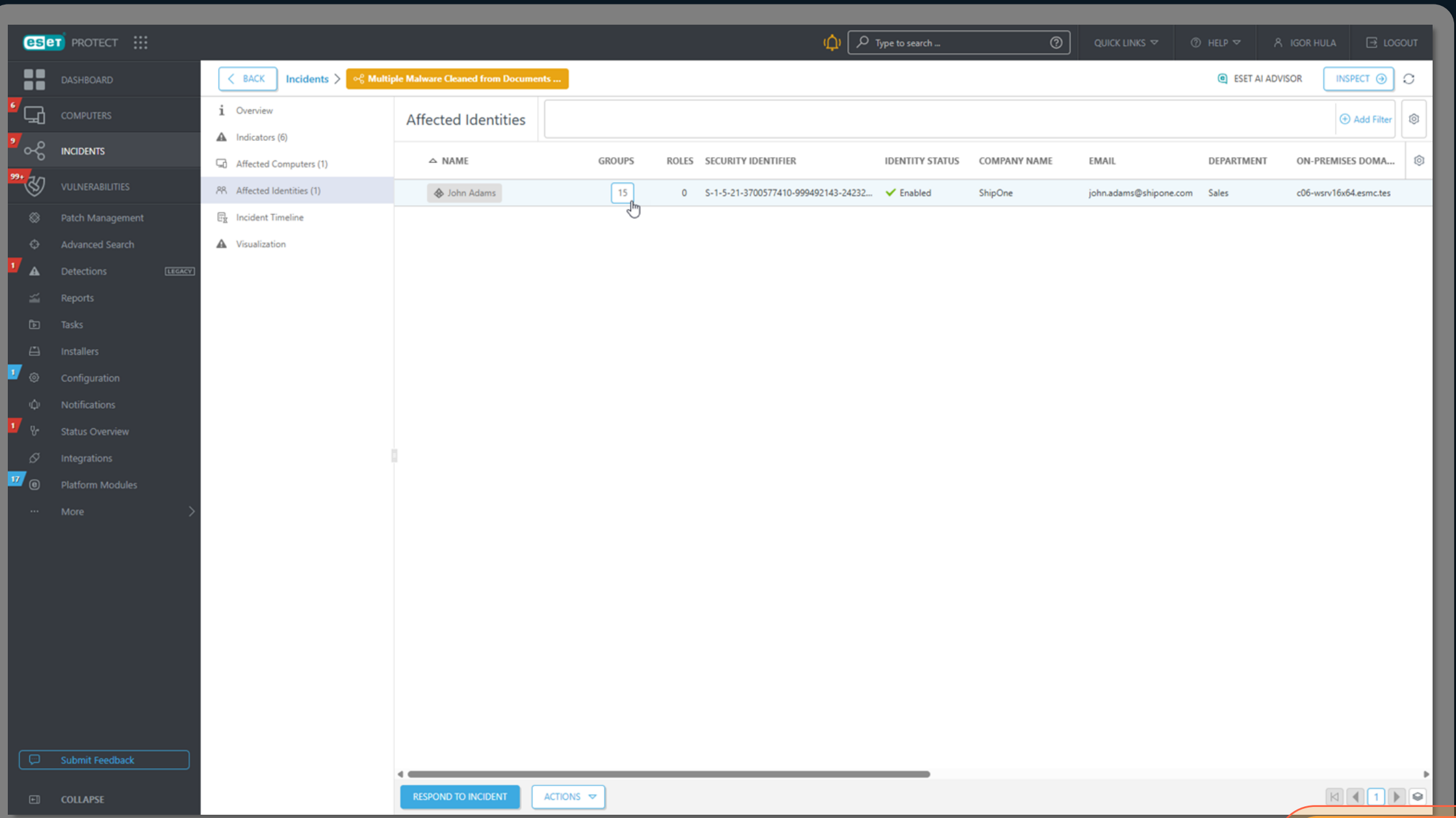
В ПРОЦЕСІ


PROTECT
Type to search ...
QUICK LINKS
HELP
JOHN DEER
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
Advanced Search
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
BACK
Incidents
Malicious Activity and Botnet Detection on ...
INSPECT
Overview
Graph
Indicators (21)
Affected Computers (1)
Affected Identities (0)
Incident Timeline
nt authority\system
searchprotoc
lWin11Gama
reg.exe(11256)
Script
powershell.exe(11028)
%TMP%\nano.exe
onedrivestandaloneu...
%CDROM%\version.dll
runtimebroker.exe(8...
powershell.exe(5572)
svchost.exe(924)
powershell.exe(11028)
View details
powershell.exe (11028)
Command Line
-WindowStyle hidden -ExecutionPolicy Bypass -noprofile -c "$keep = Get...
Path
%SYSTEM%\windowspowershell\v1.0\powershell.exe
Parent process
runtimebroker.exe (8548)
Integrity level
Medium
User name
ADVANCED SEARCH
powershell.exe
Signature type
Trusted
Signer name
Microsoft Windows
First seen
5 months ago - Jul 22, 2025, 12:44:00 PM
SHA-256
C7D4E119149A7150871010...
ADVANCED SEARCH
09/01/2025, 9:38 PM
09/02/2025, 2:11 AM
09/02/2025, 6:44 AM
09/02/2025, 11:17 AM
09/02/2025, 3:50 PM
09/02/2025, 8:23 PM
RESPOND TO INCIDENT
ACTIONS

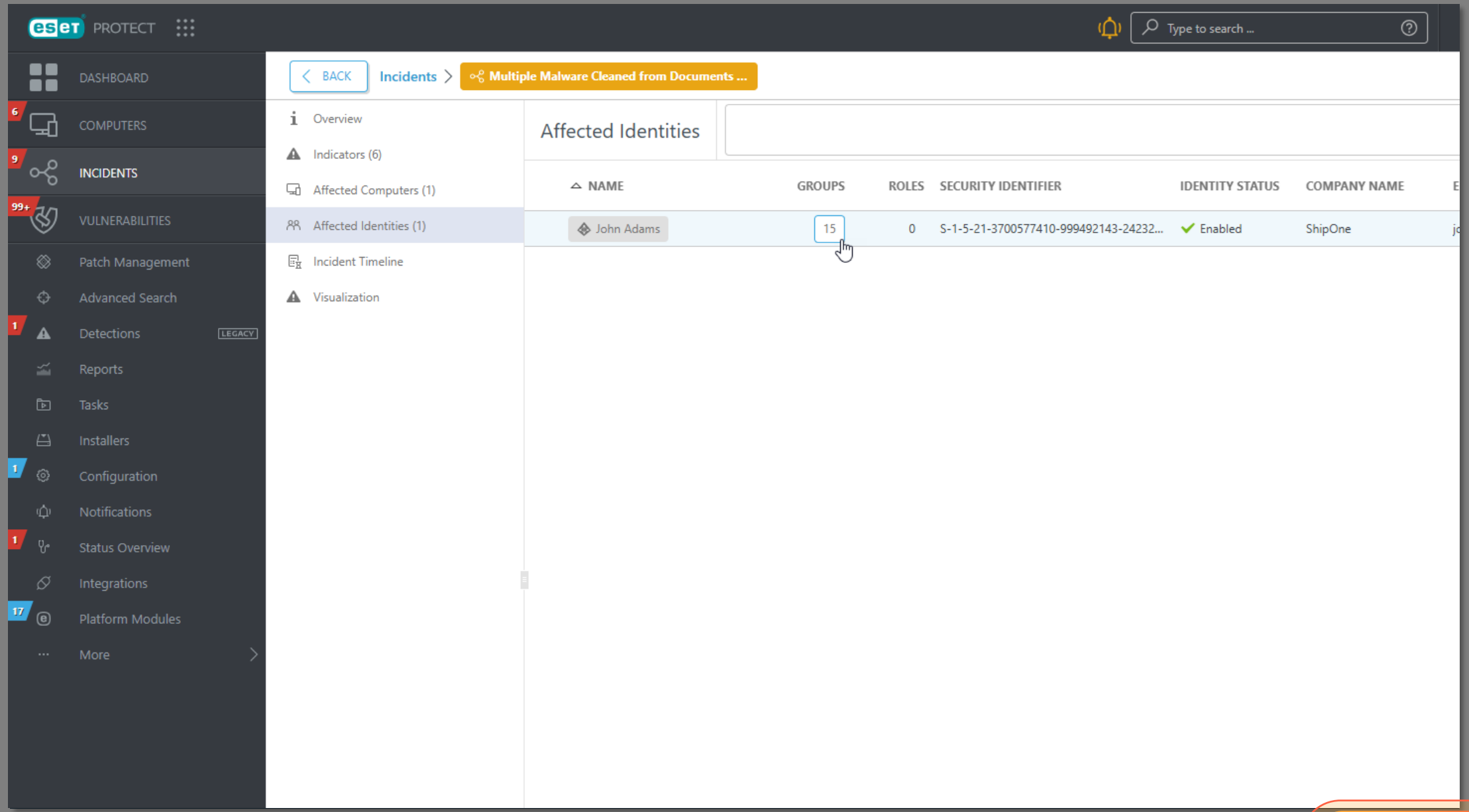
В ПРОЦЕСІ


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
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.

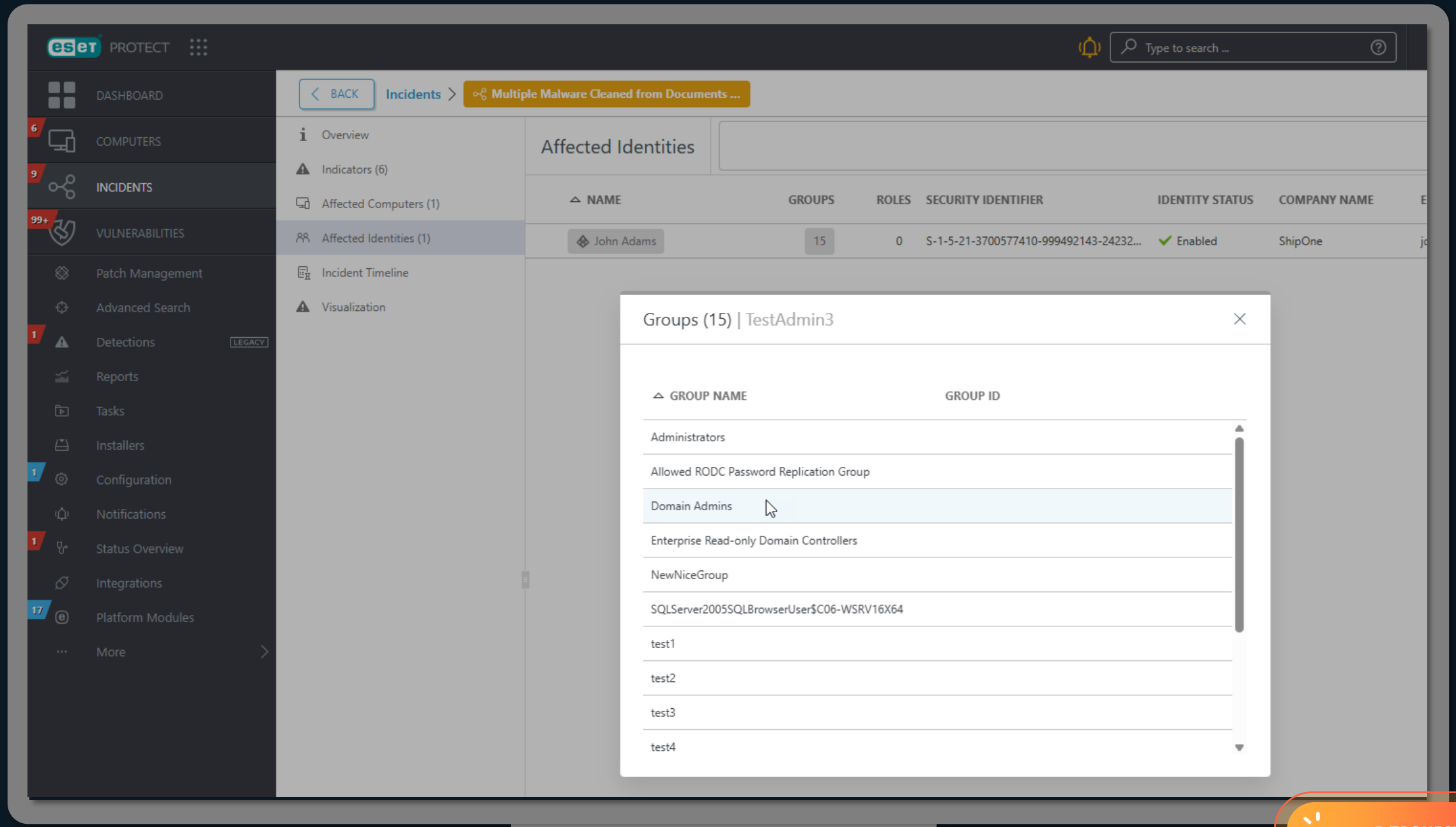
В ПРОЦЕСІ


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
Multiple Malware Cleaned from Documents ...
ESET AI ADVISOR
INSPECT
Overview
Indicators (6)
Affected Computers (1)
Affected Identities (1)
Incident Timeline
Visualization
Affected Identities
Add Filter
NAME
GROUPS
ROLES
SECURITY IDENTIFIER
IDENTITY STATUS
COMPANY NAME
EMAIL
DEPARTMENT
ON-PREMISES DOMA...
John Adams
15
0
S-1-5-21-3700577410-999492143-24232...
Enabled
ShipOne
john.adams@shipone.com
Sales
c06-wsrv16x64.esmc.tes
RESPOND TO INCIDENT
ACTIONS
1

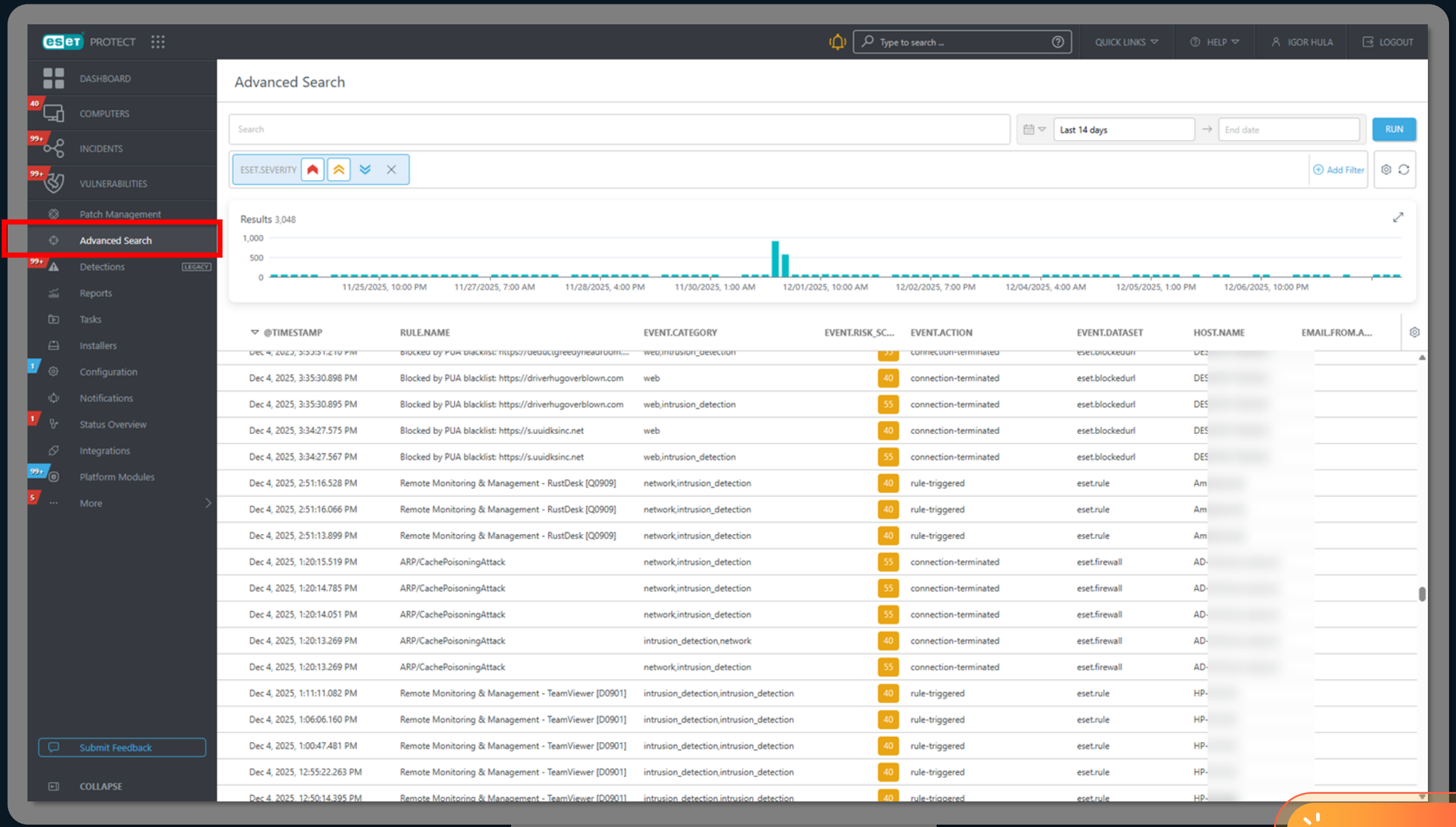
В ПРОЦЕСІ


ESET PROTECT
Type to search ...
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
BACK
Incidents
Multiple Malware Cleaned from Documents ...
Overview
Indicators (6)
Affected Computers (1)
Affected Identities (1)
Incident Timeline
Visualization
Affected Identities
NAME
GROUPS
ROLES
SECURITY IDENTIFIER
IDENTITY STATUS
COMPANY NAME
John Adams
15
0
S-1-5-21-3700577410-999492143-24232...
Enabled
ShipOne

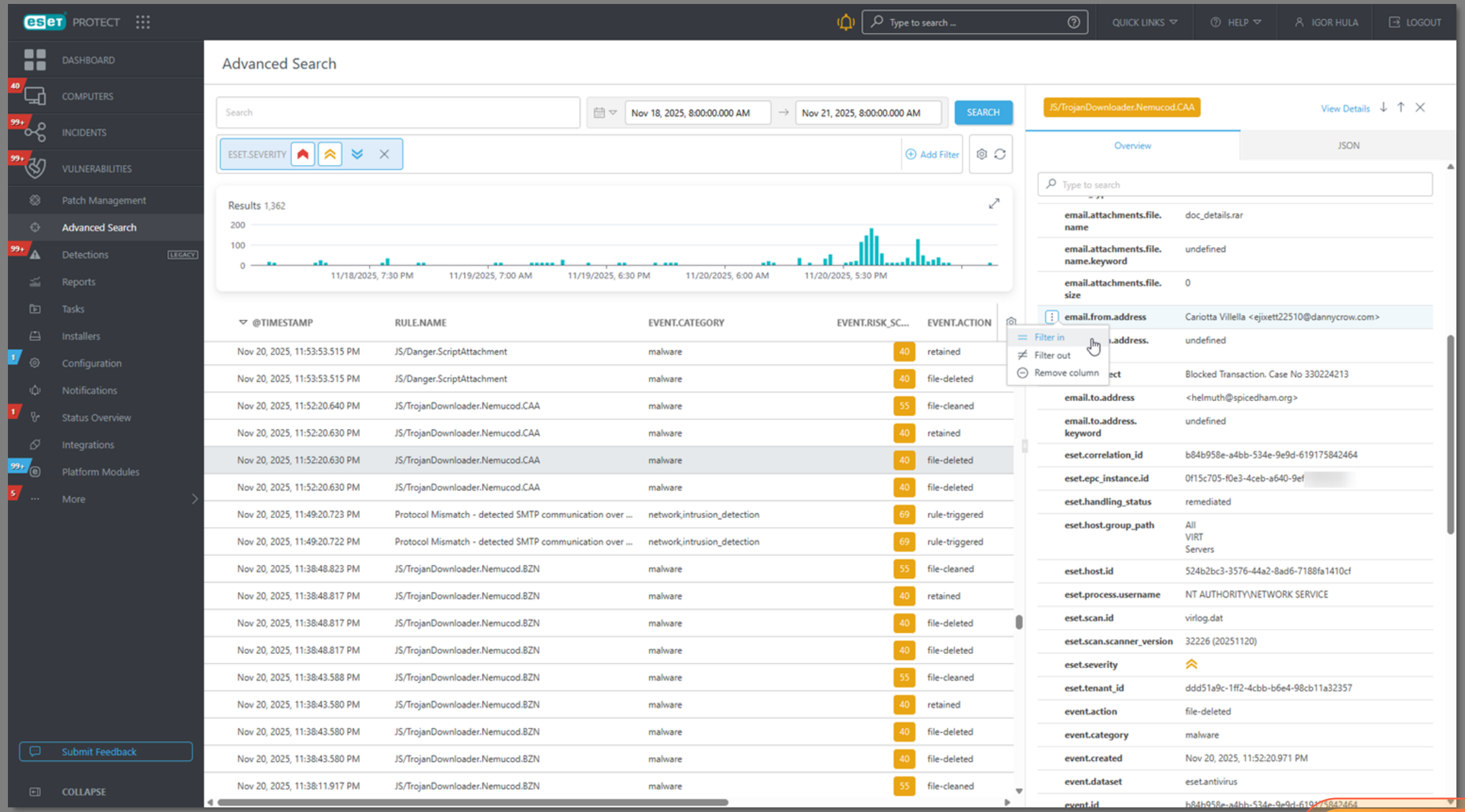
В ПРОЦЕСІ


ESET PROTECT
Type to search ...
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
LEGACY
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
BACK
Incidents
Multiple Malware Cleaned from Documents ...
Overview
Indicators (6)
Affected Computers (1)
Affected Identities (1)
Incident Timeline
Visualization
Affected Identities
NAME
GROUPS
ROLES
SECURITY IDENTIFIER
IDENTITY STATUS
COMPANY NAME
John Adams
15
0
S-1-5-21-3700577410-999492143-24232...
Enabled
ShipOne
Groups (15) | TestAdmin3
GROUP NAME
GROUP ID
Administrators
Allowed RODC Password Replication Group
Domain Admins
Enterprise Read-only Domain Controllers
NewNiceGroup
SQLServer2005SQLBrowserUser$C06-WSRV16X64
test1
test2
test3
test4

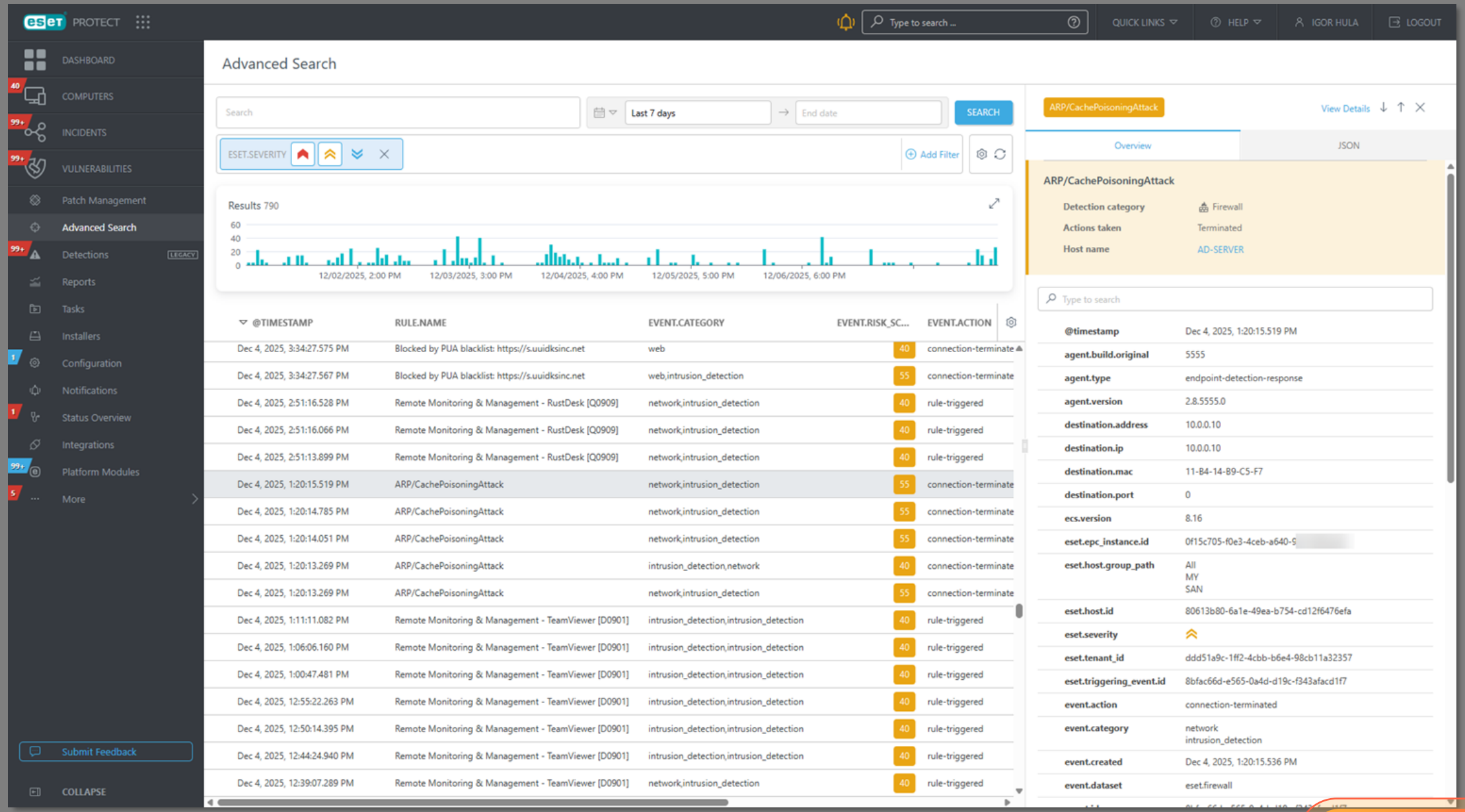
В ПРОЦЕСІ


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
Advanced Search
Search
Last 14 days
End date
RUN
ESET.SEVERITY
Add Filter
Results 3,048
1,000
500
0
11/25/2025, 10:00 PM
11/27/2025, 7:00 AM
11/28/2025, 4:00 PM
11/30/2025, 1:00 AM
12/01/2025, 10:00 AM
12/02/2025, 7:00 PM
12/04/2025, 4:00 AM
12/05/2025, 1:00 PM
12/06/2025, 10:00 PM
@TIMESTAMP
RULE.NAME
EVENT.CATEGORY
EVENT.RISK_SC...
EVENT.ACTION
EVENT.DATASET
HOST.NAME
EMAIL.FROM.A...
Dec 4, 2025, 3:35:30.898 PM
Blocked by PUA blacklist: https://driverhugoverblown.com
web
40
connection-terminated
eset.blockedurl
Dec 4, 2025, 3:35:30.895 PM
Blocked by PUA blacklist: https://driverhugoverblown.com
web,intrusion_detection
55
connection-terminated
eset.blockedurl
Dec 4, 2025, 3:34:27.575 PM
Blocked by PUA blacklist: https://s.uuidksinc.net
web
40
connection-terminated
eset.blockedurl
Dec 4, 2025, 3:34:27.567 PM
Blocked by PUA blacklist: https://s.uuidksinc.net
web,intrusion_detection
55
connection-terminated
eset.blockedurl
Dec 4, 2025, 2:51:16.528 PM
Remote Monitoring & Management - RustDesk [Q0909]
network,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 2:51:16.066 PM
Remote Monitoring & Management - RustDesk [Q0909]
network,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 2:51:13.899 PM
Remote Monitoring & Management - RustDesk [Q0909]
network,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 1:20:15.519 PM
ARP/CachePoisoningAttack
network,intrusion_detection
55
connection-terminated
eset.firewall
Dec 4, 2025, 1:20:14.785 PM
ARP/CachePoisoningAttack
network,intrusion_detection
55
connection-terminated
eset.firewall
Dec 4, 2025, 1:20:14.051 PM
ARP/CachePoisoningAttack
network,intrusion_detection
55
connection-terminated
eset.firewall
Dec 4, 2025, 1:20:13.269 PM
ARP/CachePoisoningAttack
intrusion_detection,network
40
connection-terminated
eset.firewall
Dec 4, 2025, 1:20:13.269 PM
ARP/CachePoisoningAttack
network,intrusion_detection
55
connection-terminated
eset.firewall
Dec 4, 2025, 1:11:11.082 PM
Remote Monitoring & Management - TeamViewer [D0901]
intrusion_detection,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 1:06:06.160 PM
Remote Monitoring & Management - TeamViewer [D0901]
intrusion_detection,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 1:00:47.481 PM
Remote Monitoring & Management - TeamViewer [D0901]
intrusion_detection,intrusion_detection
40
rule-triggered
eset.rule
Dec 4, 2025, 12:55:22.263 PM
Remote Monitoring & Management - TeamViewer [D0901]
intrusion_detection,intrusion_detection
40
rule-triggered
eset.rule

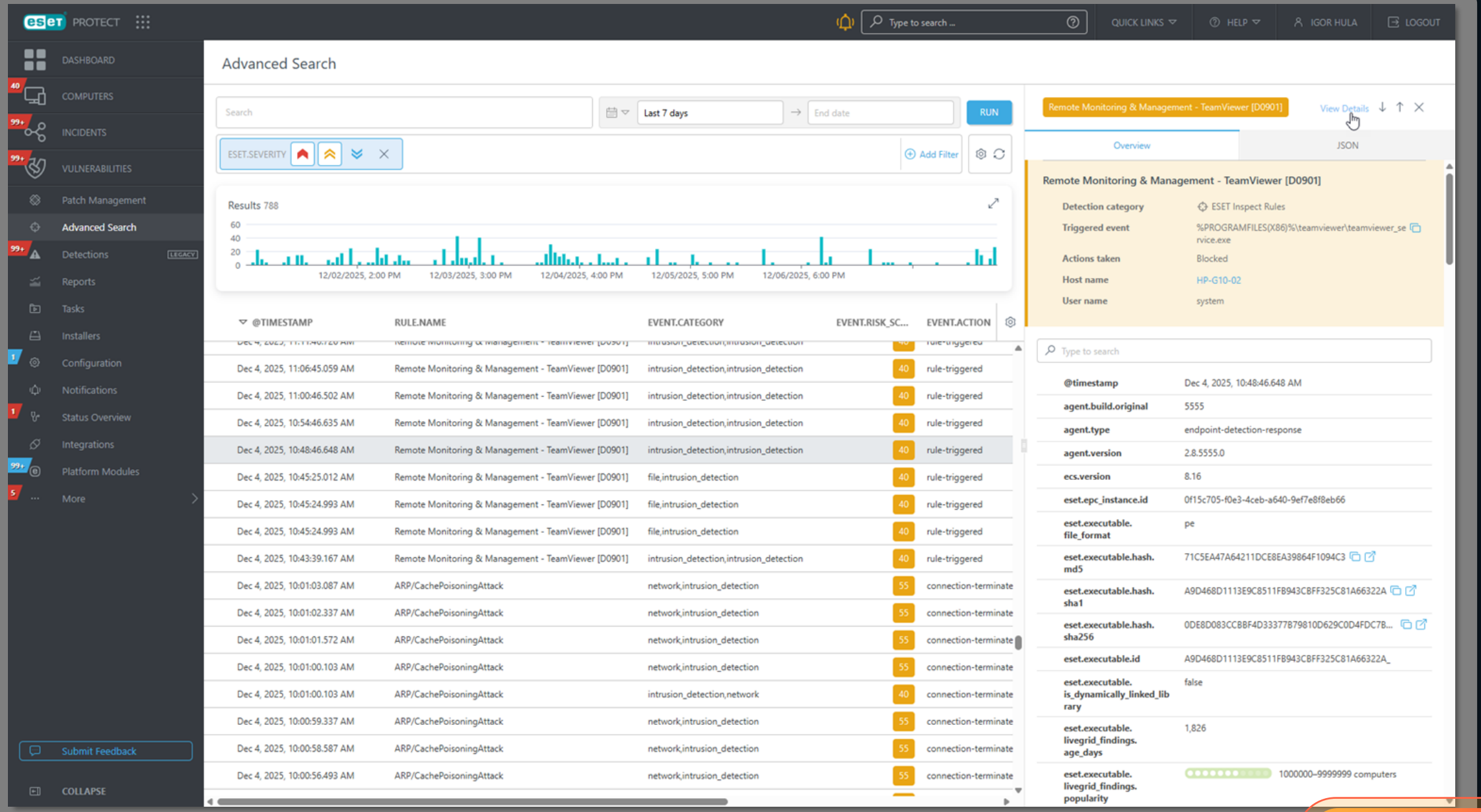
В ПРОЦЕСІ


PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Advanced Search
Search
Nov 18, 2025, 8:00:00.000 AM
Nov 21, 2025, 8:00:00.000 AM
SEARCH
ESET.SEVERITY
Add Filter
Results 1,362
200
100
0
11/18/2025, 7:30 PM
11/19/2025, 7:00 AM
11/19/2025, 6:30 PM
11/20/2025, 6:00 AM
11/20/2025, 5:30 PM
@TIMESTAMP
RULE.NAME
EVENT.CATEGORY
EVENT.RISK_SC...
EVENT.ACTION
Nov 20, 2025, 11:53:53.515 PM JS/Danger.ScriptAttachment malware 40 retained
Nov 20, 2025, 11:53:53.515 PM JS/Danger.ScriptAttachment malware 40 file-deleted
Nov 20, 2025, 11:52:20.640 PM JS/TrojanDownloader.Nemucod.CAA malware 55 file-cleaned
Nov 20, 2025, 11:52:20.630 PM JS/TrojanDownloader.Nemucod.CAA malware 40 retained
Nov 20, 2025, 11:52:20.630 PM JS/TrojanDownloader.Nemucod.CAA malware 40 file-deleted
Nov 20, 2025, 11:52:20.630 PM JS/TrojanDownloader.Nemucod.CAA malware 40 file-deleted
Nov 20, 2025, 11:49:20.723 PM Protocol Mismatch - detected SMTP communication over ... network,intrusion_detection 69 rule-triggered
Nov 20, 2025, 11:49:20.722 PM Protocol Mismatch - detected SMTP communication over ... network,intrusion_detection 69 rule-triggered
Nov 20, 2025, 11:38:48.823 PM JS/TrojanDownloader.Nemucod.BZN malware 55 file-cleaned
Nov 20, 2025, 11:38:48.817 PM JS/TrojanDownloader.Nemucod.BZN malware 40 retained
Nov 20, 2025, 11:38:48.817 PM JS/TrojanDownloader.Nemucod.BZN malware 40 file-deleted
Nov 20, 2025, 11:38:48.817 PM JS/TrojanDownloader.Nemucod.BZN malware 40 file-deleted
Nov 20, 2025, 11:38:43.588 PM JS/TrojanDownloader.Nemucod.BZN malware 55 file-cleaned
Nov 20, 2025, 11:38:43.580 PM JS/TrojanDownloader.Nemucod.BZN malware 40 retained
Nov 20, 2025, 11:38:43.580 PM JS/TrojanDownloader.Nemucod.BZN malware 40 file-deleted
Nov 20, 2025, 11:38:43.580 PM JS/TrojanDownloader.Nemucod.BZN malware 40 file-deleted
Nov 20, 2025, 11:38:11.917 PM JS/TrojanDownloader.Nemucod.BZN malware 55 file-cleaned
Filter in
Filter out
Remove column
JS/TrojanDownloader.Nemucod.CAA
View Details
Overview
JSON
Type to search
email.attachments.file.name doc_details.rar
email.attachments.file.name.keyword undefined
email.attachments.file.size 0
email.from.address Cariotta Villella <ejixett22510@dannycrow.com>
email.to.address undefined
Blocked Transaction. Case No 330224213
email.to.address <helmuth@spicedham.org>
email.to.address.keyword undefined
eset.correlation_id b84b958e-a4bb-534e-9e9d-619175842464
eset.epc_instance.id 0f15c705-f0e3-4ceb-a640-9ef
eset.handling_status remediated
eset.host.group_path All VIRT Servers
eset.host.id 524b2bc3-3576-44a2-8ad6-7188fa1410cf
eset.process.username NT AUTHORITY\NETWORK SERVICE
eset.scan.id virlog.dat
eset.scan.scanner_version 32226 (20251120)
eset.severity
eset.tenant_id ddd51a9c-1ff2-4cbb-b6e4-98cb11a32357
event.action file-deleted
event.category malware
event.created Nov 20, 2025, 11:52:20.971 PM
event.dataset eset.antivirus

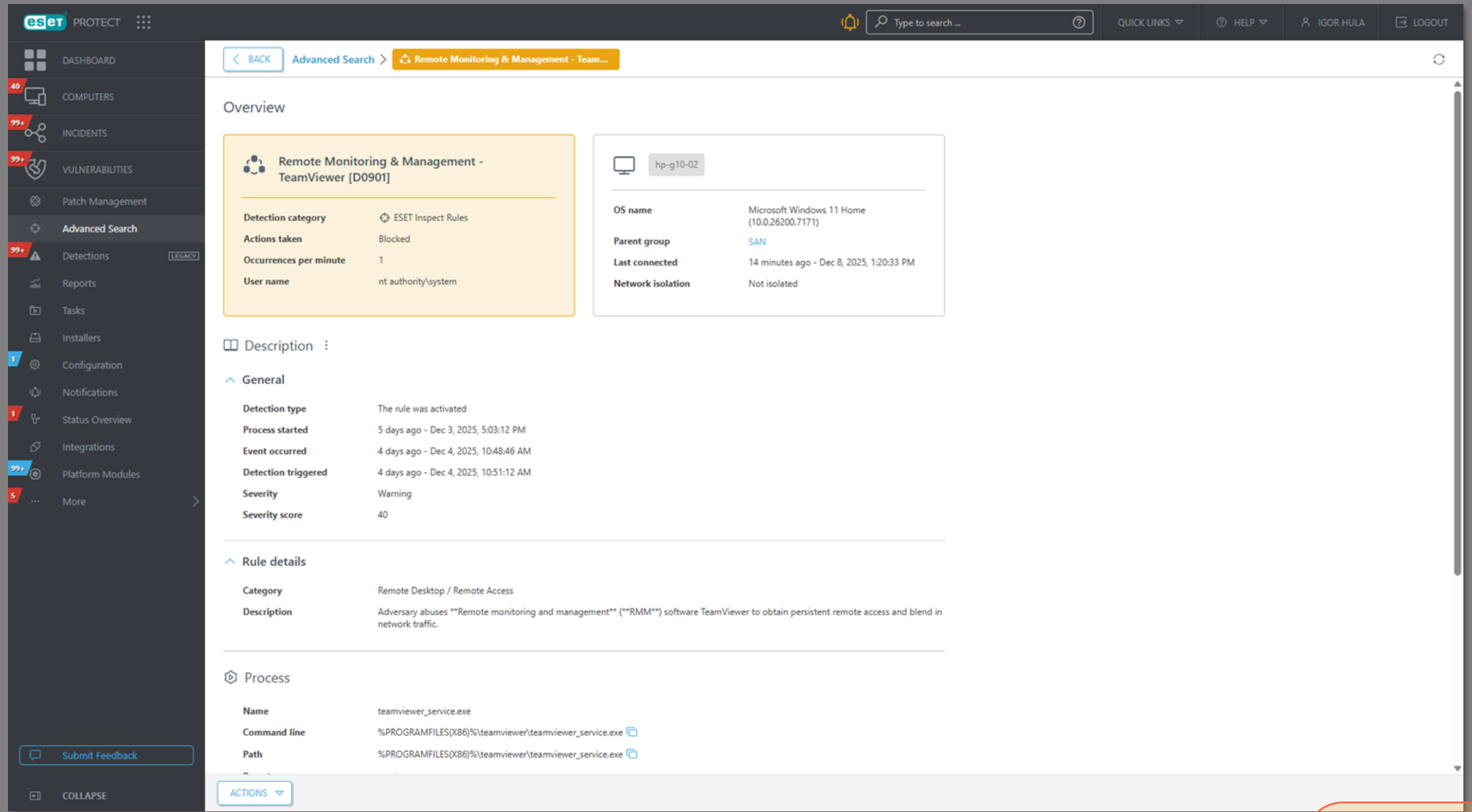
В ПРОЦЕСІ


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Advanced Search
Search
Last 7 days
End date
SEARCH
ESET.SEVERITY
Add Filter
Results 790
60
40
20
0
12/02/2025, 2:00 PM
12/03/2025, 3:00 PM
12/04/2025, 4:00 PM
12/05/2025, 5:00 PM
12/06/2025, 6:00 PM
@TIMESTAMP
RULE.NAME
EVENT.CATEGORY
EVENT.RISK_SC...
EVENT.ACTION
Dec 4, 2025, 3:34:27.575 PM Blocked by PUA blacklist: https://s.uuidksinc.net web 40 connection-terminate
Dec 4, 2025, 3:34:27.567 PM Blocked by PUA blacklist: https://s.uuidksinc.net web,intrusion_detection 55 connection-terminate
Dec 4, 2025, 2:51:16.528 PM Remote Monitoring & Management - RustDesk [Q0909] network,intrusion_detection 40 rule-triggered
Dec 4, 2025, 2:51:16.066 PM Remote Monitoring & Management - RustDesk [Q0909] network,intrusion_detection 40 rule-triggered
Dec 4, 2025, 2:51:13.899 PM Remote Monitoring & Management - RustDesk [Q0909] network,intrusion_detection 40 rule-triggered
Dec 4, 2025, 1:20:15.519 PM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 1:20:14.785 PM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 1:20:14.051 PM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 1:20:13.269 PM ARP/CachePoisoningAttack intrusion_detection,network 40 connection-terminate
Dec 4, 2025, 1:20:13.269 PM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 1:11:11.082 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 1:06:06.160 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 1:00:47.481 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 12:55:22.263 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 12:50:14.395 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 12:44:24.940 PM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 12:39:07.289 PM Remote Monitoring & Management - TeamViewer [D0901] network,intrusion_detection 40 rule-triggered
ARP/CachePoisoningAttack
View Details
Overview
JSON
ARP/CachePoisoningAttack
Detection category Firewall
Actions taken Terminated
Host name AD-SERVER
Type to search
@timestamp Dec 4, 2025, 1:20:15.519 PM
agent.build.original 5555
agent.type endpoint-detection-response
agent.version 2.8.5555.0
destination.address 10.0.0.10
destination.ip 10.0.0.10
destination.mac 11-B4-14-B9-C5-F7
destination.port 0
ecs.version 8.16
eset.epc_instance.id 0f15c705-f0e3-4ceb-a640-9
eset.host.group_path All MY SAN
eset.host.id 80613b80-6a1e-49ea-b754-cd12f6476efa
eset.severity
eset.tenant_id ddd51a9c-1ff2-4cbb-b6e4-98cb11a32357
eset.triggering_event.id 8bfac66d-e565-0a4d-d19c-f343afacd1f7
event.action connection-terminated
event.category network intrusion_detection
event.created Dec 4, 2025, 1:20:15.536 PM
event.dataset eset.firewall

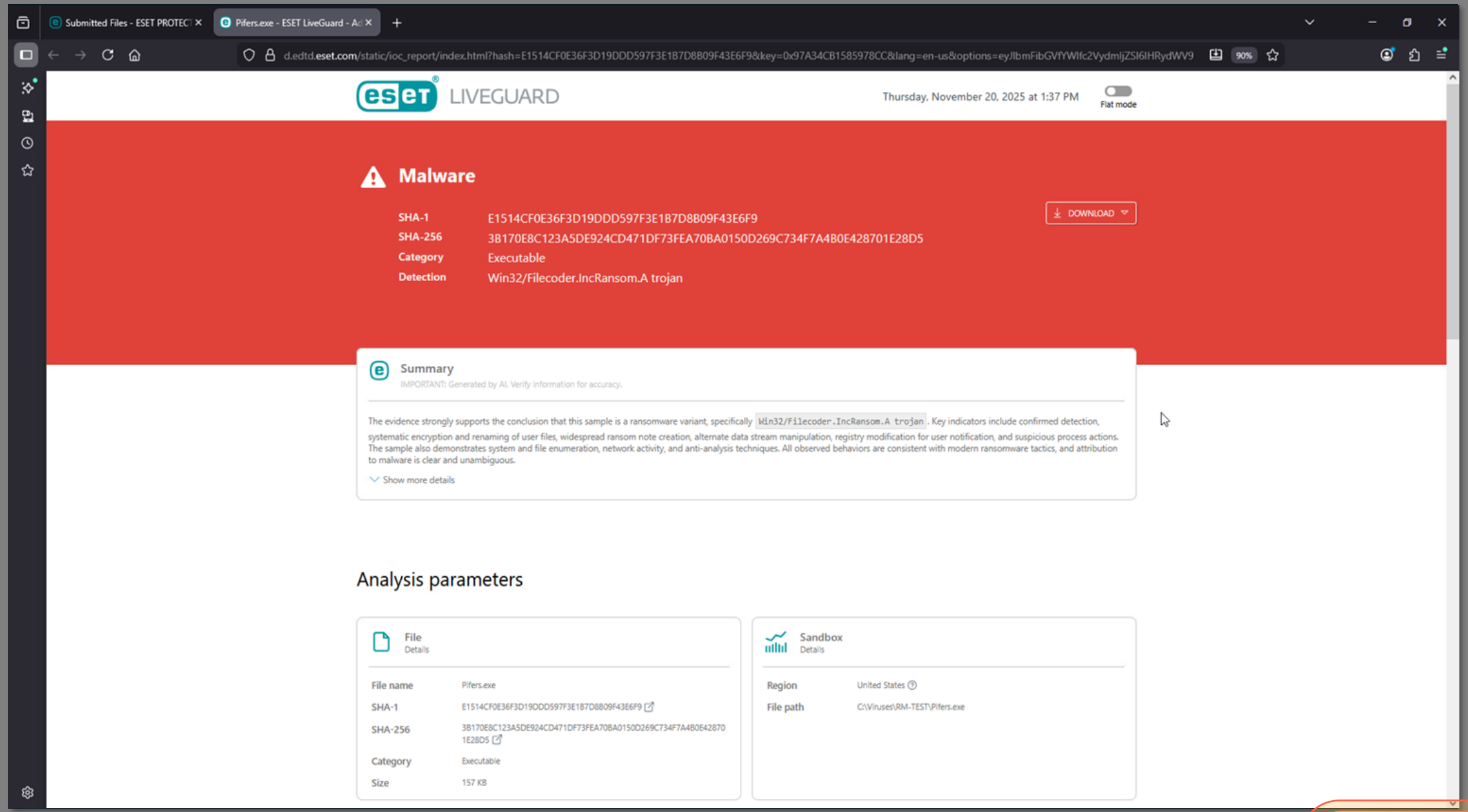
В ПРОЦЕСІ


ESET PROTECT
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
INCIDENTS
VULNERABILITIES
Patch Management
Advanced Search
Detections
Reports
Tasks
Installers
Configuration
Notifications
Status Overview
Integrations
Platform Modules
More
Submit Feedback
COLLAPSE
Advanced Search
Search
Last 7 days
End date
RUN
ESET.SEVERITY
Add Filter
Results 788
60
40
20
0
12/02/2025, 2:00 PM
12/03/2025, 3:00 PM
12/04/2025, 4:00 PM
12/05/2025, 5:00 PM
12/06/2025, 6:00 PM
@TIMESTAMP
RULE.NAME
EVENT.CATEGORY
EVENT.RISK_SC...
EVENT.ACTION
Dec 4, 2025, 11:06:45.059 AM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 11:00:46.502 AM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:54:46.635 AM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:48:46.648 AM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:45:25.012 AM Remote Monitoring & Management - TeamViewer [D0901] file,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:45:24.993 AM Remote Monitoring & Management - TeamViewer [D0901] file,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:45:24.993 AM Remote Monitoring & Management - TeamViewer [D0901] file,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:43:39.167 AM Remote Monitoring & Management - TeamViewer [D0901] intrusion_detection,intrusion_detection 40 rule-triggered
Dec 4, 2025, 10:01:03.087 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:01:02.337 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:01:01.572 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:01:00.103 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:01:00.103 AM ARP/CachePoisoningAttack intrusion_detection,network 40 connection-terminate
Dec 4, 2025, 10:00:59.337 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:00:58.587 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Dec 4, 2025, 10:00:56.493 AM ARP/CachePoisoningAttack network,intrusion_detection 55 connection-terminate
Remote Monitoring & Management - TeamViewer [D0901]
View Details
Overview
JSON
Remote Monitoring & Management - TeamViewer [D0901]
Detection category ESET Inspect Rules
Triggered event %PROGRAMFILES(X86)%\teamviewer\teamviewer_service.exe
Actions taken Blocked
Host name HP-G10-02
User name system
Type to search
@timestamp Dec 4, 2025, 10:48:46.648 AM
agent.build.original 5555
agent.type endpoint-detection-response
agent.version 2.8.5555.0
ecs.version 8.16
eset.epc_instance.id 0f15c705-f0e3-4ceb-a640-9ef7e8f8eb66
eset.executable.file_format pe
eset.executable.hash.md5 71C5EA47A64211DCE8EA39864F1094C3
eset.executable.hash.sha1 A9D468D1113E9C8511FB943CBFF325C81A66322A
eset.executable.hash.sha256 0DE8D083CCBBF4D33377B79810D629C0D4FDC7B...
eset.executable.id A9D468D1113E9C8511FB943CBFF325C81A66322A_
eset.executable.is_dynamically_linked_library false
eset.executable.livegrid_findings.age_days 1,826
eset.executable.livegrid_findings.popularity 1000000–9999999 computers

В ПРОЦЕСІ


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
Advanced Search
Remote Monitoring & Management - Team...
Overview
Remote Monitoring & Management - TeamViewer [D0901]
Detection category
ESET Inspect Rules
Actions taken
Blocked
Occurrences per minute
1
User name
nt authority\system
hp-g10-02
OS name
Microsoft Windows 11 Home (10.0.26200.7171)
Parent group
SAN
Last connected
14 minutes ago - Dec 8, 2025, 1:20:33 PM
Network isolation
Not isolated
Description
General
Detection type
The rule was activated
Process started
5 days ago - Dec 3, 2025, 5:03:12 PM
Event occurred
4 days ago - Dec 4, 2025, 10:48:46 AM
Detection triggered
4 days ago - Dec 4, 2025, 10:51:12 AM
Severity
Warning
Severity score
40
Rule details
Category
Remote Desktop / Remote Access
Description
Adversary abuses **Remote monitoring and management** (**RMM**) software TeamViewer to obtain persistent remote access and blend in network traffic.
Process
Name
teamviewer_service.exe
Command line
%PROGRAMFILES(X86)%\teamviewer\teamviewer_service.exe
Path
%PROGRAMFILES(X86)%\teamviewer\teamviewer_service.exe
ACTIONS

В ПРОЦЕСІ


Submitted Files - ESET PROTEC
Pifers.exe - ESET LiveGuard - Ac
d.edtd.eset.com/static/ioc_report/index.html?hash=E1514CF0E36F3D19DDD597F3E1B7D8B09F43E6F9&key=0x97A34CB1585978CC&lang=en-us&options=eyJlbmFibGVfYWlfc2VydmljZSI6IHRydWV9
90%
ESET LIVEGUARD
Thursday, November 20, 2025 at 1:37 PM
Flat mode
Malware
SHA-1 E1514CF0E36F3D19DDD597F3E1B7D8B09F43E6F9
SHA-256 3B170E8C123A5DE924CD471DF73FEA70BA0150D269C734F7A4B0E428701E28D5
Category Executable
Detection Win32/Filecoder.IncRansom.A trojan
DOWNLOAD
Summary
IMPORTANT: Generated by AI. Verify information for accuracy.
The evidence strongly supports the conclusion that this sample is a ransomware variant, specifically Win32/Filecoder.IncRansom.A trojan. Key indicators include confirmed detection, systematic encryption and renaming of user files, widespread ransom note creation, alternate data stream manipulation, registry modification for user notification, and suspicious process actions. The sample also demonstrates system and file enumeration, network activity, and anti-analysis techniques. All observed behaviors are consistent with modern ransomware tactics, and attribution to malware is clear and unambiguous.
Show more details
Analysis parameters
File
Details
File name Pifers.exe
SHA-1 E1514CF0E36F3D19DDD597F3E1B7D8B09F43E6F9
SHA-256 3B170E8C123A5DE924CD471DF73FEA70BA0150D269C734F7A4B0E428701E28D5
Category Executable
Size 157 KB
Sandbox
Details
Region United States
File path C:\Viruses\RM-TEST\Pifers.exe

В ПРОЦЕСІ

The Dawn of Intent-Aware Access

Архітектурні недоліки сучасної безпеки

- Прямий доступ до мережі
- Схильність систем до експлуатації
- Виявлення є реактивним
- Розрив у доступі
- VPN, ZTNA, PAM, брандмауер

Не можна вирішити сьогоднішні проблеми за допомогою вчорашньої архітектури

Можливості	**Класичний PAM**	**Excalibur - Новий Стандарт!**
Основна філософія	Захист «привілейованих»	Забезпечення безпеки всього підприємства
Архітектура	Мережецентричний	Ідентичність орієнтована
Модель безпеки	Реактивна (Detect & Respond)	Превентивна (Isolation)
Фокус	Захист облікових даних	Забезпечення безпеки кожної дії та наміру
Докази	Неоднозначні мережеві журнали	Детерміновані, відтворювані докази
Результат	**Залишає відкритим «пробіл доступності»**	**Цілеспрямовано усуває «пробіл доступності».**

Excalibur

PAM = Управління привілейованим доступом

SAM = Потокове управління доступом

Excalibur

Excalibur

SAM

Повна та сучасна
ізоляція за допомогою стримінгу.

Архітектура без агентів

Доступ через стандартний HTML5-браузер

Безпарольна та орієнтована на телефон
вбудована багатофакторна автентифікація

Комплексний підхід
Можливість відстеження та аудиту

Excalibur

Чому саме управління потоковим доступом?

1. Більшість порушень безпеки відбувається через людські помилки або методи соціальної інженерії.
2. Компрометовані облікові дані – найпоширеніший початковий вектор атаки.
3. Нормативні акти (наприклад, NIS2) потребують суворих механізмів автентифікації та контролю доступу.
4. Багаторівневий захист в одному доступному, простому у реалізації та використанні рішенні.

Excalibur

Рівні кібербезпеки SAM

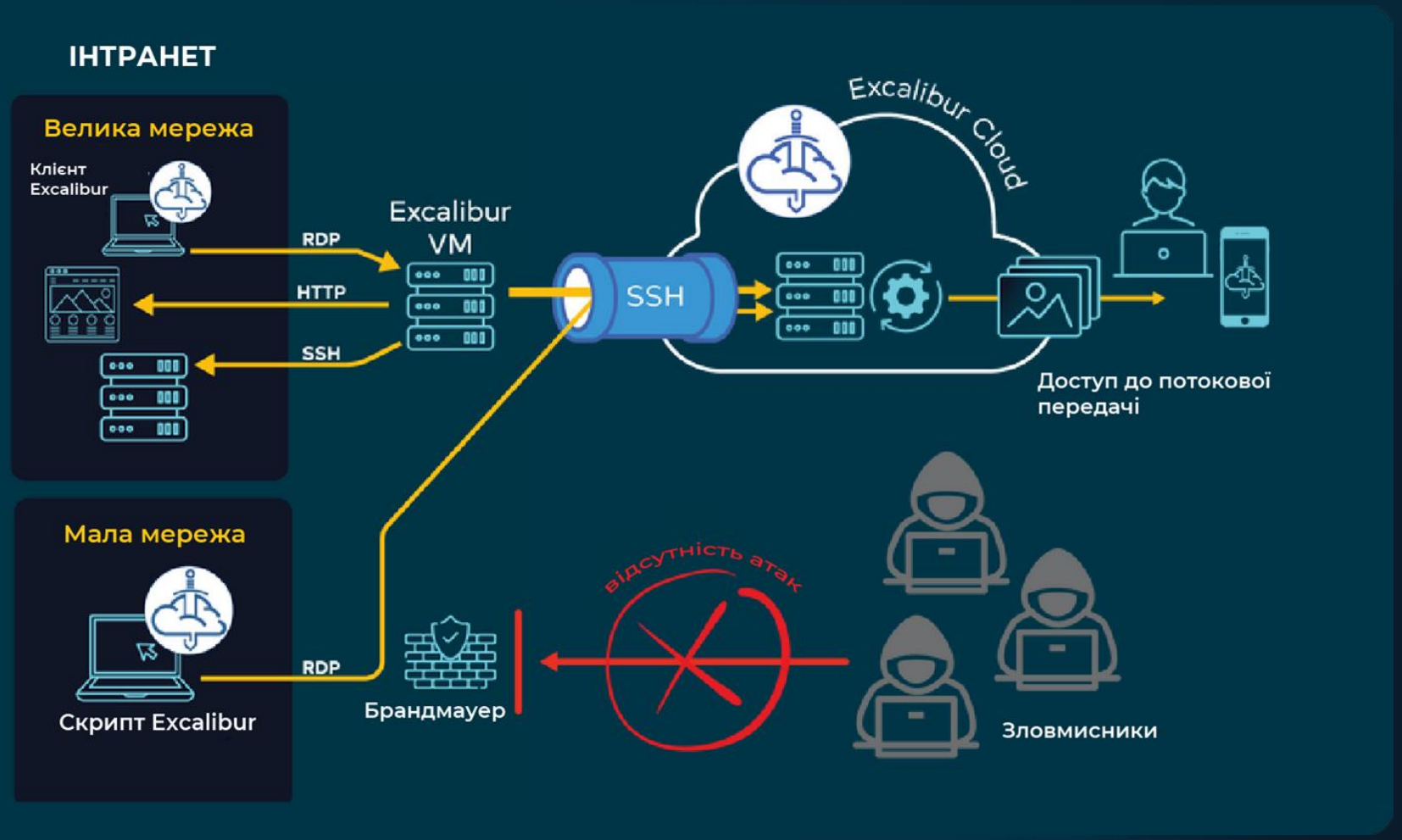
Багатофакторна автентифікація
Шлюз для доступу до всієї системи з факторами, що повністю налаштовуються, щоб забезпечити надійну перевірку авторизованих користувачів.

Панель управління SAM
Детальні обмеження, що налаштовуються, дозволяють гарантувати, що авторизовані користувачі мають доступ тільки до необхідної кількості частин системи.

Можливість аудиту та прозорість
Дії, підписані криптографічно, та запис даних всіх авторизованих користувачів для забезпечення повної незаперечності.

Під наглядом ШІ
Аналіз дій користувачів у реальному часі та офлайн-режимі з функцією примусового завершення сеансу при виявленні загроз.

Excalibur

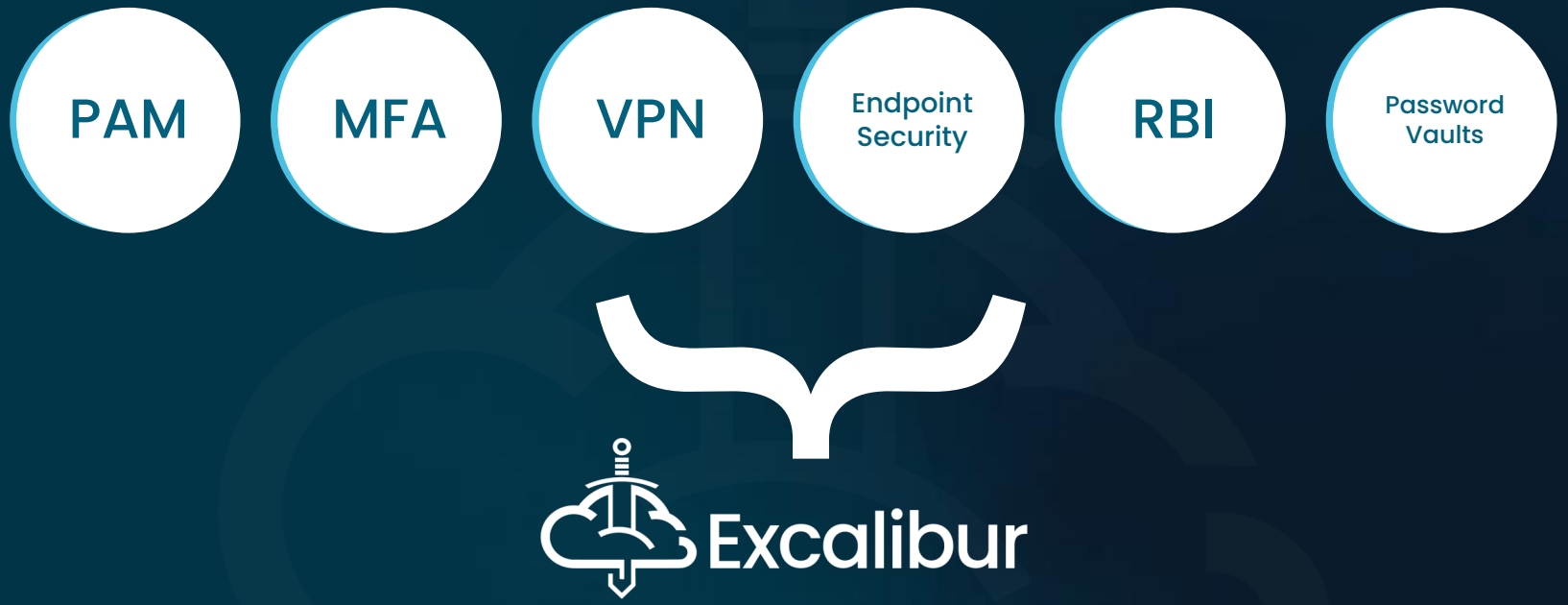


1. **Багатофакторна автентифікація**
2. **Панель управління SAM**
3. **Можливість аудиту та прозорість**
4. **Під наглядом ШІ**

Excalibur

Поєднуйте технології. Спрощуйте безпеку.

Уніфікована платформа замість різних інструментів.



Переваги

- Зниження сукупної вартості володіння (TCO)
- Оптимізація стека вендорів та агентів
- Спрощення архітектури безпеки та взаємодії з користувачем

Excalibur

Варіанти розгортання

Kubernetes (SaaS)

- Мінімальні операційні витрати
- Автоматичні оновлення та масштабованість
- Повністю управляється Excalibur

Kubernetes (Локальна/Приватна хмара)

- Повний контроль над інфраструктурою, мережею, відповідністю вимогам та доступністю
- Підходить для середовищ із суворим дотриманням суверенітету даних / нормативних актів

Excalibur

ВИНИКЛИ ПИТАННЯ?

+380 44 545 77 26

support@eset.ua

Офіційний WhatsApp-канал