ENJOY SAFER TECHNOLOGY™

# EDR nástroj ESET Enterprise Inspector

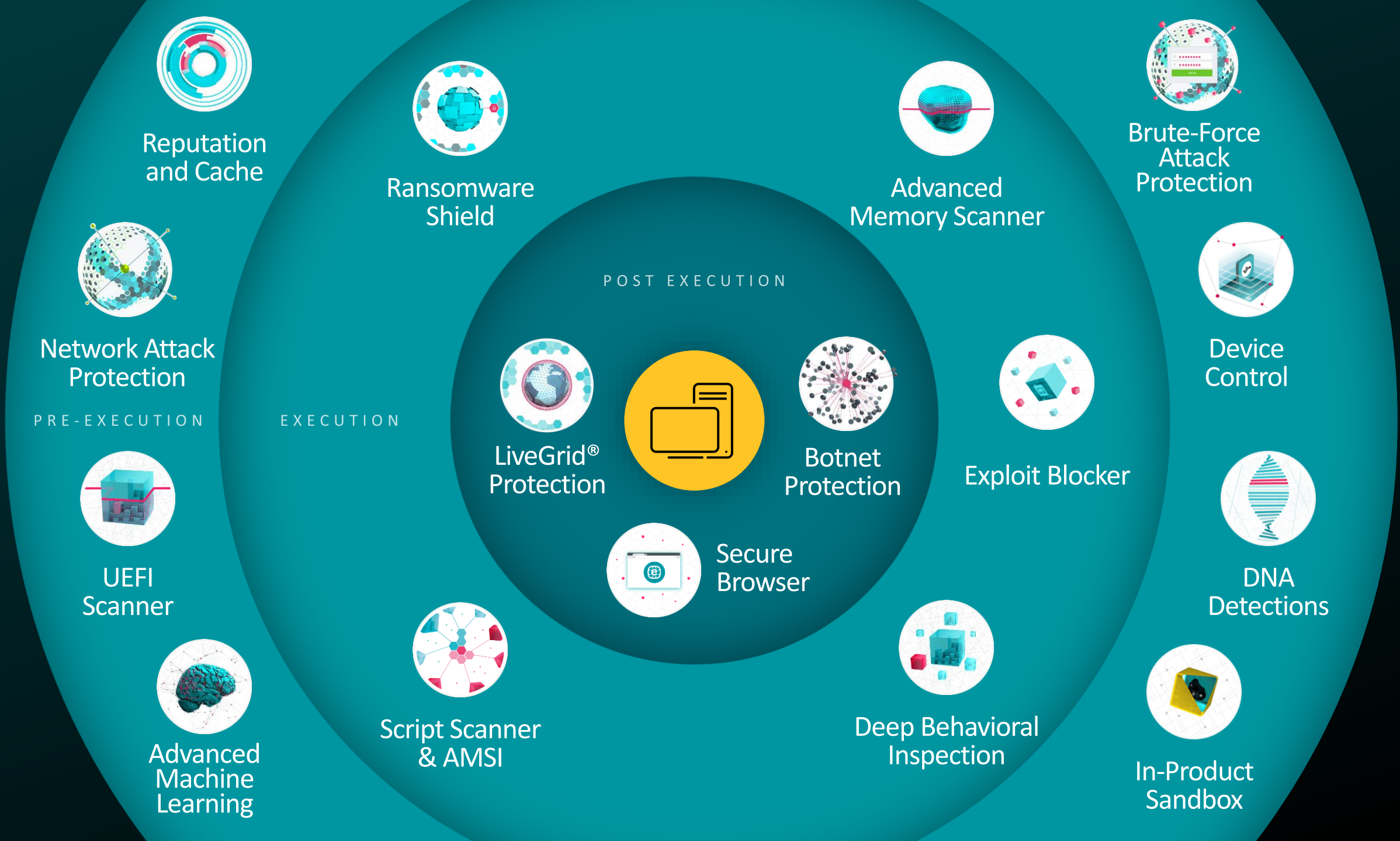
## (praktické využitie)

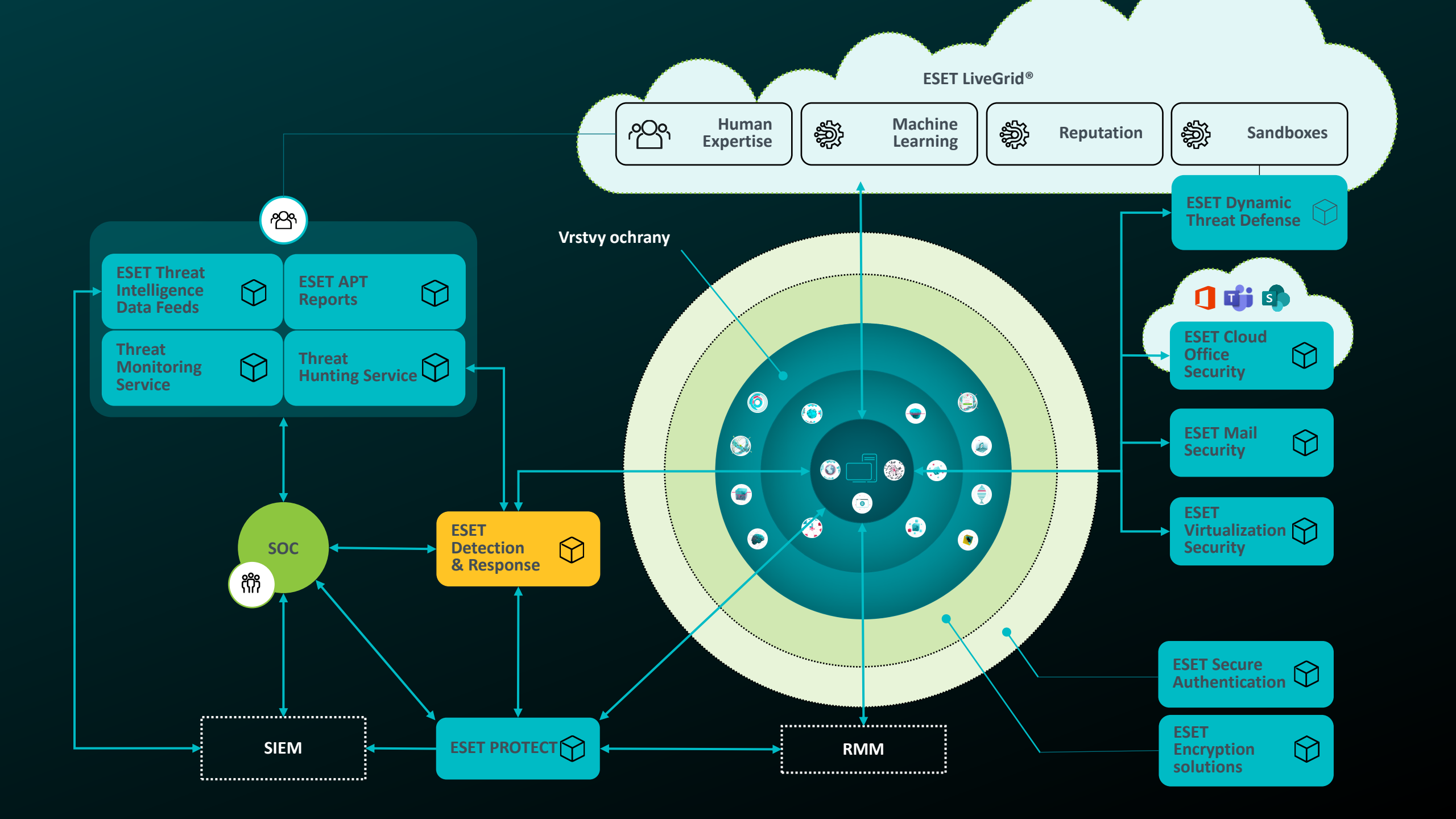
# Prečo Endpoint Detection and Response

- Komplexnosť útokov
- Dĺžka útoku
- Iné ako spustiteľné súbory
- Pretrvávajúce hrozby
- 69/2018 Z. z. o kybernetickej bezpečnosti

# ENTERPRISE INSPECTOR


Predikcia
Prevencia
Reakcia
Detekcia

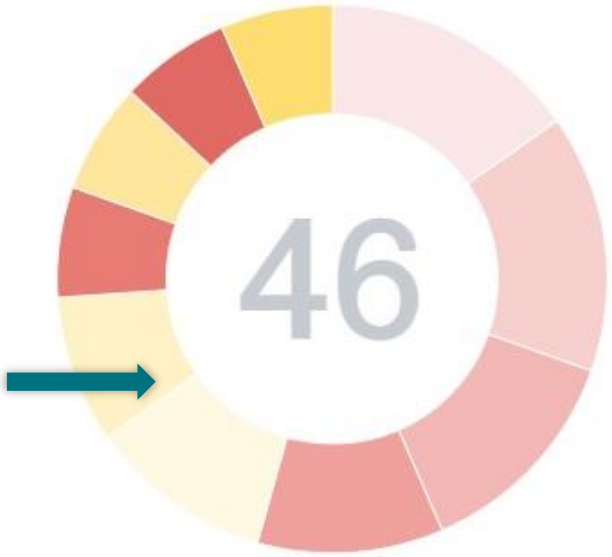

Reputation and Cache
Ransomware Shield
Advanced Memory Scanner
Brute-Force Attack Protection
Network Attack Protection
Device Control
PRE-EXECUTION
EXECUTION
POST EXECUTION
LiveGrid® Protection
Botnet Protection
Exploit Blocker
UEFI Scanner
DNA Detections
Secure Browser
Advanced Machine Learning
Script Scanner & AMSI
Deep Behavioral Inspection
In-Product Sandbox


ESET LiveGrid®
Human Expertise
Machine Learning
Reputation
Sandboxes
ESET Dynamic Threat Defense
Vrstvy ochrany
ESET Threat Intelligence Data Feeds
ESET APT Reports
Threat Monitoring Service
Threat Hunting Service
ESET Cloud Office Security
ESET Mail Security
ESET Virtualization Security
SOC
ESET Detection & Response
ESET Secure Authentication
ESET Encryption solutions
SIEM
ESET PROTECT
RMM

Dashboard
ADD FILTER

Detections | Executables | Computers | More | Server status | Events load

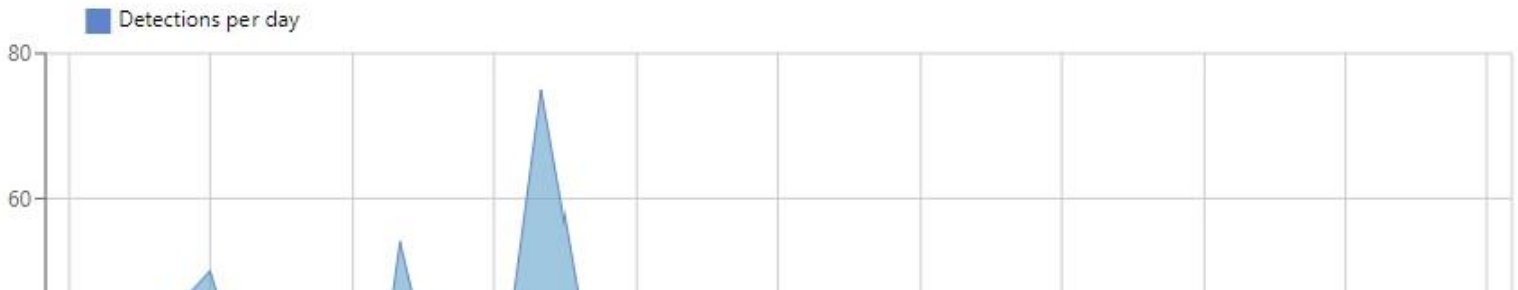
## Top 10 Unresolved Threat and Warning Detections

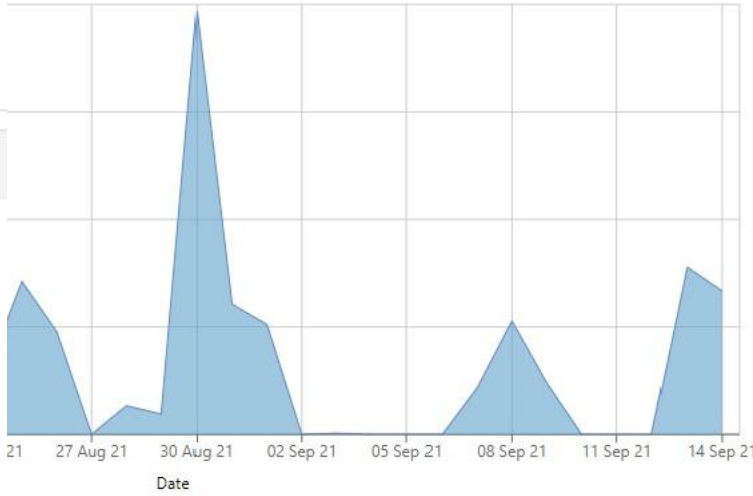


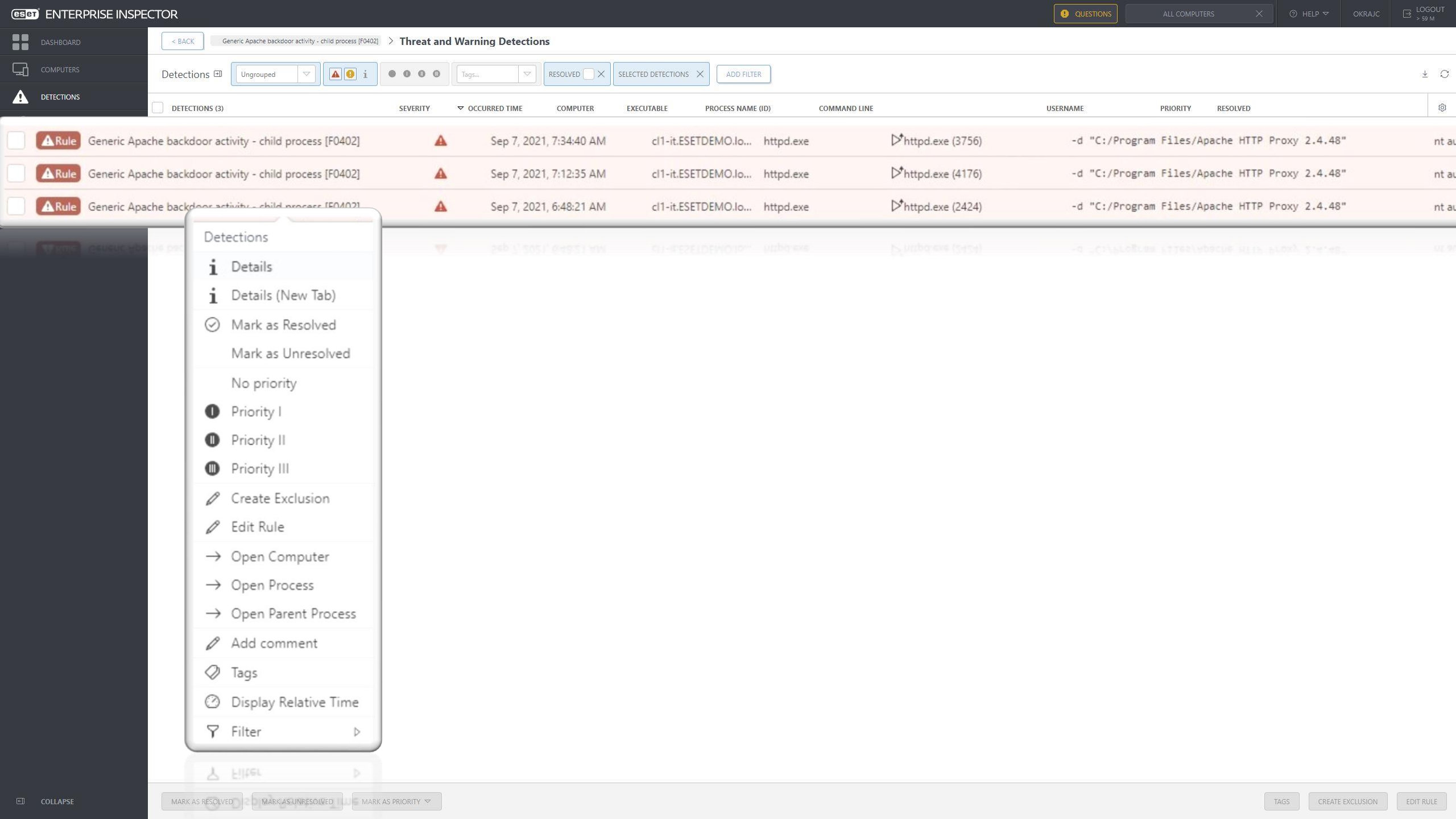

- Ransomnote file was written - filecoders [C0611] (7)
- Ransomnote behavioral detection - filecoders [C0619] (7)
- Common AutoStart registry modified by an unpopular process [A0103a] (6)
- MS Office application has invoked script interpreter [D0807] (5)
- Detected by ESET Endpoint Security product (5)
- Suspicious script interpreter process tree - Microsoft Office [F0420b] (4)
- Suspicious service executed [B0902] (3)
- Modification of "hosts" file [B1002] (3)
- Generic Apache backdoor activity - child process [F0402] (3)
- Windows Firewall rules manipulation [B0202] (3)

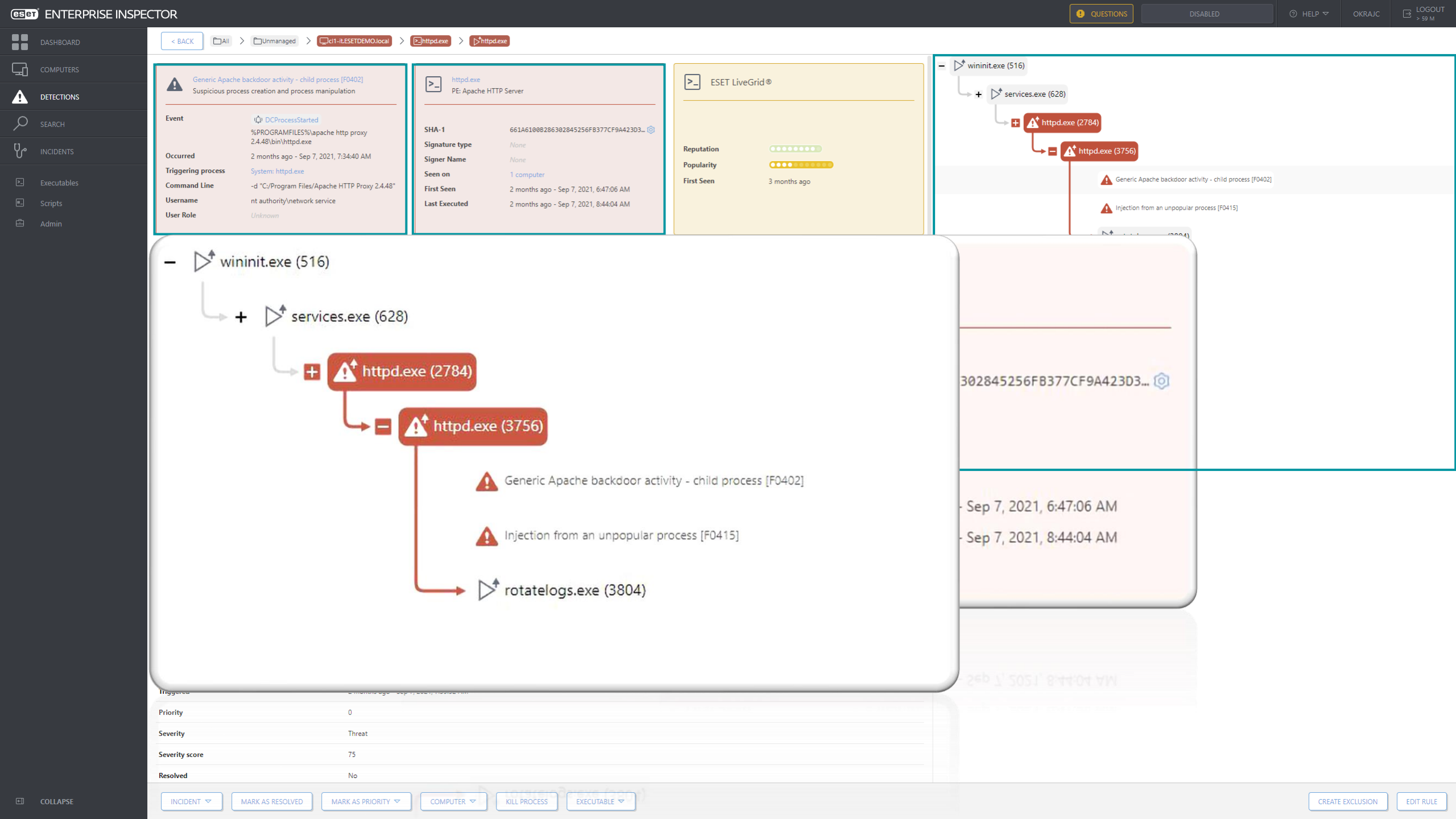
- Network connection from System temp folder [A0509] (157)
- Suspicious rundll32 process [F0430] (28)
- Process from SysWOW64 started by unpopular process [A0416] (18)
- Netsh firewall rules manipulation [F0453] (14)
- System utility was executed test [A0403] (14)
- Unpopular process has started from %Temp% [Z0402] (8)
- Non-browser process makes HTTP request to a popular Web Service [E0501] (8)
- Common AutoStart registry modified by an unpopular process [A0103] (8)
- Cmd.exe executed with '/c' by an unpopular process [A0400] (7)
- Network connection from Windows Installer (msiexec) [A0512] (7)

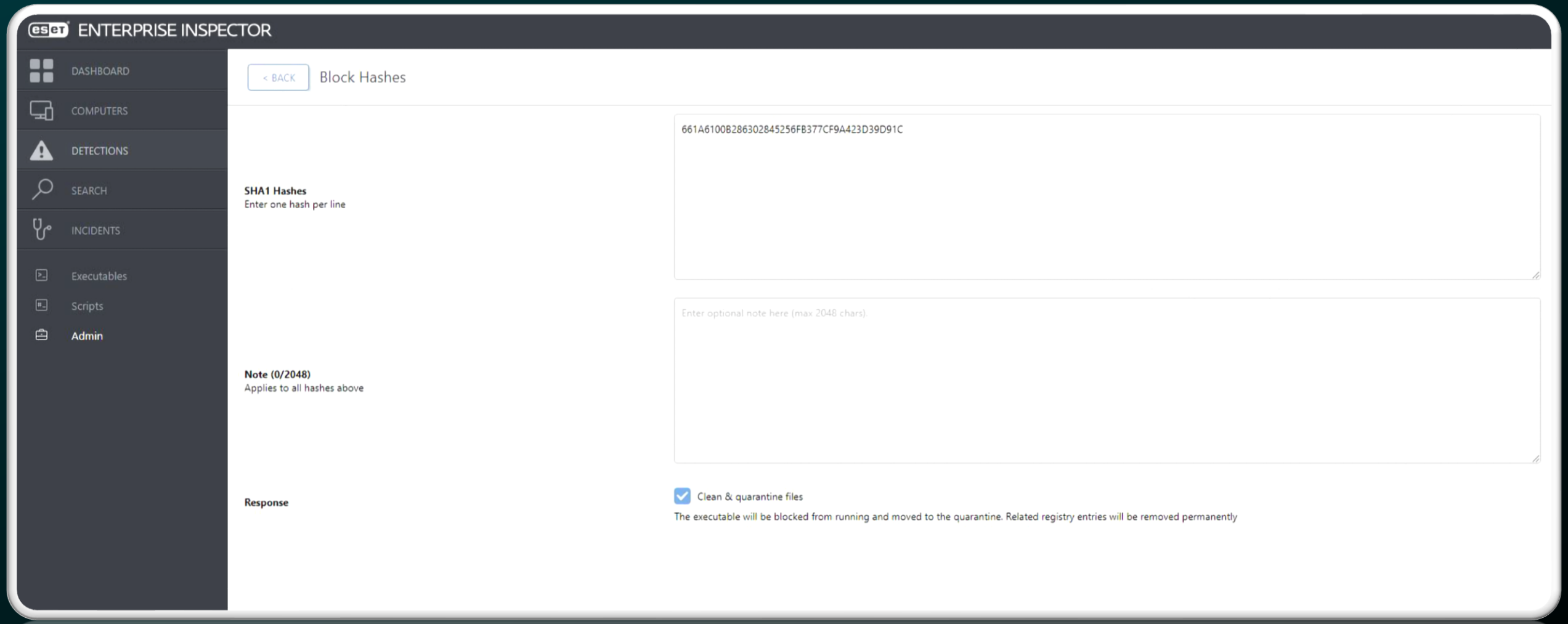
## Threat and Warning Detections

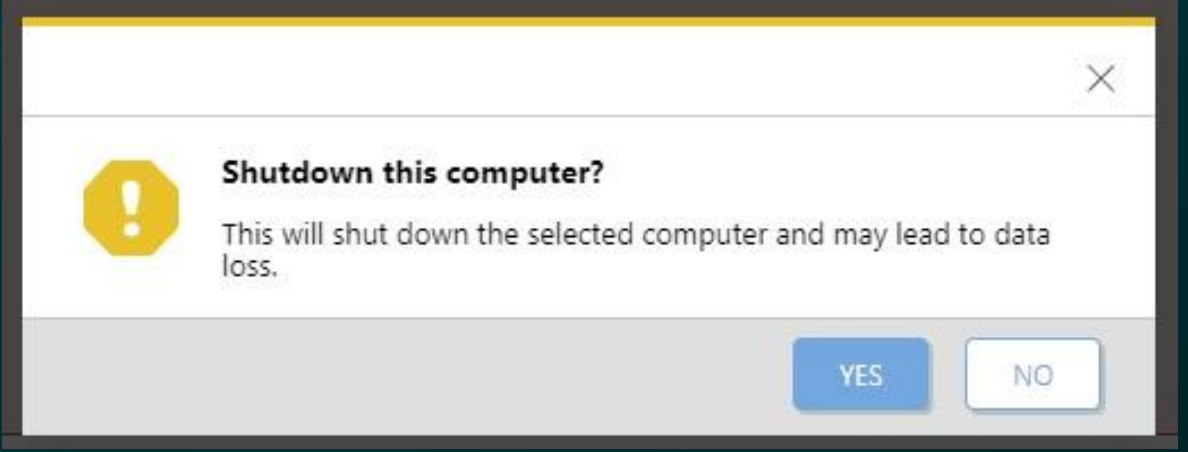


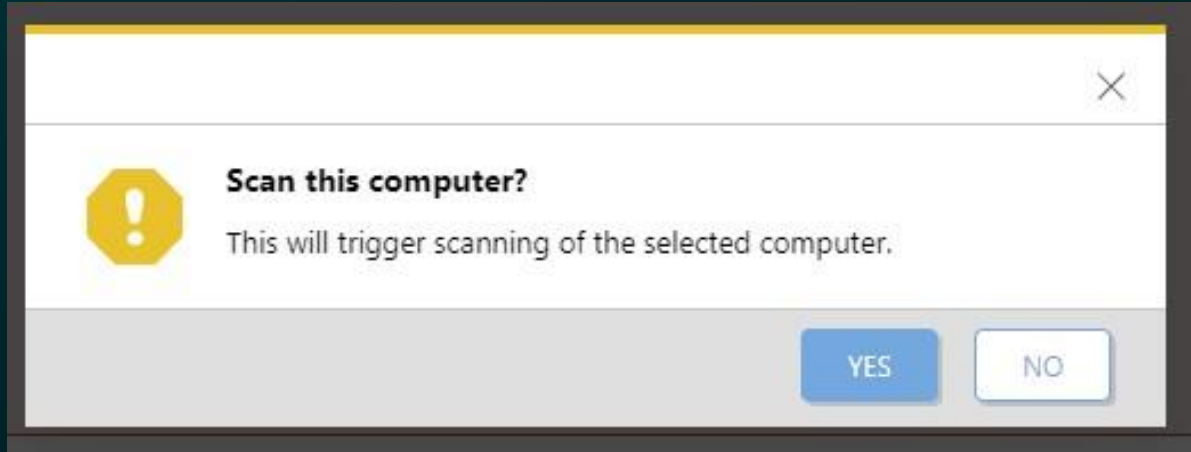



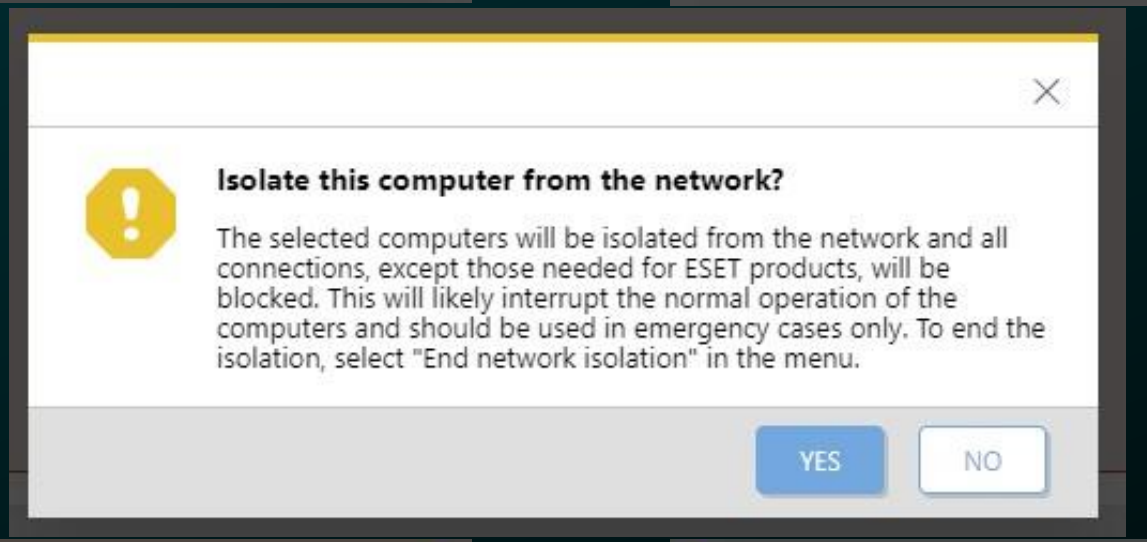

ENTERPRISE INSPECTOR
QUESTIONS
ALL COMPUTERS
HELP
OKRAJC
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
< BACK
Generic Apache backdoor activity - child process [F0402]
Threat and Warning Detections
Detections
Ungrouped
Tags...
RESOLVED
SELECTED DETECTIONS
ADD FILTER
DETECTIONS (3)
SEVERITY
OCCURRED TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
COMMAND LINE
USERNAME
PRIORITY
RESOLVED
Rule Generic Apache backdoor activity - child process [F0402] Sep 7, 2021, 7:34:40 AM cl1-it.ESETDEMO.lo... httpd.exe httpd.exe (3756) -d "C:/Program Files/Apache HTTP Proxy 2.4.48"
Rule Generic Apache backdoor activity - child process [F0402] Sep 7, 2021, 7:12:35 AM cl1-it.ESETDEMO.lo... httpd.exe httpd.exe (4176) -d "C:/Program Files/Apache HTTP Proxy 2.4.48"
Rule Generic Apache backdoor activity - child process [F0402] Sep 7, 2021, 6:48:21 AM cl1-it.ESETDEMO.lo... httpd.exe httpd.exe (2424) -d "C:/Program Files/Apache HTTP Proxy 2.4.48"
Detections
Details
Details (New Tab)
Mark as Resolved
Mark as Unresolved
No priority
Priority I
Priority II
Priority III
Create Exclusion
Edit Rule
Open Computer
Open Process
Open Parent Process
Add comment
Tags
Display Relative Time
Filter
COLLAPSE
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS PRIORITY
TAGS
CREATE EXCLUSION
EDIT RULE

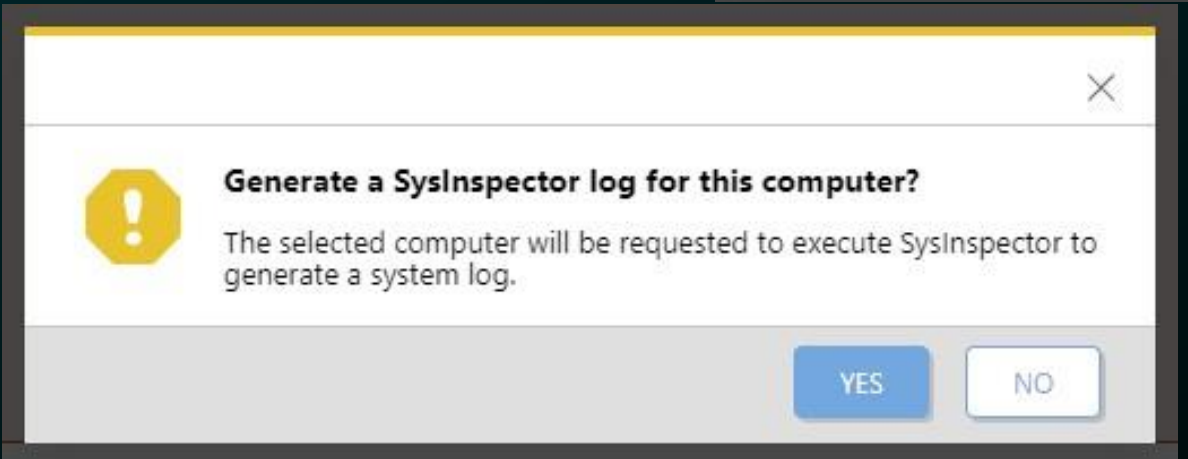

ENTERPRISE INSPECTOR
QUESTIONS
DISABLED
HELP
OKRAJC
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Admin
COLLAPSE
< BACK
All
Unmanaged
cl1-it.ESETDEMO.local
httpd.exe
httpd.exe
Generic Apache backdoor activity - child process [F0402]
Suspicious process creation and process manipulation
Event
DCProcessStarted
%PROGRAMFILES%\apache http proxy 2.4.48\bin\httpd.exe
Occurred
2 months ago - Sep 7, 2021, 7:34:40 AM
Triggering process
System: httpd.exe
Command Line
-d "C:/Program Files/Apache HTTP Proxy 2.4.48"
Username
nt authority\network service
User Role
Unknown
httpd.exe
PE: Apache HTTP Server
SHA-1
661A6100B286302845256FB377CF9A423D3...
Signature type
None
Signer Name
None
Seen on
1 computer
First Seen
2 months ago - Sep 7, 2021, 6:47:06 AM
Last Executed
2 months ago - Sep 7, 2021, 8:44:04 AM
ESET LiveGrid®
Reputation
Popularity
First Seen
3 months ago
wininit.exe (516)
services.exe (628)
httpd.exe (2784)
httpd.exe (3756)
Generic Apache backdoor activity - child process [F0402]
Injection from an unpopular process [F0415]
rotatelogs.exe (3804)
Priority
0
Severity
Threat
Severity score
75
Resolved
No
INCIDENT
MARK AS RESOLVED
MARK AS PRIORITY
COMPUTER
KILL PROCESS
EXECUTABLE
CREATE EXCLUSION
EDIT RULE

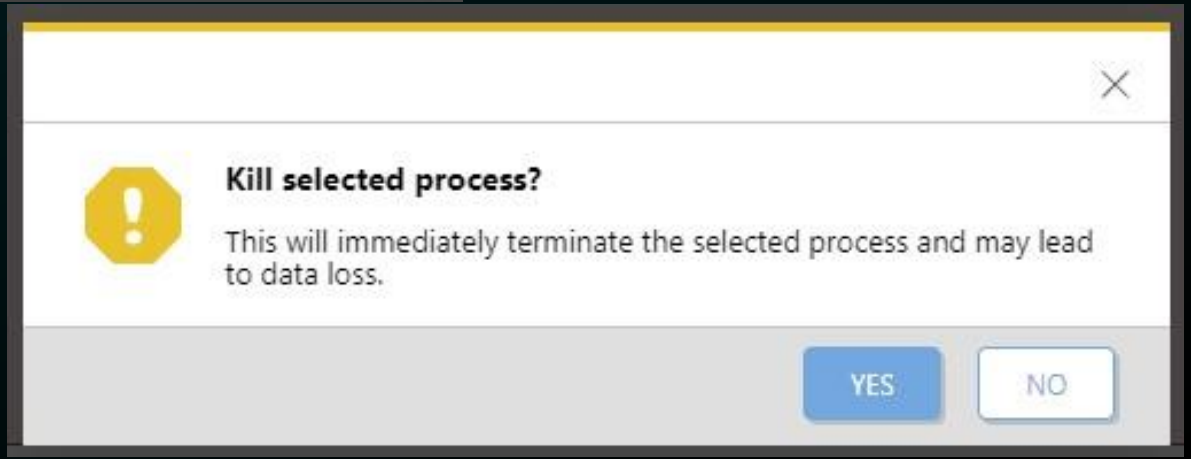

ENTERPRISE INSPECTOR
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Admin
< BACK
Block Hashes
661A6100B286302845256FB377CF9A423D39D91C
SHA1 Hashes
Enter one hash per line
Enter optional note here (max 2048 chars)
Note (0/2048)
Applies to all hashes above
Response
Clean & quarantine files
The executable will be blocked from running and moved to the quarantine. Related registry entries will be removed permanently

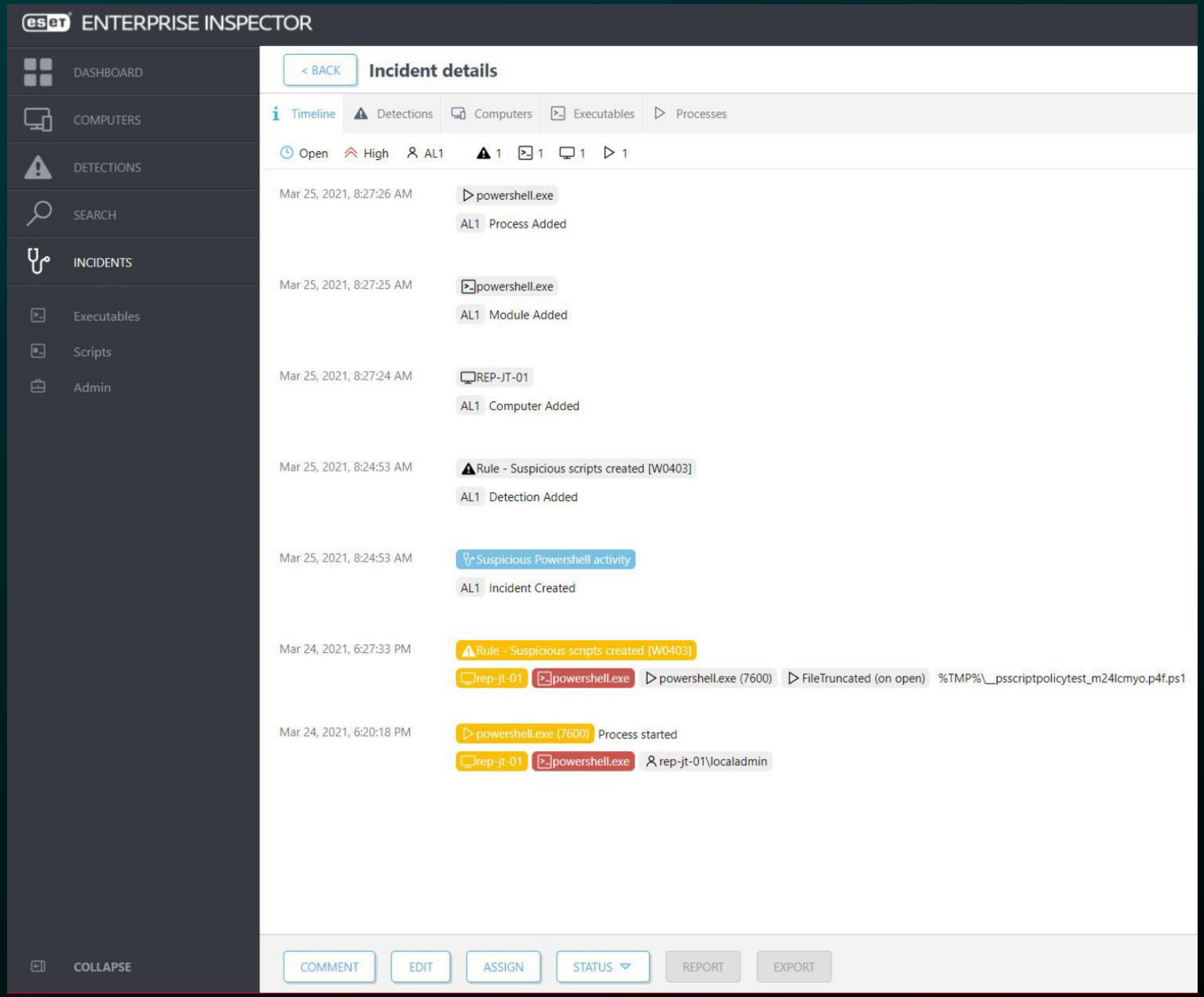

Shutdown this computer?
This will shut down the selected computer and may lead to data loss.
YES
NO

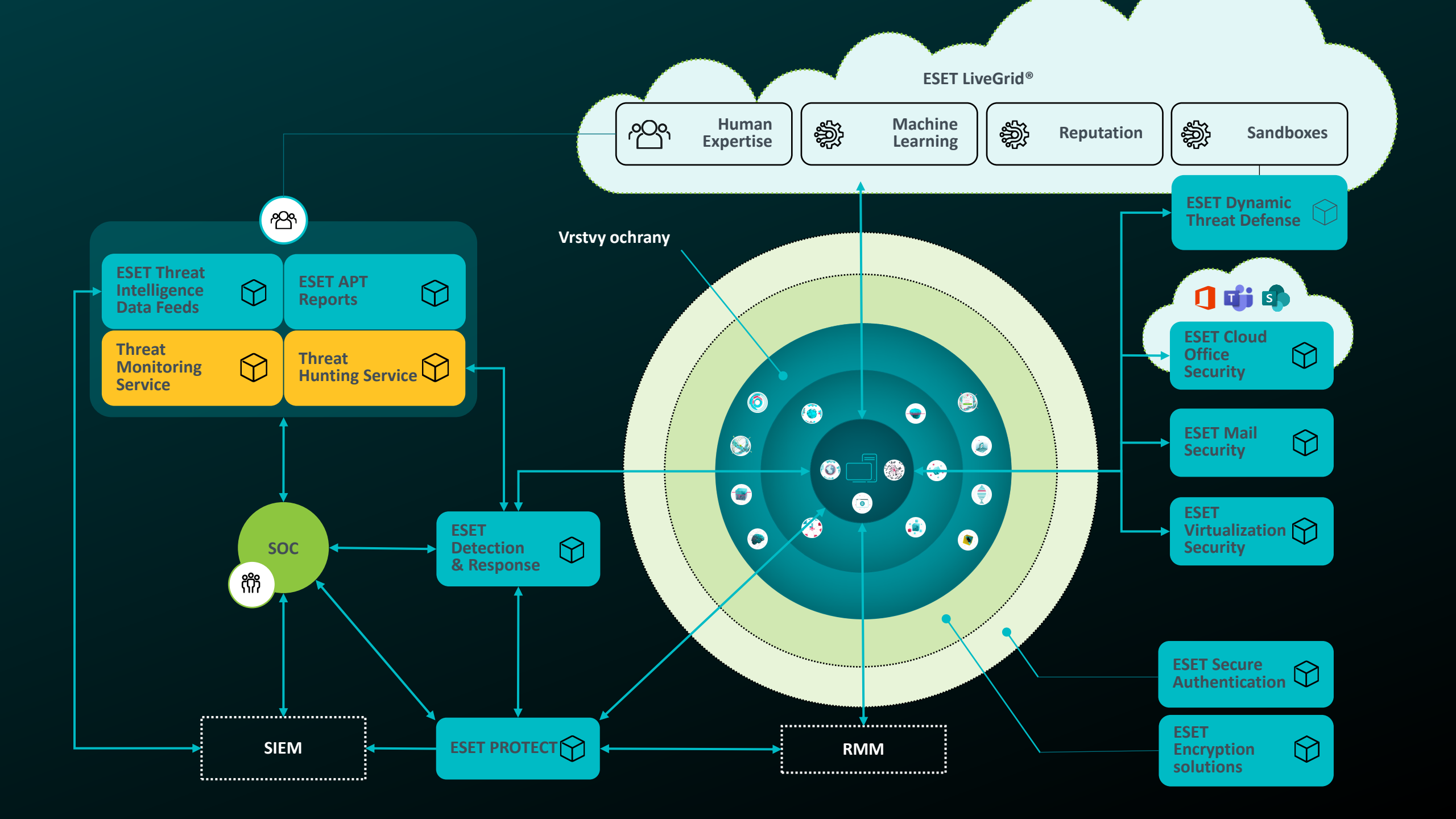

Scan this computer?
This will trigger scanning of the selected computer.
YES
NO


Isolate this computer from the network?
The selected computers will be isolated from the network and all connections, except those needed for ESET products, will be blocked. This will likely interrupt the normal operation of the computers and should be used in emergency cases only. To end the isolation, select "End network isolation" in the menu.
YES
NO


Generate a SysInspector log for this computer?
The selected computer will be requested to execute SysInspector to generate a system log.
YES
NO


Kill selected process?
This will immediately terminate the selected process and may lead to data loss.
YES
NO


ENTERPRISE INSPECTOR
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Admin
COLLAPSE
< BACK
Incident details
Timeline
Detections
Computers
Executables
Processes
Open
High
AL1
1
1
1
1
Mar 25, 2021, 8:27:26 AM
powershell.exe
AL1 Process Added
Mar 25, 2021, 8:27:25 AM
powershell.exe
AL1 Module Added
Mar 25, 2021, 8:27:24 AM
REP-JT-01
AL1 Computer Added
Mar 25, 2021, 8:24:53 AM
Rule - Suspicious scripts created [W0403]
AL1 Detection Added
Mar 25, 2021, 8:24:53 AM
Suspicious Powershell activity
AL1 Incident Created
Mar 24, 2021, 6:27:33 PM
Rule - Suspicious scripts created [W0403]
rep-jt-01
powershell.exe
powershell.exe (7600)
FileTruncated (on open)
%TMP%__psscriptpolicytest_m24lcmyo.p4f.ps1
Mar 24, 2021, 6:20:18 PM
powershell.exe (7600)
Process started
rep-jt-01
powershell.exe
rep-jt-01\localadmin
COMMENT
EDIT
ASSIGN
STATUS
REPORT
EXPORT


ESET LiveGrid®
Human Expertise
Machine Learning
Reputation
Sandboxes
ESET Dynamic Threat Defense
Vrstvy ochrany
ESET Threat Intelligence Data Feeds
ESET APT Reports
Threat Monitoring Service
Threat Hunting Service
ESET Cloud Office Security
ESET Mail Security
ESET Virtualization Security
SOC
ESET Detection & Response
ESET Secure Authentication
ESET Encryption solutions
SIEM
ESET PROTECT
RMM

| KATEGÓRIA AKTIVÍT | AKTIVITA | ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA | DETECTION AND RESPONSE ESSENTIAL | DETECTION AND RESPONSE ADVANCED | DETECTION AND RESPONSE ULTIMATE |
|---|---|---|---|---|---|
| **Bezpečnostná podpora pre koncové zariadenia** | Malvér: nezachytená detekcia | áno | áno | áno | áno |
| | Malvér: problém s liečením | áno | áno | áno | áno |
| | Malvér: infekcia ransomvérom | áno | áno | áno | áno |
| | Nesprávna detekcia | áno | áno | áno | áno |
| | Všeobecné: preskúmanie podozrivého správania | áno | áno | áno | áno |
| **Vyšetrenie incidentov a reakcia na ne** | Základná analýza súborov | ✗ | áno | áno | áno |
| | Podrobná analýza súborov | ✗ | áno | áno | áno |
| | Digitálna forenzná analýza | ✗ | áno | áno | áno |
| | Digitálna forenzná pomoc pri reakcii na incidenty | ✗ | áno | áno | áno |
| **Bezpečnostná podpora pre EEI** | Technická podpora – pravidlá | ✗ | ✗ | áno | áno |
| | Technická podpora – vylúčenia | ✗ | ✗ | áno | áno |
| | Všeobecné: otázky týkajúce sa bezpečnostného nástroja EEI | ✗ | ✗ | áno | áno |
| | EEI: počiatočná optimalizácia | ✗ | ✗ | áno | áno |
| | EEI: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie) | ✗ | ✗ | áno | áno |
| **Bezpečnostné služby pre EEI** | EEI: ESET Threat Monitoring (monitorovanie hrozieb) | ✗ | ✗ | ✗ | áno |
| | EEI: ESET Threat Hunting (proaktívne vyhľadávanie hrozieb) | ✗ | ✗ | ✗ | áno |
| **Profesionálne Služby** | ESET Deployment & Upgrade | ✗ | ✗ | ✗ | áno |

# Ďakujem za pozornosť

**ONDREJ KRAJČ**
Senior Technical Pre-Sales Representative
ondrej.krajc@eset.sk