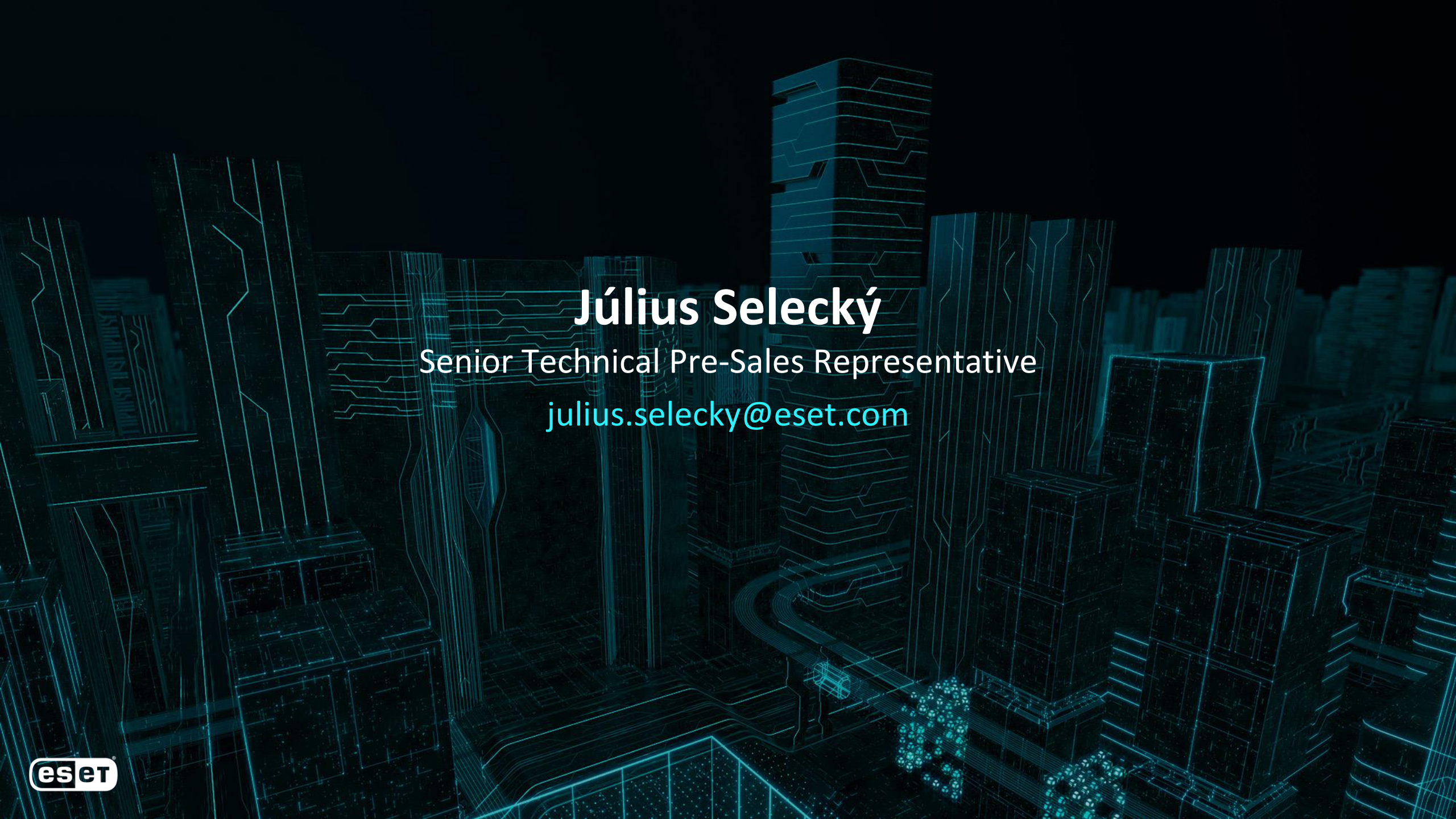
Digital Security
Progress. Protected.

ESET MDR

eset software

30 rokov

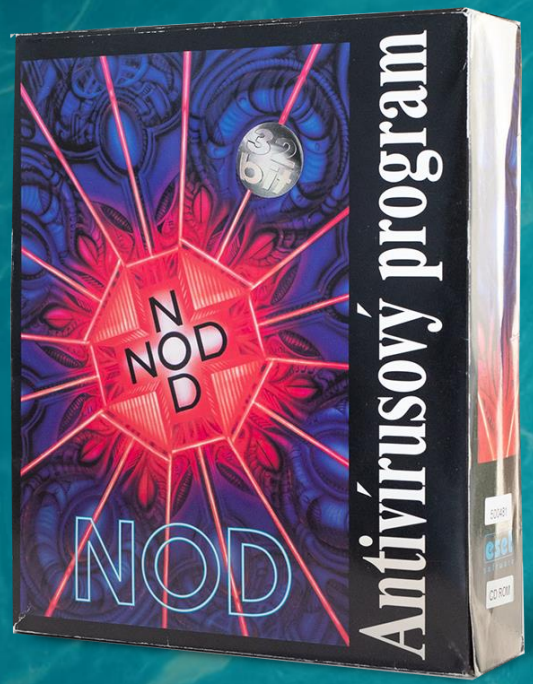


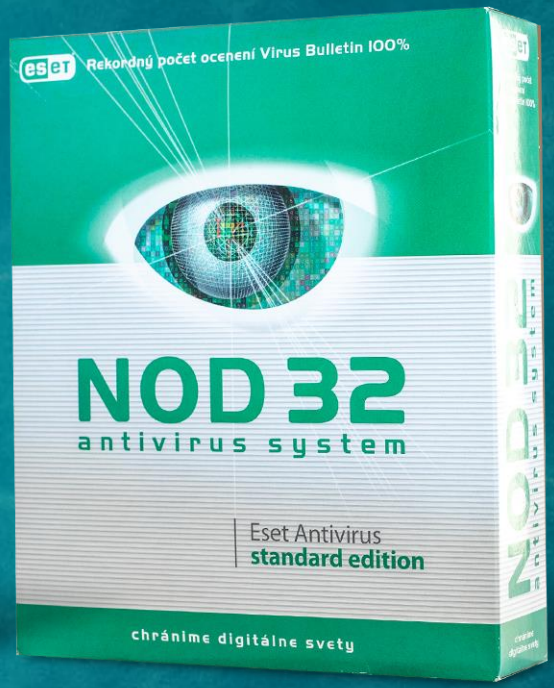
Július Selecký

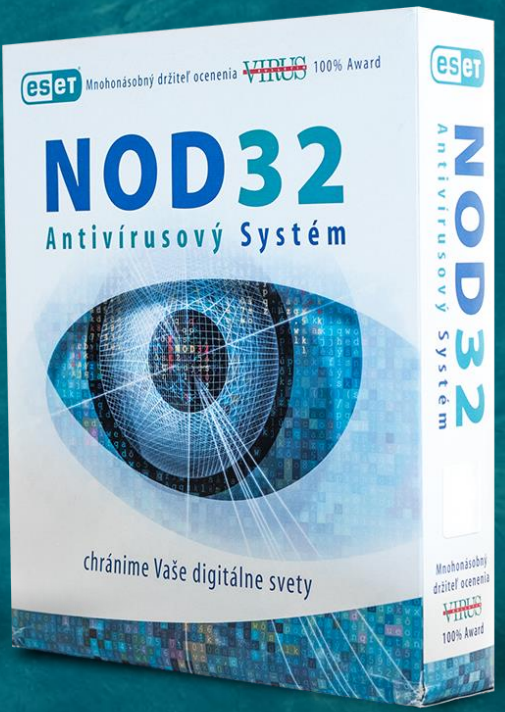
Senior Technical Pre-Sales Representative

julius.selecky@eset.com


30
years of complete
independence
& innovation
One of very few private global IT security companies



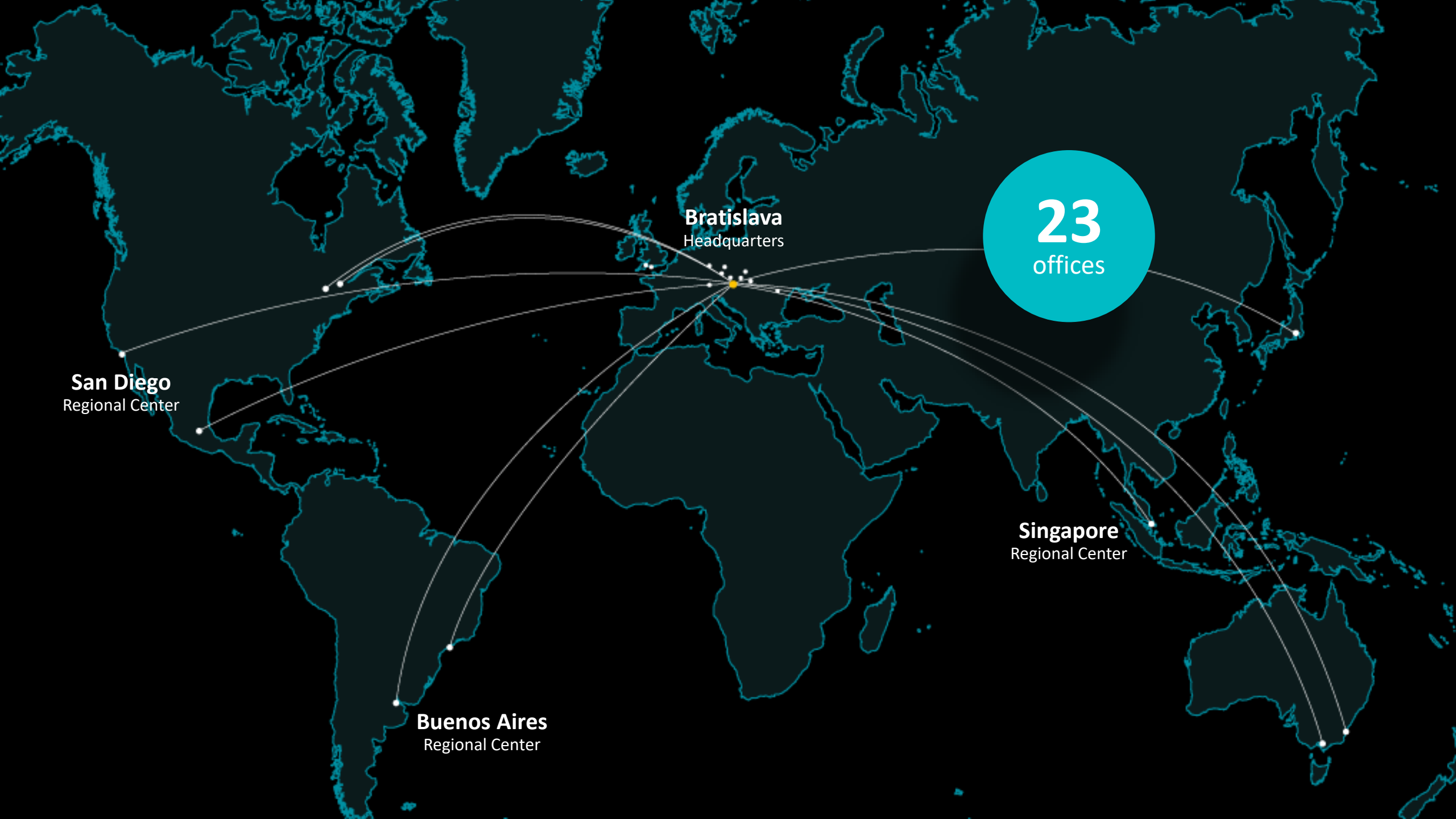


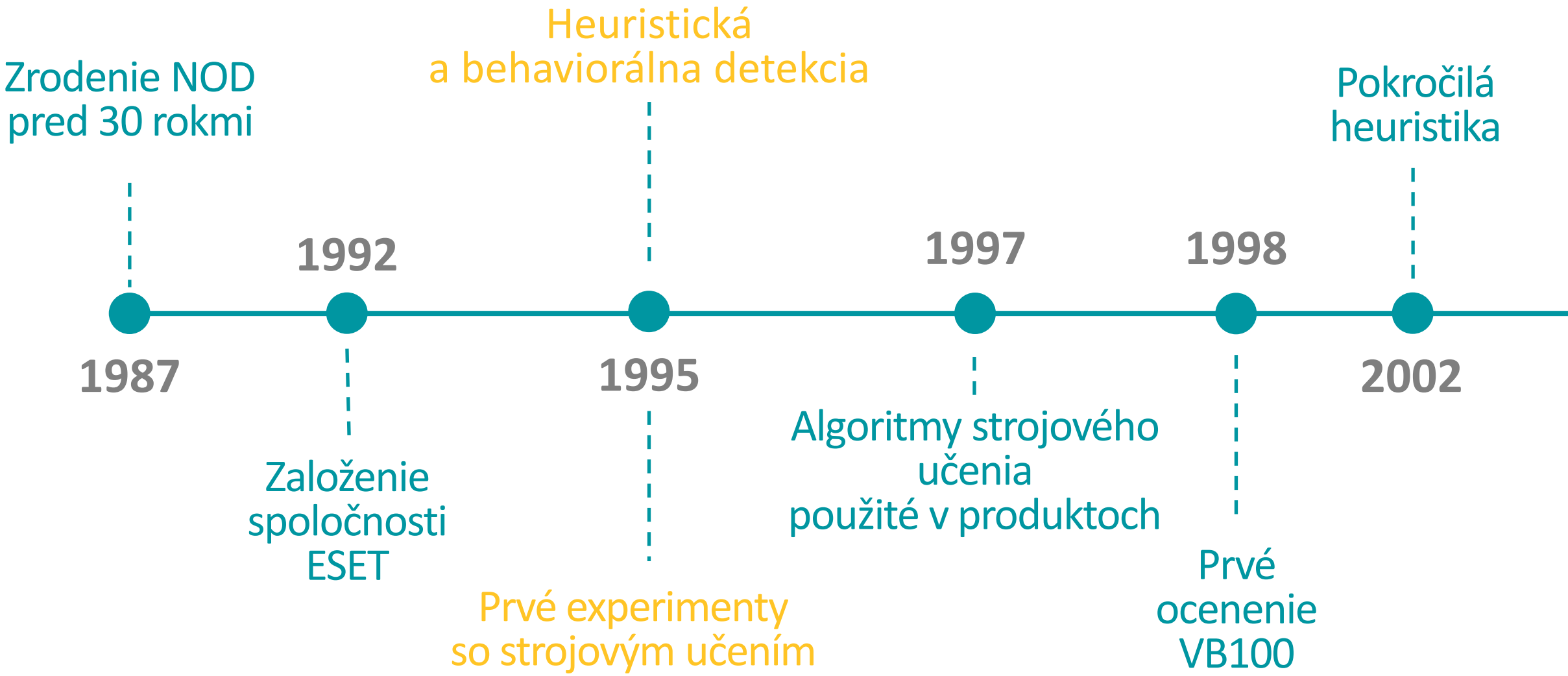


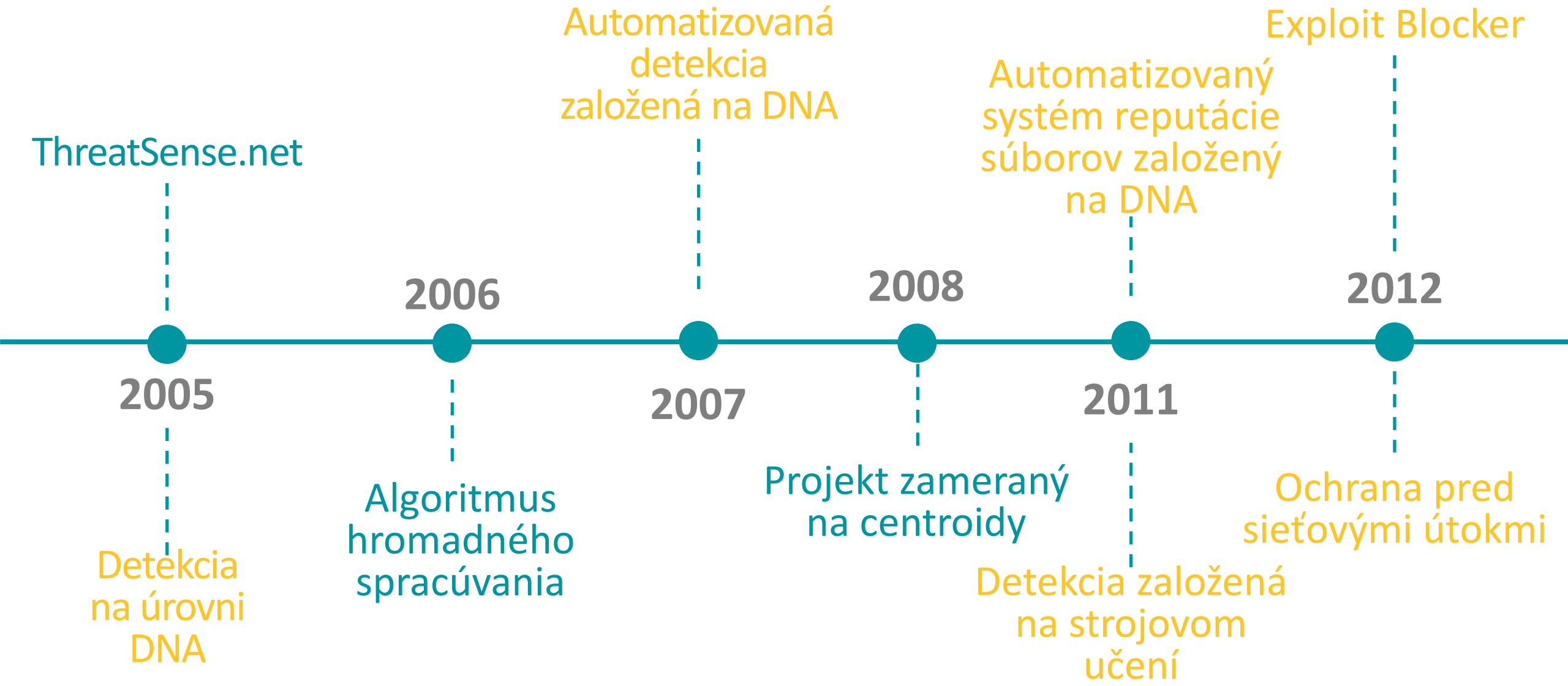
eset®
Digital Security
Progress. Protected.

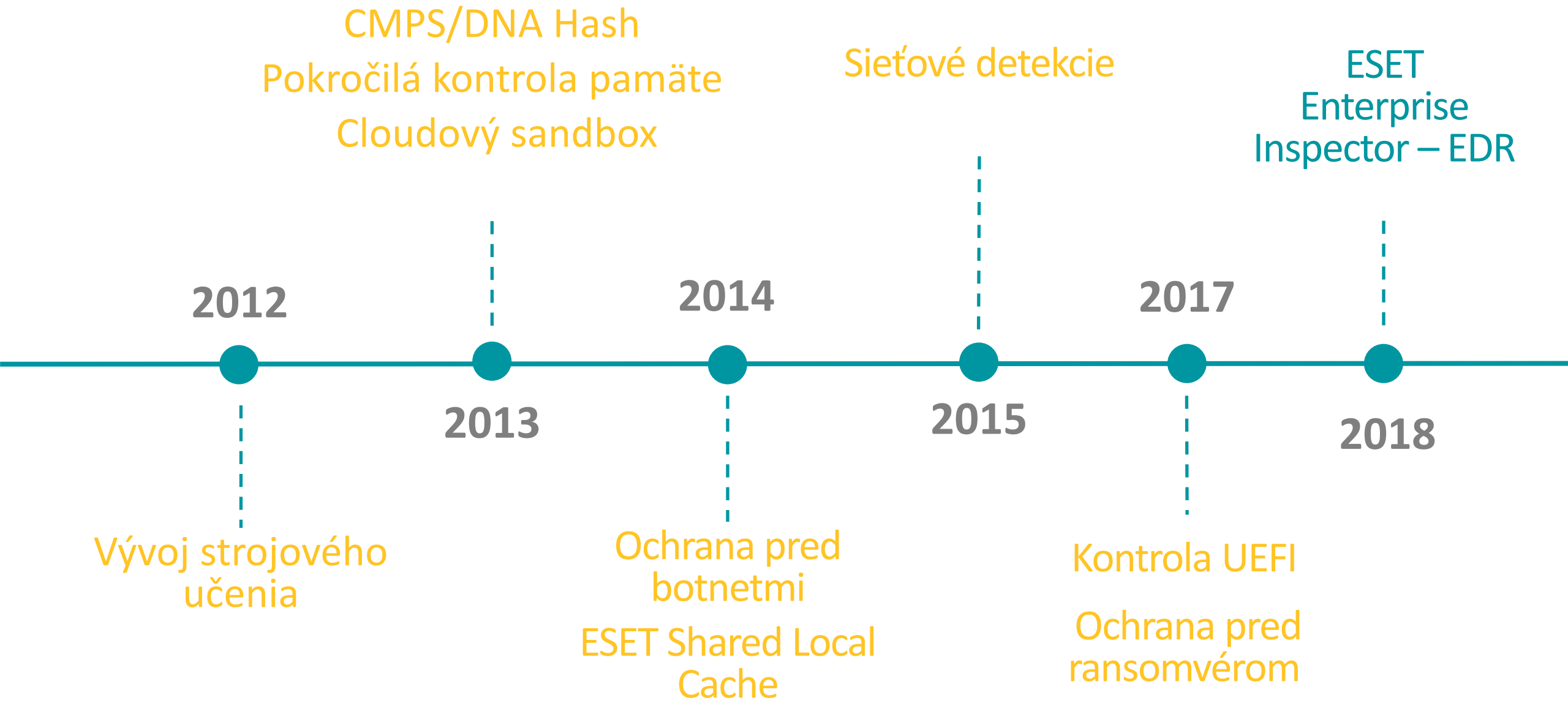
Number One
Cybersecurity
Company in EU

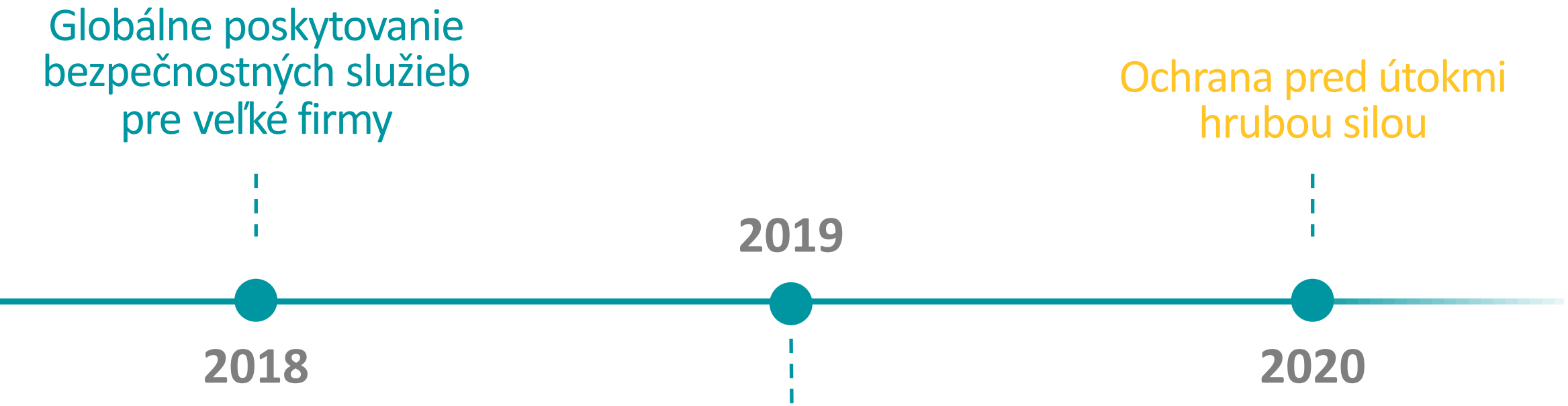

100M Direct Users
1BN+ INTERNET USERS
protected by our technology


Bratislava
Headquarters
23
offices
San Diego
Regional Center
Singapore
Regional Center
Buenos Aires
Regional Center


Zrodenie NOD
pred 30 rokmi
1987
1992
Založenie
spoločnosti
ESET
Heuristická
a behaviorálna detekcia
1995
Prvé experimenty
so strojovým učením
1997
Algoritmy strojového
učenia
použité v produktoch
1998
Prvé
ocenenie
VB100
Pokročilá
heuristika
2002

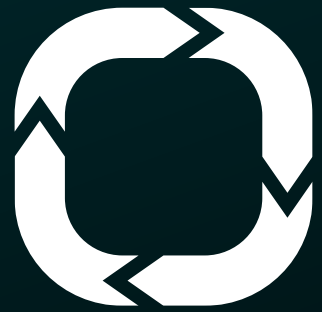

ThreatSense.net
2005
Detekcia na úrovni DNA
2006
Algoritmus hromadného spracúvania
Automatizovaná detekcia založená na DNA
2007
2008
Projekt zameraný na centroidy
Automatizovaný systém reputácie súborov založený na DNA
2011
Detekcia založená na strojovom učení
Exploit Blocker
2012
Ochrana pred sieťovými útokmi


CMPS/DNA Hash
Pokročilá kontrola pamäte
Cloudový sandbox
Sieťové detekcie
ESET Enterprise Inspector – EDR
2012
2013
2014
2015
2017
2018
Vývoj strojového učenia
Ochrana pred botnetmi
ESET Shared Local Cache
Kontrola UEFI
Ochrana pred ransomvérom


Globálne poskytovanie bezpečnostných služieb pre veľké firmy
2018
2019
Hĺbková kontrola správania
Kontrola v izolovanom prostredí
Pokročilé strojové učenie na koncovom zariadení
Ochrana pred útokmi hrubou silou
2020

PREDVÍDANIE HROZIEB

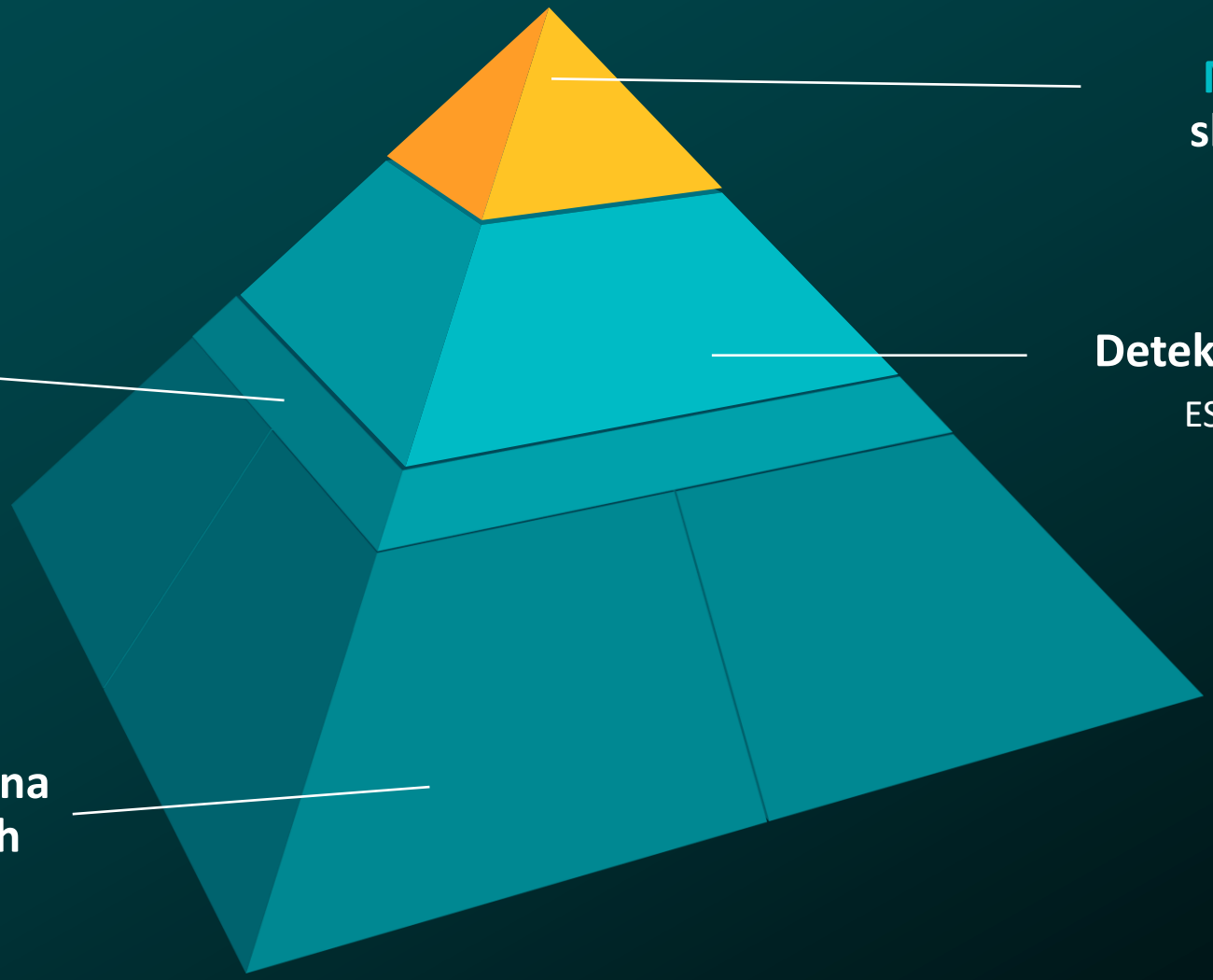
PREVENCIA



REAKCIA

DETEKCIA

VIACÚROVŇOVÉ ZABEZPEČENIE

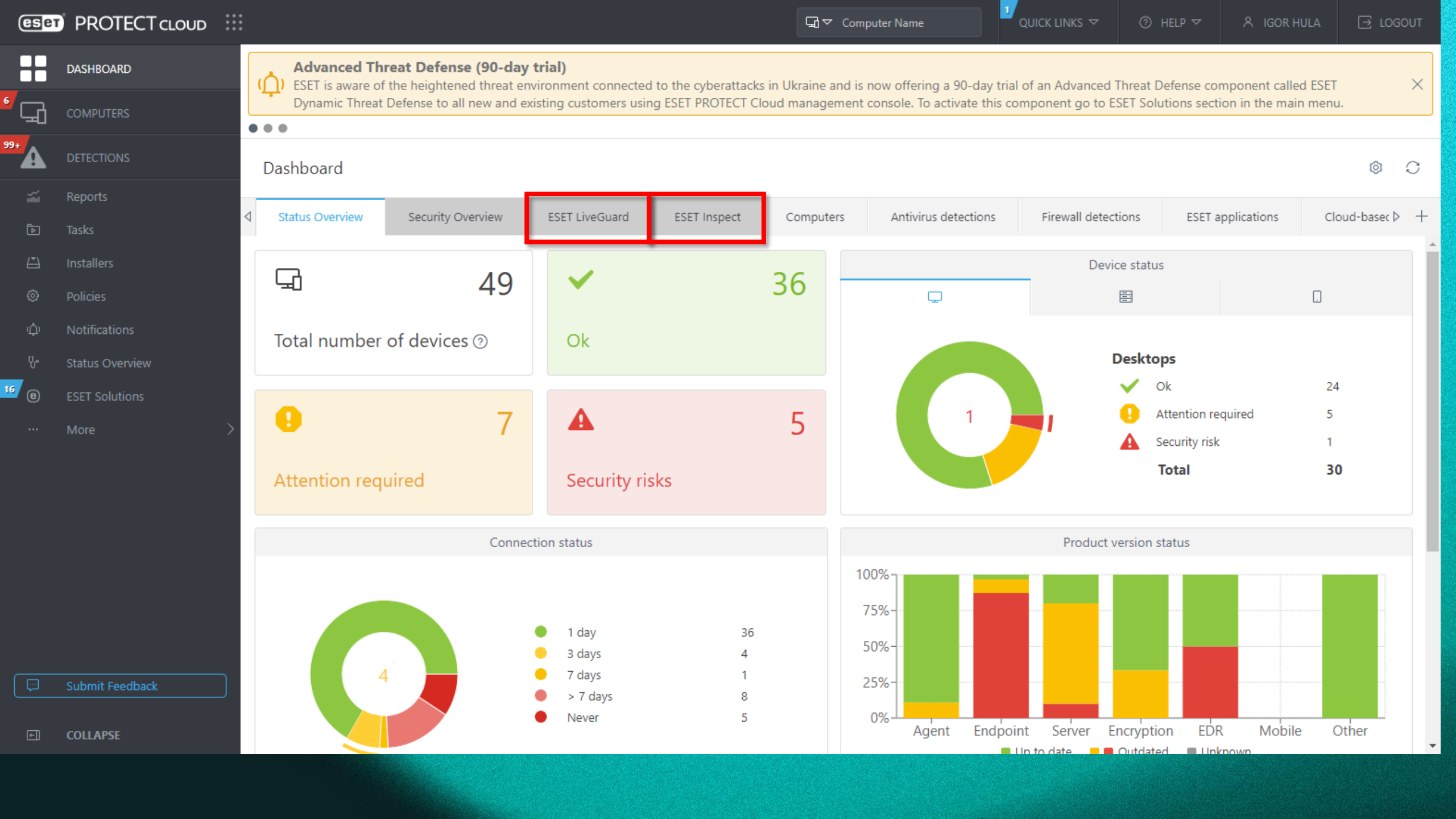


MDR
služby

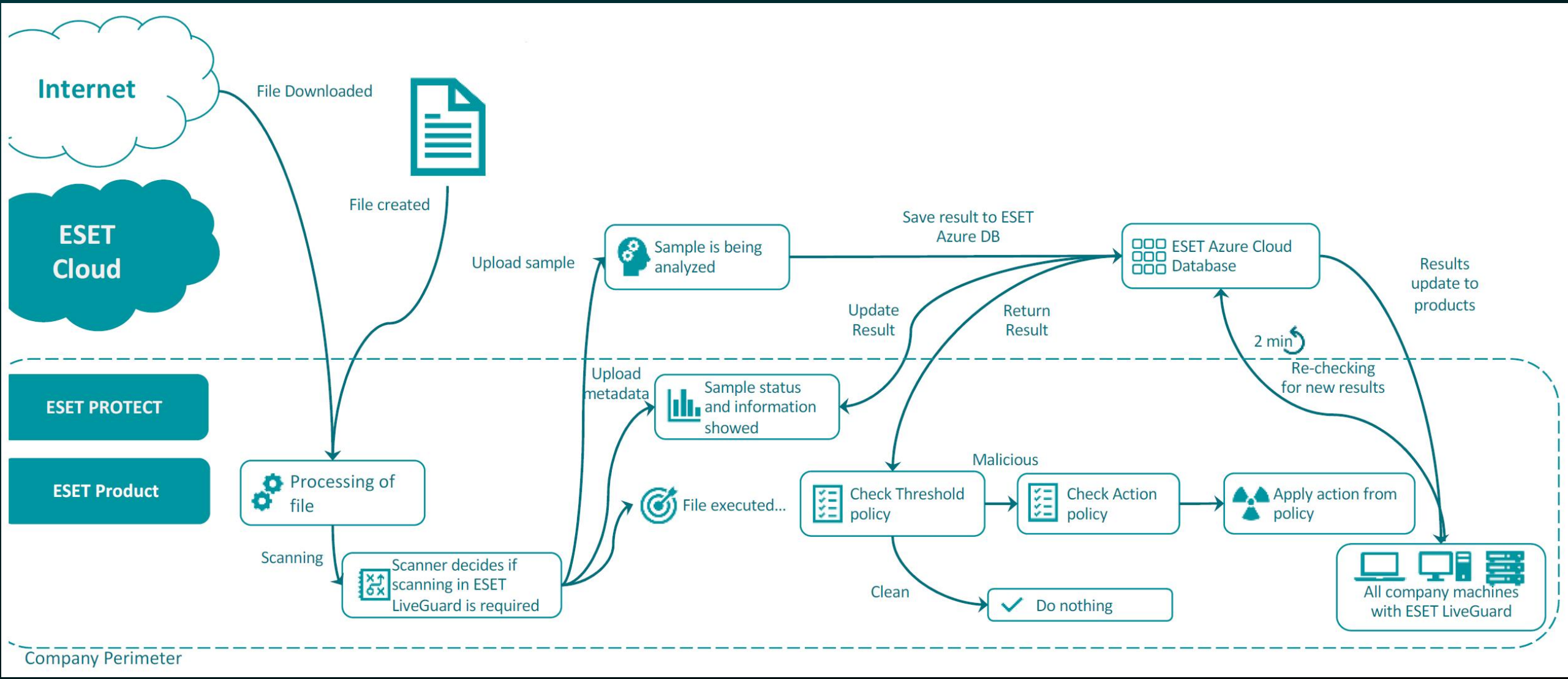
XDR
Detekcia a Reakcia
ESET Inspect

Analýza v cloudovom sandboxe
ESET LiveGuard Advanced

XDR platforma
Viacvrstvová ochrana na všetkých platformách
ESET PROTECT


PROTECT CLOUD
Computer Name
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Advanced Threat Defense (90-day trial)
ESET is aware of the heightened threat environment connected to the cyberattacks in Ukraine and is now offering a 90-day trial of an Advanced Threat Defense component called ESET Dynamic Threat Defense to all new and existing customers using ESET PROTECT Cloud management console. To activate this component go to ESET Solutions section in the main menu.
Dashboard
Status Overview
Security Overview
ESET LiveGuard
ESET Inspect
Computers
Antivirus detections
Firewall detections
ESET applications
Cloud-basec
49
Total number of devices
36
Ok
7
Attention required
5
Security risks
Device status
1
Desktops
Ok 24
Attention required 5
Security risk 1
Total 30
Connection status
4
1 day 36
3 days 4
7 days 1
> 7 days 8
Never 5
Product version status
100%
75%
50%
25%
0%
Agent
Endpoint
Server
Encryption
EDR
Mobile
Other
Up to date
Outdated
Unknown

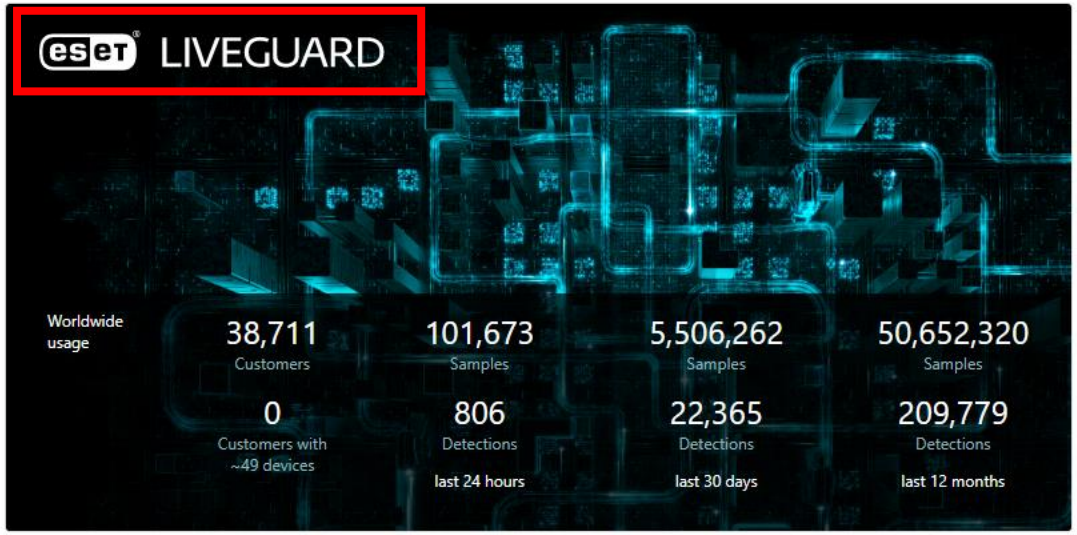
VIACÚROVŇOVÉ ZABEZPEČENIE



DASHBOARD
COMPUTERS
DETECTIONS
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE

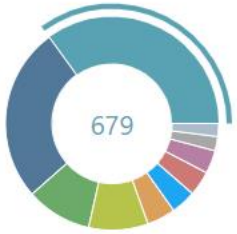
Dashboard

Status Overview | Security Overview | ESET LiveGuard | ESET Inspect | Computers | Antivirus detections | Firewall detections | ESET applications | Cloud-based protection



Analyzed samples & results

Top computers submitting files



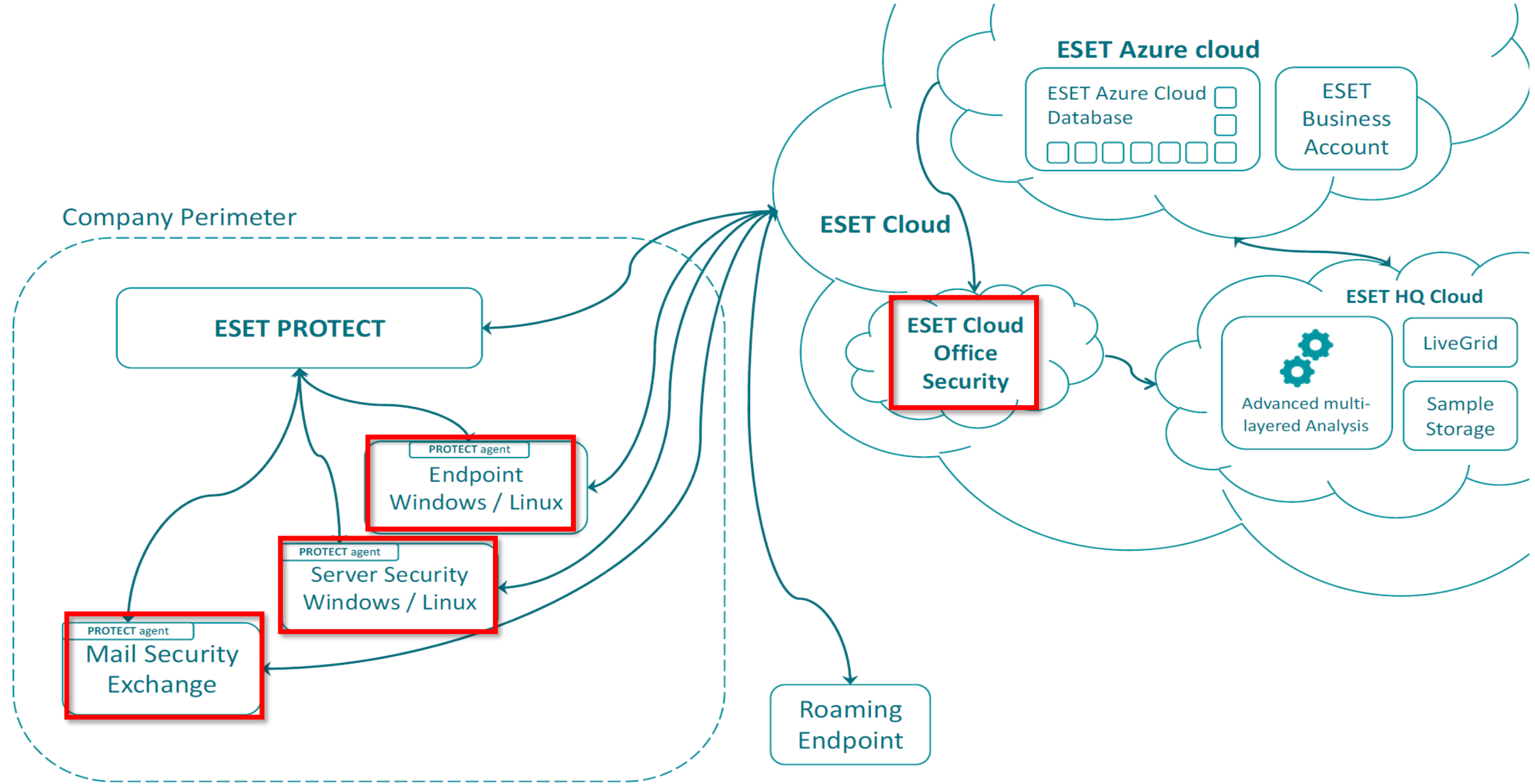
msi-JNK	679
DW-S-NEW	514
AD-S	193
desktop-k0ngpps	175
VLST-NB	84
hb-c-e05	73
dark-nb	73
dw-hp-01	68
SERVER-NEW	42
Ab-c-e01	38

Top computers with detections

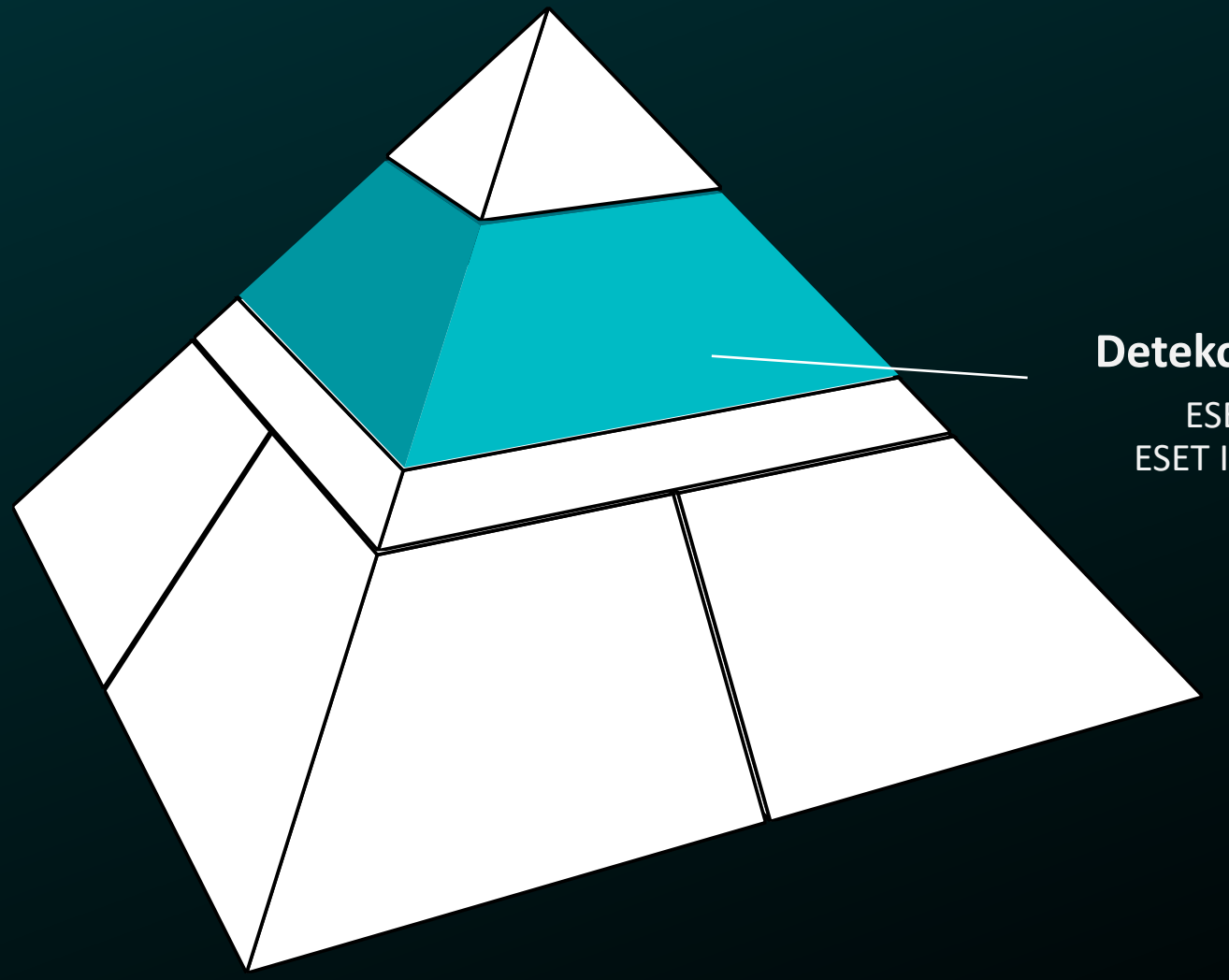
Ab-c-e01	8
hb-c-e03	3
msi-JNK	2

File types submitted

File types detected


ESET Azure cloud
ESET Azure Cloud Database
ESET Business Account
ESET Cloud
ESET Cloud Office Security
ESET HQ Cloud
Advanced multi-layered Analysis
LiveGrid
Sample Storage
Company Perimeter
ESET PROTECT
PROTECT agent
Endpoint Windows / Linux
PROTECT agent
Server Security Windows / Linux
PROTECT agent
Mail Security Exchange
Roaming Endpoint

VIACÚROVŇOVÉ ZABEZPEČENIE



XDR

Detekcia a Reakcia

ESET Inspect
ESET Inspect Cloud

FEATURED

Cyberattacks in Ukraine

Cyberattacks in Ukraine

HermeticWiper
deployed

23 Feb 2022

24 Feb 2022

Russian invasion
of Ukraine

Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

HermeticWiper

100s

systems

5+

organizations

Dec 28, 2021

compilation timestamp

Cyberattacks in Ukraine

HermeticWiper
deployed

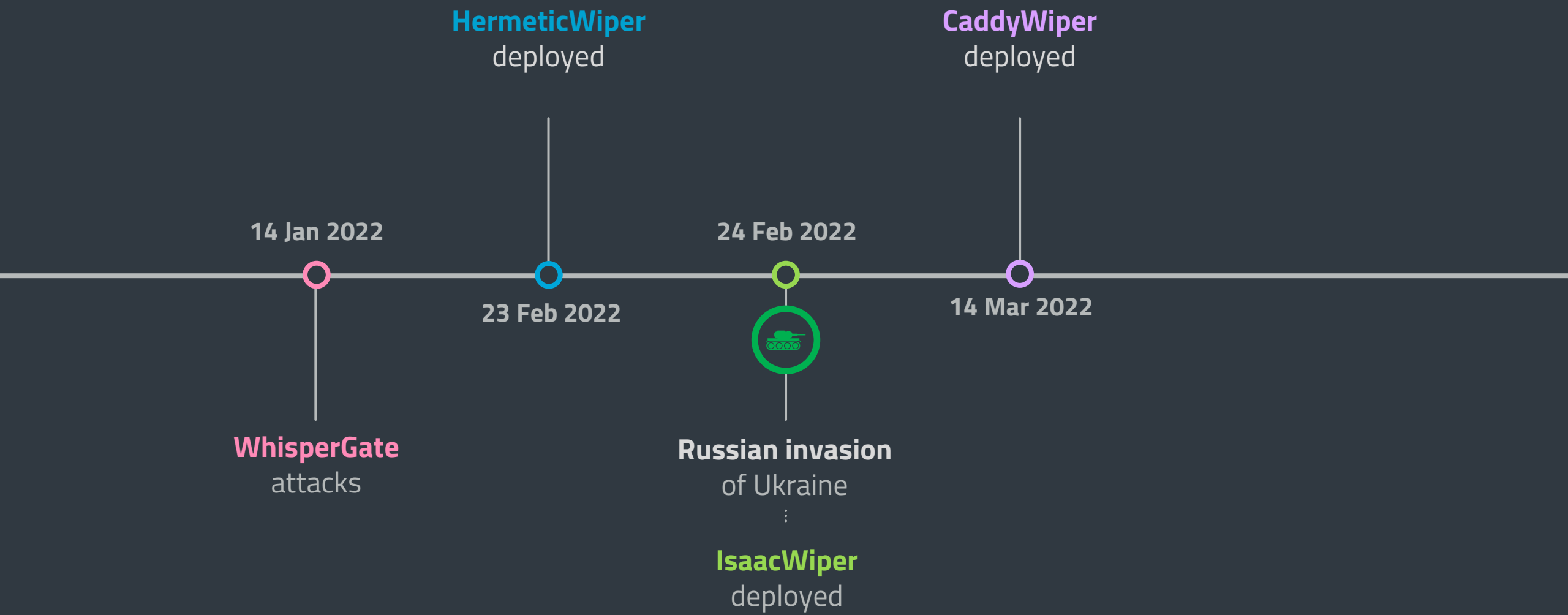
23 Feb 2022

24 Feb 2022

Russian invasion
of Ukraine

Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

Cyberattacks in Ukraine



Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

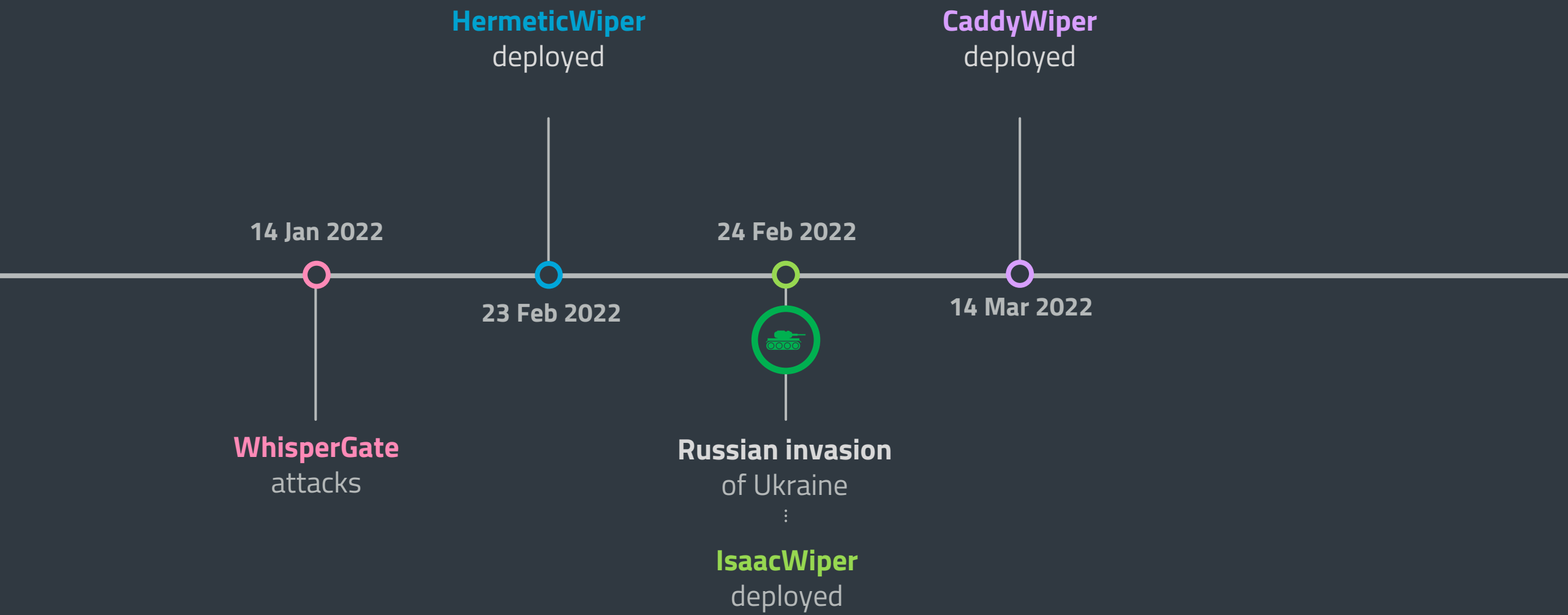
CaddyWiper

Dozens of systems

Targeted financial sector

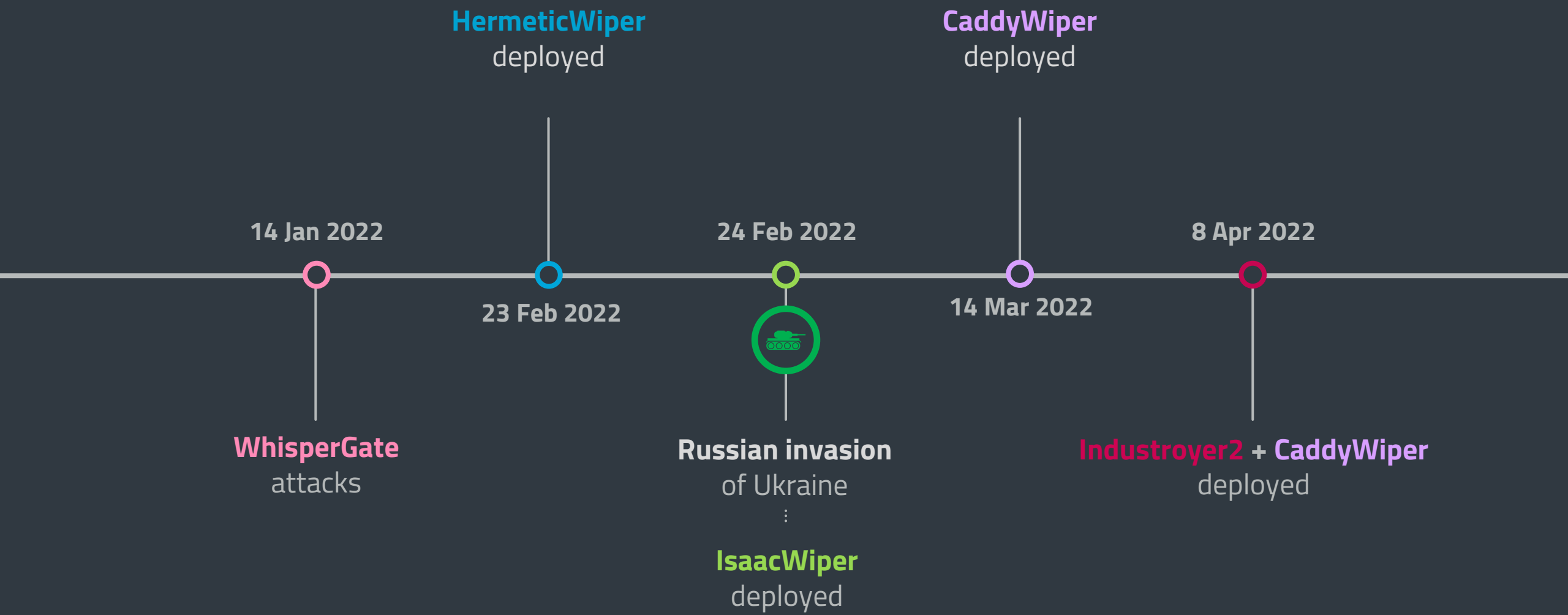
Technically advanced wiper

Cyberattacks in Ukraine



Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

Cyberattacks in Ukraine



Timeline of the attacks detected by ESET researchers around the time of the Russian invasion of Ukraine

Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

12.04.2022

ШПЗ

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA вжито

За темою «ШПЗ»

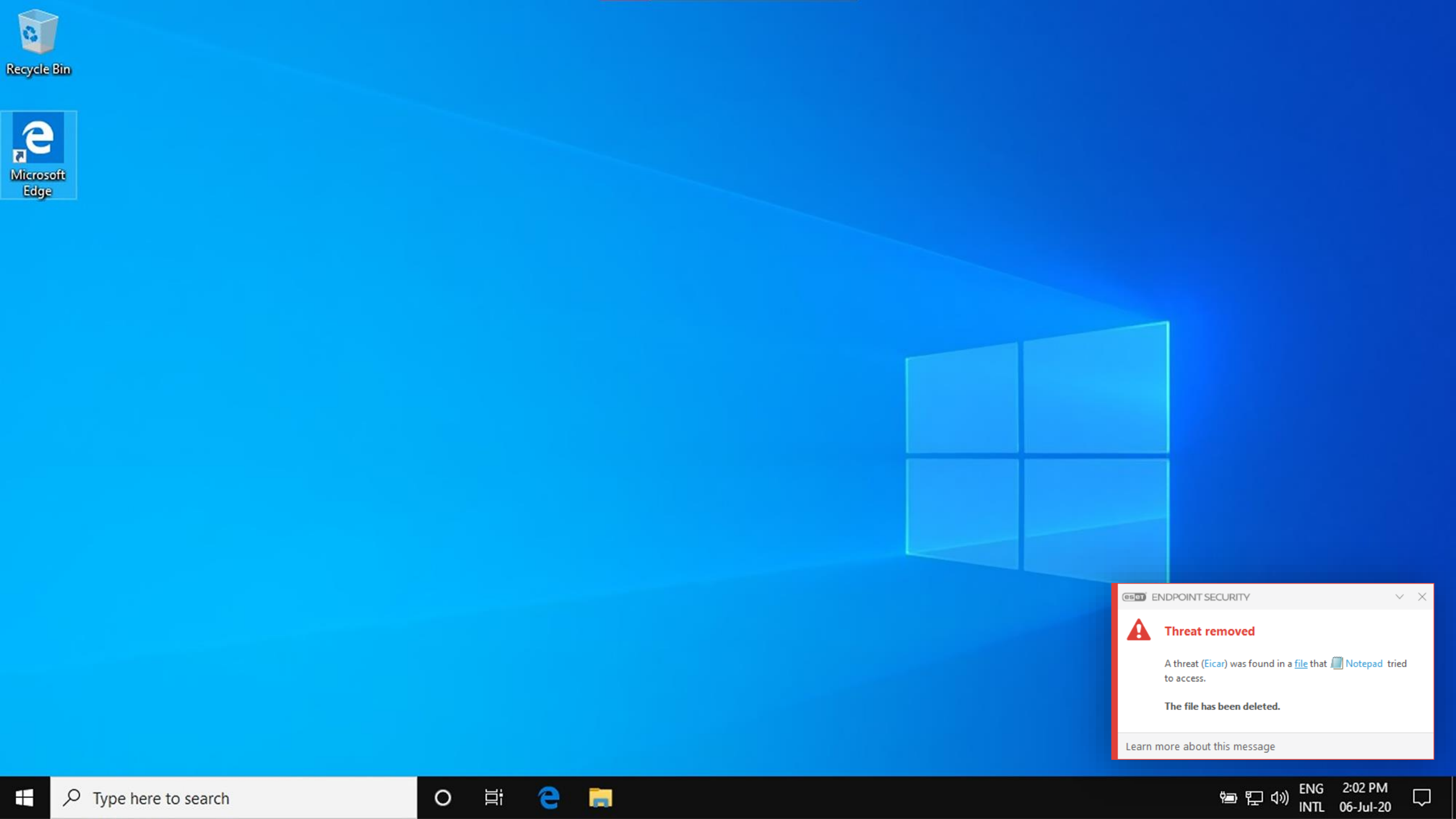
18.04.2022

after its historic cyberattacks on the Ukrainian power grid in 2015 and 2016, still the only confirmed blackouts known to have been caused by hackers.

ESET and CERT-UA say the malware was planted on target systems within a regional Ukrainian energy firm on Friday. CERT-UA says that the attack was successfully detected in progress and stopped before any actual blackout could be triggered. But an earlier, private advisory from CERT-UA last week, first reported by *MIT Technology Review* today, stated that power had been temporarily switched off to nine electrical substations.

Both CERT-UA and ESET declined to name the affected utility. But more than 2 million people live in the area it serves, according to Farid Safarov, Ukraine's deputy minister of energy.

"The hack attempt did not affect the provision of electricity at the power company. It was promptly detected and mitigated," says Viktor Zhora, a senior official at Ukraine's cybersecurity agency, known as the State Services for Special Communication and Information Protection (SSSCIP). “But the intended disruption was huge.” Asked about the earlier report that seemed to describe an attack that was at least partially successful, Zhora described it as a "preliminary report" and stood by his and CERT-UA's most recent public statements.


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?

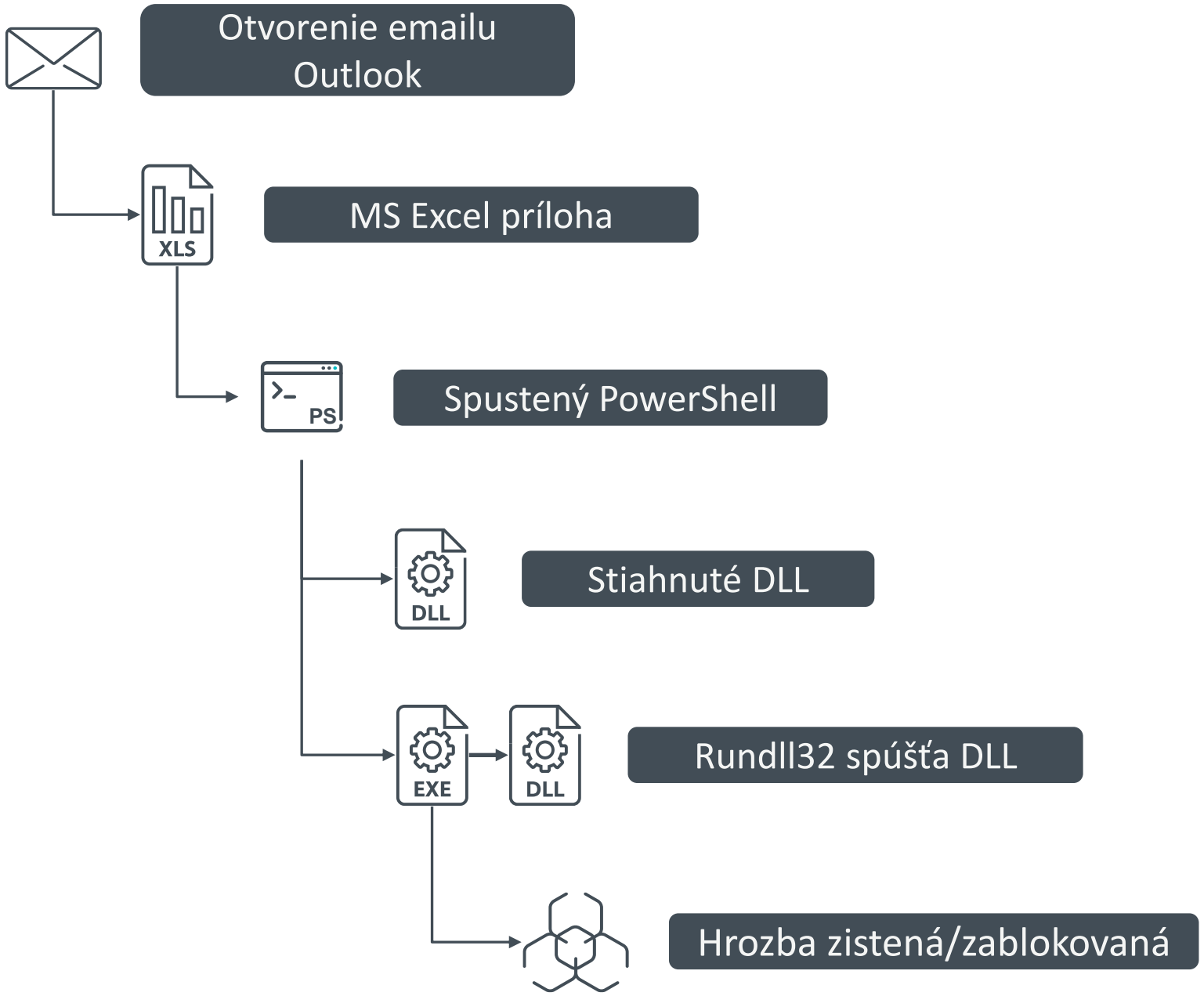
Ako sa to začalo?
Kde sa to začalo?
Kedy sa to začalo?
Čo to obsahuje?
Ako tomu vieme predísť?

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

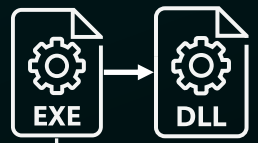

Extended Detection
& Response


Otvorenie emailu Outlook
XLS
MS Excel príloha
PS
Spustený PowerShell
DLL
Stiahnuté DLL
EXE
DLL
Rundll32 spúšťa DLL
Hrozba zistená/zablokovaná

Bez podpory XDR - ESET Inspect

Minimálna vizibilita

Neistota



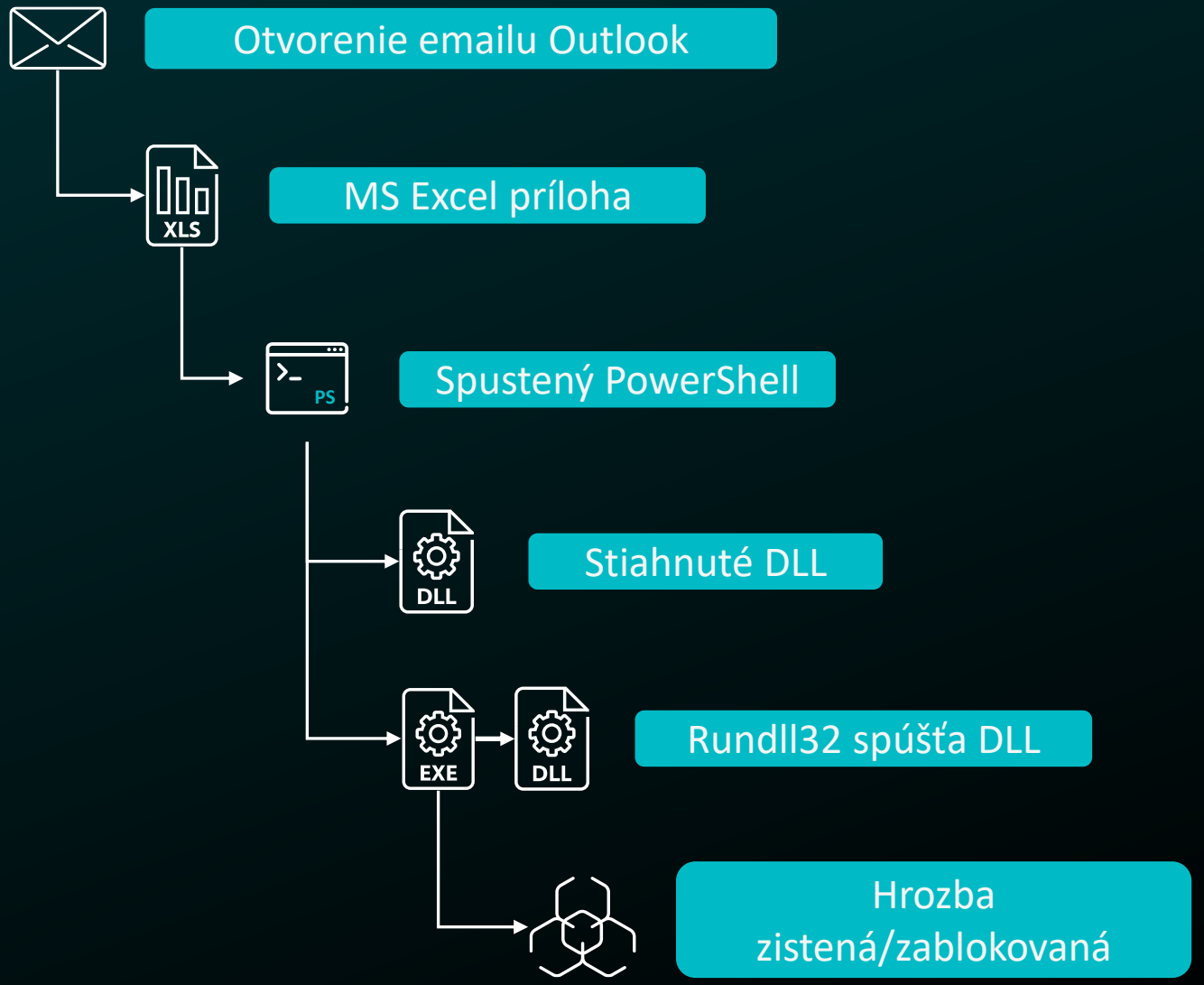
Rundll32 spúšťa DLL

Hrozba zistená/zablokovaná

S podporou XDR - ESET Inspect

Zvýšená viditeľnosť

Pokoj v duši :)



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

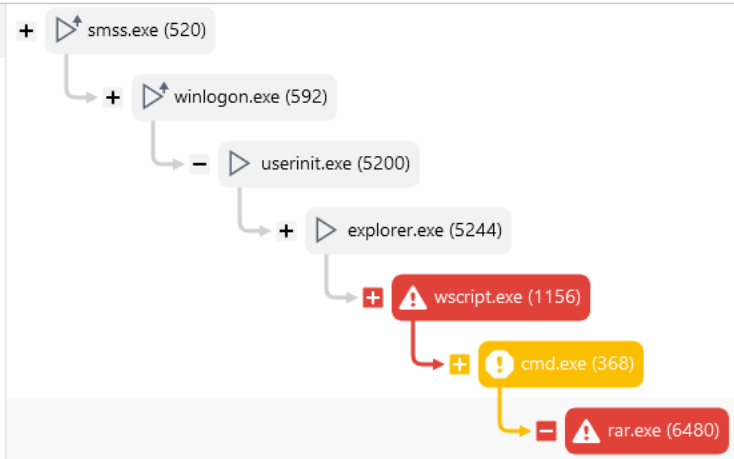
File	Registry	Network
4	0	0

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]


Extended Detection
& Response

XDR – “R” ako Reakcia

Blokovanie Hash
Ukončenie procesu

Spustenie skenovania
Stiahnutie súboru

Reštartovanie
Vypnutie

Sieťová izolácia

Vzdialený prístup PowerShell

Prečo XDR?

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

Možnosti riešenia

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

LockBit 3.0 introduces the first ransomware bug bounty program

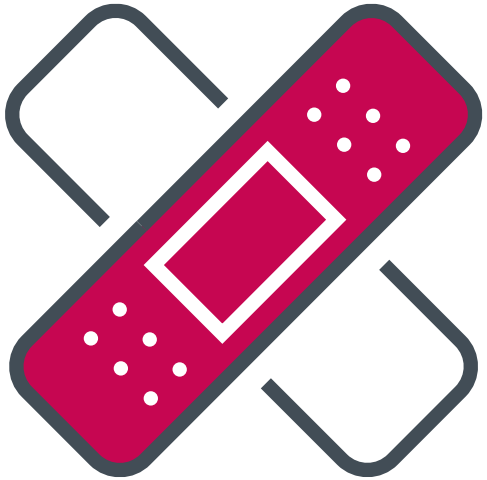
By Lawrence Abrams

June 27, 2022 11:09 AM 0

The LockBit ransomware operation has released 'LockBit 3.0,' introducing the first ransomware bug bounty program and leaking new extortion tactics and Zcash cryptocurrency payment options.

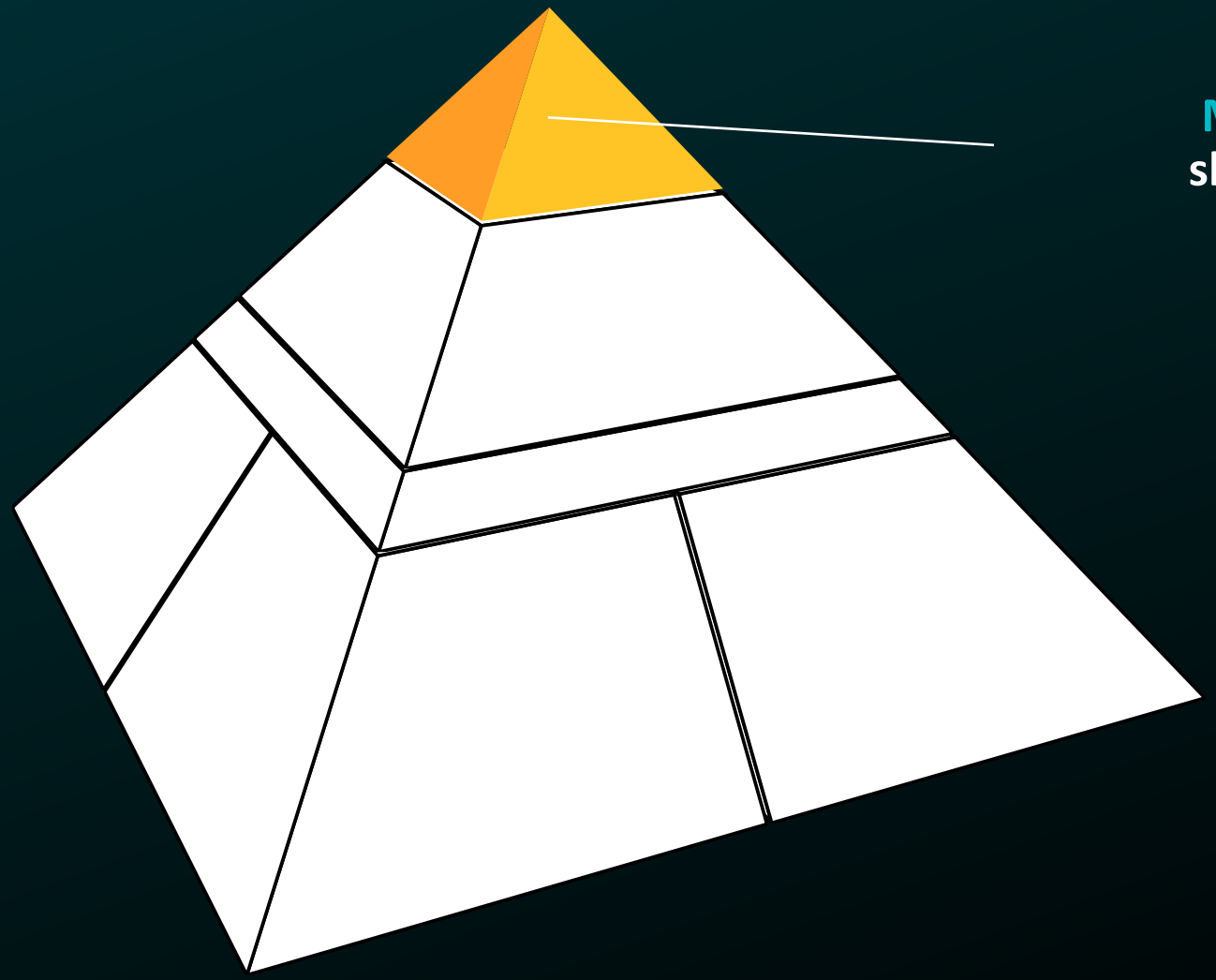
The ransomware operation launched in 2019 and has since grown to be the most prolific ransomware operation, accounting for 40% of all known ransomware attacks in May 2022.

Over the weekend, the cybercrime gang released a revamped ransomware-as-a-service (RaaS) operation called LockBit 3.0 after beta testing for the past two months, with the new version already used in attacks.



$1,000-$1,000,000

VIACÚROVŇOVÉ ZABEZPEČENIE



MDR
služby

Prečo MDR?

Potenciálne problémy

Komplexnosť nástroja

Viacero upozornení

Nedostatok kvalifikovaných IT špecialistov

Obmedzený čas na monitorovanie hrozieb v XDR

Problémy vyriešené vďaka MDR

Komplexnosť nástroja

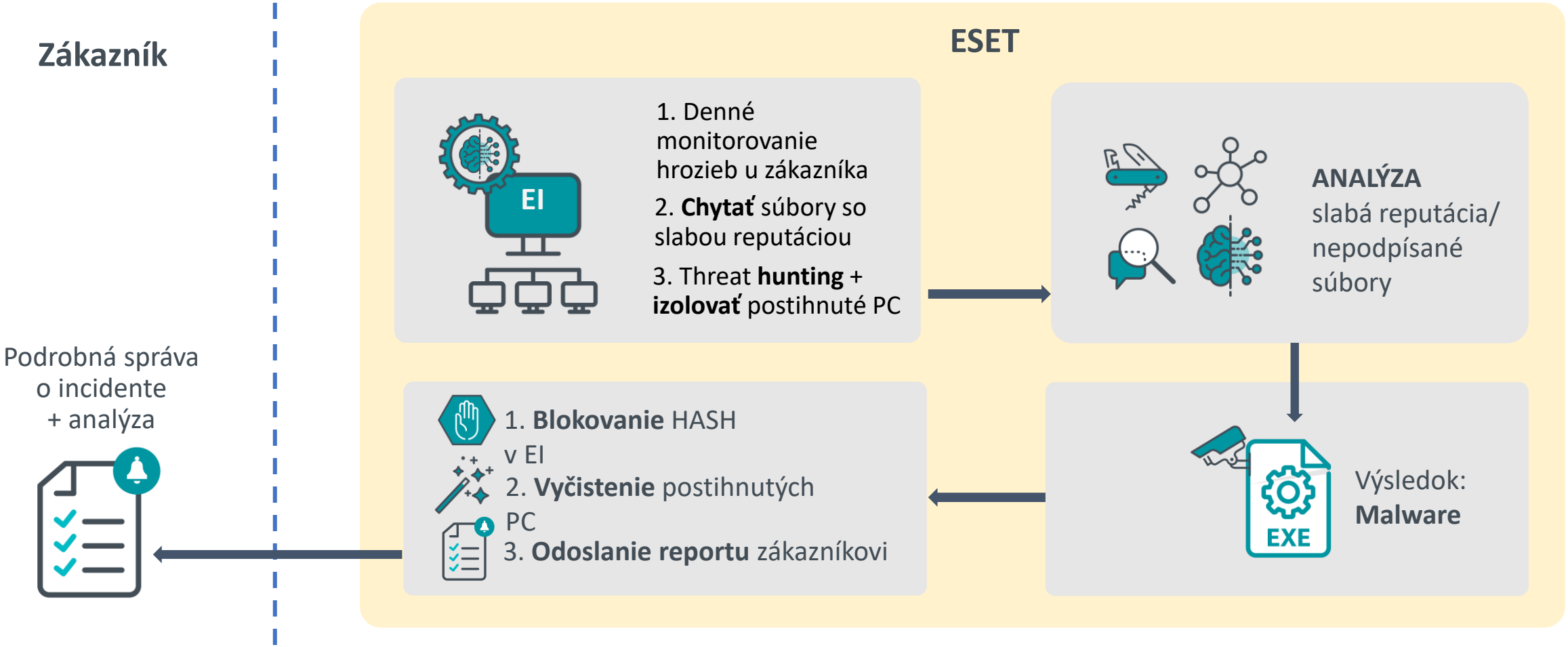
Viacero upozornení

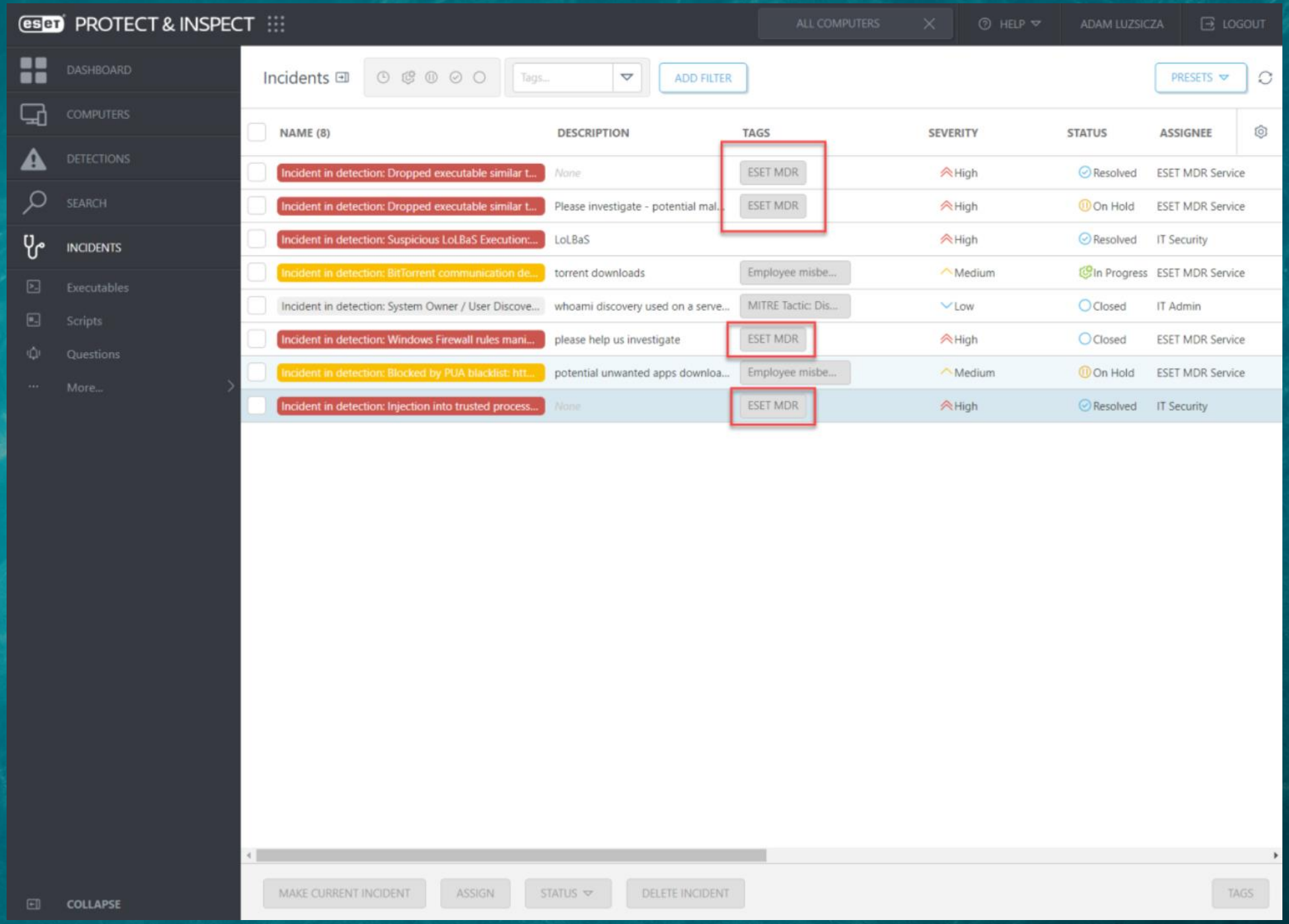
Nedostatok kvalifikovaných IT špecialistov

Obmedzený čas na monitorovanie hrozieb v XDR

MANAGED DETECTION & RESPONSE

- Plne monitorovaná bezpečnostná služba pre zákazníkov **ESET Inspect.**





Digital Security
Progress. Protected.

ESET PROTECT MDR

		ESET PROTECT MDR
Základné komponenty	Platforma ESET PROTECT	●
	Moderná ochrana koncových zariadení	●
	Zabezpečenie súborových serverov	●
	Pokročilá ochrana pred hrozbami	●
	Šifrovanie celého disku	●
	Ochrana e-mailovej komunikácie	◐
	Ochrana cloudových aplikácií	◐
	Detekcia a reakcia	●
Voliteľné riešenia	Zabezpečenie SharePointu	◐
	Šifrovanie koncových zariadení	◐
	Overovanie	◐
Služby	Doplnková technická podpora	●
	ESET Premium Support Advanced	●
	ESET Deployment & Upgrade	●
	ESET Security Services	●
	ESET Managed Detection & Response	●

- Urýchlite detekciu, kontrolu a nápravu kybernetických bezpečnostných incidentov s odbornými znalosťami ESET špecialistov pomocou služby **Managed Detection and Response (MDR)**.
- Rýchla pomoc od spoločnosti ESET v ktorúkoľvek dennú alebo nočnú hodinu, vrátane víkendov a štátnych sviatkov
- Jedinečné správanie a **detekcia založená na reputácii**, ktorá je plne transparentná pre bezpečnostné tímy. Poskytuje spätnú väzbu v reálnom čase získanú z viac ako 100 miliónov koncových bodov v našom LiveGrid.
- Vylepšená ochrana pred ransomware a zero-day hrozbami prostredníctvom **cloudovej sandbox technológie**.

KATEGÓRIE SLUŽIEB

PROFESIONÁLNE SLUŽBY

- ✓ Riešenie problémov s ESET produktami
- ✓ Prioritná a garantovaná technická podpora (SLA)
- ✓ Inštalácia a konfigurácia ESET produktov
- ✓ Kontrola nastavení a odporúčania

BEZPEČNOSTNÉ SLUŽBY

- ✓ Analýza podozrivých súborov
- ✓ Pomoc pri reakcii na malvérové incidenty
- ✓ Bezpečnostná podpora pre ESET Inspect
- ✓ Threat monitoring / Threat hunting

ESET
PROFESIONÁLNE
SLUŽBY

ESET ŠTANDARDNÁ TECHNICKÁ PODPORA

	ŠTANDARDNÁ PODPORA
Časový limit odpovede na kritické incidenty (A)	podľa dostupnosti
Časový limit odpovede na závažné incidenty (B)	podľa dostupnosti
Časový limit odpovede na bežné požiadavky (C)	podľa dostupnosti
Dostupnosť technickej podpory	8:00 – 18:30 len v pracovných dňoch
Kontaktné osoby na strane zákazníka	obmedzené

ESET PREMIUM SUPPORT ADVANCED

	ŠTANDARDNÁ PODPORA	ESET PREMIUM SUPPORT ESSENTIAL	ESET PREMIUM SUPPORT ADVANCED
Časový limit odpovede na kritické incidenty (A)	podľa dostupnosti	2 hodiny	2 hodiny
Časový limit odpovede na závažné incidenty (B)	podľa dostupnosti	4 hodiny	4 hodiny
Časový limit odpovede na bežné požiadavky (C)	podľa dostupnosti	1 pracovný deň	1 pracovný deň
Dostupnosť technickej podpory	8:00 – 18:30 len v pracovných dňoch	nepretržite	nepretržite
Kontaktné osoby na strane zákazníka	obmedzené	neobmedzené	neobmedzené
Priorita v rámci telefonických požiadaviek	✗	áno	áno
Počet žiadostí oprávnených na spracovanie v rámci prémiovej podpory	✗	obmedzené	neobmedzené
Dedikovaný Technical Account Manager	✗	✗	áno
Prioritný prístup k podpore od ESET vývojárskych tímov	✗	✗	áno
Proaktívne informačné služby	✗	✗	áno
ESET Deployment & Upgrade	✗	✗	1
ESET Healthcheck	✗	✗	1

ESET PREMIUM SUPPORT ADVANCED

- zahŕňa **ESET DEPLOYMENT AND UPGRADE**

Služba ESET Deployment

-kompletná inštalácia a počiatočná konfigurácia novo-zakúpených produktov ESET
-rozsah je vyšpecifikovaný v ponuke služby
-cieľom je efektívne a správne nasadenie

Služba ESET Upgrade

-aktualizácia a konfigurácia už predtým nasadených produktov ESET
-rozsah je vyšpecifikovaný v ponuke služby
-cieľom je efektívne a správne nasadenie nových verzií

ESET PREMIUM SUPPORT ADVANCED

- zahŕňa **ESET HEALTHCHECK**

Služba ESET HEALTHCHECK

-kontrola prostredia s nasadenými ESET produktami
-celkové preskúmanie integrácie ESET produkov
-kontrola konfigurácií a nastavení
-dokument s užitočnými radami a odporúčaniami
-cieľom je dosiahnuť optimálne fungovanie produktov

ESET BEZPEČNOSTNÉ SLUŽBY

Digital Security
Progress. Protected.

ESET DETECTION AND RESPONSE ESSENTIAL

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno
	Malvér: problém s liečením	áno	áno
	Malvér: infekcia ransomvérom	áno	áno
	Nesprávna detekcia	áno	áno
	Všeobecné: preskúmanie podozrivého správania	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	✗	áno
	Podrobná analýza súborov	✗	áno
	Digitálna forenzná analýza	✗	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	✗	áno

ESET DETECTION AND RESPONSE ADVANCED

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno
	Nesprávna detekcia	áno	áno	áno
	Všeobecné: preskúmanie podozrivého správania	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	✗	áno	áno
	Podrobná analýza súborov	✗	áno	áno
	Digitálna forenzná analýza	✗	áno	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	✗	áno	áno
Bezpečnostná podpora pre EI	Technická podpora – pravidlá	✗	✗	áno
	Technická podpora – vylúčenia	✗	✗	áno
	Všeobecné: otázky týkajúce sa nástroja EI	✗	✗	áno
	EI: počiatočná optimalizácia	✗	✗	áno
	EI: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	✗	✗	áno

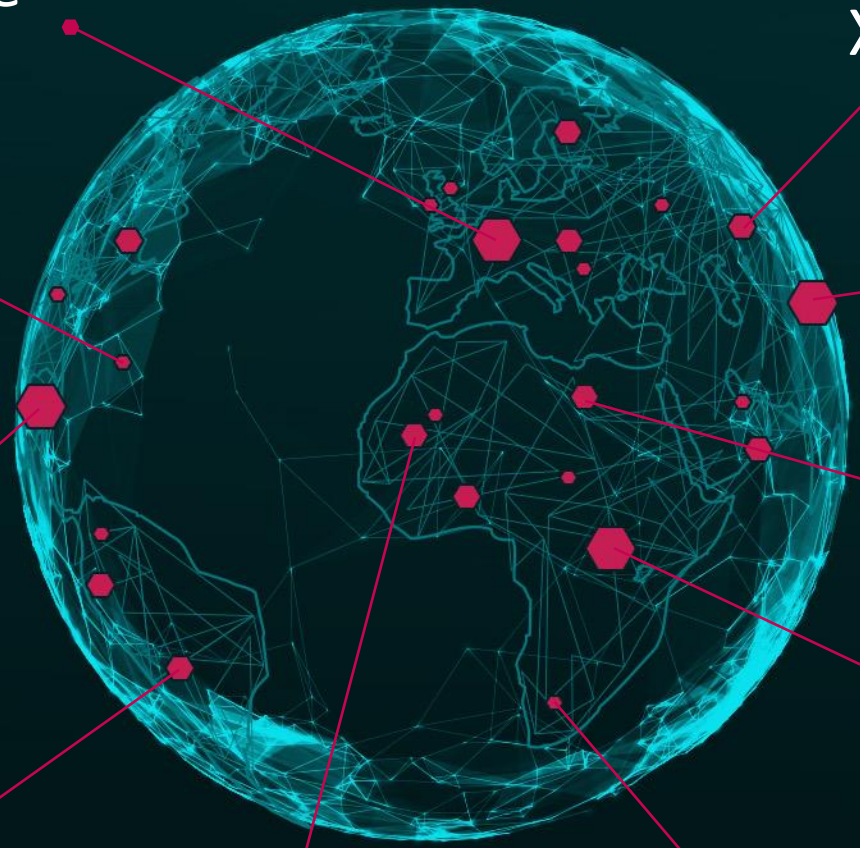
ESET DETECTION AND RESPONSE ULTIMATE

KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno
	Nesprávna detekcia	áno	áno	áno
	Všeobecné: preskúmanie podozrivého správania	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Malvér: nezachytená detekcia	✗	áno	áno
	Malvér: problém s liečením	✗	áno	áno
	Malvér: infekcia ransomvérom	✗	áno	áno
	Nesprávna detekcia	✗	áno	áno
	Všeobecné: preskúmanie podozrivého správania	✗	áno	áno
Bezpečnostná podpora pre EI	Technická podpora – pravidlá	✗	áno	áno
	Technická podpora – vylúčenia	✗	áno	áno
	Všeobecné: otázky týkajúce sa bezpečnostného nástroja EI	✗	áno	áno
	Technická podpora – pravidlá (vyhľadávanie hrozieb na vyžiadanie)	✗	áno	áno
Bezpečnostné služby pre EI	Všeobecné: otázky týkajúce sa nástroja EI	✗	✗	áno
	EI: počiatočná optimalizácia	✗	✗	áno
	EI: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	✗	✗	áno
Profesionálne služby	ESET Deployment & Upgrade	✗	✗	áno

Digital Security
Progress. Protected.

*EI - ESET Inspect (EDR)

Svet sa mení a rovnako aj ESET



Cielené útoky

XDR

Analýza hrozieb

Detekcia správania

Strojové učenie

Ransomware

Bezsúborové útoky

UEFI

IoT

Kybernetická vojna

ĎAKUJEME ZA POZORNOSŤ