



**SECURITY
DAYS**

BEZPEČNOSŤ Z INÉHO UHLA, AKO ESET XDR PLATFORMA POMÁHA CHRÁNIŤ FIREMNÚ INFRAŠTRUKTÚRU

Ondrej Krajč



Digital Security
Progress. Protected.

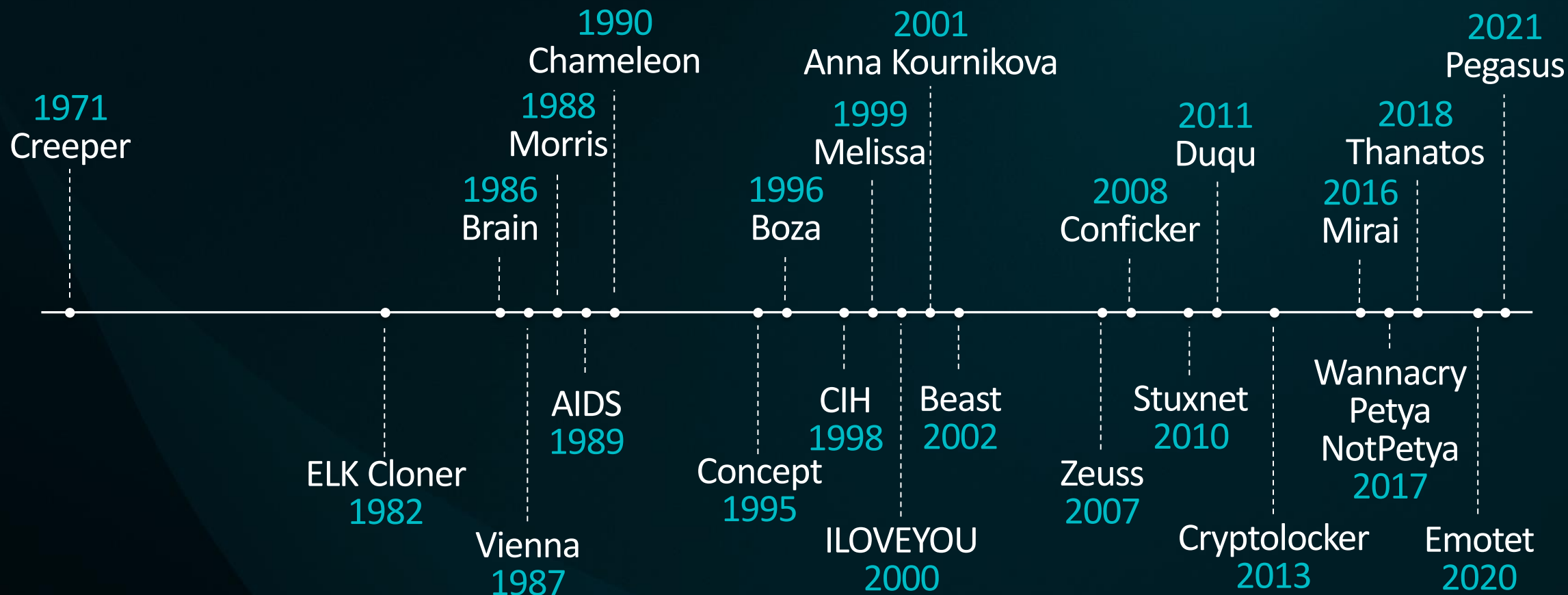
&



konferencie

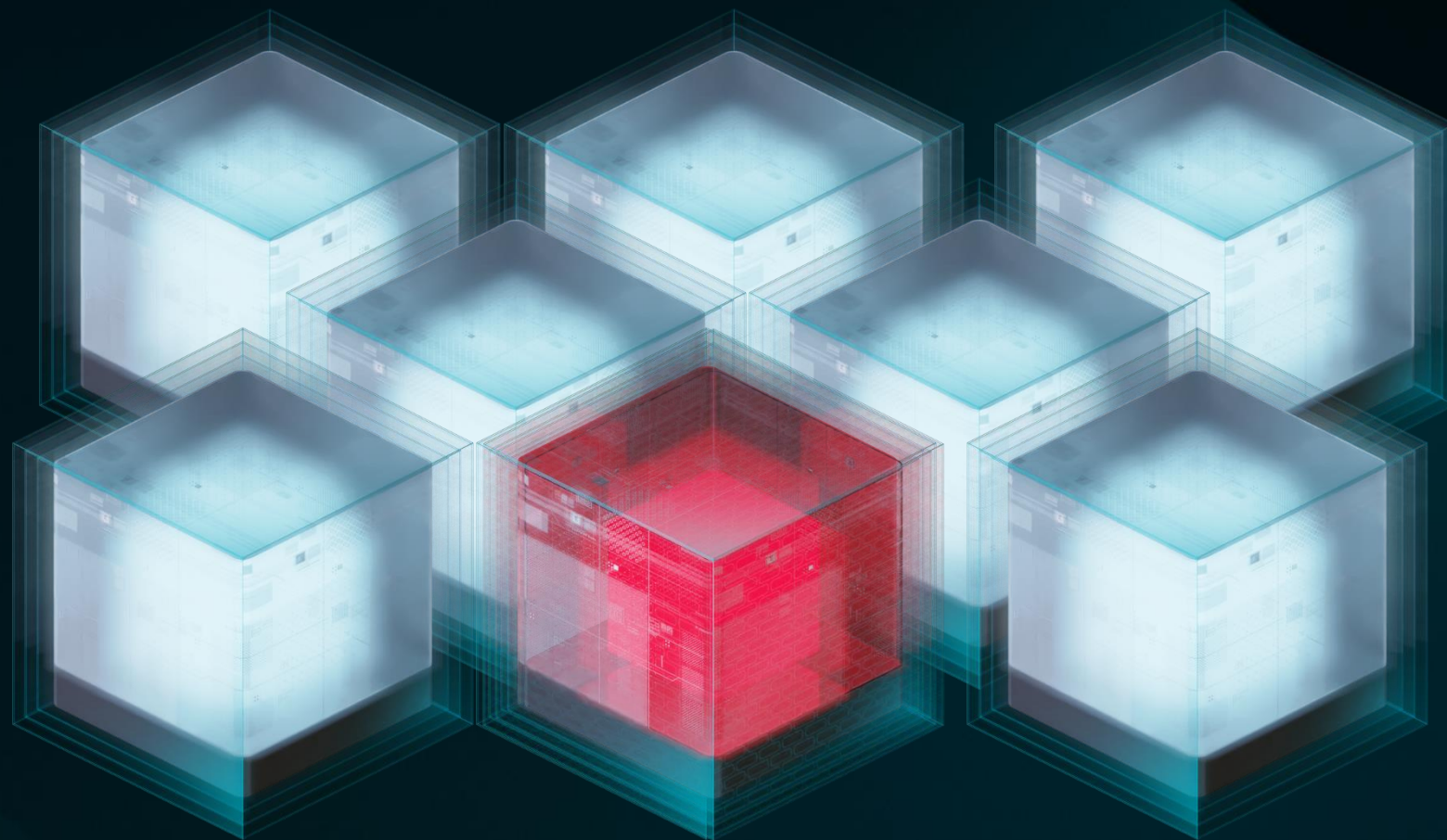
Technológie urýchľujú ľudský pokrok

Vznik nových aspektov trestnej činnosti



Súčasnost'

Éra pokročilých
kybernetických
útokov



PREVENCIA

DETEKCIA

REAKCIA

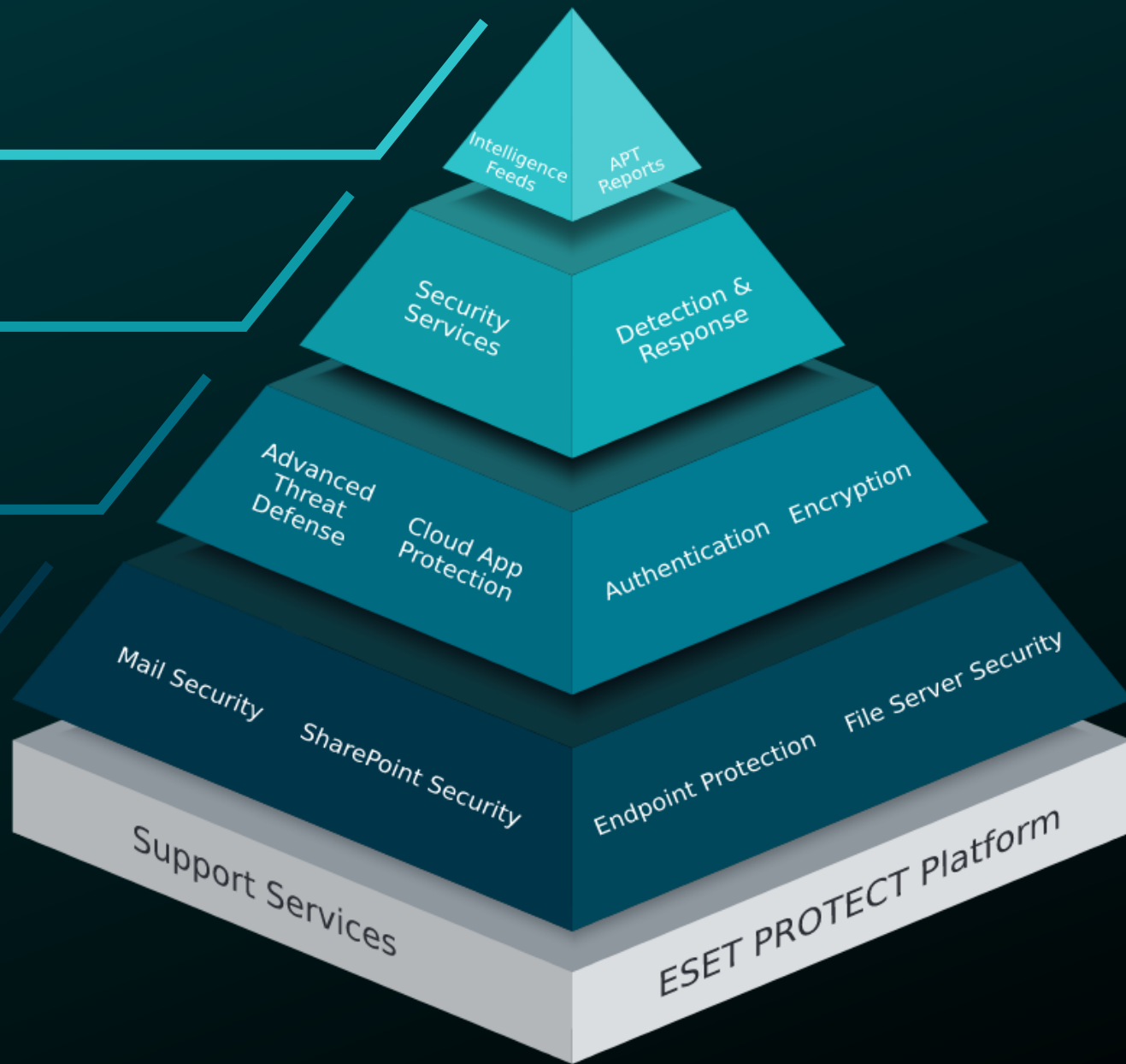
VIACÚROVŇOVÉ ZABEZPEČENIE

INFORMÁCIE O HROZBÁCH

DETEKCIA A REAKCIA

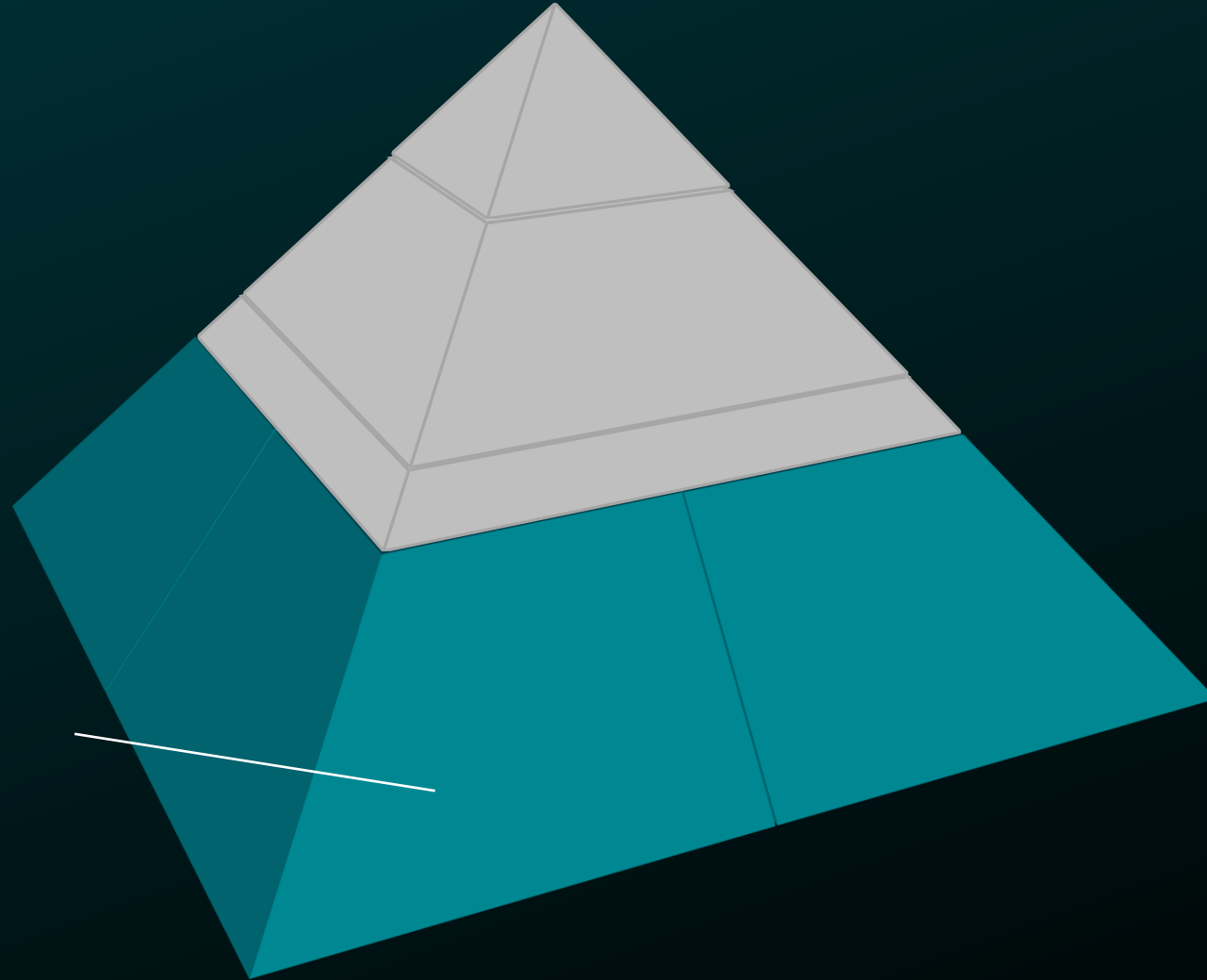
ROZŠÍRENÁ
OCHRANA

ZÁKLADNÁ
OCHRANA



VIACÚROVNŇOVÉ ZABEZPEČENIE

XDR Platforma





Jednotná platforma pre správu
všetkých bezpečnostných riešení ESET



ESET Protect



Plná kontrola nad ESET produktami



LiveGuard



Hardware & Software
Inventory



Automatizácia



Jednoduché rozhranie



Reporting & Notifikácie

Funkcionalita

Úlohy

Politiky

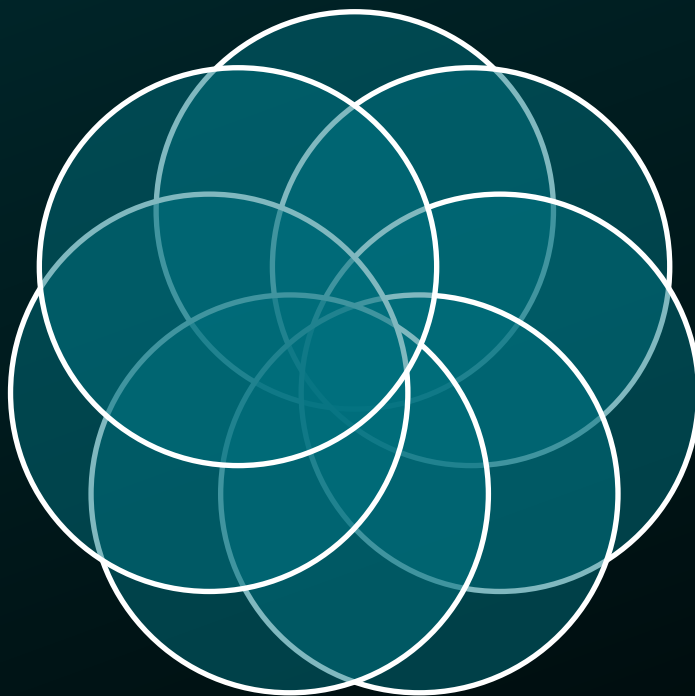
Skupiny

Karanténa

Reporty

HW a SW info

LiveGuard a
Inspect



ESET PROTECT vylepšenia

- Automatické aktualizácie
- Brute-force attack protection management
- Live Guard dashboard
- Rýchly náhľad na PC a detekcie



Automatické aktualizácie

Automatic Product Updates×



Automatic product updates will be enabled in your company network to ensure that you'll always have access to the latest features and achieve the highest possible security.

This change will be enabled for your network from .

To receive product updates automatically, install a product version that supports the auto-update feature.

[Which ESET products and versions support automatic updates?](#)
[I want to install a product version that supports the auto-update feature](#)

[Configure product updates](#)

ENABLE NOW

REMIND ME LATER

Configure product updates

ENABLE NOW

REMIND ME LATER

Brute force attack protection

The screenshot displays the ESET Protect management console. On the left is a sidebar with navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies, Notifications, Status Overview, and More. The main area shows the 'New Policy' screen with tabs for Policies, Basic, Settings, Assign, and Summary. The 'Rules' dialog box is open, showing a list of existing rules and an 'Add rule' sub-dialog.

Rules

Define incoming and outgoing network connections used by the system.

Name
Block RDP brute force attack from a private network
Block RDP brute force attack from any network
Ignore SMB log attempt from a private network
Block SMB brute force attack from any network

Buttons: Add, Edit, Remove

Add rule

Name: Untitled

Enabled: ☒

Action: Allow

Protocol: Remote Desktop Protocol (RDP)

Profile: Any profile

Max attempts: 10

Blacklist retention period (min): 30

Source IP: [Empty text box]

Source zones: [Empty list box]

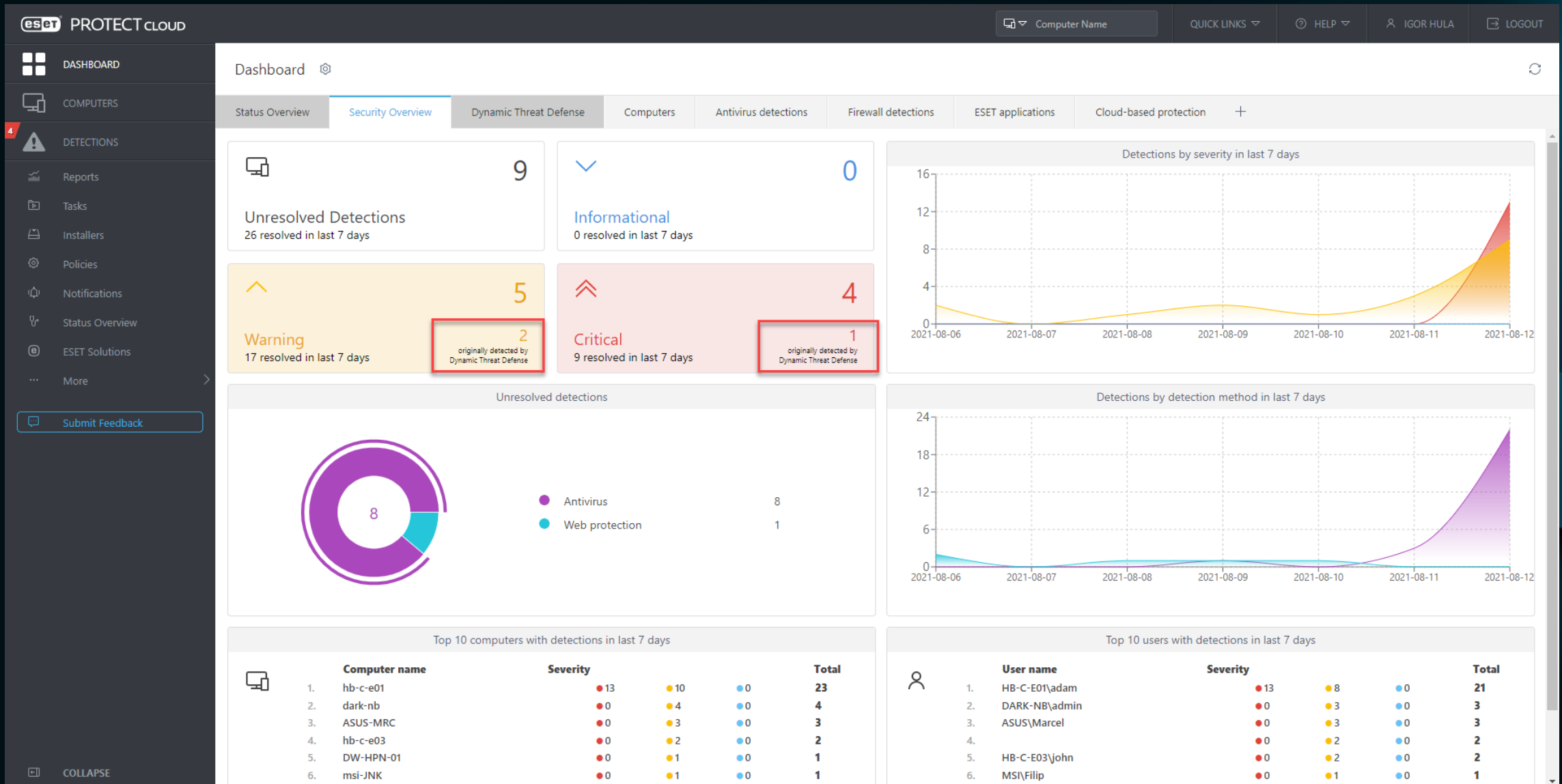
Buttons: Add, Remove, OK

Table (Background)

	Max attempts	Blacklist retention period (min)
1	12	10
2	10	10
3	0	0
4	40	10

Buttons: Save, Cancel

Live Guard dashboard



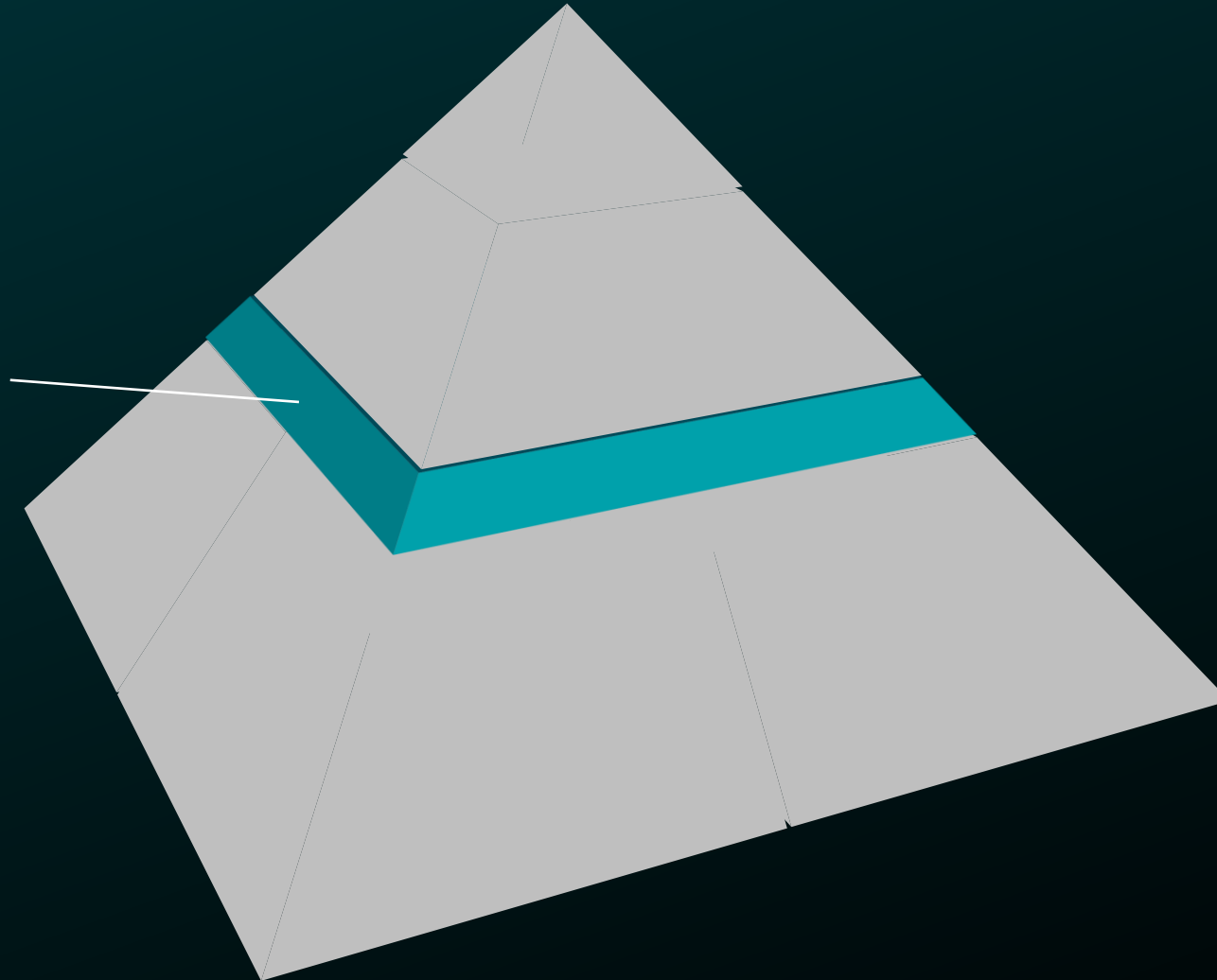
Zvyšné vylepšenia

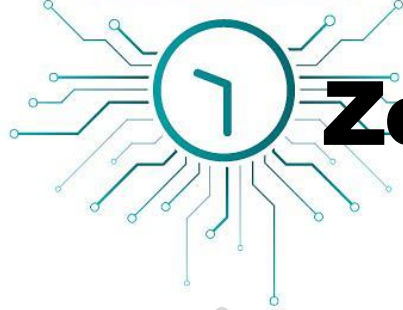
- indikátor posledného pripojenia
- prihlásený užívateľ na PC
- system updates management pre Android
- možnosť vytvoriť spúšťač priamo zo záložky client task details
- verzia Windows OS je reportovaná ako a samostatný symbol (napr. v Dynamických skupinách)
- zoznam analyzovaných súborov ESET LiveGuard Advanced v záložkách detaily počítača
- nové produktové kategórie
- možnosť zrušiť upozornenia v rámci notifikácií pre „muted“ počítače
- podpora Java 17
- nové oprávnenie pre Inspect "Remote Shell Access"

VIACÚROVNŇOVÉ ZABEZPEČENIE

**Analýza v cloudovom
sandboxe**

ESET LiveGuard Advanced





Zero Day Hrozby





LIVEGUARD ADVANCED

Proaktívna ochrana pred doposiaľ neznámymi
a zero-day hrozbami

LiveGuard Advanced

(ESET Dynamic Threat Defense)



Cloudový sandbox

Čo robí LiveGuard

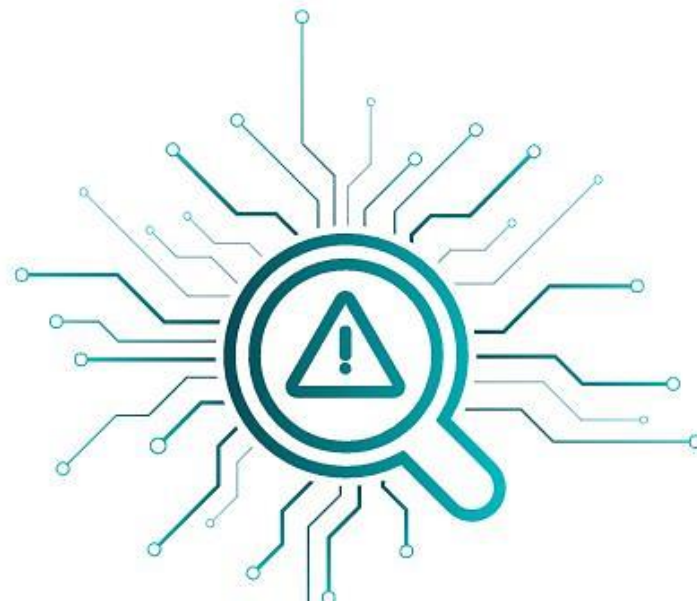
Behaviorálna analýza



Zero-day detekcia



Viacvrstvová ochrana



Fungovanie

Endpoint

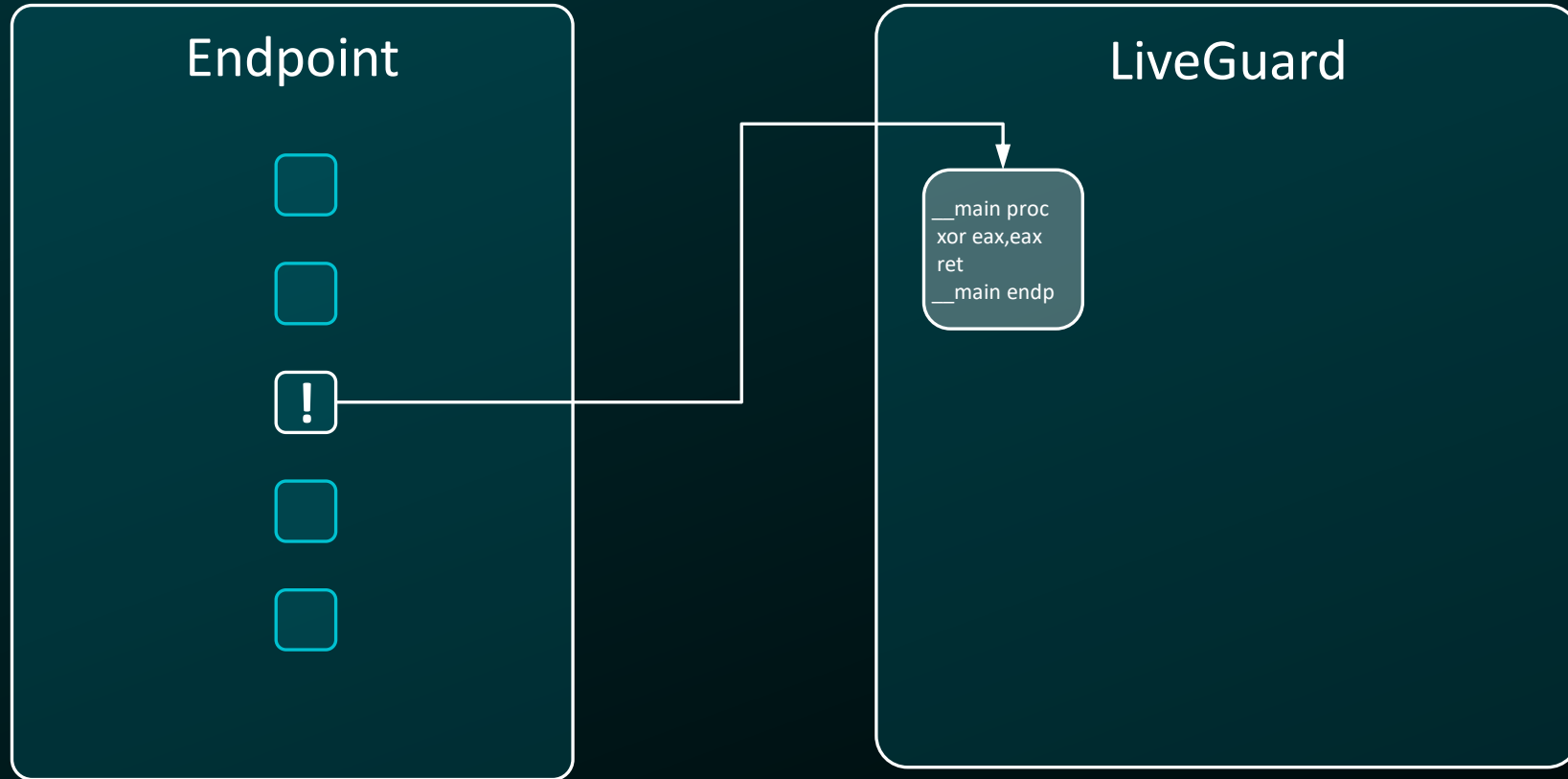
☐☐☐☐☐

Fungovanie

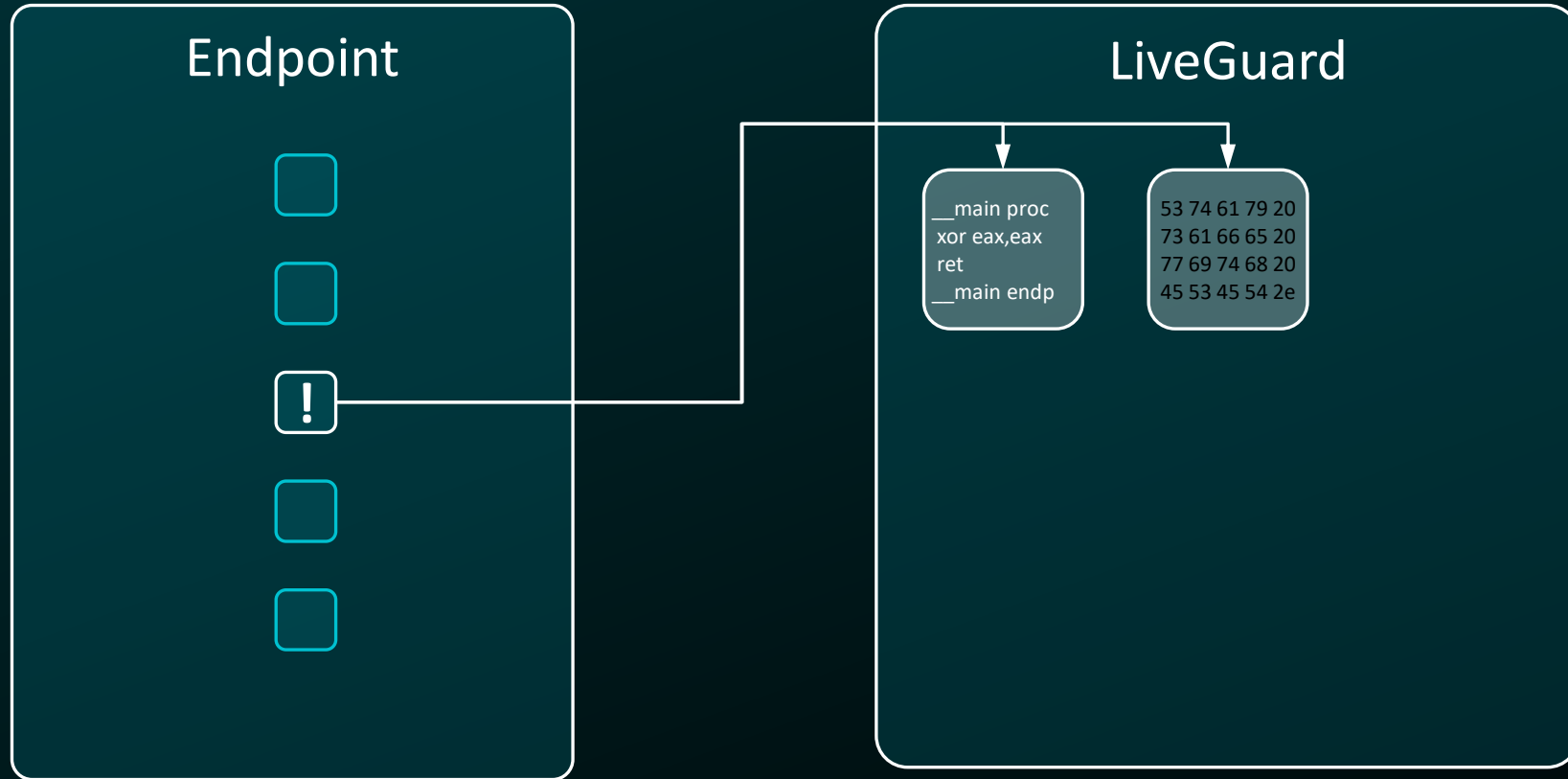
Endpoint



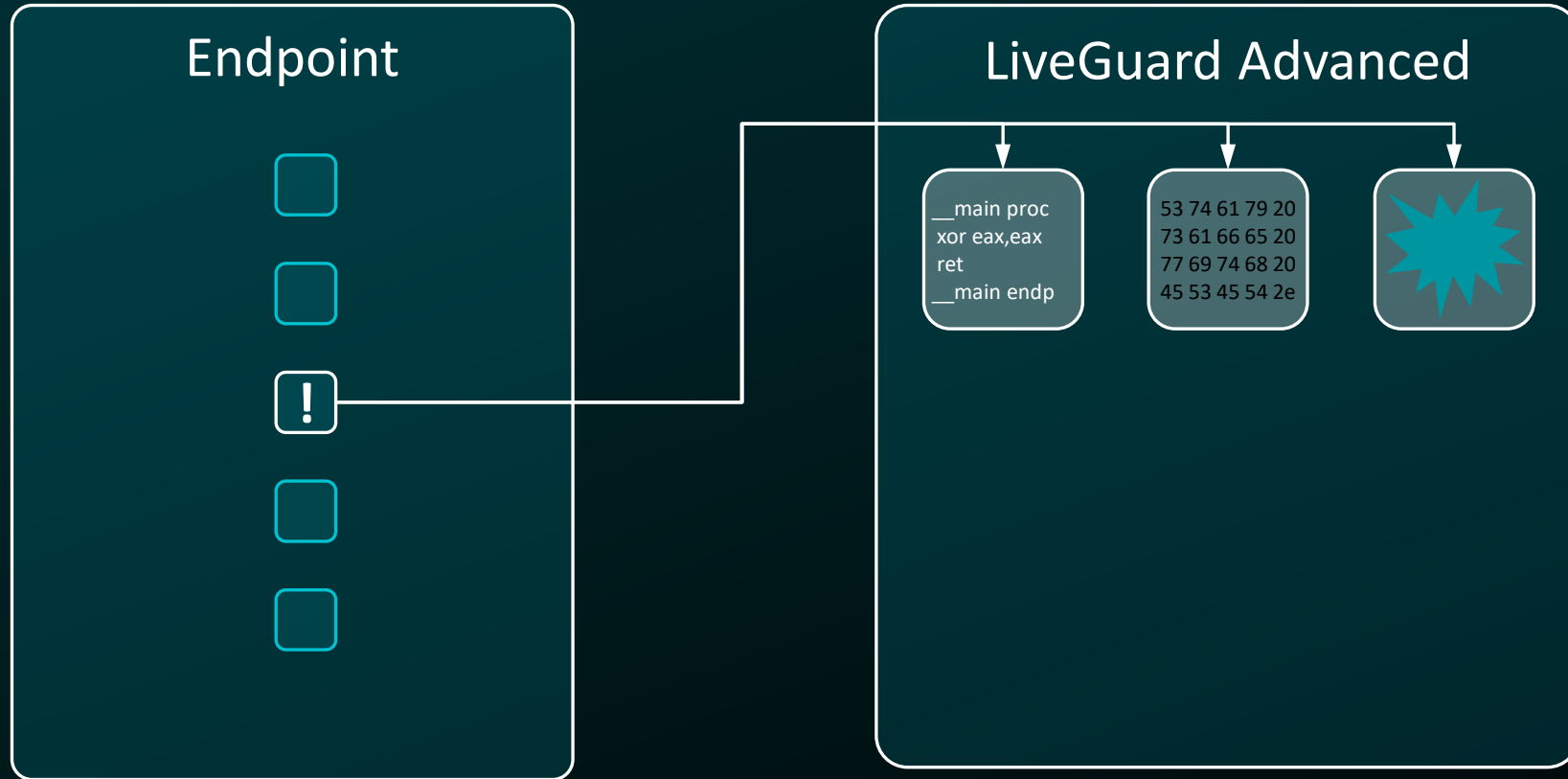
Fungovanie



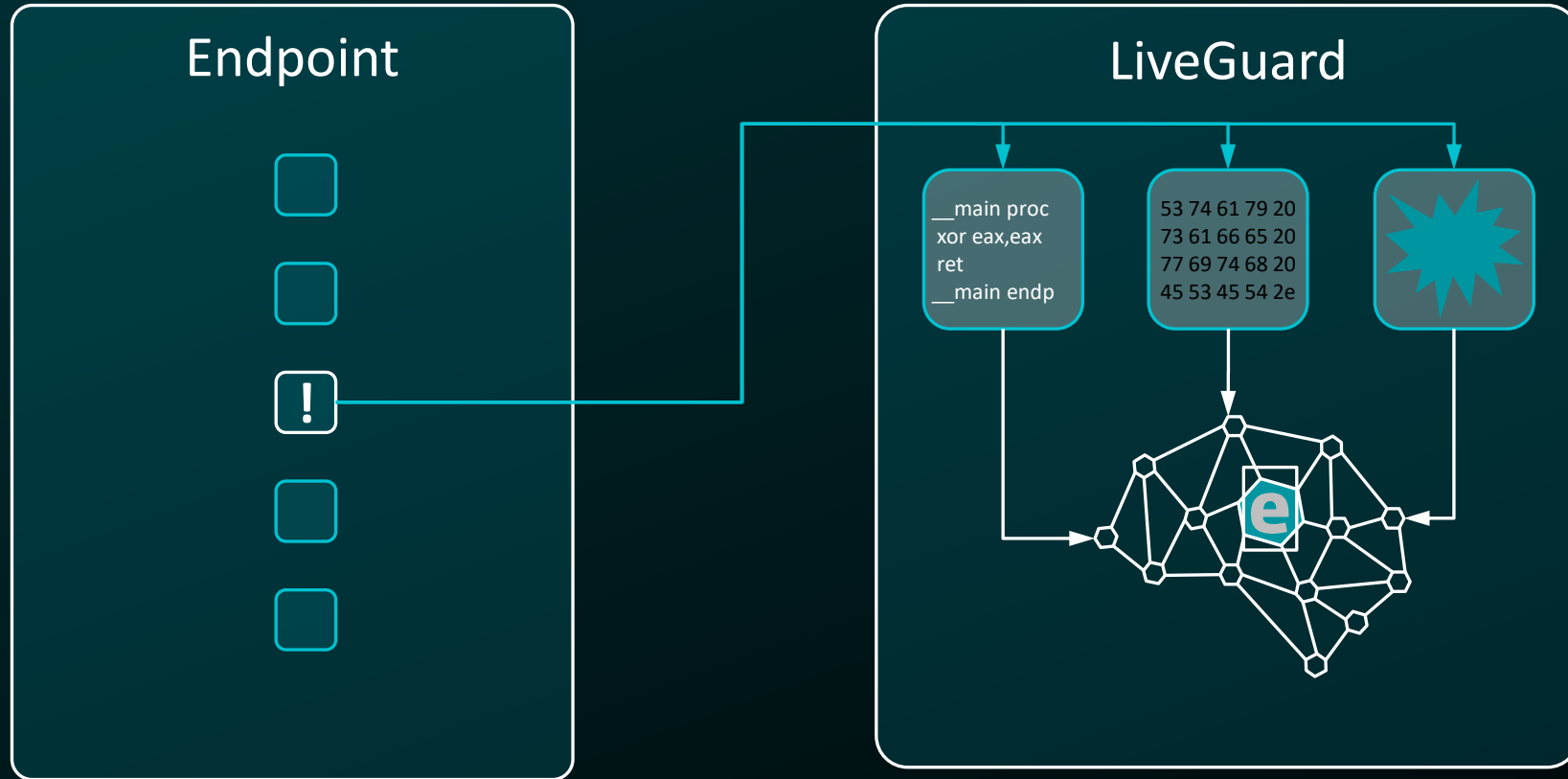
Fungovanie



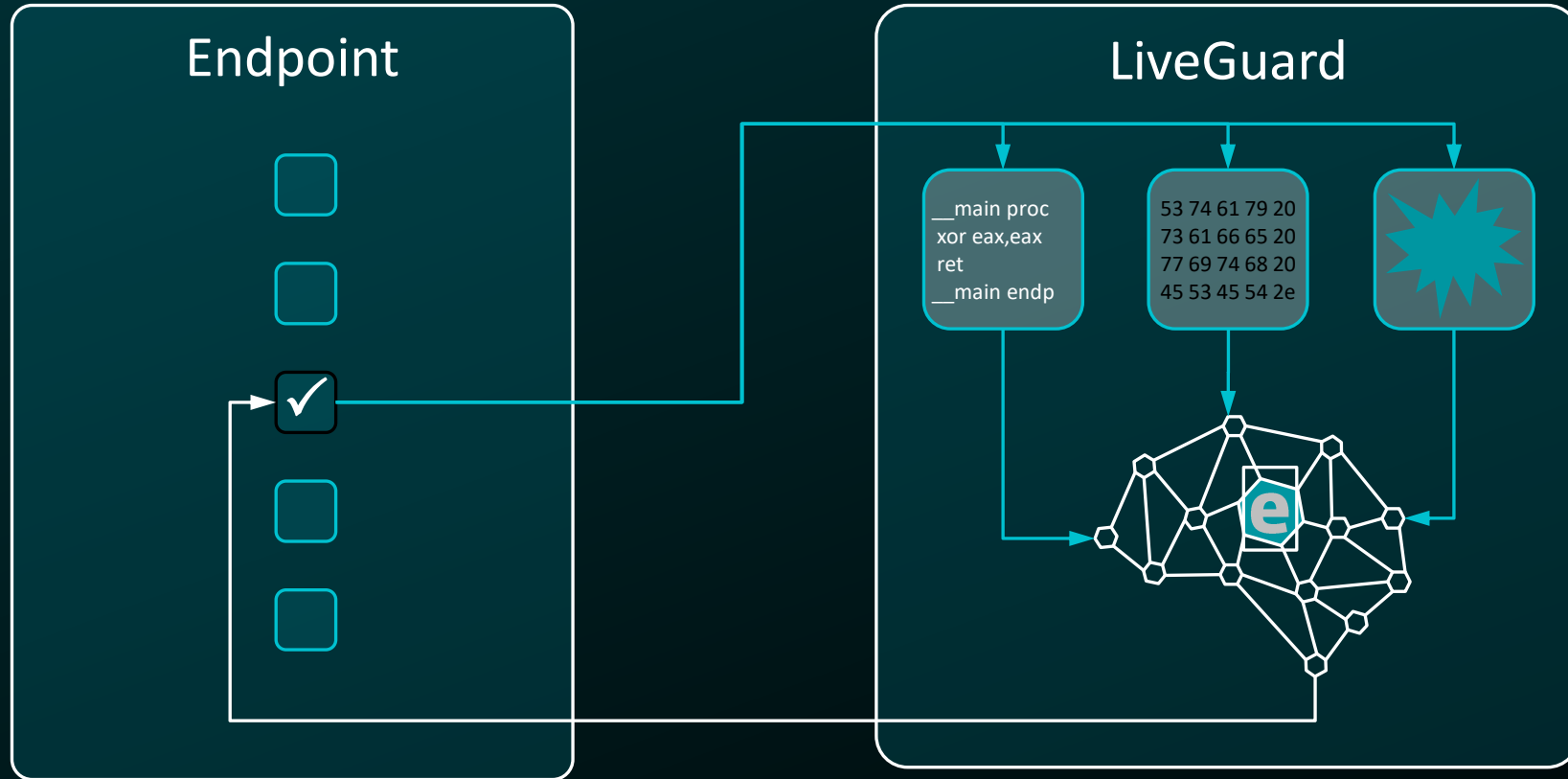
Fungovanie



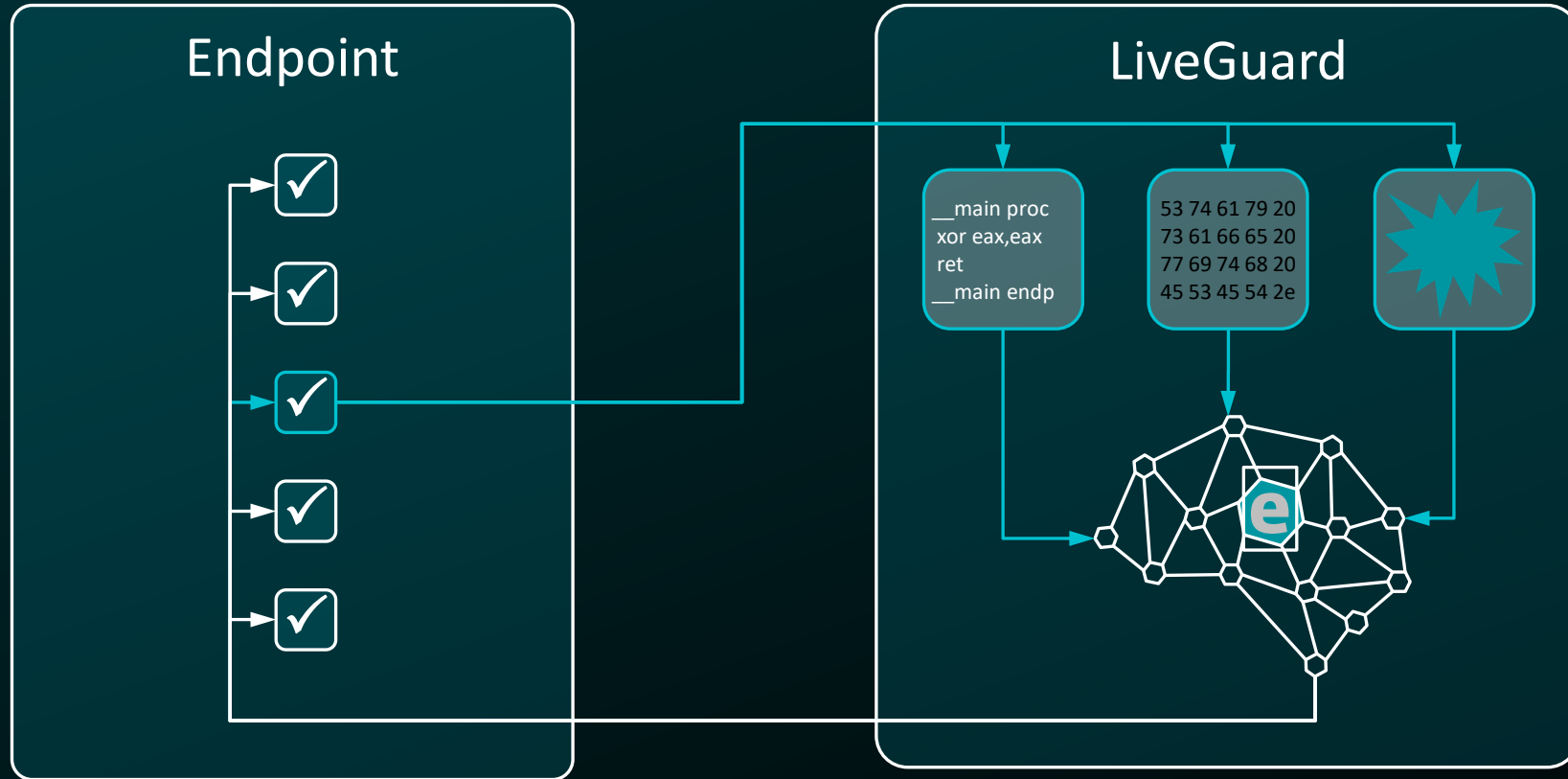
Fungovanie



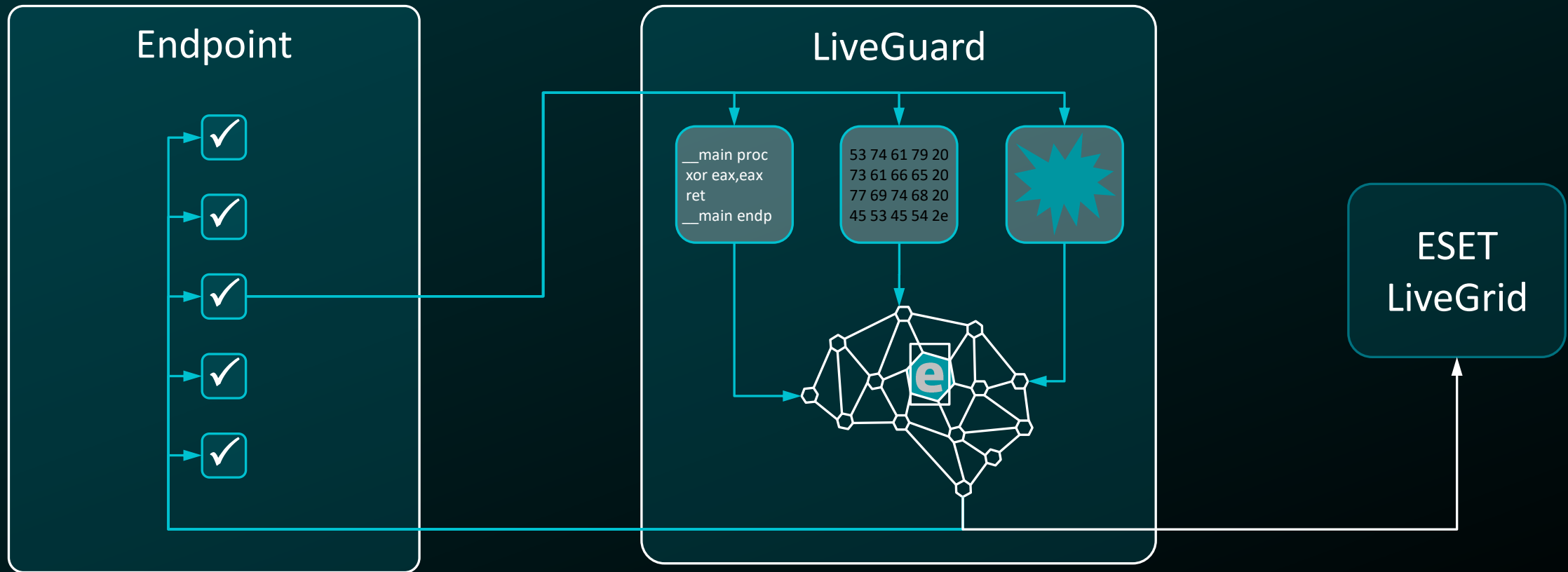
Fungovanie

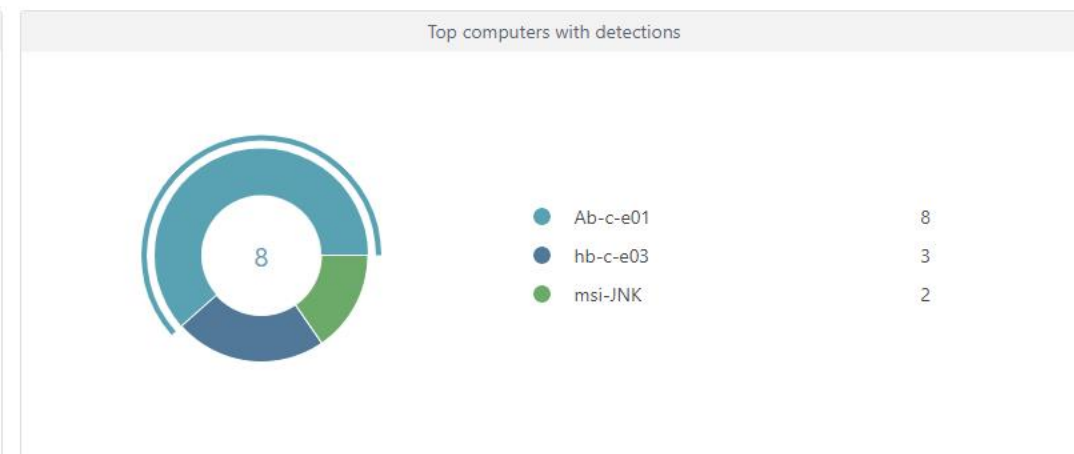
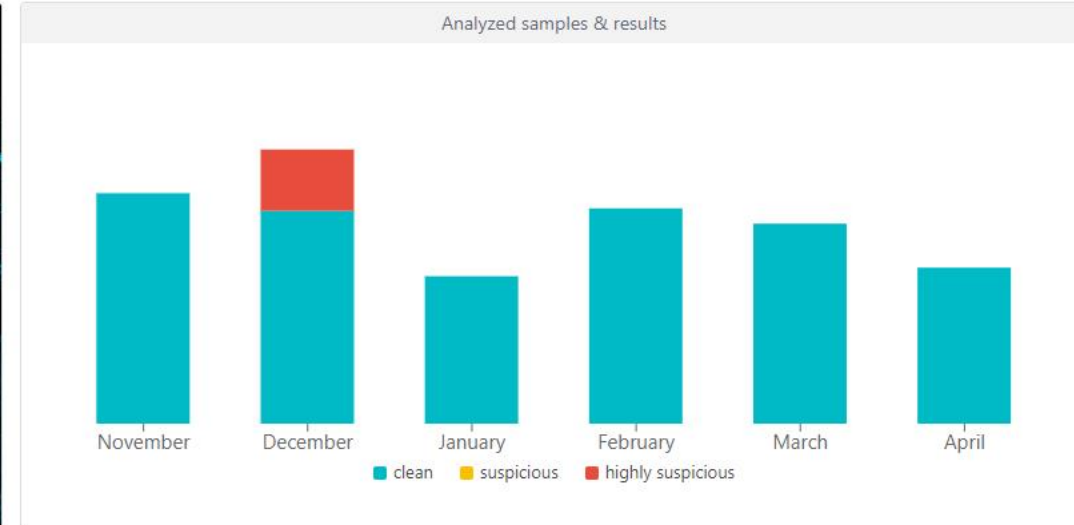


Fungovanie



Fungovanie





PRESETS ▾

INSPECT 🔍

🔄

Antivirus

Potentially unsafe application

📄 ⏏ ⬆ ⬆ ⚙ ⛔

Antivirus

eset

LIVEGUARD

⚠

Potentially unsafe application

Occurred

August 12, 2021 14:09:03

Occurrences

Total 1
✔ Resolved 0
✔ Handled by product 0

Circumstances

First seen on

August 12, 2021 14:03:15

Restart required

no

Hash

3BD9FD175A098192A48D6257FDED4FC5064FD5C2 ▾

Name

Win32/Sniffer.SniffPass.A

Detection Type

Potentially unsafe application

Object type

File

Uniform Resource Identifier (URI)

file:///C:/Users/Adam/Desktop/E-use/sniffpass/SniffPass.exe

Process name

C:\Program Files\ESET\ESET Security\egui.exe

User

HB-C-E01\adam

INVESTIGATE (INSPECT) 🔍

Scan

🔍

Scanner

On-demand scanner

Originally detected by

eset

LIVEGUARD

Detection engine version

23781 (20210812)

Current engine version

25086 (20220410)

Scan targets

C:\Users\Adam\Desktop\E-use\sniffpass\S sniffPass.exe

Number of scanned items

1

Infected

1

⏪ ⏴ 1 ⏵ ⏩

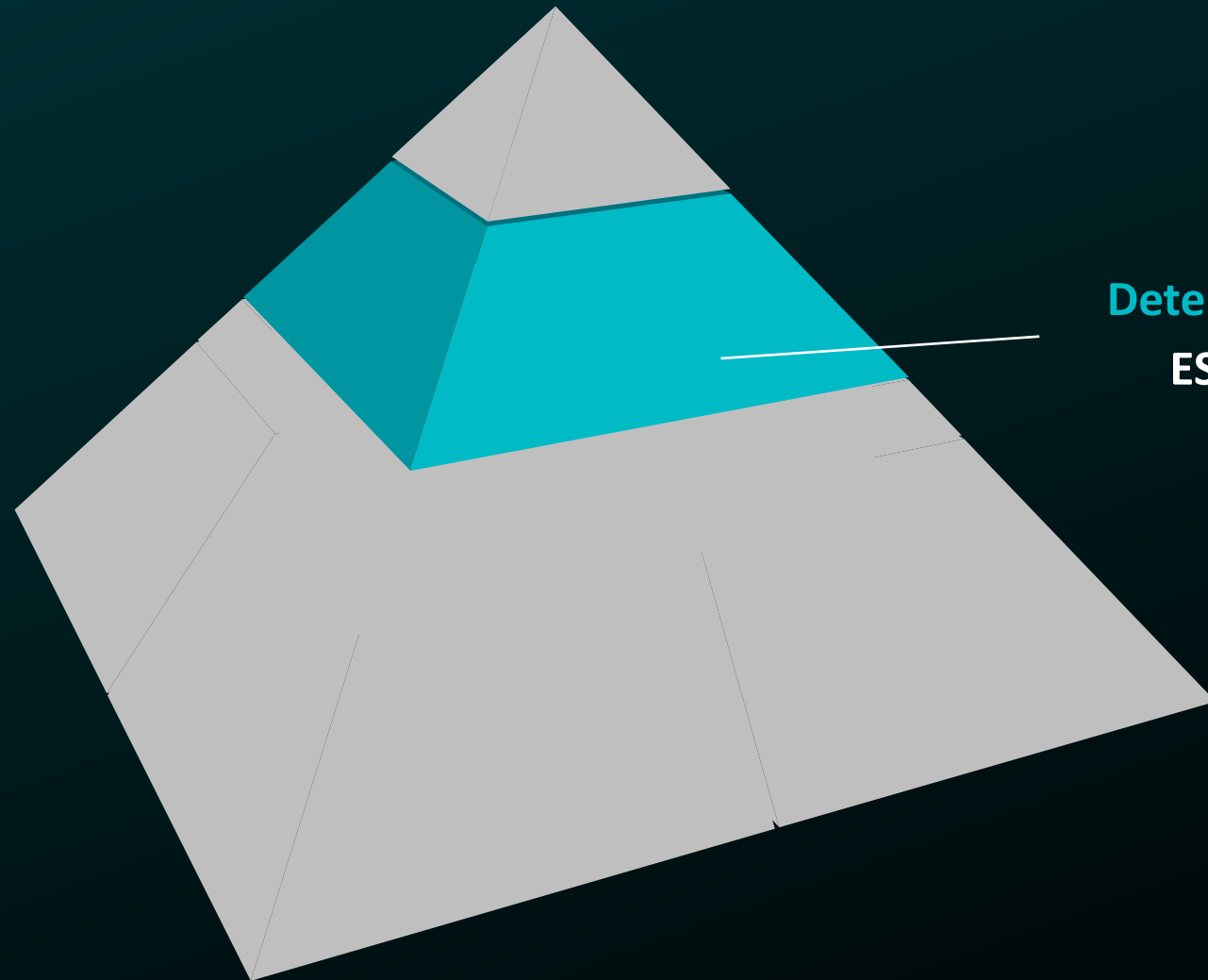
🛡

LiveGuard ↔ ECOS integração

Výhody

- automatická 0-day ochrana
- pokročilé metódy (Machine learning, emulation...)
- ochrana endpointov aj mimo LAN perimetra
- integrálna súčasť security produktov ako (EEA\EES etc.)
- detailný reporting
- možnosť kontroly nad odosielanými súbormi

VIACÚROVŇOVÉ ZABEZPEČENIE



Detekcia a Reakcia
ESET Inspect

Endpoint Detection and Response?

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.

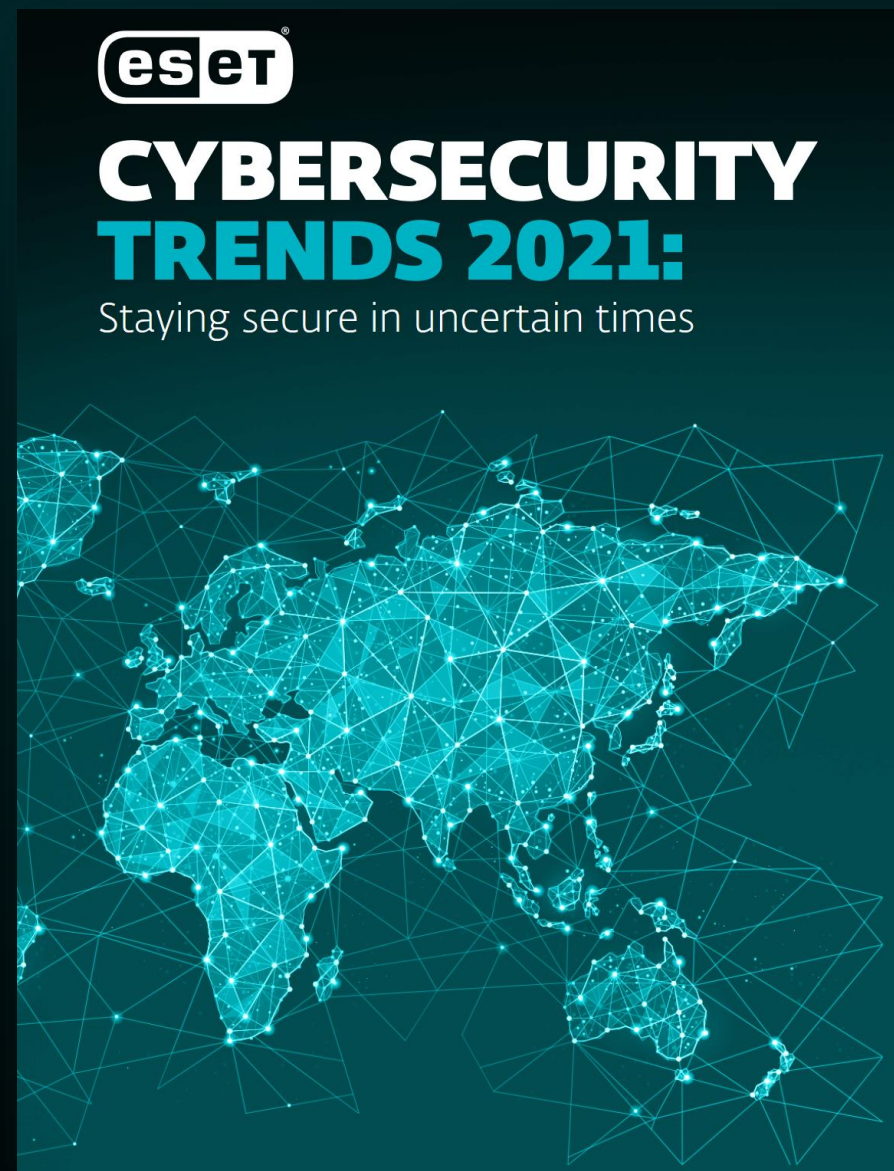
Nie sme si istí.

Nie sme si istí.

Nie sme si istí.

Prečo Endpoint Detection and Response

- Komplexnosť útokov
- IOC
- APT
- Dĺžka útoku
- Hrozby z vnútra inštitúcie
- Iné ako spustiteľné súbory
- 69/2018 Z. z. o kybernetickej bezpečnosti



esense [®] **SPECTR** [®] Enterprise Inspector

Prispôsobiteľné riešenie na detekciu
a následnú reakciu na útoky na koncové zariadenia



VIACÚROVŇOVÉ ZABEZPEČENIE



detekcia



prehľad



reakcia

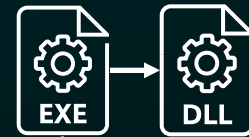
Bez podpory ESET Inspect



Minimálny prehľad



Neistota



Rundll32 spúšťa DLL



Hrozba zistená/zablokovaná

S podporou ESET Inspect



Zvýšený prehľad



Pokoj v duši :)



Otvorenie emailu Outlook



MS Excel príloha



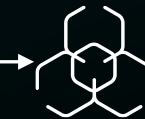
Spustený PowerShell



Stiahnuté DLL



Rundll32 spúšťa DLL



Hrozba
zistená/zablokovaná

Select Tags

3D42B2C0C6A7CBBADD299BD981B43FACE...

Trusted

win.rar GmbH

1 computer

16 days ago - Mar 28, 2022, 1:29:04 PM

16 days ago - Mar 28, 2022, 1:56:41 PM



● ● ● ● ● ● ● ● ● ●

2 years ago



Events



Desktops

11 hours ago - Apr 13, 2022, 1:37:01 AM

11 hours ago - Apr 13, 2022, 1:36:26 AM

1.7.1909

Microsoft Windows 10 Enterprise

10.0.19044.1645

rar.exe (6480)

```
a -dw -ep1 -inul -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"
```

%TMP%\winrar\

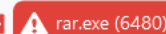
16 days ago - Mar 28, 2022, 1:56:41 PM

16 days ago - Mar 28, 2022, 1:56:41 PM

cmd.exe (368)

7zq.exe (10992)

KILL PROCESS



 RAR encrypts and deletes files [B0601]

ESET Inspect “R” ako Reakcia



Blokovanie Hashu
Ukončenie procesu



Spustenie skenovania
Stiahnutie súboru



Reštartovanie
Vypnutie



Sieťová izolácia

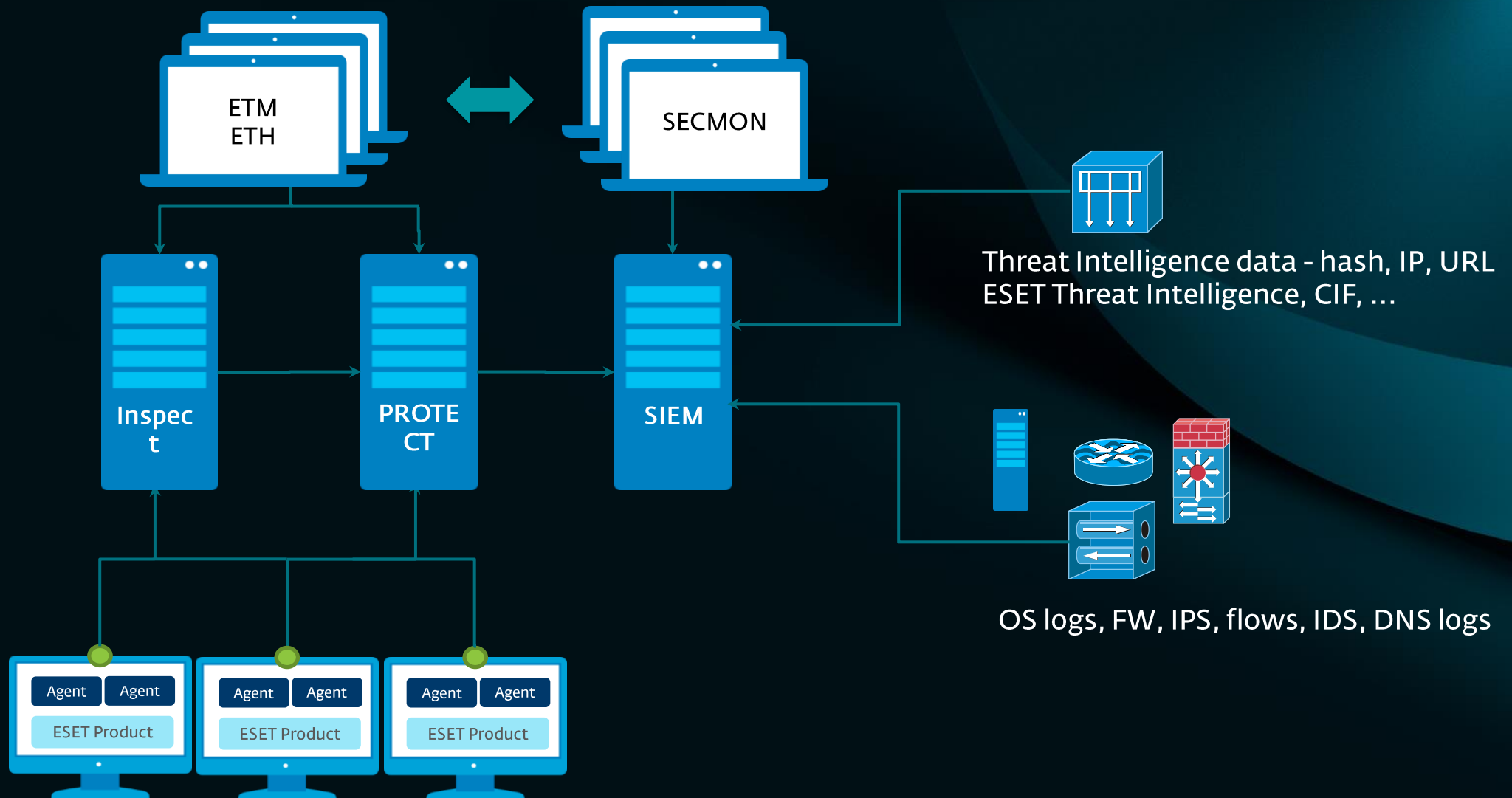


Vzdialený prístup
PowerShell

Funkcionalita

- blokovanie
- mazanie
- izolácia
- označovanie problematických staníc
- detekcia dumpingu hesiel
- pass the hash detekcia
- PowerShell
- WMI detekcia
- Virus Total
- MITRE&ATTACK
- API
- 2FA

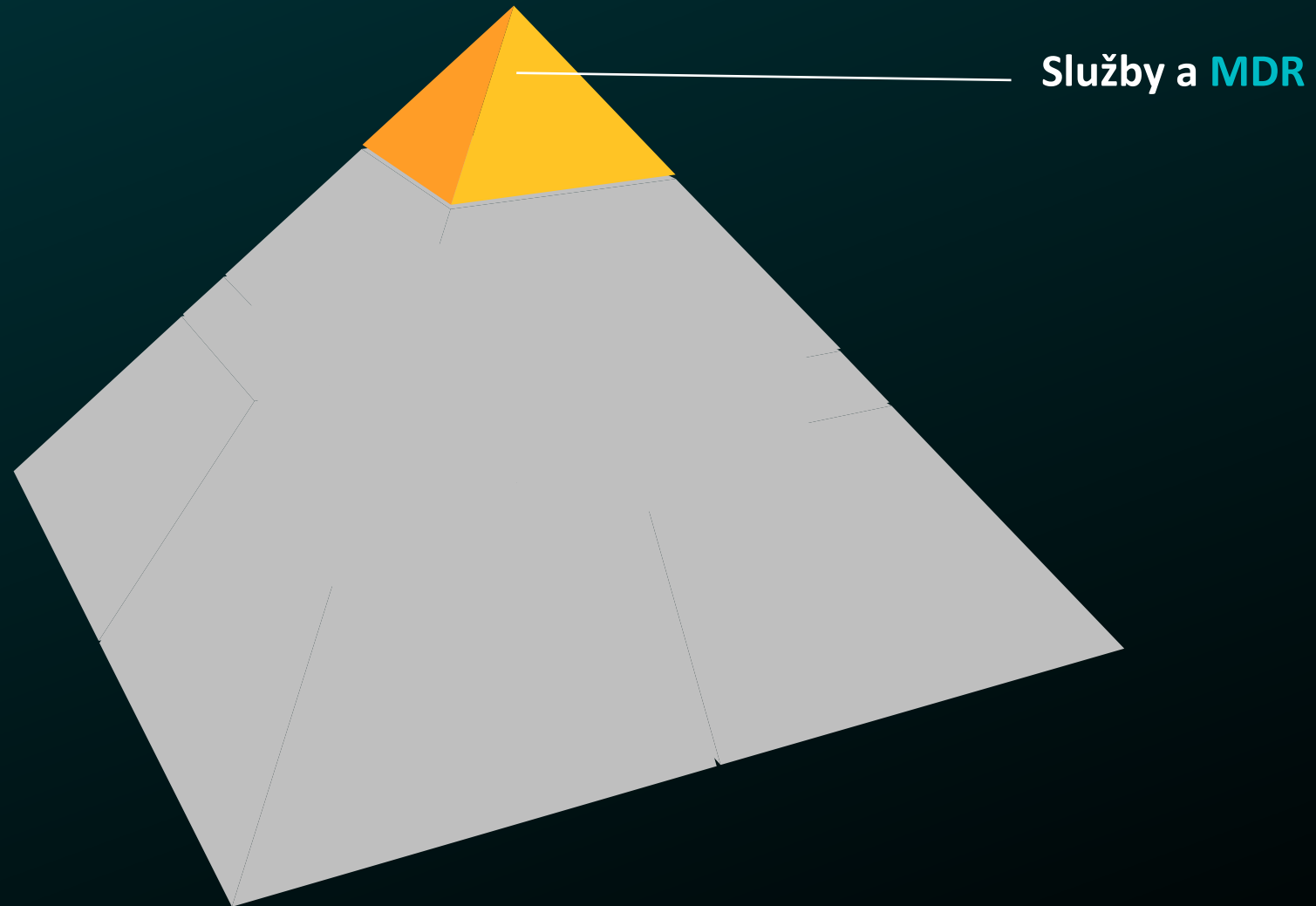
Infraštruktúra a nasadenie



Hlavné výhody

- zrýchlenie odozvy na 0-day zraniteľnosti a APT's
- odhalovanie problematických užívateľov
- izolovanie problematických staníc
- kompletný prehľad
- možnosť integrácie so SIEM

VIACÚROVNŇOVÉ ZABEZPEČENIE



ESET služby

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 EDR
- ✓ Threat monitoring / Threat hunting

Profesionálne služby

ESET PREMIUM SUPPORT **ESSENTIAL**

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

Bezpečnostné služby

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	X	áno
	Podrobná analýza súborov	X	áno
	Digitálna forenzná analýza	X	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	X	áno

ESET DETECTION AND RESPONSE **ADVANCED**

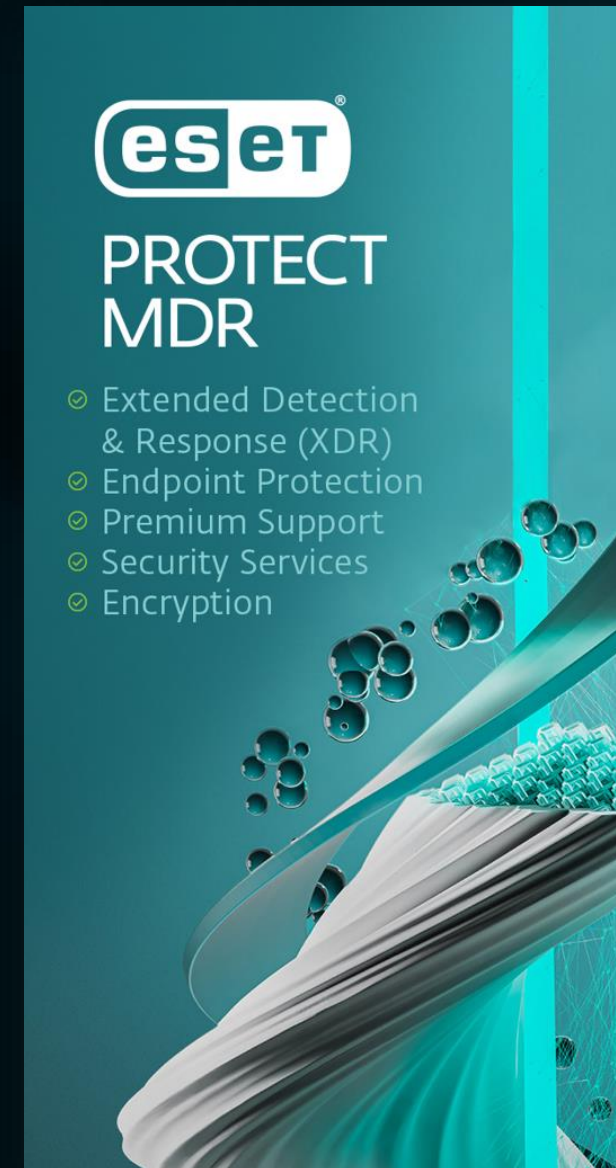
KATEGÓRIA AKTIVÍT	AKTIVITA	ŠTANDARDNÁ BEZPEČNOSTNÁ PODPORA	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED
Bezpečnostná podpora pre koncové zariadenia	Malvér: nezachytená detekcia	áno	áno	áno
	Malvér: problém s liečením	áno	áno	áno
	Malvér: infekcia ransomvérom	áno	áno	áno
	Nesprávna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

ESET DETECTION AND RESPONSE **ULTIMATE**

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: preskúvanie podozrivého správania	áno	áno	áno	áno
Vyšetrenie incidentov a reakcia na ne	Základná analýza súborov	X	áno	áno	áno
	Podrobná analýza súborov	X	áno	áno	áno
	Digitálna forenzná analýza	X	áno	áno	áno
	Digitálna forenzná pomoc pri reakcii na incidenty	X	áno	áno	áno
Bezpečnostná podpora pre ESET Inspect	Technická podpora – pravidlá	X	X	áno	áno
	Technická podpora – vylúčenia	X	X	áno	áno
	Všeobecné: otázky týkajúce sa bezpečnostného nástroja EDR	X	X	áno	áno
	EDR: počiatočná optimalizácia	X	X	áno	áno
	EDR: ESET Threat Hunting (vyhľadávanie hrozieb na vyžiadanie)	X	X	áno	áno
Bezpečnostné služby pre ESET Inspect	EDR: ESET Threat Monitoring (monitorovanie hrozieb)	X	X	X	áno
	EDR: ESET Threat Hunting (proaktívne vyhľadávanie hrozieb)	X	X	X	áno
Profesionálne služby	ESET Deployment & Upgrade	X	X	X	áno

ESET PROTECT MDR

		 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	●



Prečo MDR?



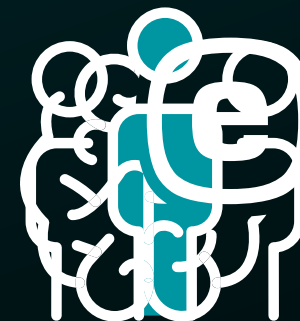
Komplexnosť nástroja



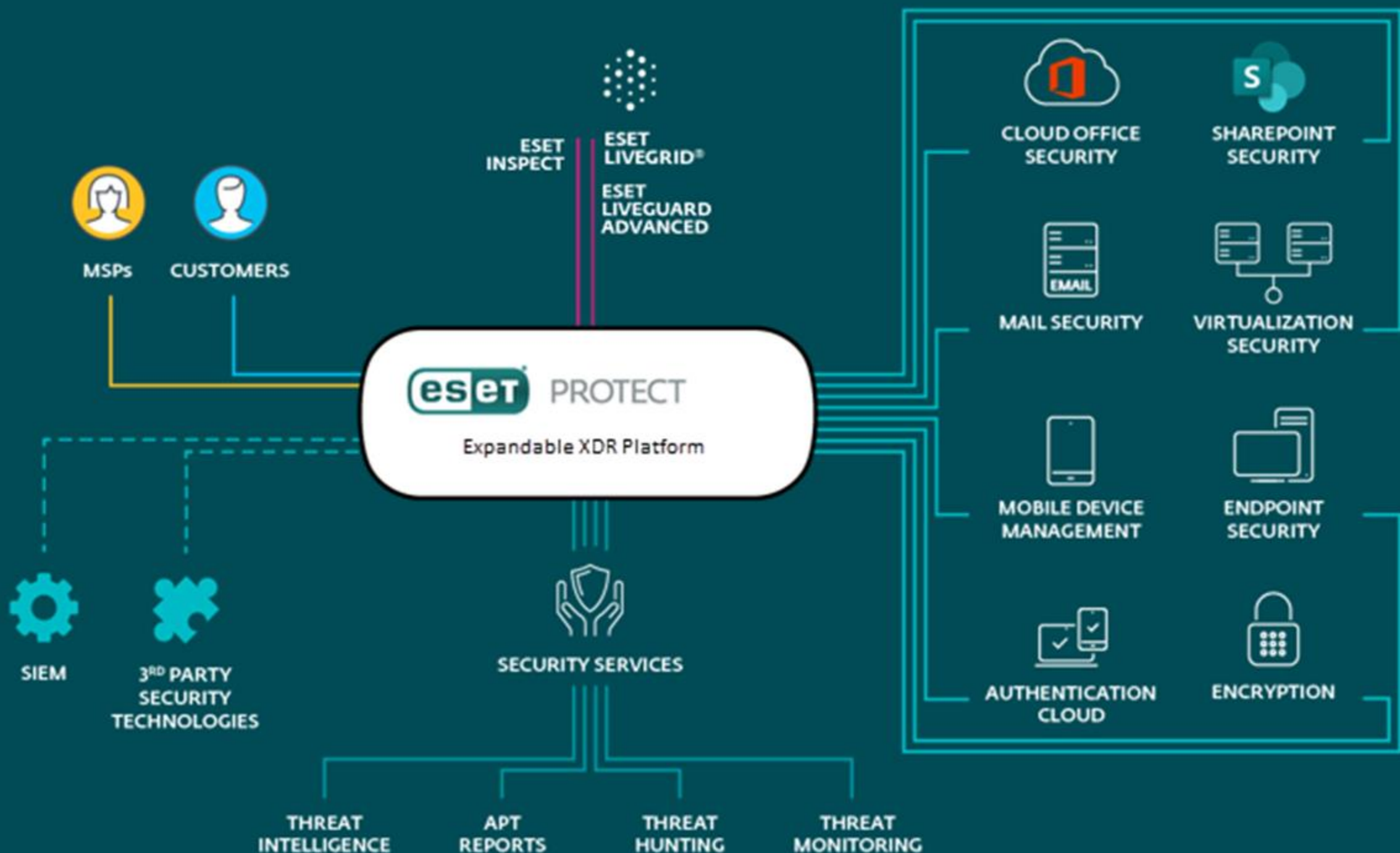
Viacero upozornení



Obmedzený čas na
monitorovanie hrozieb v
XDR



Nedostatok
kvalifikovaných IT
špecialistov





**SECURITY
DAYS**

ĎAKUJEM ZA POZORNOST



Digital Security
Progress. Protected.

&



konferencie