SECURITY DAYS

ESET SLUŽBY RIADENEJ BEZPEČNOSTI

Ondrej Krajč

Digital Security
Progress. Protected.

& SME KONFERENCIE

Populárne vektory útokov

- Phishing
- Zraniteľnosť
- Kompromitované účty
- Nesprávne konfigurované služby
- Škodlivé prílohy a stiahnuté súbory

Zákon o kybernetickej bezpečnosti **69/2018 Z. z.**

Povinnosti prevádzkovateľa základnej služby

- riešiť kybernetický bezpečnostný incident
- bezodkladne hlásiť závažný kybernetický bezpečnostný incident
- v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní

Bezpečnostné opatrenia musia zahŕňať:

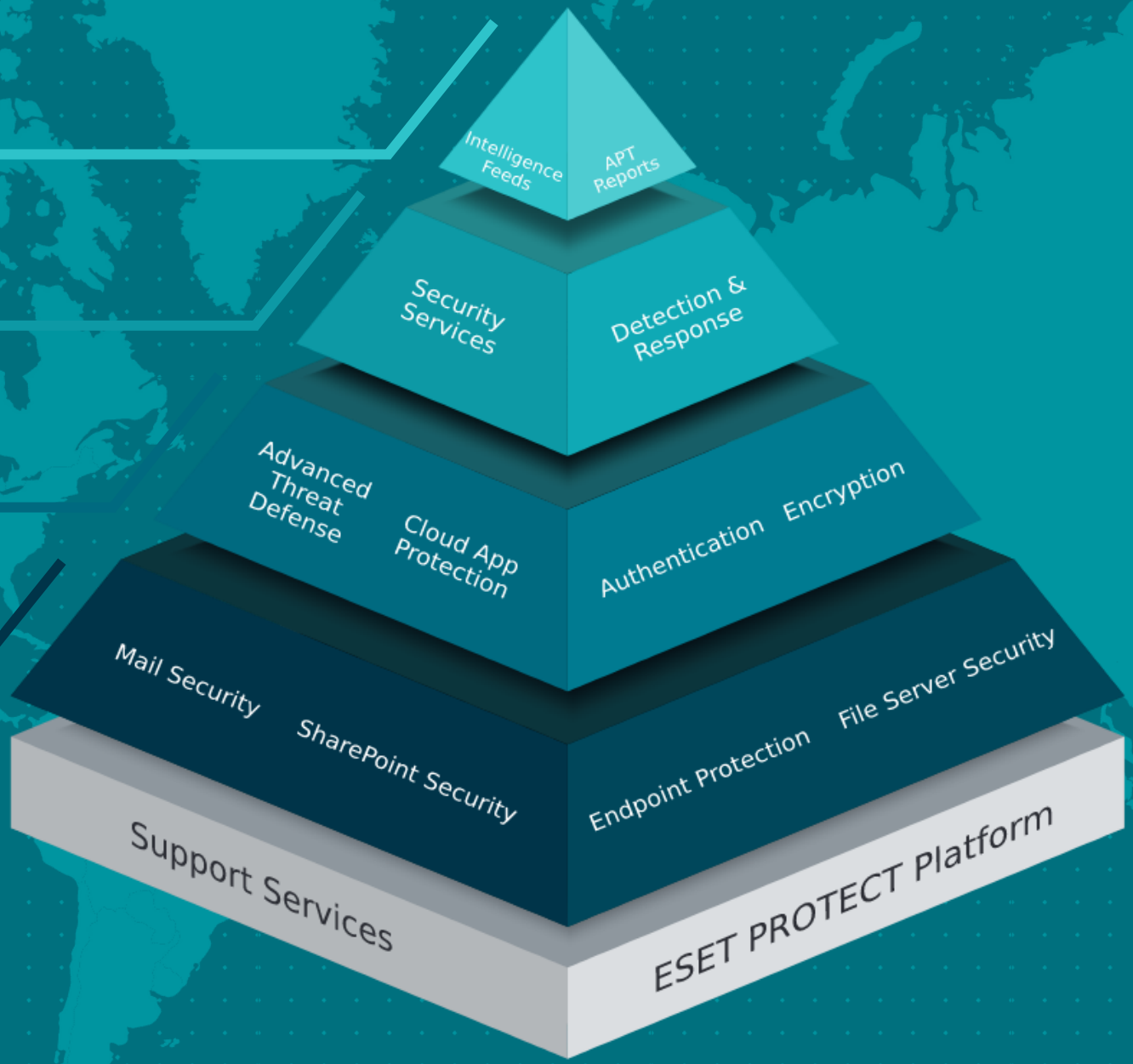
- detekciu kybernetických bezpečnostných incidentov,
- evidenciu kybernetických bezpečnostných incidentov,
- postupy riešenia a riešenie kybernetických bezpečnostných incidentov

Threat Intelligence

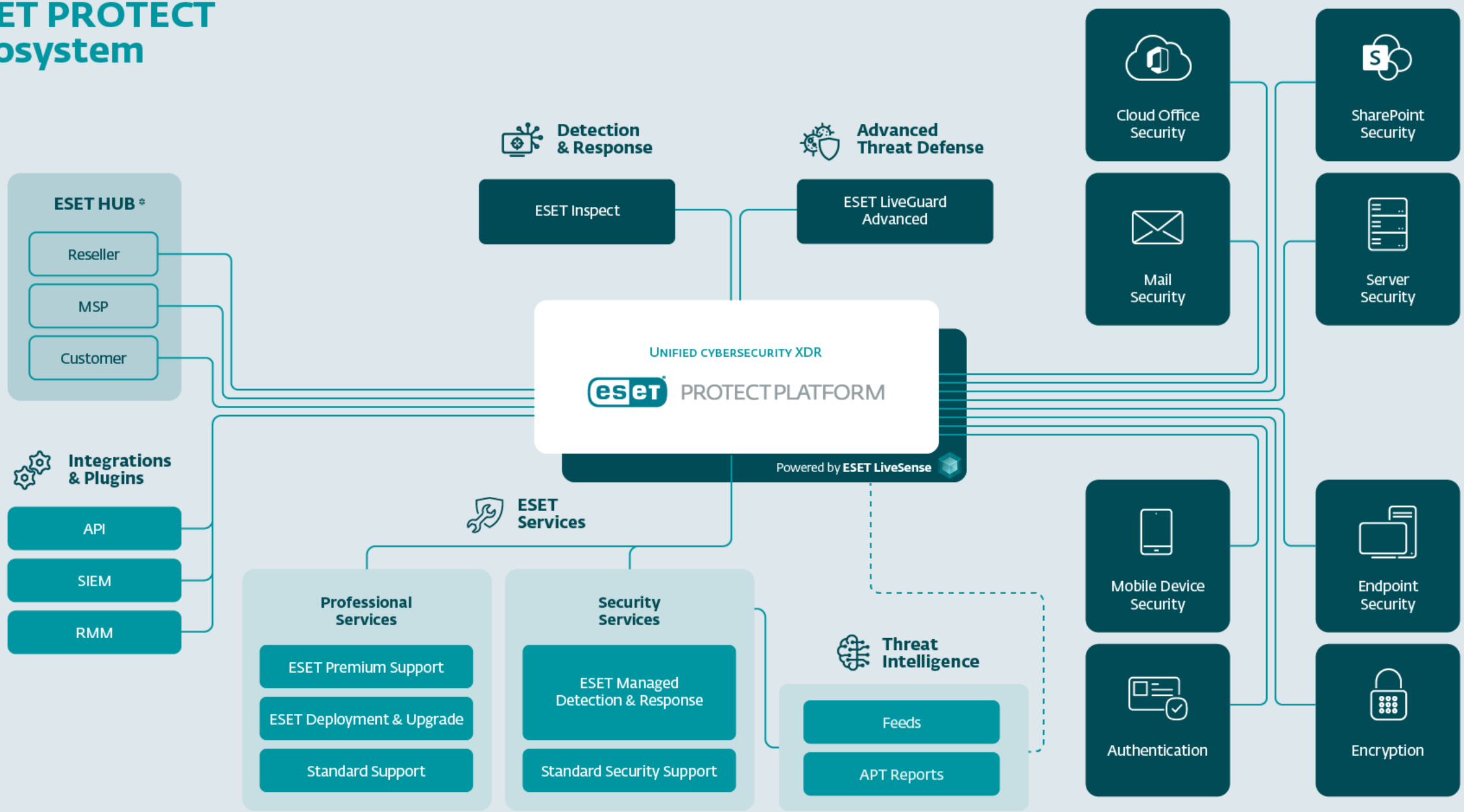
Detekcia a reakcia

Rozšírená ochrana

Základná ochrana



ESET PROTECT Ecosystem



* Coming H1/2023

EDR/XDR/MDR

Bez ESET Inspect riešenia :

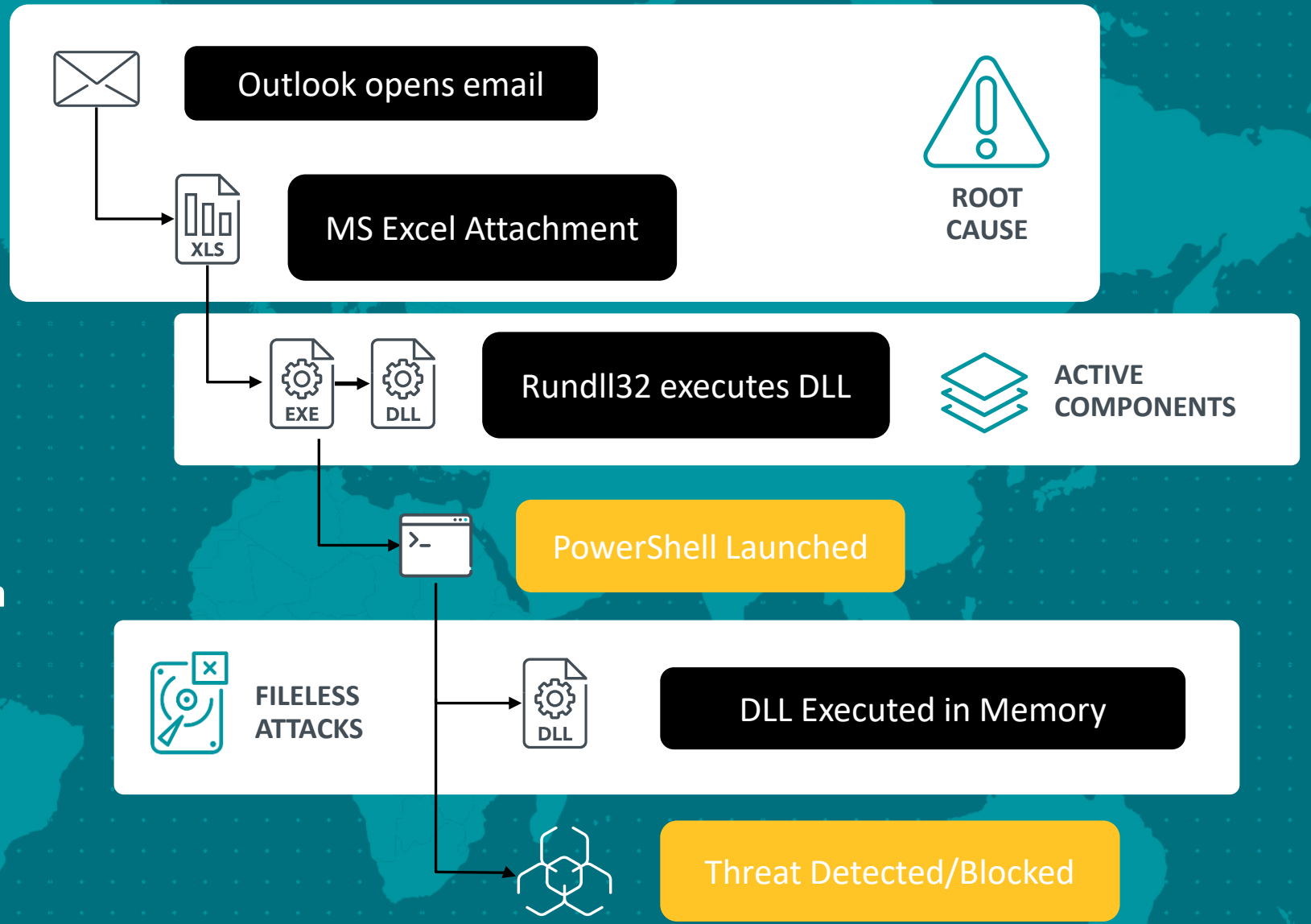
minimálna viditeľnosť

neistota

S ESET Inspect riešením:

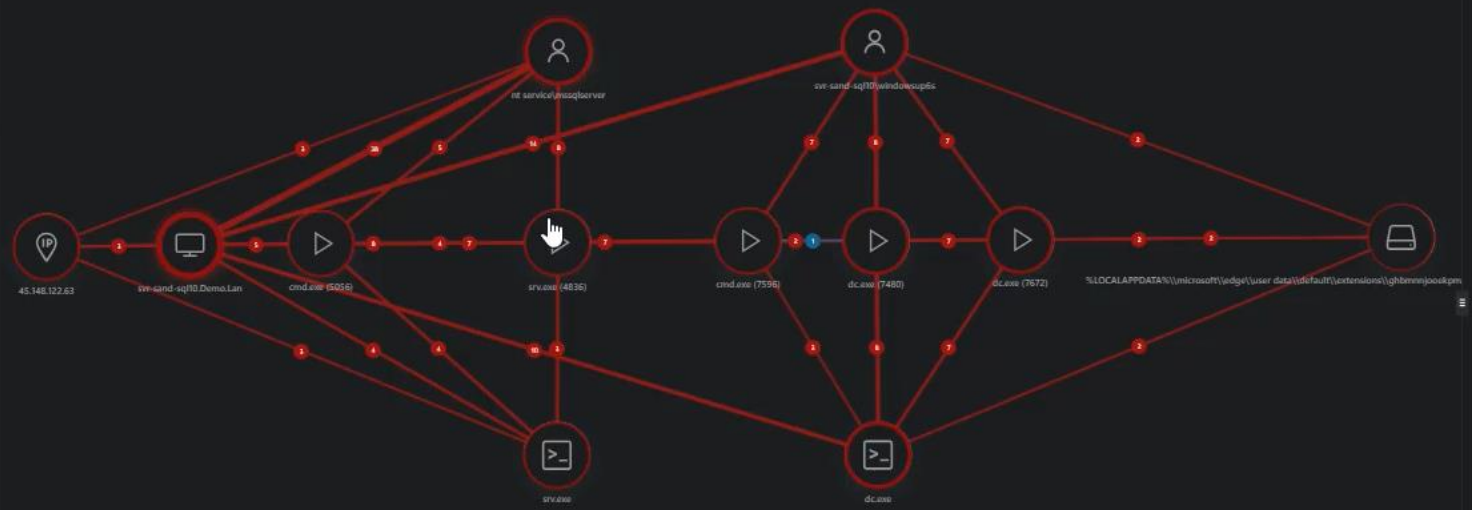
zvýšená viditeľnosť

dodatočná kontrola



BACK nt service\mssqlserver,svr-sand-sql10.demo.lan

Incident graph | Timeline | Detections | Computers | Executables | Processes



Incident | Timeline

Oct 31, 2023, 12:57:47 PM
Rule - File deleted from documents folder [C0306]
Mitre att&ck™ techniques
T1485 - Data Destruction
svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)
FileDelete %HOME%\documents\desktop.ini

Oct 31, 2023, 12:57:47 PM
Rule - File with unexpected extension is written into documents folder [C0628]
Mitre att&ck™ techniques
T1486 - Data Encrypted for Impact
svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)
FileTruncated (on open)
%HOME%\documents\desktop.ini.freeworldencryption

Oct 31, 2023, 12:50:47 PM
Rule - File modified in %startup% folder by suspicious process [A0127a]
Mitre att&ck™ techniques
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)
FileTruncated (on open) %STARTUP%\desktop.ini.freeworldencryption

Oct 31, 2023, 12:50:36 PM
Rule - Filecoder behavior [Z0601]
Mitre att&ck™ techniques
T1486 - Data Encrypted for Impact
svr-sand-sql10.demo.lan | dc.exe | dc.exe (7672)
FileTruncated (on open)
%LOCALAPPDATA%\microsoft\edge\user data\default\extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.69.2_0\128.png.freeworldencryption

Oct 31, 2023, 12:50:35 PM
Rule - Process reading sensitive files - Browser-based Credential Stores [E1108]
Mitre att&ck™ techniques
T1552.001 - Unsecured Credentials: Credentials In Files

INCIDENT | REMEDIATION | COMMENT | EDIT | ASSIGN | PROGRESS | GRAPH

Threat indicators | Behaviors | Analyst actions

Problémy

Komplexita nástrojov

Únava z veľkého množstva upozornení

Nedostatok kvalifikovaných ľudí

Limitovaný čas na reakciu

Služby manažovanej bezpečnosti (MDR)

ESET MDR služba je navrhnutá pre zákazníkov s cieľom pomôcť :

- Zvýšiť zabezpečenie a reakčnú rýchlosť na prípadné incidenty
- Zabezpečiť nevyhnutné znalosti na efektívne riešenie incidentov
- Napomáhať pri plnení regulácií a smerníc

ESET Služby manažovanej bezpečnosti

Plne monitorovaná bezpečnostná služba pre zákazníkov s **ESET XDR platformou**

Zákazník

Report

ESET

1. **Monitoring**
2. **Hunting**
3. **Izolácia**

ANALÝZA

- reputácia
- podpis súboru

Výsledok:

Malware

1. **Blokovanie** Hash
2. **Vyčistenie** PC
3. **Report**

ESET Služby manažovanej bezpečnosti

rýchla reakcia

dashboardy

reporting

Služby MDR a MDR Ultimate

ESET MDR a Ultimate poskytujú 24/7 bezpečnostné služby pod vedením odborníkov

- nepretržité monitorovanie
- vyhľadávanie hrozieb
- kategorizáciu
- reakciu

ESET MDR ponúka spoľahlivú ochranu a ESET MDR Ultimate ju posúva o krok ďalej

Výhody ESET MDR

- 24/7 monitorovanie, vyhľadávanie, triedenie a reakcia na hrozby
- Threat Hunting pod vedením expertov
- Reakcia na aktívne prebiehajúce kampane útočníkov
- Knižnica príznakov podozrivého správania
- Optimalizácia príznakov podozrivého správania a výnimiek
- Neustále zlepšovanie detekcie a automatizácie
- Prispôsobené reporty
- Využívanie znalostí globálneho tímu ESET Threat Intelligence

Výhody ESET Detection and Response Ultimate

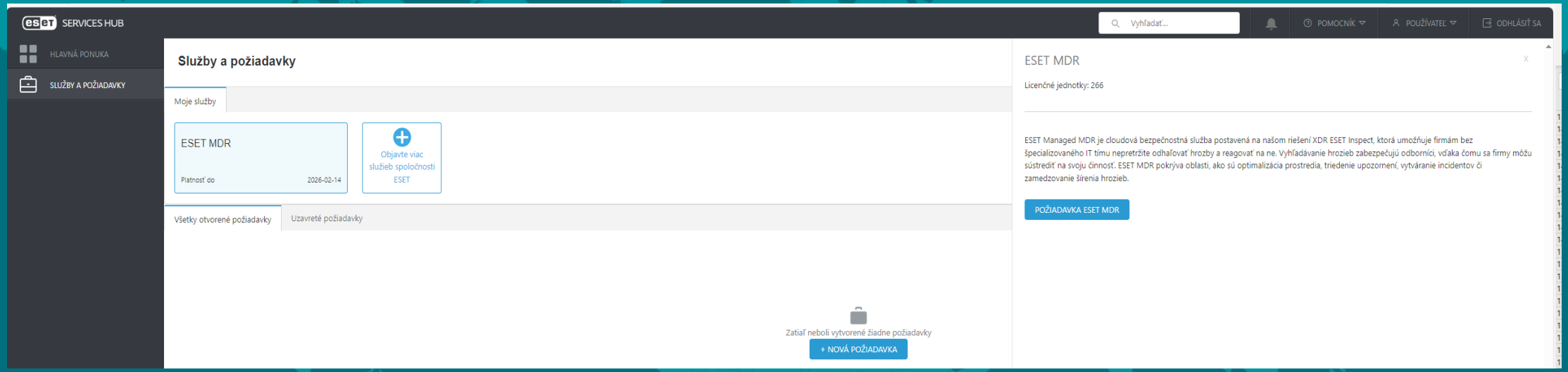
- Pokročilý Threat Hunting
- Threat Hunting zameraný na aktuálne šíriace sa hrozby
- Digitálna forenzná pomoc pri reakcii na incidenty
- Upozornenia na potenciálne vektory útoku pre konkrétne prostredie zákazníka
- Podrobná analýza malvéru
- Špecializovaná pomoc pre vysvetlenie XDR upozornení s doplňujúcim kontextom
- Príprava špecifických detekčných pravidiel vo väzbe na malvér
- Služba Deployment & Upgrade
- Reakcia na incidenty v spolupráci s dedikovaným ESET expertom

	ESET MDR Managed Detection & Response	ESET Detectiocn & Response Ultimate Premium Managed Detection & Response
THREAT HUNTING AND RESPONSE:		
Využívanie znalostí globálneho tímu ESET Threat Intelligence	✓	✓
Reakcia na aktívne prebiehajúce kampane útočníkov	✓	✓
Neustále zlepšovanie detekcie a automatizácie	✓	✓
Knižnica príznakov podozrivého správania	✓	✓
Optimalizácia príznakov podozrivého správania a výnimiek	✓	✓
Neustály Threat Hunting pod vedením expertov	✓	✓
Prispôsobené reporty	✓	✓
24/7 monitorovanie, vyhľadávanie, triedenie a reakcia na hrozby pod vedením expertov	✓	✓
Upozornenia na potenciálne vektory útoku pre konkrétne prostredie zákazníka	–	✓
Reakcia na incidenty v spolupráci s dedikovaným ESET expertom	–	✓
Digitálna forenzná pomoc pri reakcii na incidenty	–	✓
Príprava špecifických detekčných pravidiel vo väzbe na malvér	–	✓
Podrobná analýza malvéru	–	✓
Rozšírený Threat Hunting zameraný na aktuálne šíriace sa hrozby	–	✓
Pokročilý Threat Hunting	–	✓
Služba Deployment & Upgrade	–	✓
Špecializovaná pomoc pre vysvetlenie XDR upozornení s doplňujúcim kontextom	–	✓

Rozdiely služieb ESET MDR

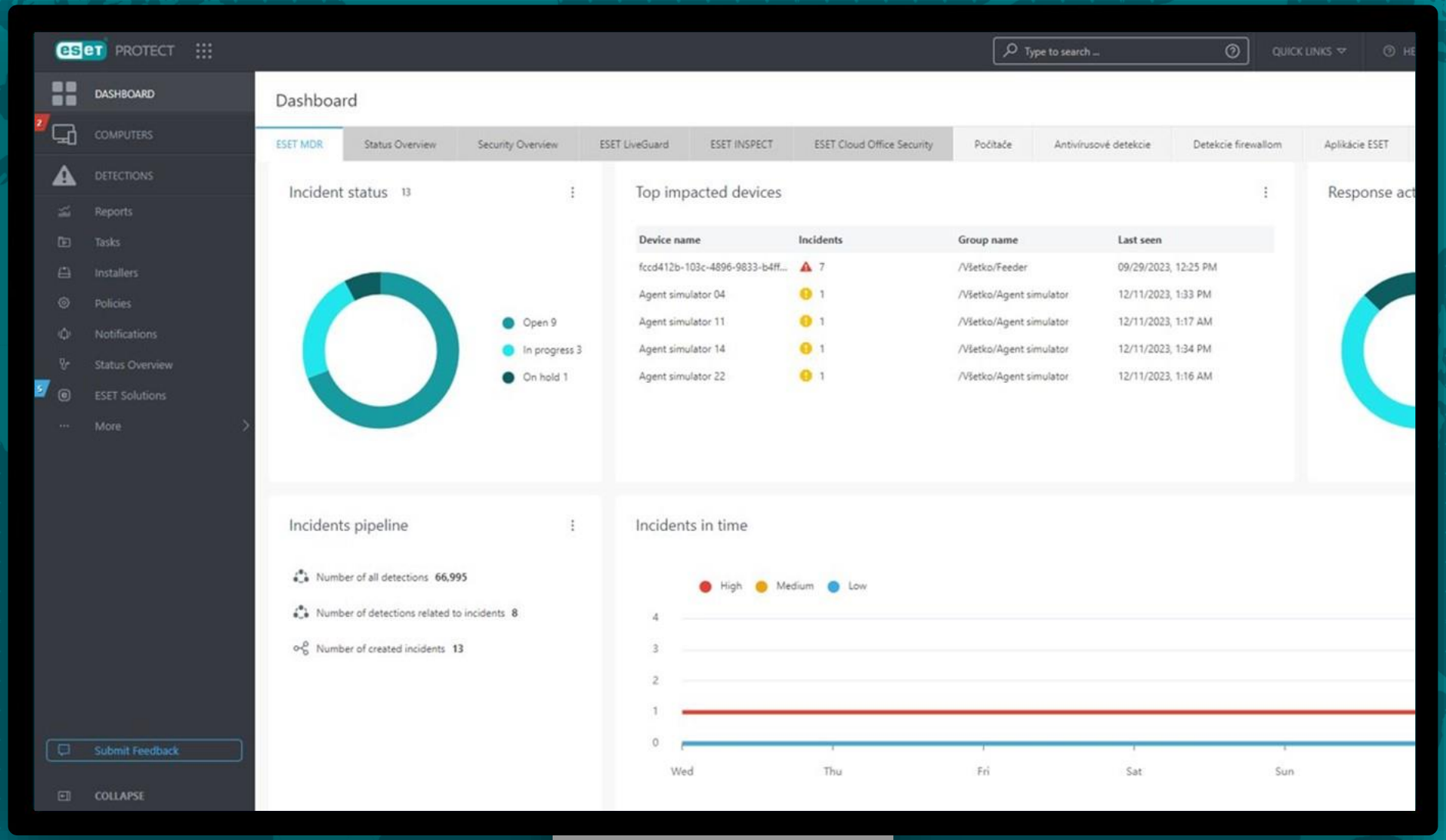
	ESET MDR	ESET Detection and response ultimate
Platforma	Cloud	On-prem a cloud
Pravidlá a optimalizácia	Na úrovni ESET SIEM / SOAR	Priamo v zákazníckom prostredí
Reporting	Týždenný/Mesačný	Podrobný Hero report
Riešenie incidentov	ESET SIEM/ SOAR a zákazníkom	Manažované ESET analytikom
Manažovanie koncových staníc	Zákazníkom	Sspolupráca s ESET expertami
Podpora ESET analytika	Nie (guidelines/playbooks)	Analytik
Deployment (and upgrade)	Priamo zákazníkom	ESET

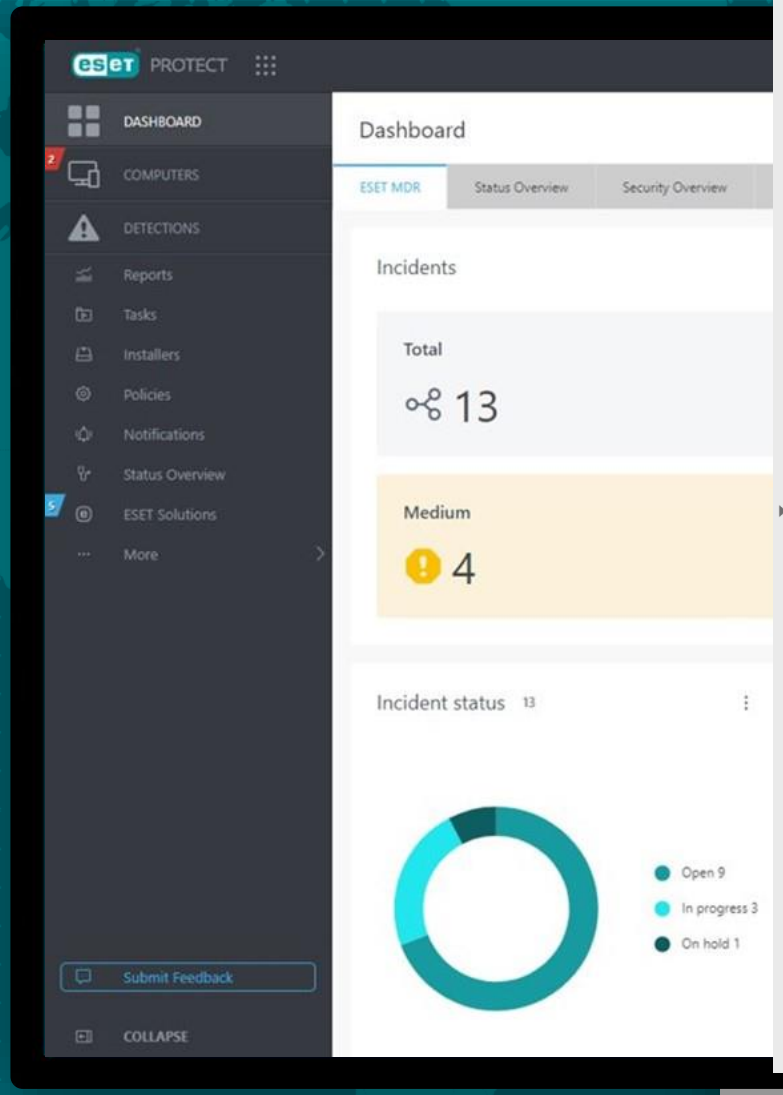
ESET Services Hub



Ako sa rozhodnúť

MDR	MDR a Ultimate	Ultimate
25-499 licencií	**500-999 licencií**	**1000+ licencií**
Zákazník s bežným IT oddelením zloženým z všeobecných IT pracovníkov, bez riadnych znalostí bezpečnosti, bez bezpečnostných špecialistov alebo SOC tímu, s nedostatkom času na prešetrenie incidentov.		
Zákazník hľadá cenovo dostupnú cloudovú službu, ktorá by riešila väčšinu incidentov a pomohla dodržiavať požiadavky poisťovní, bez potreby podpory MSP alebo MSSP poskytovateľa	Zákazník vyžadujúci prispôsobené Enterprise služby, prípadne dodávané lokálne (on-premise), alebo uprednostňujúci nižšiu cenu a všeobecnejšie cloudové služby. Je dôležité ponúkať škálu riešení vyhovujúcu rôznym potrebám kybernetickej bezpečnosti	Vyžaduje cloudovú alebo lokálnu službu, ktorá bude riešiť všetky incidenty a nápravu. Vyžaduje maximálnu ochranu poskytovanú špecializovanými bezpečnostnými expertmi, pravidelnú ľudskú podporu a asistenciu


eset PROTECT
Type to search ...
QUICK LINKS
DASHBOARD
COMPUTERS
DETECTIONS
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Dashboard
ESET MDR
Status Overview
Security Overview
ESET LiveGuard
ESET INSPECT
ESET Cloud Office Security
Počítače
Antivírusové detekcie
Detekcie firewallom
Aplikácie ESET
Incident status 13
Open 9
In progress 3
On hold 1
Top impacted devices
Device name
Incidents
Group name
Last seen
fccd412b-103c-4896-9833-b4ff...
7
/Všetko/Feeder
09/29/2023, 12:25 PM
Agent simulator 04
1
/Všetko/Agent simulator
12/11/2023, 1:33 PM
Agent simulator 11
1
/Všetko/Agent simulator
12/11/2023, 1:17 AM
Agent simulator 14
1
/Všetko/Agent simulator
12/11/2023, 1:34 PM
Agent simulator 22
1
/Všetko/Agent simulator
12/11/2023, 1:16 AM
Response act
Incidents pipeline
Number of all detections 66,995
Number of detections related to incidents 8
Number of created incidents 13
Incidents in time
High
Medium
Low
4
3
2
1
0
Wed
Thu
Fri
Sat
Sun



ESET MDR Weekly Report

Weekly report: January 12, 2024 - January 18, 2024
Created: January 19, 2024; 08:46:18; UTC+1:00

ESET Digital Security Progress. Protected.

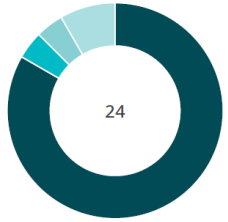
Incident overview

All incidents from all sources according to severity

24	14	4	6
All incidents	High ↓121% decrease	Medium ↓250% decrease	Low ↓383% decrease

Incidents according to status

Key insight into the progression of incidents within the incident cycle



Open	20 ↓
Resolved	1 ↓
Closed	1 ↓
Invalid	2 ↓

Open - Recently created incidents that were triggered by a detection pattern
Resolved - Incidents where an issue was identified and addressed by ESET MDR
Closed - Incidents that were marked as closed by the user
Invalid - Incidents that were marked as false positives

Incident pipeline

An overview of all detections, total incidents, and incidents resulting from detections, providing insight into service efficiency

	All detections	Detections related to incidents	Created incidents
January 12	31,252	1	1
January 13	31,252	1	1

ESET PROTECT MDR

Konzola na správu	ESET PROTECT
Moderná ochrana koncových zariadení	ESET Endpoint Security ESET Server Security
Ochrana serverov	
Pokročilá ochrana pred hrozbami	ESET LiveGuard Advanced
Šifrovanie celého disku	ESET Full Disk Encryption
Ochrana e-mailovej komunikácie	ESET Mail Security
Ochrana cloudových aplikácií	ESET Cloud Office Security
Správa zraniteľností a záplat	ESET Vulnerability & Patch Management
Detekcia a reakcia	ESET Inspect
Overovanie	ESET Secure Authentication
Služby	ESET MDR

ESET PROTECT MDR Ultimate

Konzola na správu	ESET PROTECT
Moderná ochrana koncových zariadení	ESET Endpoint Security ESET Server Security
Ochrana serverov	
Pokročilá ochrana pred hrozbami	ESET LiveGuard Advanced
Šifrovanie celého disku	ESET Full Disk Encryption
Ochrana e-mailovej komunikácie	ESET Mail Security
Ochrana cloudových aplikácií	ESET Cloud Office Security
Správa zraniteľností a záplat	ESET Vulnerability & Patch Management
Detekcia a reakcia	ESET Inspect
Overovanie	ESET Secure Authentication
Služby	ESET MDR Ultimate

Problémy

Komplexita nástrojov

Únava z veľkého množstva upozornení

Nedostatok kvalifikovaných ľudí

Limitovaný čas na reakciu


Vyriešené
Vyriešené
Vyriešené
Vyriešené

krajc@eset.sk