Bitdefender

BITDEFENDER
s AI a ML za zády

Pavel Škorpil, Security Specialist

22. 5. 2025 IDEME - PARTNERSTVO PRE PROSPERITU

Jaké výzvy dnes řešíme?

Bitdefender

Je čím dál tím těžší najít, a udržet bezpečnostní specialisty

Mnoho firem a institucí bylo prolomeno nebo se museli potýkat s APT útoky.

Není dostatek času investigovat všechny incidenty a soustředit se na ty podstatné výstrahy

Nepřehledné množství konzolí a nástrojů napříč nesourodými technologiemi

Bitdefender

Jak vybrat správnou platformu ?

- Je stávající platforma, kterou užíváte připravena i na budoucí hrozby?
- Jakým vývojem prošla v poslední době?
- Jak vychází v testech?

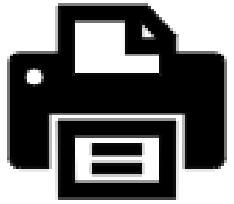
- Chrání efektivně a spolehlivě?
- Pomůže Vám s analýzou incidentů?

- Jaké potřebujete lidské zdroje pro správu?

Bitdefender

PC

CSPM+
EASM



PRINTER

VOIP

WIFI

NTB

EDR XDR

LAN

SRV

IDENTITY

DOCKER

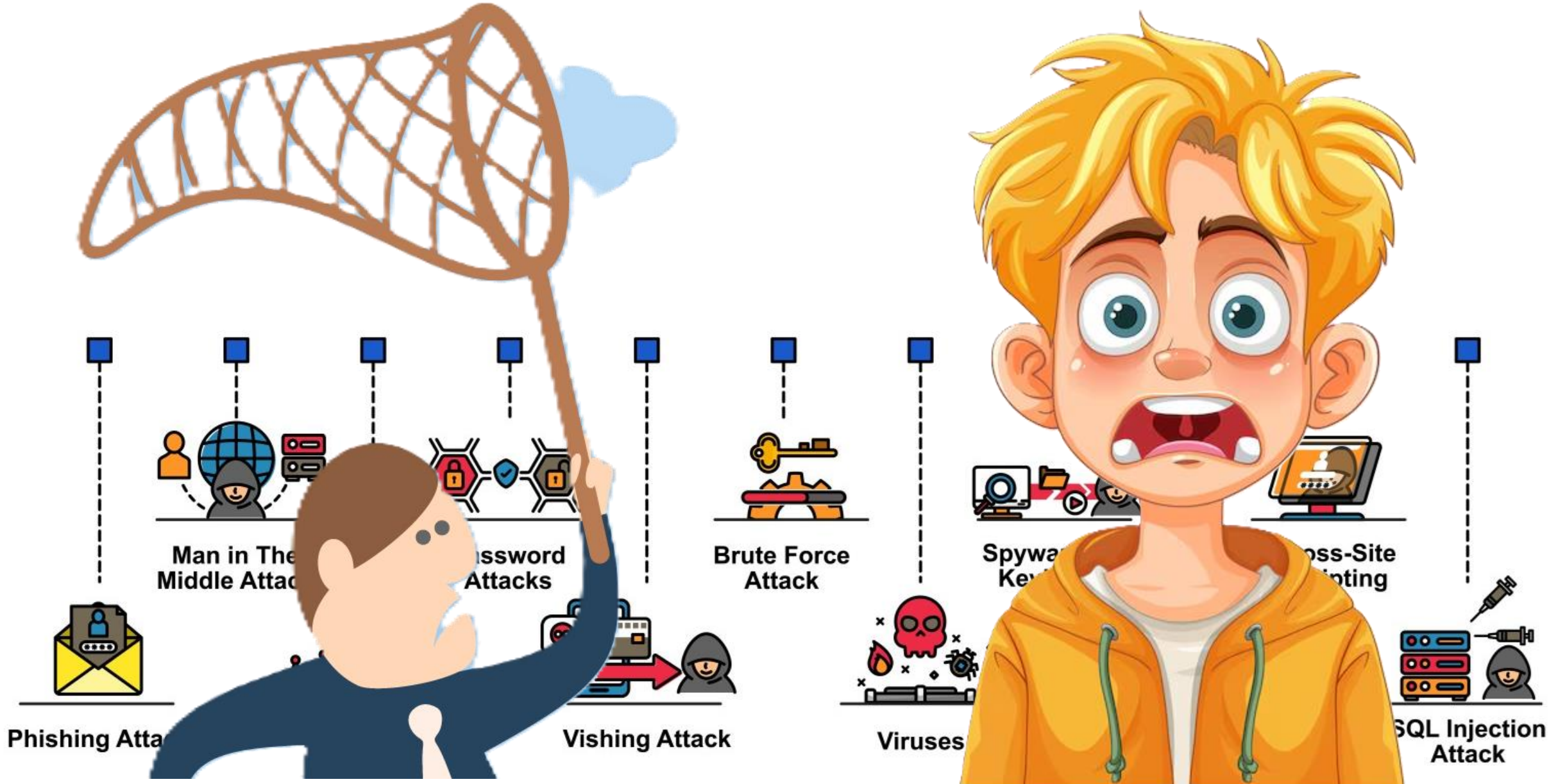
PHONE

TABLET

EMAIL

CLOUD

JAK TO ZVLÁDNOUT ?



SPOLEHLIVOST

DŮVĚRA

Bitdefender

Bitdefender
Založen roku 2001

1800+ zaměstnanců ...
>60% Vývoj a Výzkum/ engineering

Enterprise HQ v Silicon Valley (Santa Clara, California). Vývoj hlavně v Rumunsku

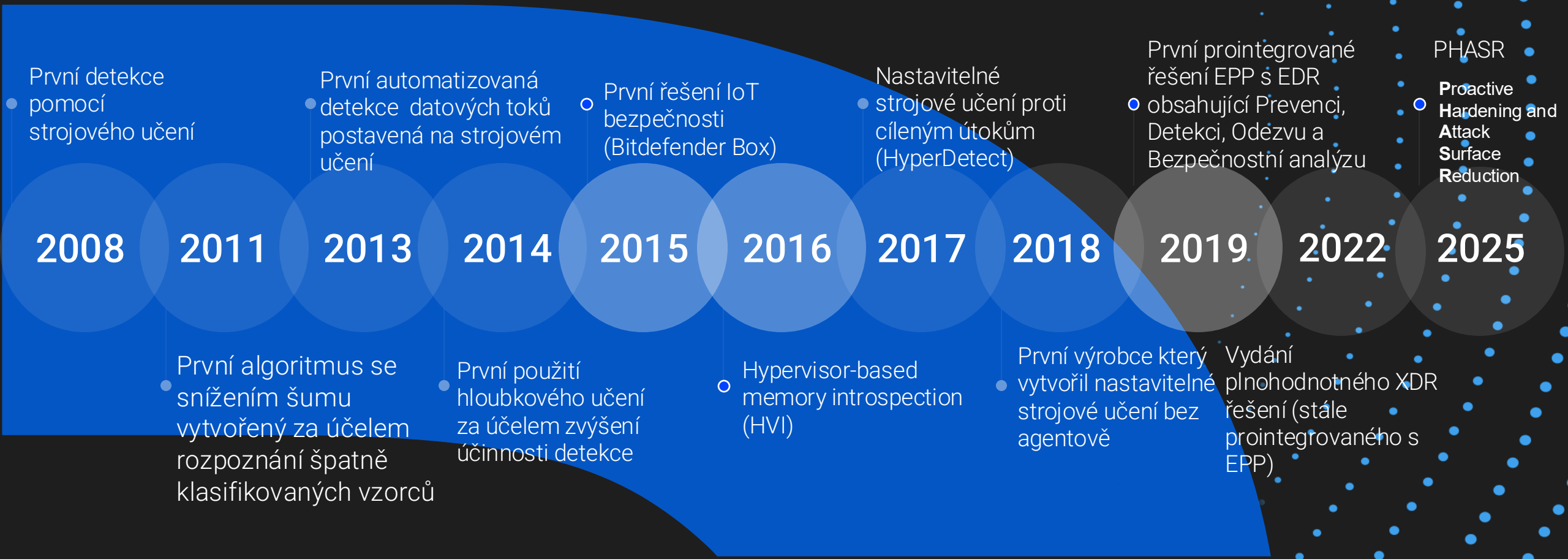
Enterprise business roste +90% rok od roku

Provozujeme celosvětově největší bezpečnostní infrastrukturu chránící >600 000 000 strojů ve 150 zemích

Bitdefender

UZNÁVANÝ INOVATIVNÍ LÍDR

PATENTOVÉ PORTFOLIO: 540+ SCHVÁLENÝCH A DALŠÍ PŘED SCHVÁLENÍM
PRŮKOPNÍK V OBLASTI NASAZENÍ STROJOVÉHO UČENÍ JIŽ OD 2008.



Bezpečnost je potřeba stavět na pevných základech

180 + OEM PARTNERŮ

Bitdefender / FERRARI TEAM PARTNER

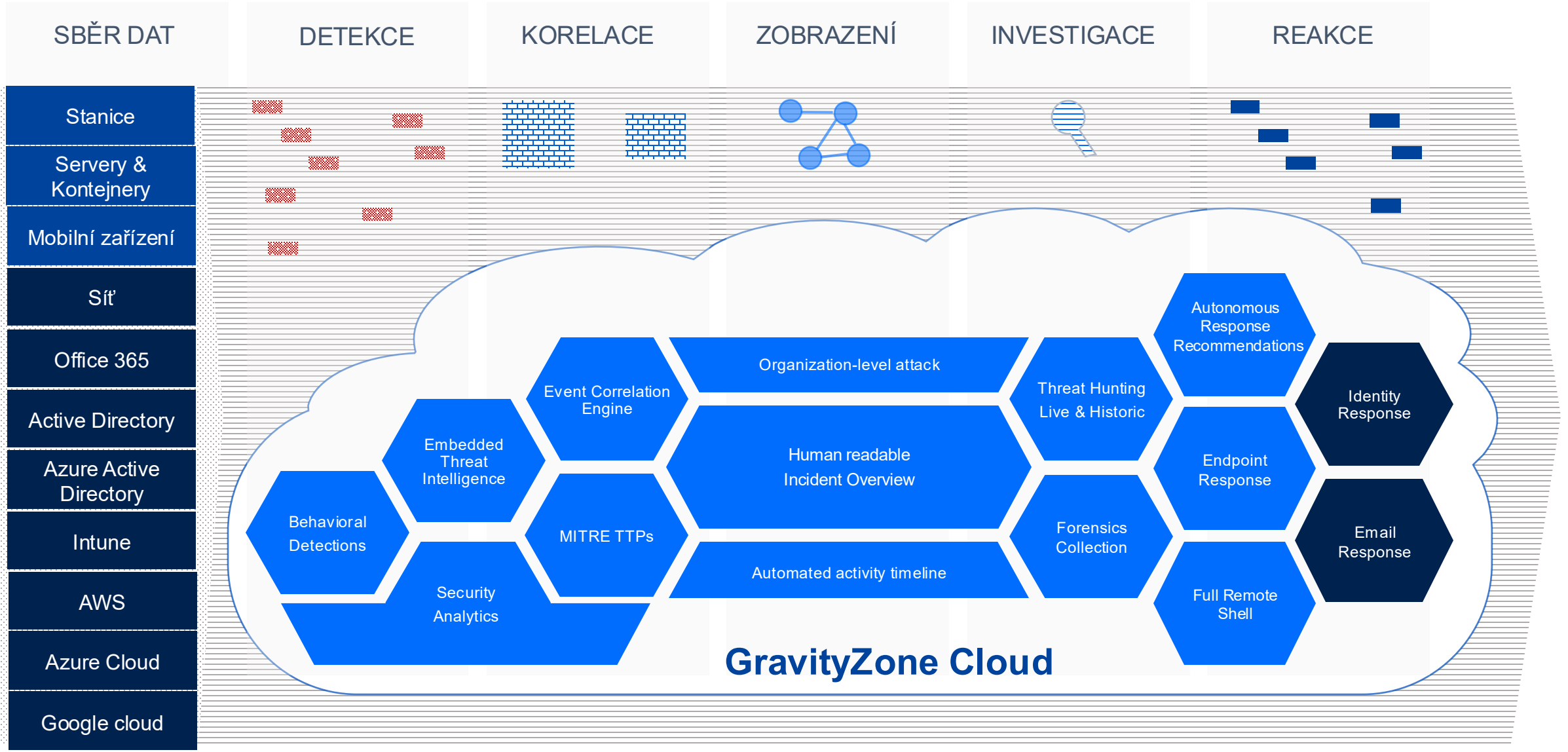
EDR A XDR

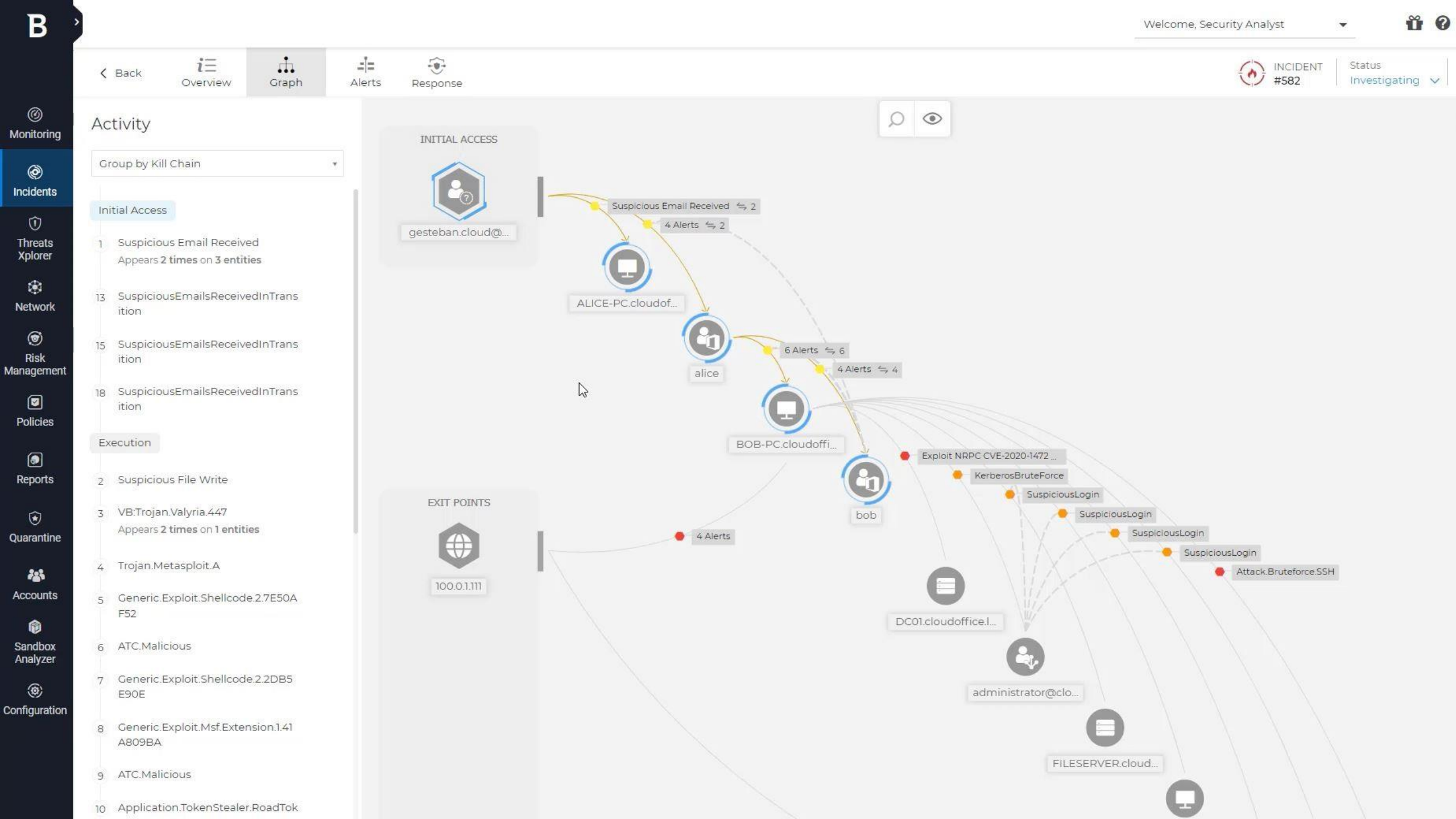
bez AI to dnes nejde

Bitdefender

Aktivace pomocí add-onů

PŘEHLED




Welcome, Security Analyst
Back
Overview
Graph
Alerts
Response
INCIDENT
#582
Status
Investigating
Monitoring
Incidents
Threats Xplorer
Network
Risk Management
Policies
Reports
Quarantine
Accounts
Sandbox Analyzer
Configuration
Activity
Group by Kill Chain
Initial Access
1 Suspicious Email Received
Appears 2 times on 3 entities
13 SuspiciousEmailsReceivedInTransition
15 SuspiciousEmailsReceivedInTransition
18 SuspiciousEmailsReceivedInTransition
Execution
2 Suspicious File Write
3 VB:Trojan.Valyria.447
Appears 2 times on 1 entities
4 Trojan.Metasploit.A
5 Generic.Exploit.Shellcode.2.7E50AF52
6 ATC.Malicious
7 Generic.Exploit.Shellcode.2.2DB5E90E
8 Generic.Exploit.Msf.Extension.1.41A809BA
9 ATC.Malicious
10 Application.TokenStealer.RoadTok
INITIAL ACCESS
gesteban.cloud@...
Suspicious Email Received 2
4 Alerts 2
ALICE-PC.cloudof...
alice
6 Alerts 6
4 Alerts 4
BOB-PC.cloudoffi...
bob
Exploit NRPC CVE-2020-1472 ...
KerberosBruteForce
SuspiciousLogin
SuspiciousLogin
SuspiciousLogin
SuspiciousLogin
Attack.Bruteforce.SSH
EXIT POINTS
100.0.1.111
4 Alerts
DC01.cloudoffice.l...
administrator@clo...
FILESERVER.cloud...

Monitoring
Incidents
Threats Xplorer
Network
Risk Management
Policies
Reports
Quarantine
Accounts
Sandbox Analyzer
Configuration

83/100
Incident Severity Score

Created: 01 Feb 2022, 13:13:48
Last updated: 01 Feb 2022, 13:19:31
Type of attack: Exfiltration, Exploit, SpearPhishing

SUMMARY

A potential network breach originating from 2 users has been detected as part of 5 alerts affecting the following: 2 managed assets and 2 users.

Lateral Movement originating from managed asset: BOB-PC and user: alice has been detected in your network as part of 12 alerts affecting the following: unmanaged asset: FILESERVER2.cloudoffice.local 5 managed assets and user: bob.Multiple attempts to gain or maintain the persistence of a possible malicious objects were detected in 3 alerts on managed asset: CFO-PC and user: administrator@cloudoffice.local.These 3 managed assets were the source of malicious actions detected in 57 alerts affecting 5 managed assets and 2 external ips.Sensitive data may have been exfiltrated to external ip: 100.0.1.111 based on 3 alerts originating from managed asset: CEO-PC.

ROOT CAUSE

The attacker gained access to the network because a malicious email was received on O365 user: alice on managed asset: ALICE-PC.cloudoffice.local from external address: gesteban.cloud@gmail.com resulting in a connection to an external ip 100.0.1.111.

ATT&CK TACTICS AND TECHNIQUES

Initial Access	T1566	Phishing
	T1078	Valid Accounts
	T1190	Exploit Public-Facing Application
Execution	T1204	User Execution
	T1059	Command and Scripting Interpreter
Persistence	T1137	Office Application Startup
	T1078	Valid Accounts

ORGANIZATION IMPACT

6 2 3 9

HIGHLIGHTS

Suspicious Email Received | Initial Access

Severity: Low

An email containing suspicious attachments has been received.

Detected by *Endpoint* on 01 Feb 2022 at 13:12:59

1 1

+ 4 OTHER INITIAL ACCESS ALERTS

Exploit NRPC CVE-2020-1472 ZeroLogon | Lateral Movement

Severity: High

Network Attack Defense has detected a crafted login attempt that exploits an elevation of privilege vulnerability via Netlogon Remote Protocol.

Detected by *Endpoint* on 01 Feb 2022 at 13:15:41

1 1

+ 11 OTHER LATERAL MOVEMENT ALERTS

KerberosBruteForce | Persistence

Severity: Medium

Possible brute force attack on a service server that uses kerberos login.

Detected by *Endpoint* on 01 Feb 2022 at 13:16:13

1 1

+ 2 OTHER PERSISTENCE ALERTS

Generic.Exploit.Shellcode.2.7E50AF52 | Execution

Severity: High

Shell code used for post exploitation has been loaded into memory

RESPONSE

ACTION NEEDED (49) | EXECUTED (3)

CONTAINMENT

3 Users to block
8 Hosts to isolate

VIEW DETAILS

MITIGATION

1 IP address to block
2 File hashes to block
1 Security solution to instal on unmanaged asset
1 Email address to block

VIEW DETAILS

REMEDIATION

1 Email to delete
8 AM scans to run
8 System repairs to run

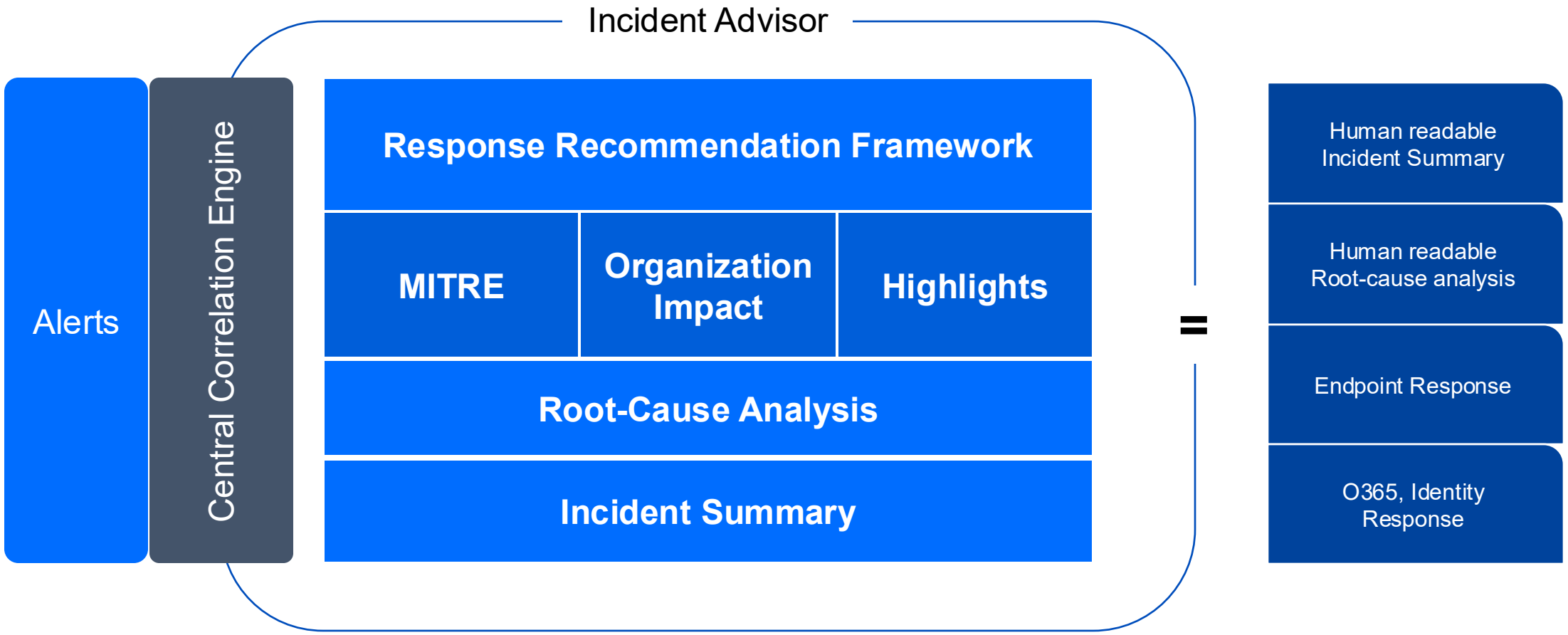
VIEW DETAILS

HARDENING

POMOCNÍK S INCIDENTY

Bitdefender

Incident Advisor



Bitdefender

Jaké otázky Vám incident Advisor automaticky zodpoví ?

Při návrhu poradce pro incidenty jsme vycházeli z následující myšlenky:

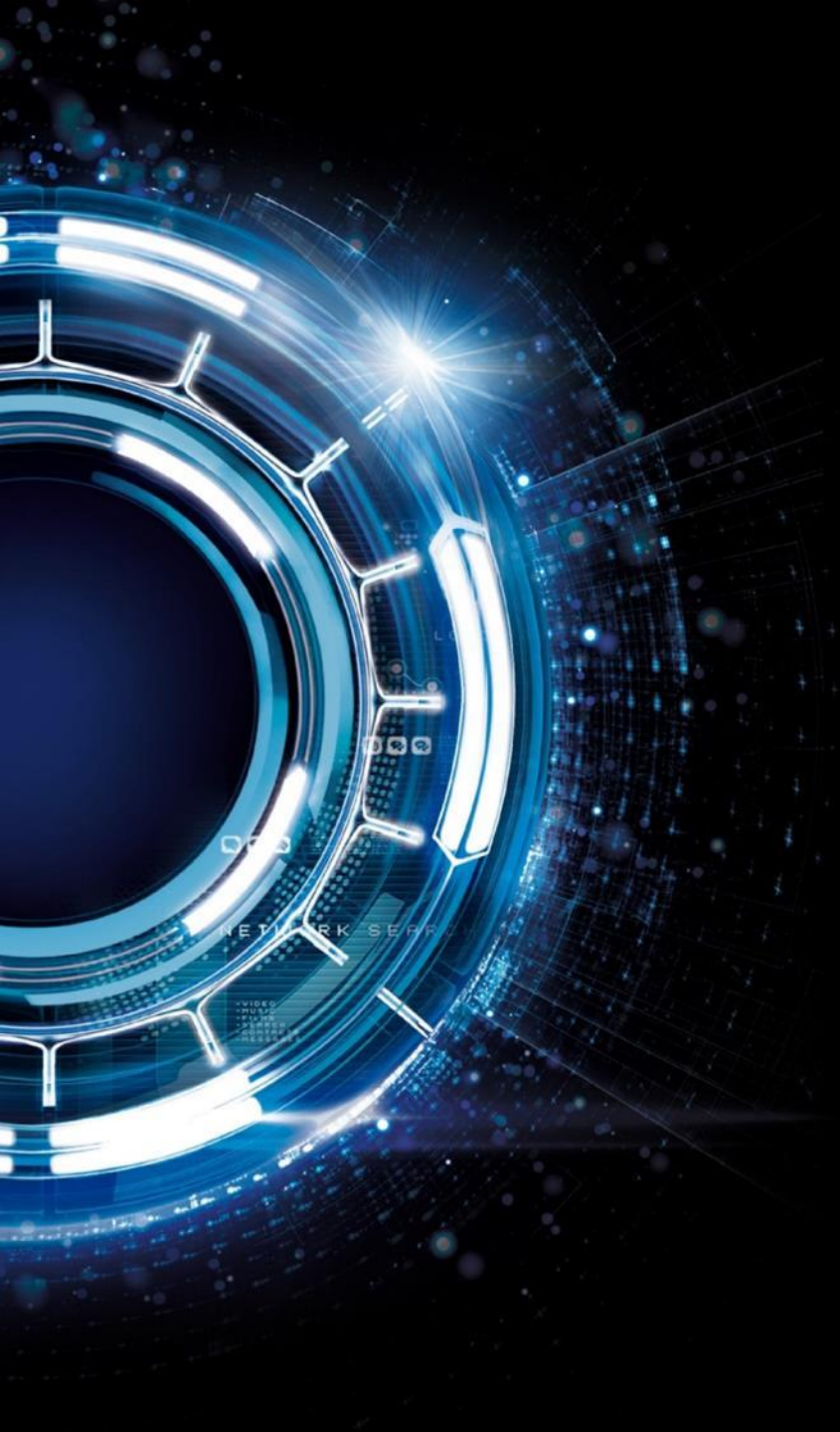
- bez ohledu na úroveň dovedností musí analytici při prvním pohledu na bezpečnostní incident pochopit následující:

- **co se vůbec stalo?**
- **kdy to začalo?**
- **kam se to rozšířilo?**
- **jak reagovat?**
- **proč to bylo vůbec možné?**
- **jak to můžeme zmírnit, vyléčit?**
- **jak máme zamezit dalšímu šíření?**

Bitdefender

MITRE Engenuity ATT&CK® Evaluations 2024

		Bitdefender	BlackBerry	CrowdStrike	Field Effect	Microsoft	Palo Alto Networks	Secureworks	SecurityHQ	SentinelOne	Sophos	Trend Micro	Mean	Median
Coverage Quality	Visibility (data collected)	100%	98%	100%	95%	100%	100%	100%	100%	100%	100%	100%	99%	100%
	Reported (not actionable)	95%	81%	98%	58%	86%	88%	58%	77%	88%	84%	84%	80%	84%
	Reported (actionable)	93%	70%	93%	47%	63%	79%	53%	56%	72%	63%	51%	65%	63%
	Were any Red Team activities missing from incident reports?	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	N/A	N/A
Speed	MTTD (minutes)	24	48	4	11	24	24	33	93	47	72	65	42	40
Noise	Emails + Alerts	82	394	579	196	385	1119	878	200	189	942	310	519	390
	Total Emails	54	307	326	98	162	37	51	125	32	24	138	130	112
	Total Alerts in Console	28	87	253	98	223	1082	827	75	157	918	172	389	198



UMĚLÁ INTELIGENCE

STROJOVÉ UČENÍ

Bitdefender

Game Changer

GeForce RTX 50 Series, powered by Blackwell and AI.

NVIDIA GEFORCE RTX
Powering Advanced AI

Inovace v AI a ML

Bitdefender

am

eam
echnologies.

2014

First use of deep learning

The first use of deep learning AI algorithms to increase detection rates.

First tunable machine learning

Bitdefender HyperDetect enables organizations to fine-tune ML detection and stop advanced attacks at pre-execution.

2017

2017

Fileless Attack Protection

Using custom ML models to perform feature extraction from command lines and PowerShell scripts stops file-less malware. This research earned us the "Key Innovators" title by the European Commission.

Anomaly Detection in EDR

Anomaly Defense leverages AI technologies to build behavior baselines and spot anomalies with minimum noise.

2020

2022

Native XDR with human-readable Incident Advisor

Bitdefender Native XDR uses ML to automatically correlate and consolidate threat signals across endpoints, identities, apps, network, clouds, mobile devices and beyond. The Incident Advisor answers all key analyst questions in a human-readable format.

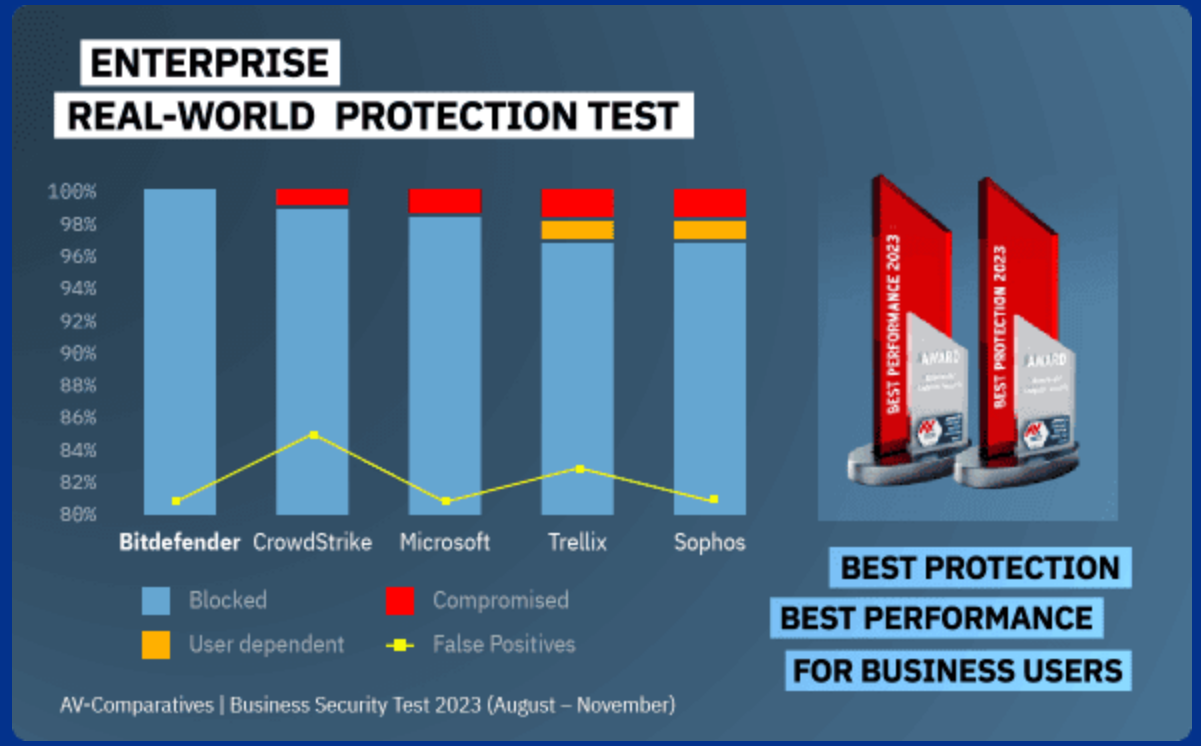
GravityZone AI Assistant

The Bitdefender GravityZone AI Assistant leverages Large Language Models (LLMs) to streamline and simplify threat investigations by answering analysts' questions instantly.

2024

Skutečná ochrana

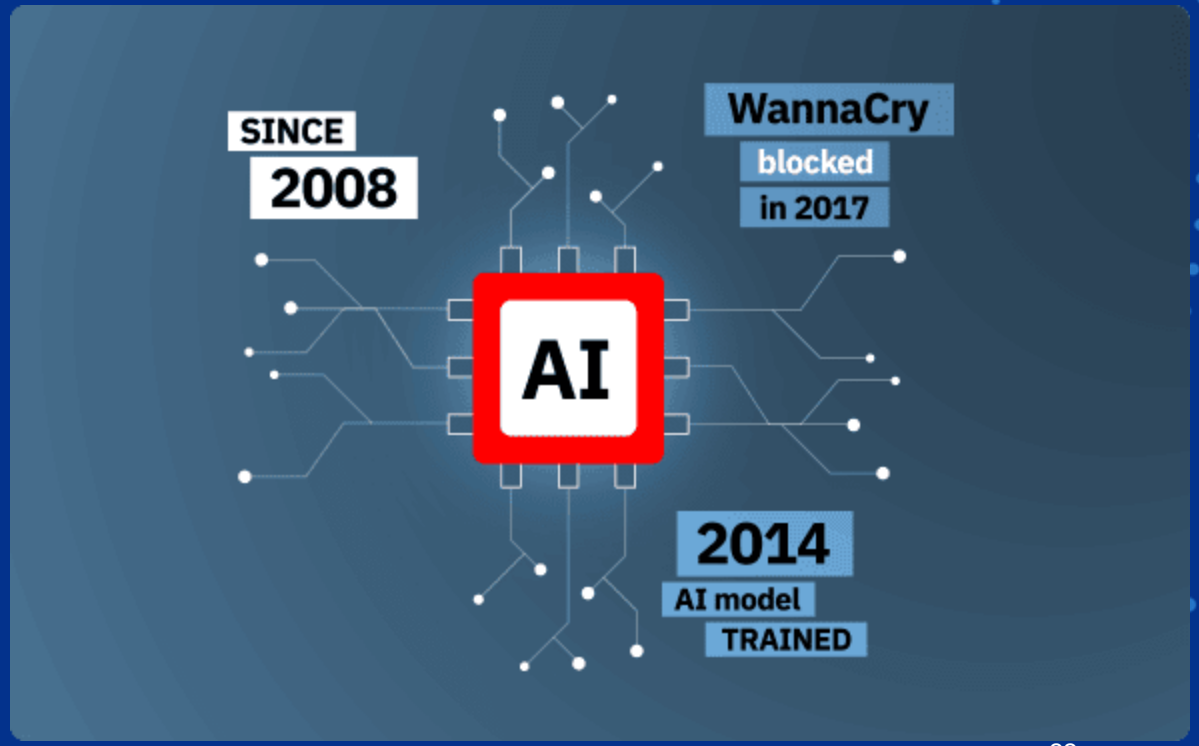
Bitdefender



Více než 80 000 vzorů chování škodlivého kódu

180+ TOP partnerů licencuje Bitdefender

Každou minutu zjistíme 400+ hrozeb



Čemu věříme a na čem stavíme

Bitdefender

Věříme, že umělá inteligence je pro obránce výhodnější než útočníky

V Bitdefenderu spoléháme na vědu, ne na spekulace

Neustále přehodnocujeme vektory útoků

Proti čemu stojíme

Bitdefender

Sociální inženýrství podporované umělou inteligencí

Malware a ransomware generovaný umělou inteligencí

Automatizované útoky a průzkum

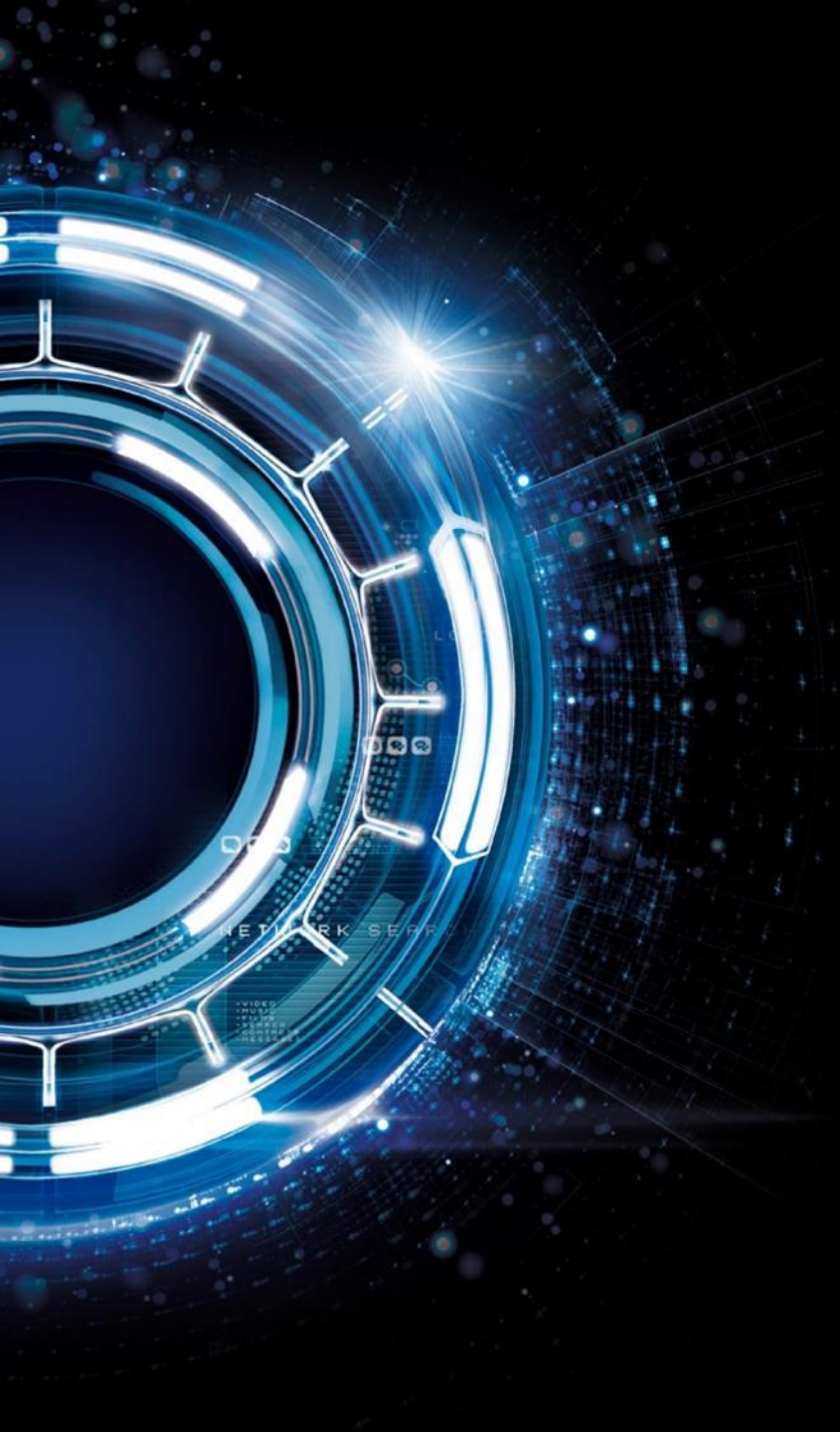
HyperDetect

Bitdefender

Bezpečnostní vrstva, která zlepšuje obranu proti pokročilým hrozbám

Využívá lokální ML k identifikaci hrozeb

- Bezsouborové útoky
- Exploitace
- Cílené útoky
- Ransomware
- Grayware



KLASICKÁ BEZPEČNOST

Bitdefender

Národné centrum kybernetickej bezpečnosti SK-CERT analyzoval nedávne medializované útoky. Tu sú podrobnosti a odporúčania

Ransomware 1

Malvér má nasledujúce schopnosti:

- deaktivácia antivírusového softvéru (vypnutím funkcií, antivírusový softvér sa po deaktivácii naďalej javí ako funkčný, ale zmeny možno pozorovať v jeho nastaveniach)
- zmazanie lokálnych údajových štruktúr, ktoré by mohli napomôcť obnove (shadow copies)
- šifrovanie lokálnych súborov
- identifikácia a šifrovanie priečinkov dostupných po sieti

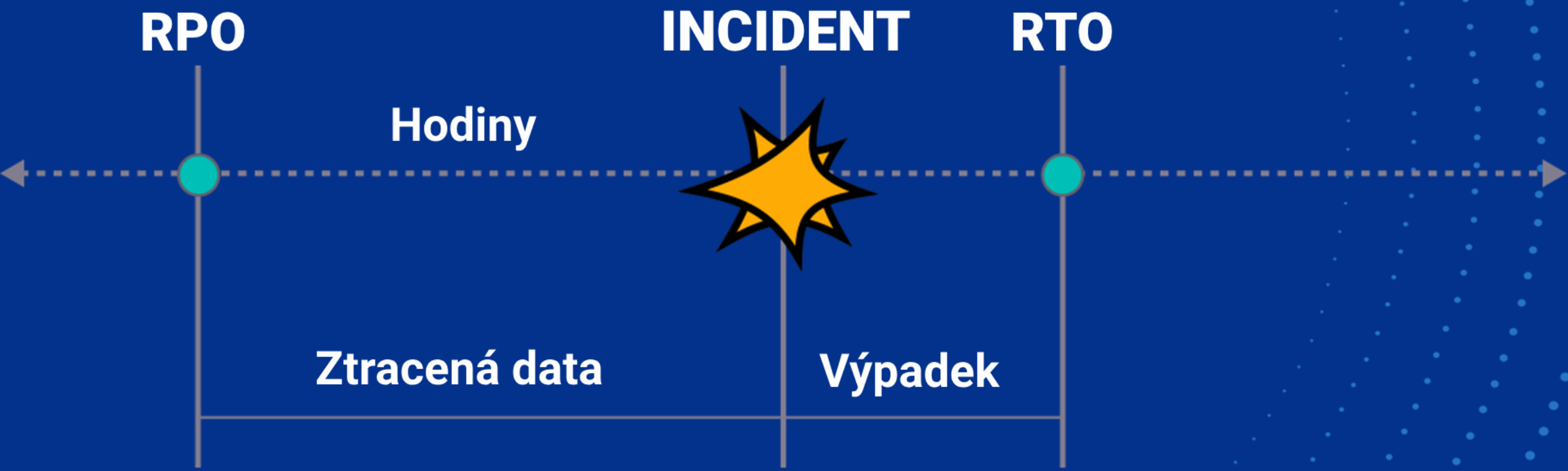
Proces je prítomný v pamäti a po vytvorení nových súborov ich automaticky znova zašifruje.

Preventívne odporúčania:

- majte k dispozícii zálohy, preferovane v offline forme (cold stand-by)
- nikdy nezálohujte formou kopírovania dát na sieťový priečinok, ale využívajte zálohovací softvér, ktorý dáta z počítačov sám sťahuje
- na zálohovací softvér, virtualizačnú platformu a diskové úložiská nikdy neumožnite prihlásenie s doménovými účtami. Používajte na nich jedinečné heslá, ktoré nebudete mať uložené na pracovných staniciach
- nepublikujte služby ako RDP a/alebo VNC na verejných IP adresách. Pri potrebe vzdialeného prístupu použite šifrovaný VPN prístup, ktorý býva bežnou súčasťou sieťových firewallov. Je tiež možné zvoliť niektorý z voľne

Zálohování vs Obnova

Bitdefender



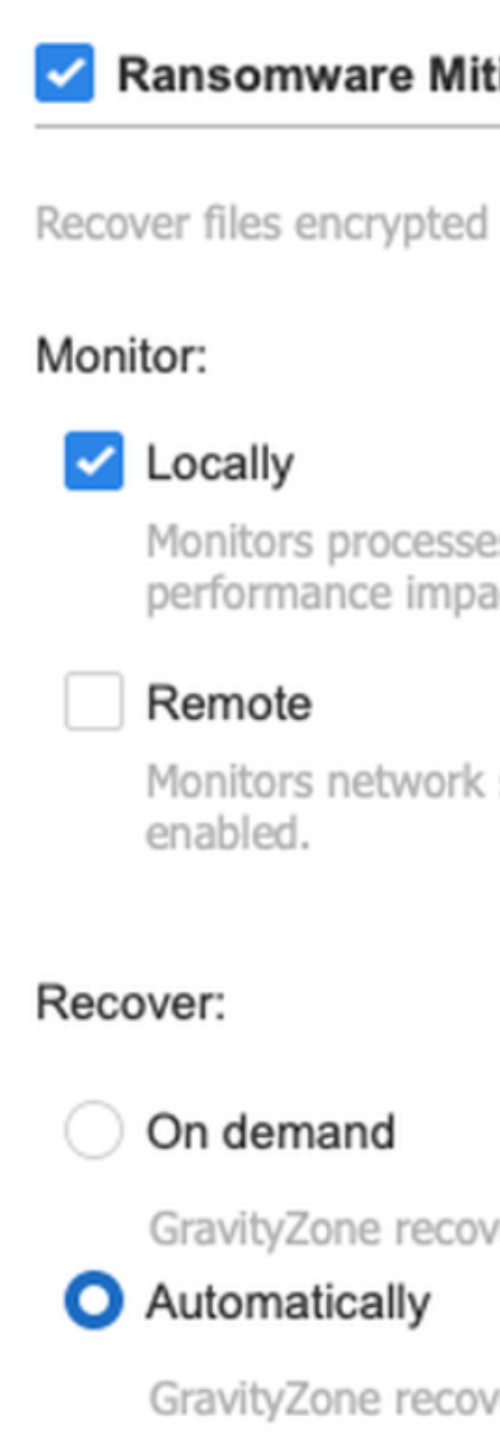
Ransomware Mitigation

Bitdefender

- Důležité je, že tato metoda nespoléhá na službu VSS Shadow Copy ani na jiná řešení statického zálohování, protože tato záložní data jsou téměř vždy odstraněna !
- Požadavky na odstranění stínových kopií jsou jedním ze spouštěčů incidentu EDR.
- Pomocí tohoto přístupu zajišťujeme zmírnění ransomwaru i proti dosud neznámým variantám ransomwaru.

Ransomware Mitigation

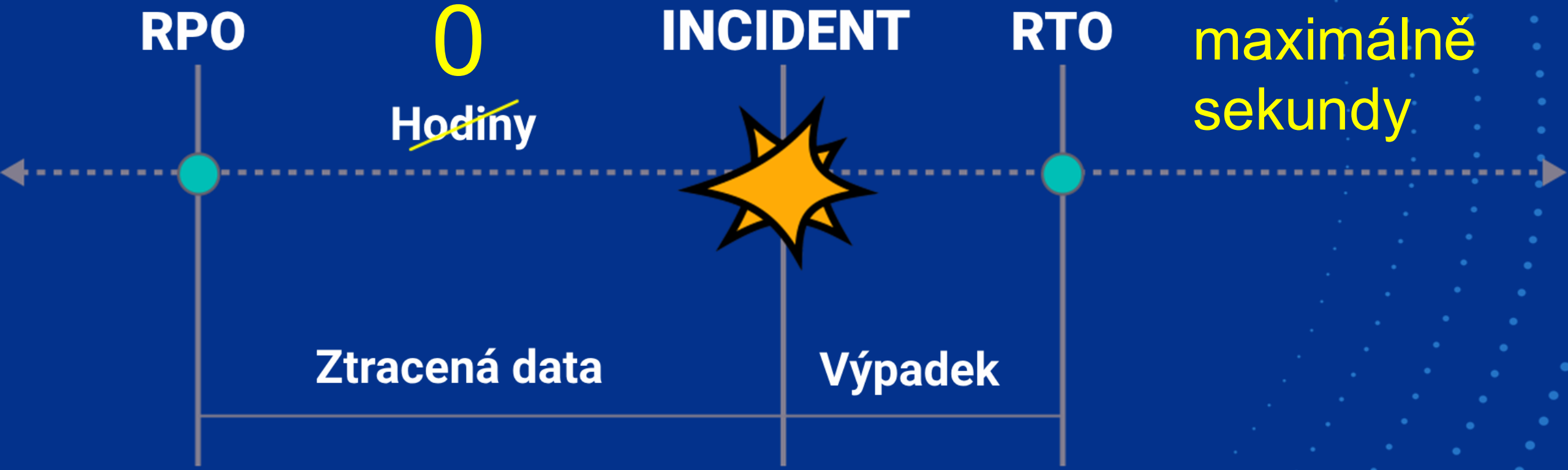
- Ransomware Mitigation využívá technologie detekce a nápravy, které chrání vaše data před útoky ransomwaru.
- Ať už se jedná o známý nebo nový ransomware, GravityZone detekuje neobvyklé pokusy o šifrování a proces zablokuje.
- Následně obnoví soubory ze záložních kopií do původního umístění.



Zálohování vs Obnova

Bitdefender

s Bitdefender Ransomware Mitigation



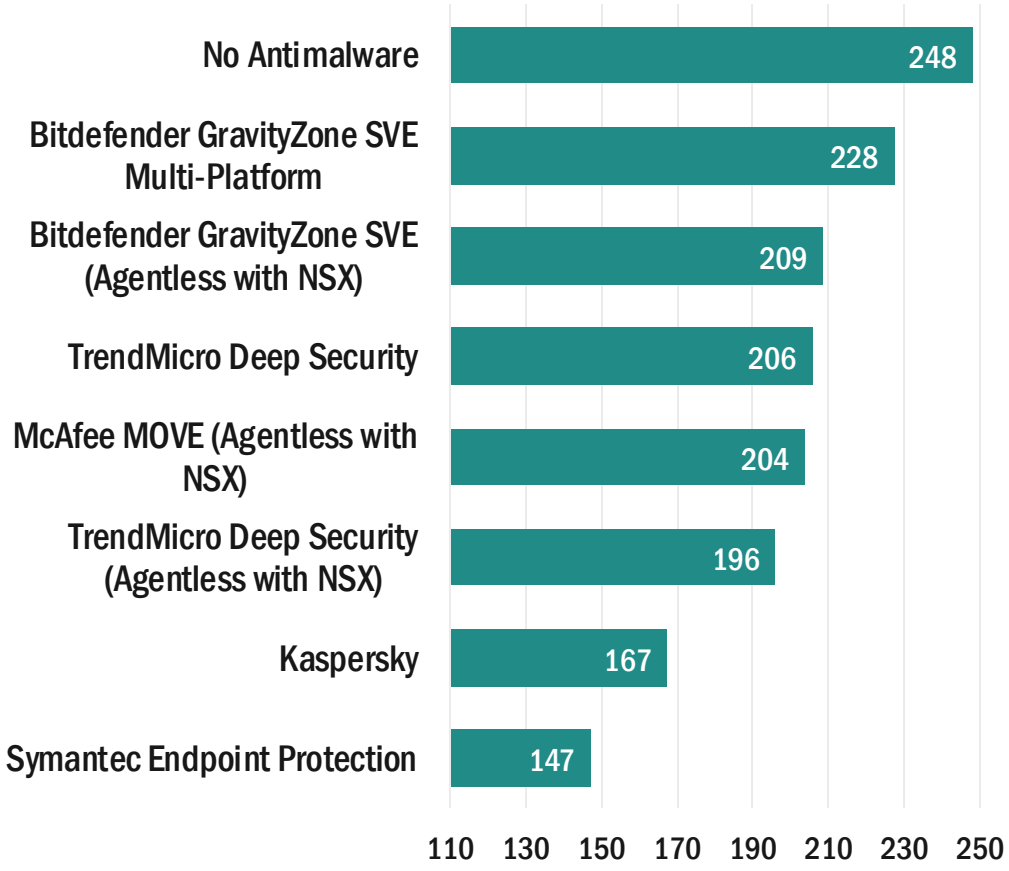
A to rozhodně není vše

Bitdefender

BEZPEČNOST VIRTUALIZACE

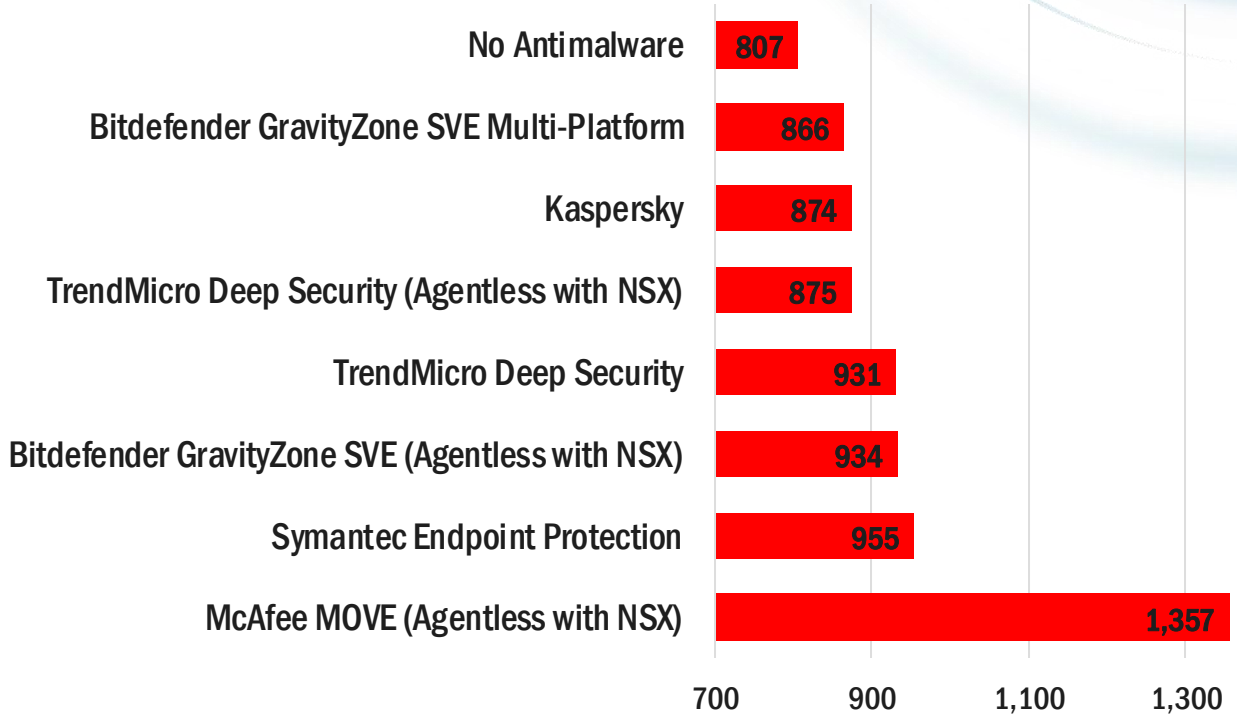
Snížení nákladů na infrastrukturu

Počet konkurentních VDI Sessions



AŽ O 36% RYCHLEJŠÍ ODEZVA APLIKACÍ

Čas odpovědi nestresovaného systému [ms]



Snížení nároků na infrastrukturu = úspora nákladů (VSI LOGIN testy)

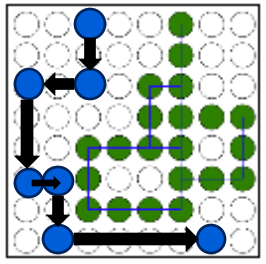
PHASR

Bitdefender

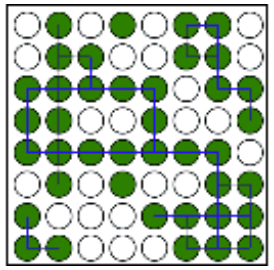
Každý uživatel je jedinečný a proto přístup k tomu jak své zařízení využívá nebo např. které aplikace či nástroje jsou nezbytné pro jeho každodenní pracovní činnost je třeba vyhodnotit zvlášť.

Proactive Hardening and Attack Surface Reduction

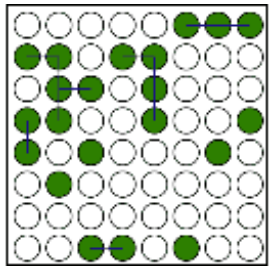
Proaktivní vytvrzení ochrany a snížení útočné plochy pro útočníky



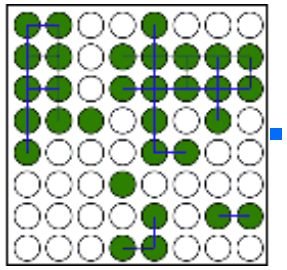
Attack Pattern Identified by the attacker



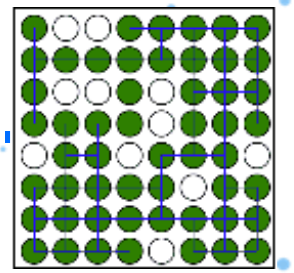
$User_1$ Attack Surface Protection



$User_2$ Attack Surface Protection



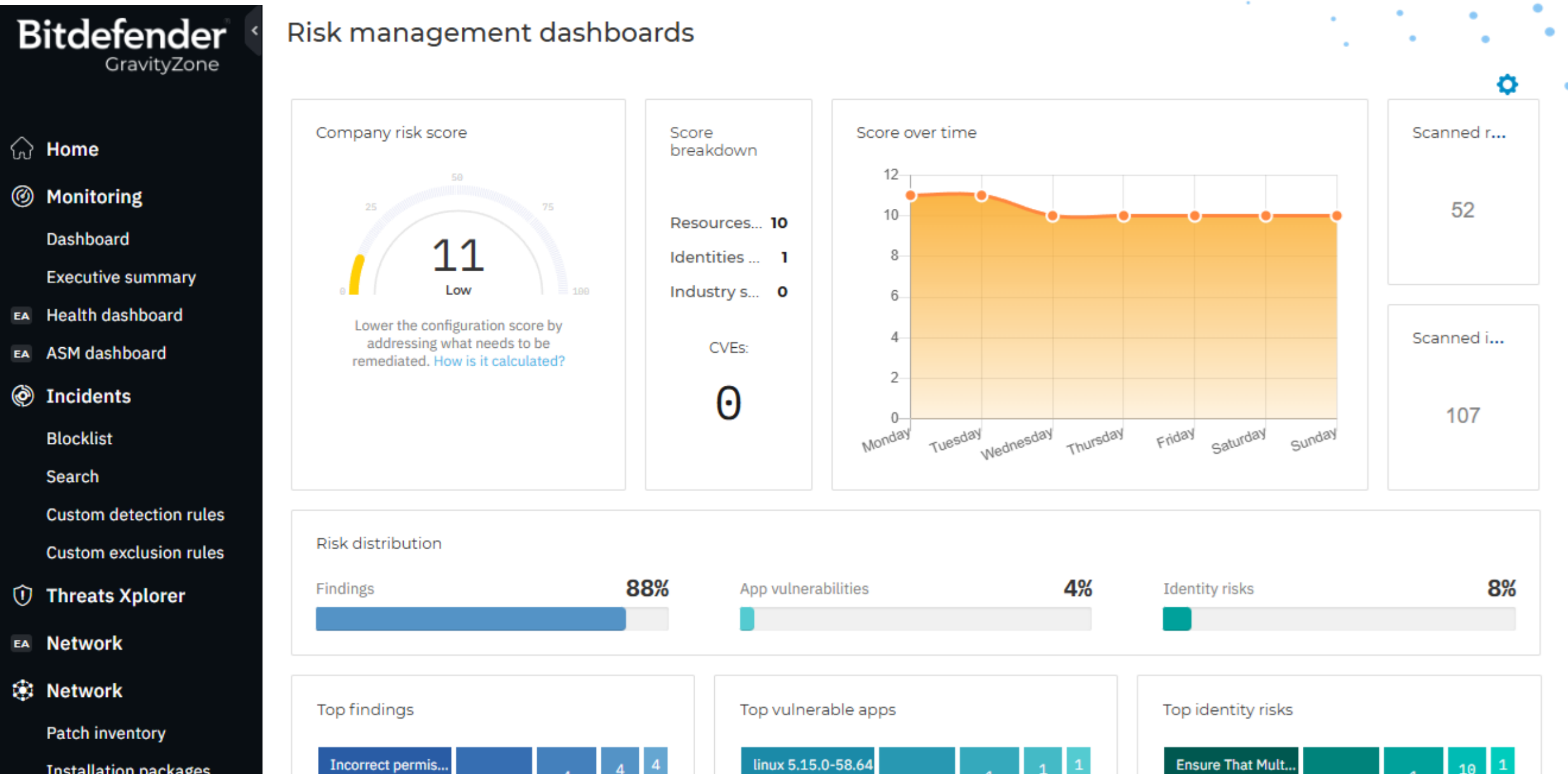
$User_3$ Attack Surface Protection



$User_n$ Attack Surface Protection

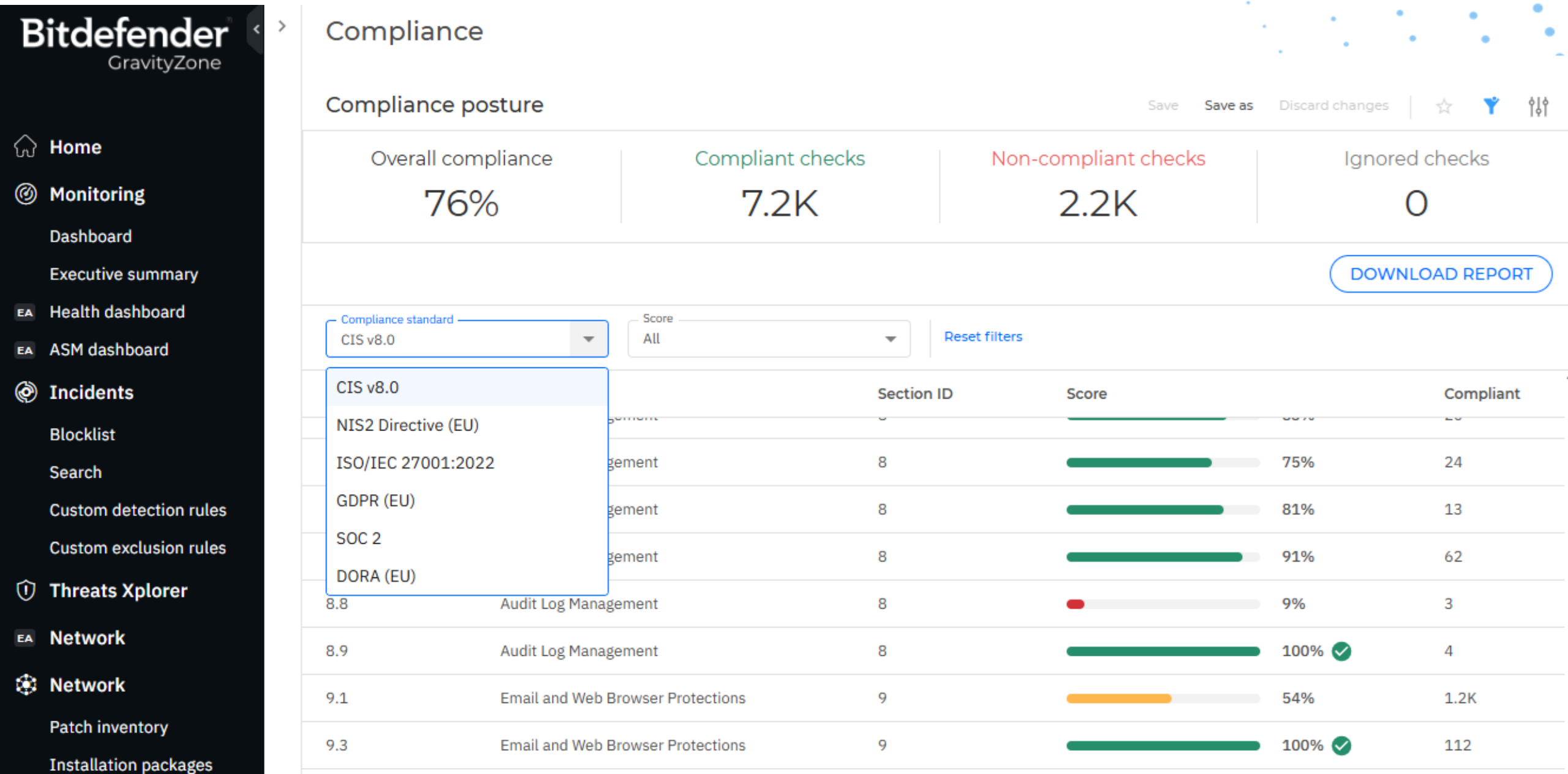
ANALÝZA RIZIK

Bitdefender



SHODA S NIS2

Bitdefender



EXTERNÍ ZRANITELNOSTI

Bitdefender

Bitdefender GravityZone

- Home
- Monitoring
  - Dashboard
  - Executive summary
  - Health dashboard
  - ASM dashboard
- Incidents
  - Blocklist
  - Search
  - Custom detection rules
  - Custom exclusion rules
- Threats Xplorer
- Network
- Network
  - Patch inventory
  - Installation packages

Attack surface management

EASM

Save | Save as | Discard changes

SCAN CONFIGURATION

Last scan
24 March 2025, 21:03

Next scheduled scan
31 March 2025, 22:00

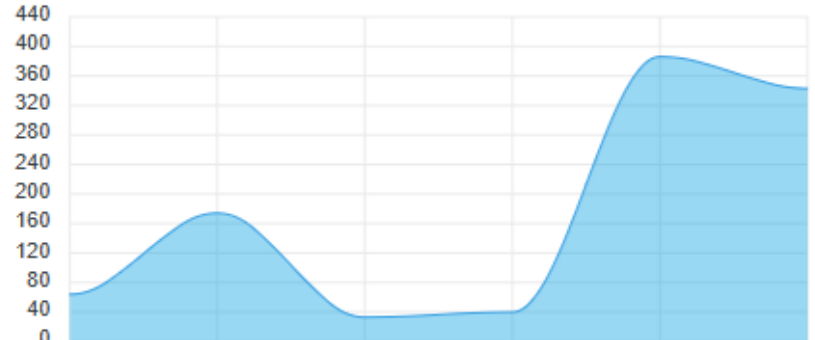
SCAN NOW

Total number of assets

ASN reports	14	Domains	84	DNS records	21	IPv4 addresses	35	Emails	0
Certificates	133	Similar domains	16	IP blocks	17	IPv6 addresses	23	Services	0

ASN reports

Discovered assets per week



Bitdefender®

BUILT FOR RESILIENCE

Děkuji za pozornost