Může ISP efektivně rozšířit NOC a začít budovat SOC?

Jan Kolmačka

Systems Engineer

Agenda

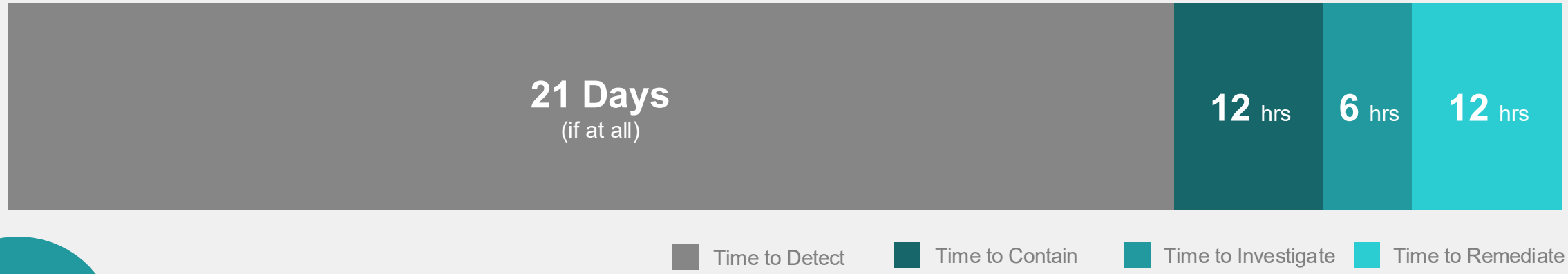
NOC & SOC platformy Fortinetu:

- FortiAnalyzer
- FortiGuard SOC-as-a-Service
- Managed FortiGate Service
- FortiSIEM

Falešný pocit bezpečí

Náklady za falešný pocit bezpečí

Průměrný čas od odhalení k vyřešení hrozby



52%

of organizations report SecOps is harder than 2 years ago, citing threats, attack surface, volume/complexity[1]

NIS2 Rule

1 Day

to initially report incident

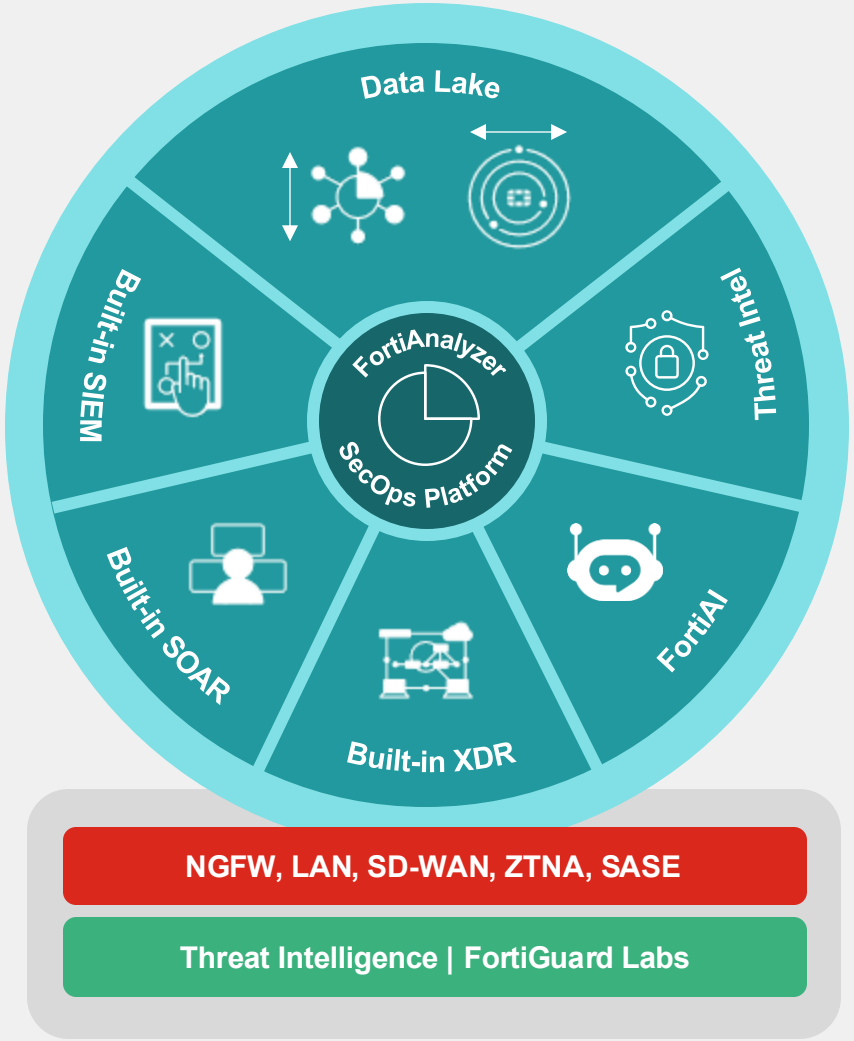
$9.4M

Avg Breach Cost

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, January 2025.

FortiAnalyzer: Funkce na klíč pro začínající SOC

Appliance | Virtual Machine | Cloud | Big Data



Unified Data Lake
Jednotný pohled na logy, dění v síti, výstrahy, hrozby a incidenty

Native Threat Intelligence
Inteligence FortiGuard Labs v reálném čase, včetně Outbreak detekce a Indicator of Compromise (IOC)

Built-in SOC Automation
Zahrnuje odhlehčené funkce SIEMu a SOARu s předkonfigurovaným obsahem

Embedded GenAI-Assistant
Integrovaná FortiAI, pomocí GenAI pro zvýšení efektivity a odezvy

Flexible Deployments
Jednoduché možnosti nasazení jako HW, virtuální appliance nebo v cloudu

FortiAnalyzer: FortiGuard IOC and Outbreak Detection Service

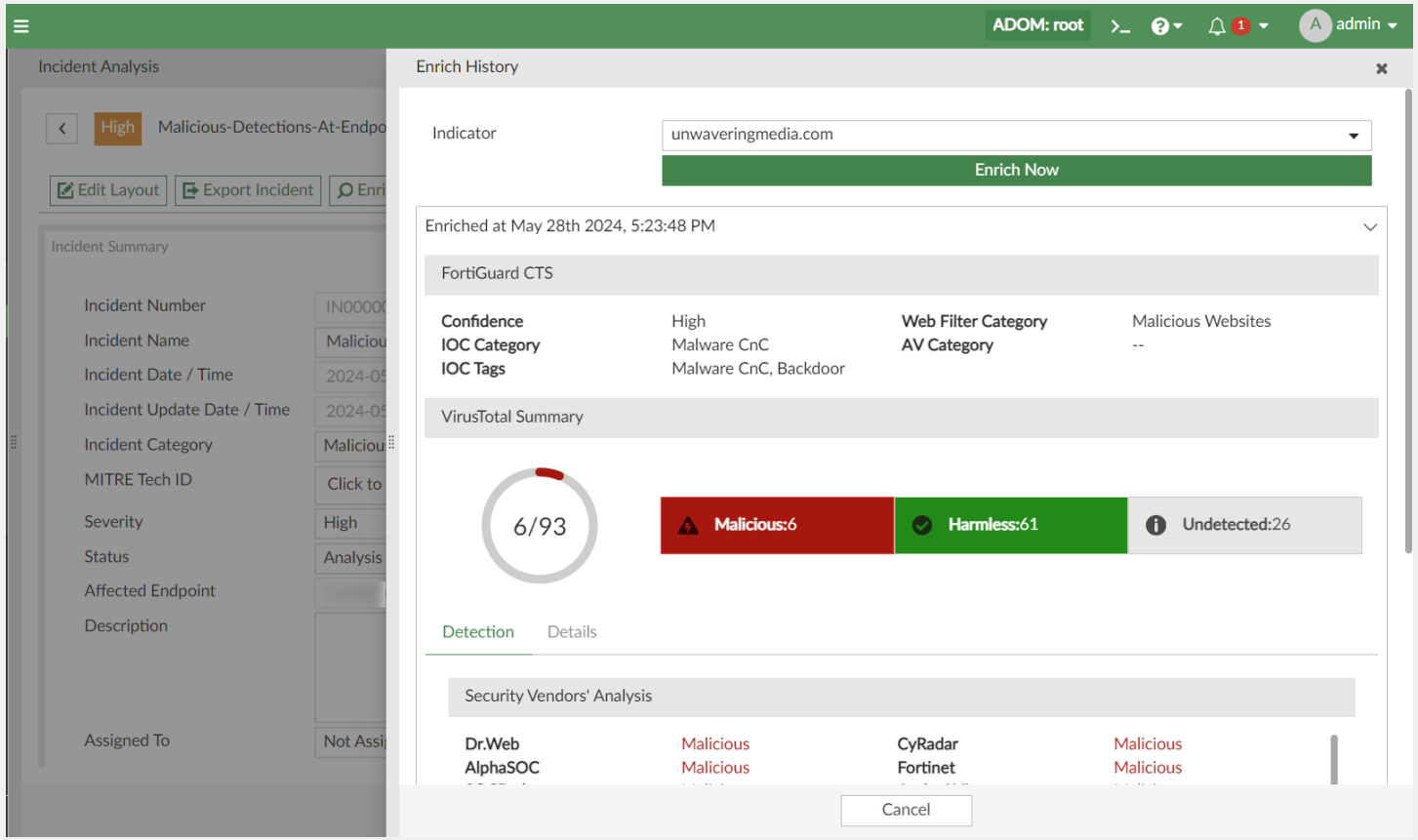
IOC (Indicator of Compromise)

- forenzní data z 500 000 IOC denně
- Seznam IP adres, domén a URL
- FortiAnalyzer identifikuje podezřelé nebo škodlivé infekce a případný průnik
- Historická analýza logů
- Volitelná automatizace pomocí předdefinovaných playbooků

Outbreak Detection

- Aktualizované balíčky hrozeb, event handlerů, korelačních pravidel a reportů
- Souhrné reporty o aktuálních rychle se šířících hrozbách

FortiAnalyzer: Obohacení indikátorů

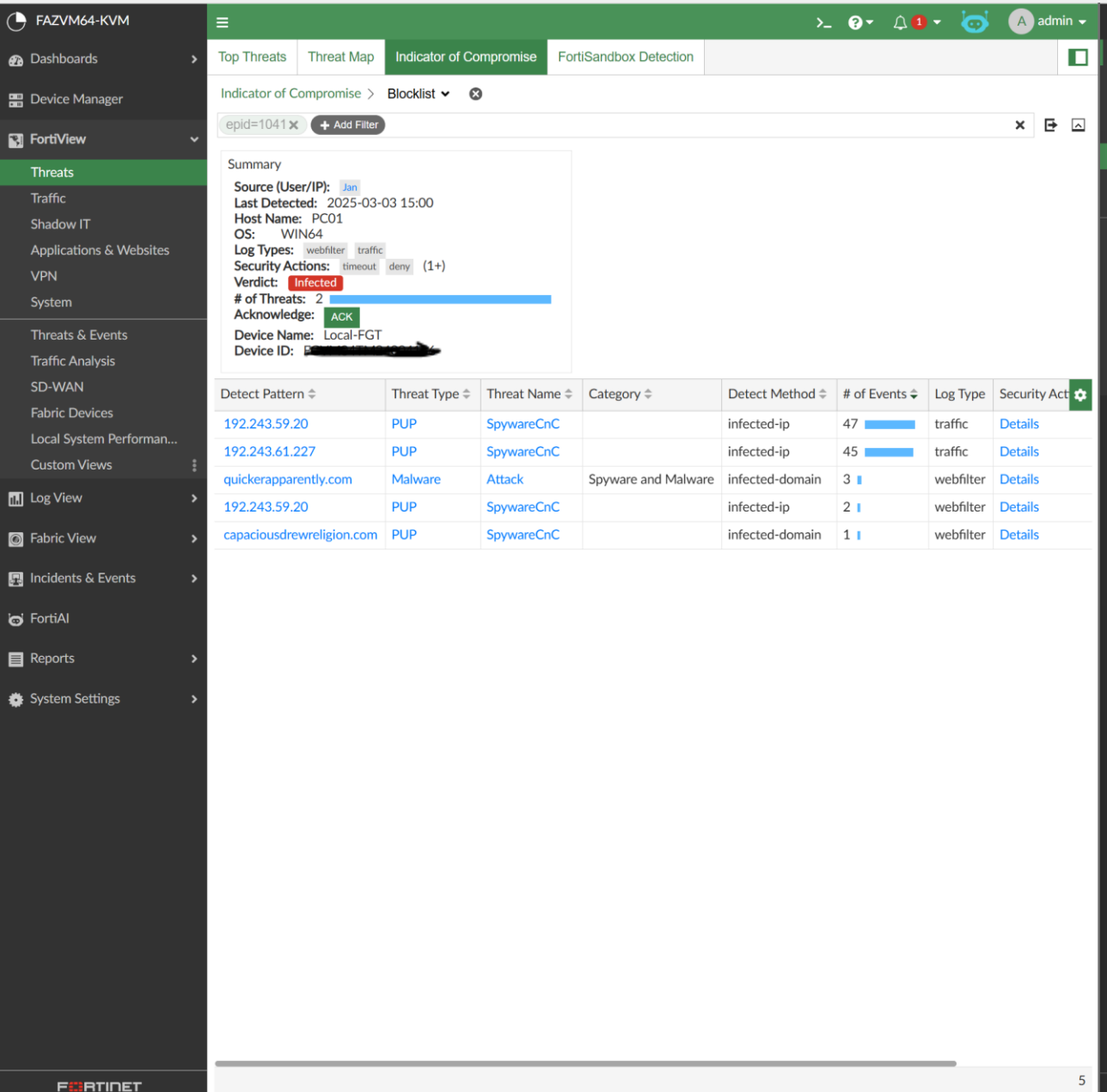


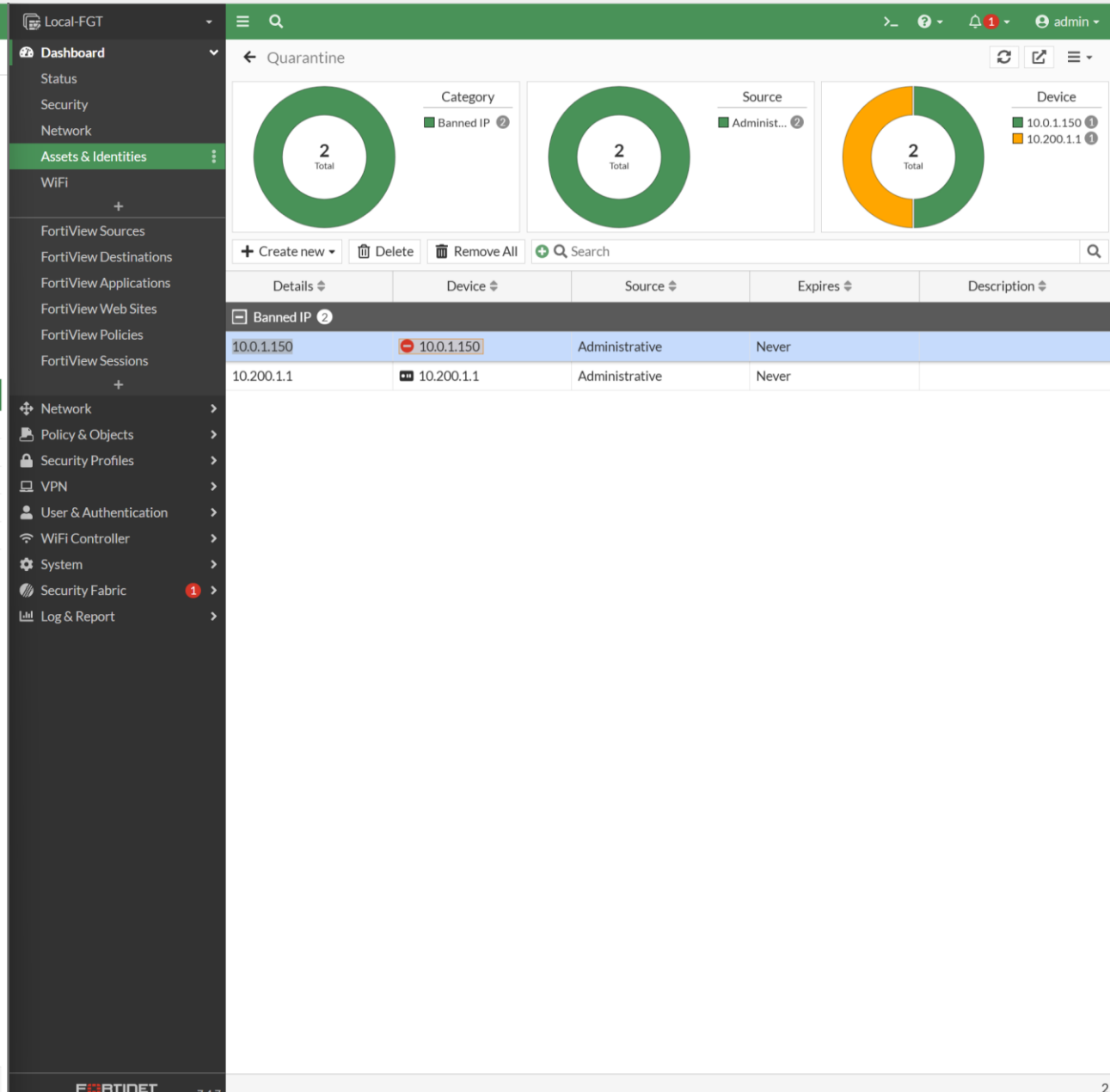
IoC

Intuitivní monitorování a detekce s real-time kontextem síťové aktivity, rizik, zranitelností a pokusů o útok

- Kategorizace hrozeb, stanovení priorit a opětovné skenování
- Vizualizace nalezených hrozeb
- Automatická odezva na detekci hrozeb

FortiAnalyzer: IOC v akci





FortiAnalyzer: Security Automation Service

- Poskytuje balíčky obsahující nové reporty, event handlery, korelační pravidla, log parsery, konektory a playbooky pro SIEM/SOAR funkce FortiAnalyzeru
- Umožní analyzovat a reagovat na bezpečnostní incidenty pomocí předdefinovaných scénářů
- Aktualizace - nové parsery a pravidla vydávány na pravidelné bázi, cca 1x za měsíc
- Duben 2025: 31 log parserů

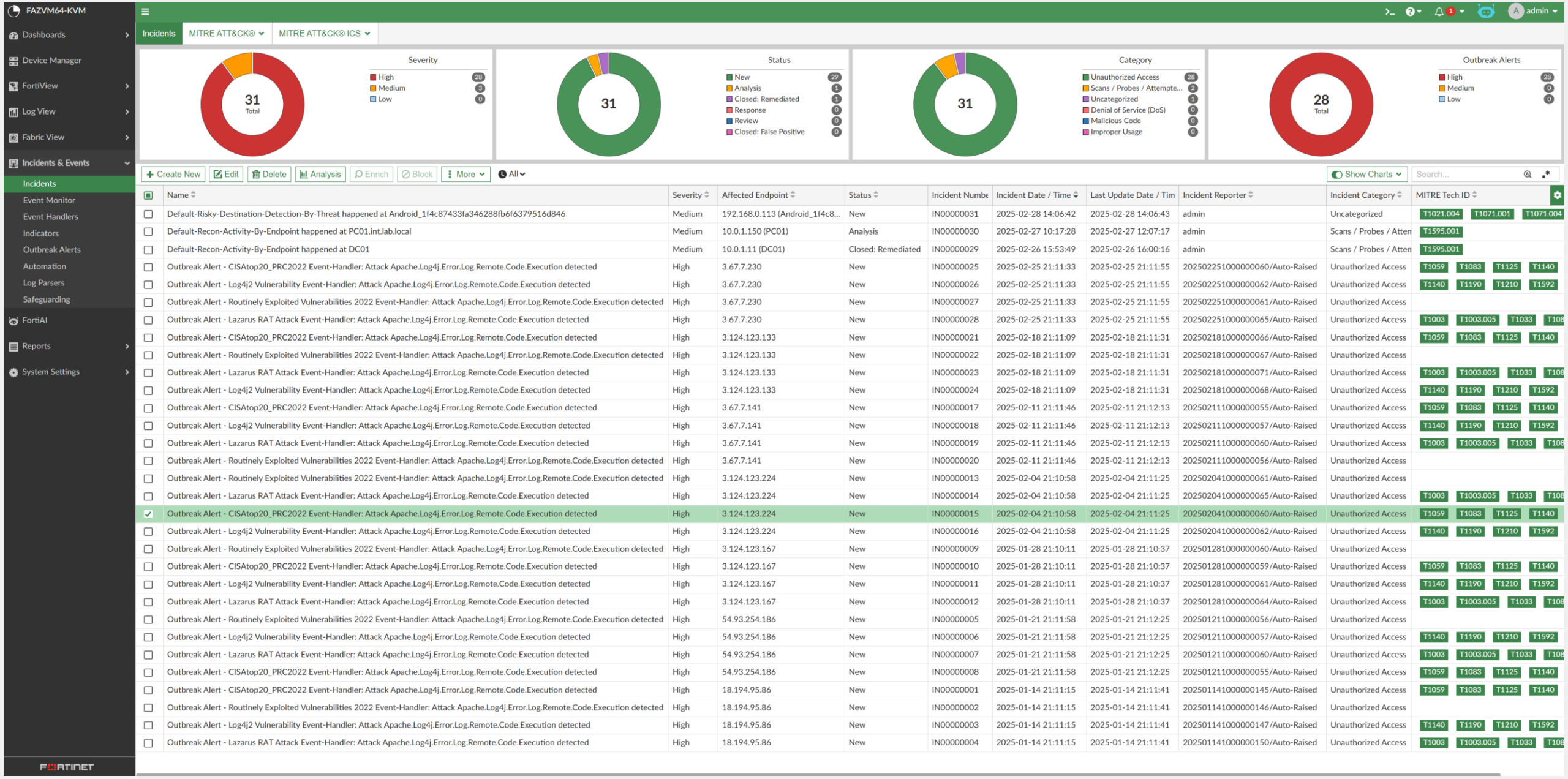
Cisco IOS, Aruba, CheckPoint, Palo Alto, Sophos, Juniper, Zscaler, SonicWall, ForcePoint, Okta, SentinelOne, CrowdStrike, Office365, WMware, Windows, Ubuntu, Apache, Nginx, atd….

Aktuální přehled zde:

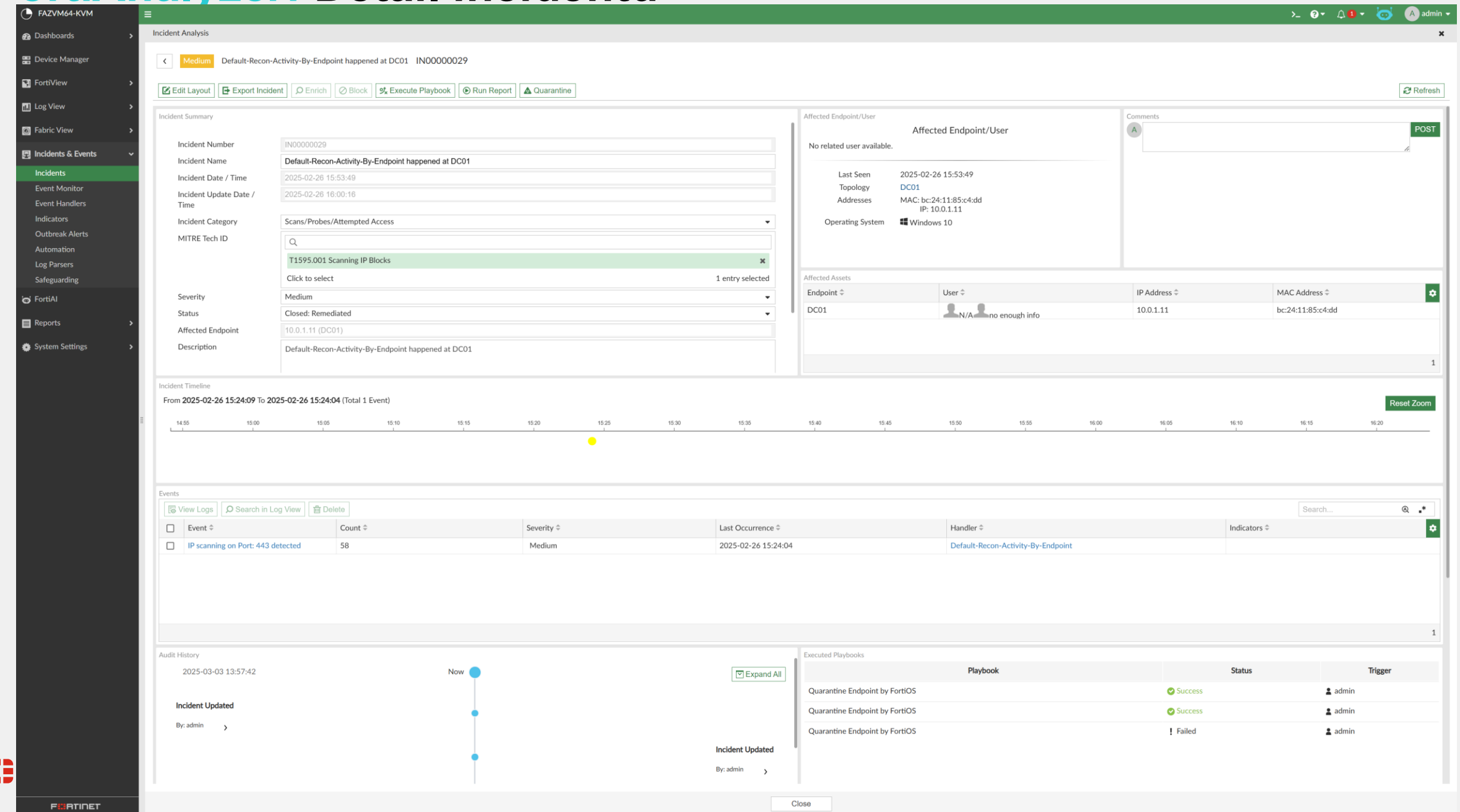
https://www.fortiguard.com/services/security-automation-service

https://docs.fortinet.com/document/fortianalyzer/7.6.0/soc-automation-content-pack

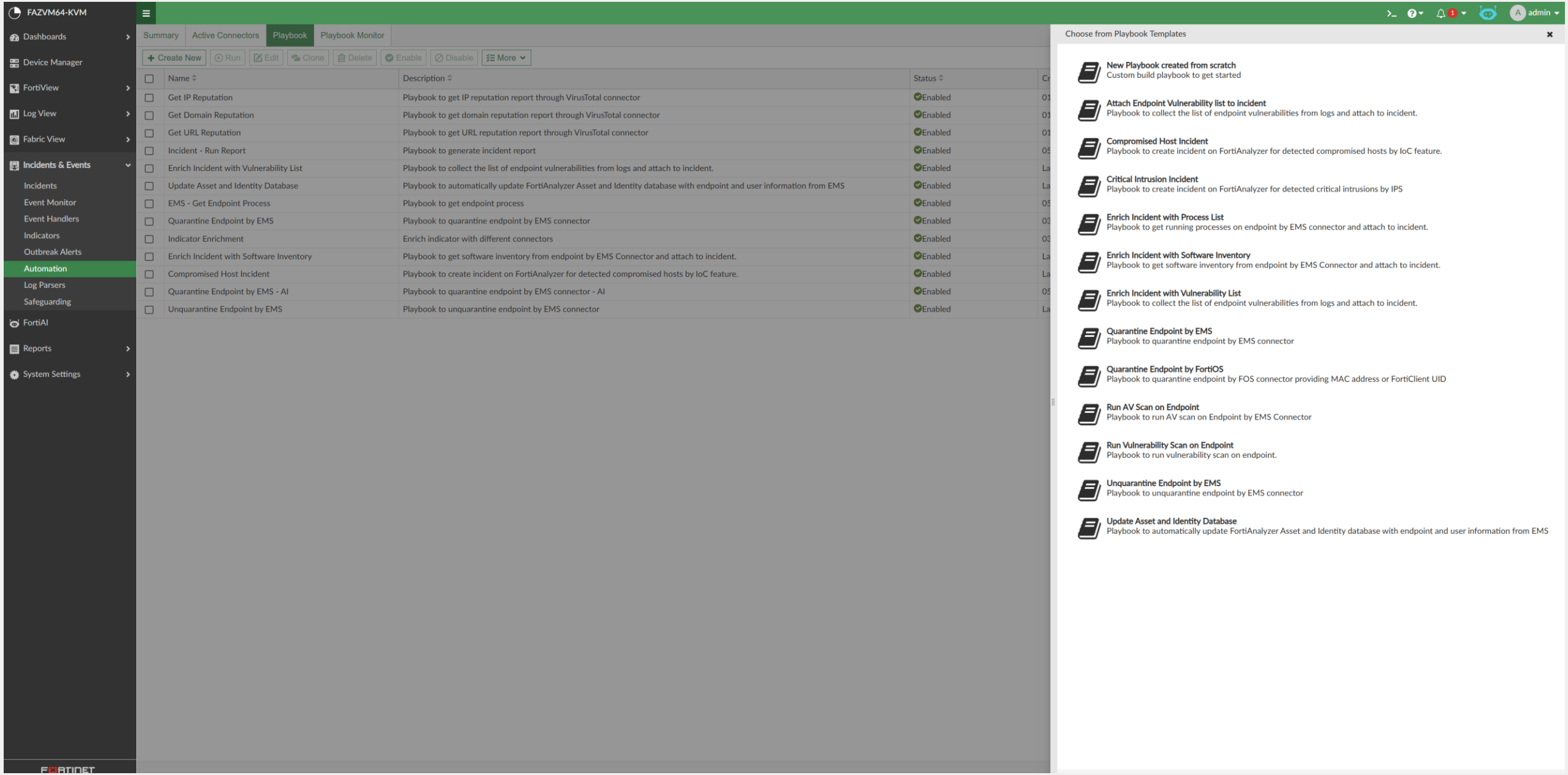
FortiAnalyzer: Incidenty



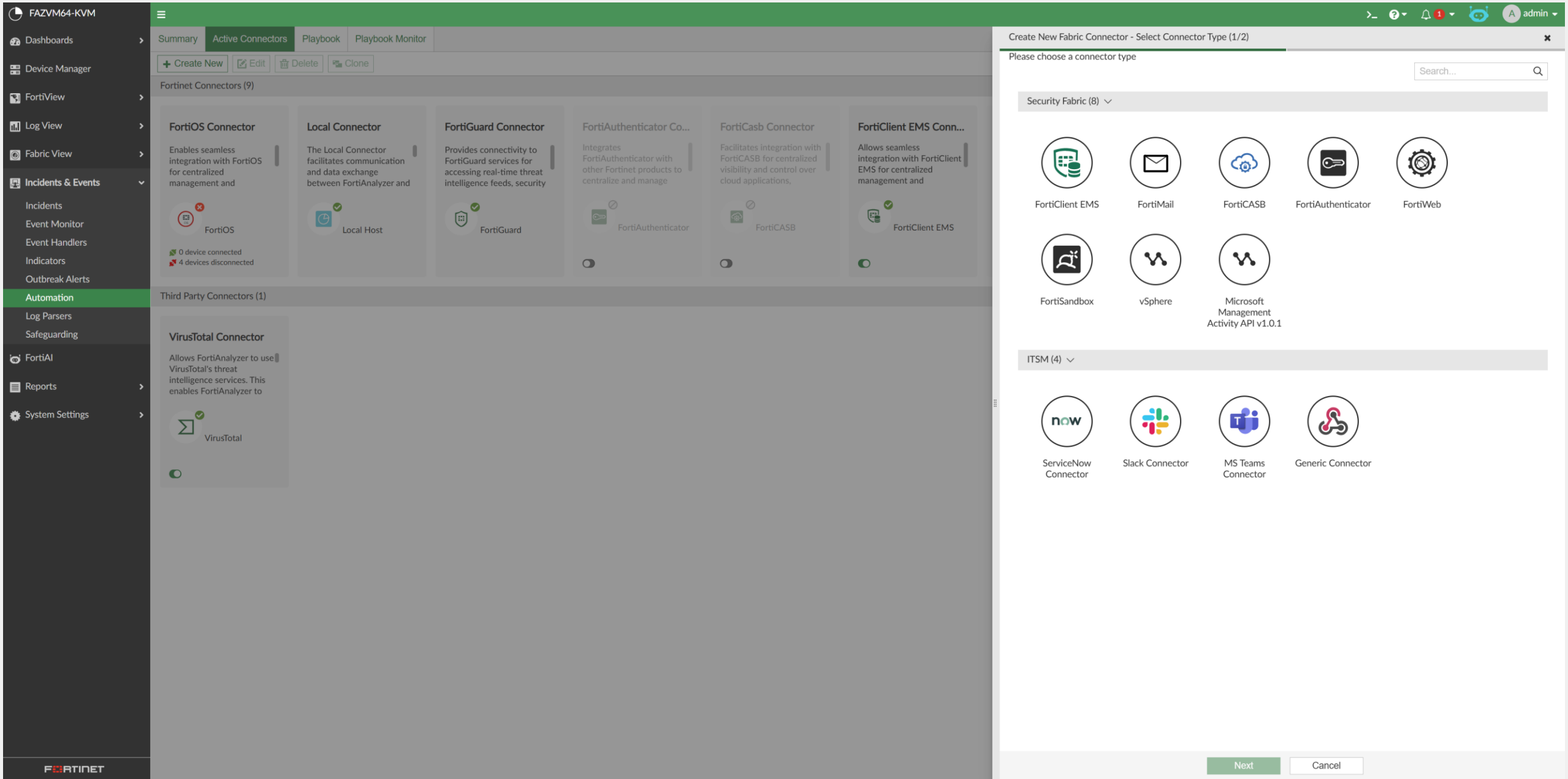
FortiAnalyzer: Detail incidentu



FortiAnalyzer: Playbooky

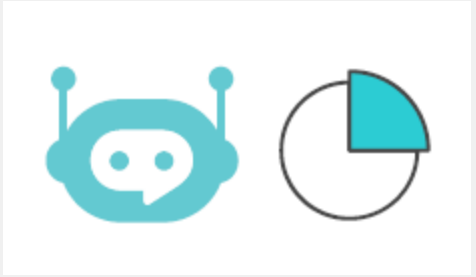


FortiAnalyzer: Konektory



FortiAnalyzer: FortiAI

- Generativní AI, umí pomocí v oblasti analýzy logů a SecOps práce
- Interpretace security eventů, generuje souhrn, vyhodnotí potenciální dopad a poskytne případná doporučení k nápravě
- Umí pomoci vytvářet složité databázové dotazy, reporty, event handlery a SIEM detekční pravidla
- Podpora 30+ jazyků včetně češtiny!



FortiAI

Hi, how can I help you?

ukaz mi hrozby za posledni 2 hodiny

A

Hrozby za poslední 2 hodiny byly zobrazeny na stránce Fortiview -> Top Threats.

Možné další akce:

1. Zhrnout události
2. Vytvořit Event Handler

Pokud budete potřebovat další informace nebo akce, dejte mi vědět.

o jake kategorie se jednalo?

A

Za poslední 2 hodiny byly zaznamenány následující kategorie hrozeb:

Kategorie	Počet incidentů	Úroveň	Hrozby
Blocked Connection	7973	High	blocked-connection
Malicious Websites	9	High	quickerapparently.com, supportsentparticle.com, experttrafficcounter.com, unseenreport.com
Phishing	1	High	cdn.show-sb.com
Failed Connection	3757	Low	failed-connection
Pornography	13	Low	ei.phncdn.com, ht-cdn2.adtng.com, pornhub.com, cdn1-smallimg.phncdn.com

Profesionální kybernetická doporučení:

1. **Blokované připojení a neúspěšné připojení**: Proveďte analýzu blokovaných a neúspěšných připojení, abyste zjistili, zda jsou legitimní nebo je třeba provést další opatření.
2. **Malicious Websites a Phishing**: Ujistěte se, že máte nasazený aktuální firewall a podpisy pro detekci škodlivých webů a phishingových útoků. Proveďte školení uživatelů o bezpečné práci s internetem.
3. **Pornografie**: Použijte filtry obsahu pro kontrolu přístupu k nevhodným webovým stránkám, aby nedocházelo k narušení pracovní morálky a bezpečnosti.

Máte zájem o bližší analýzu některé z kategorií nebo další akce?

pro škodlivé stránky za poslední 2 hodiny.

Můžeme nyní pokračovat s analýzou nalezených škodlivých stránek. Pokud potřebujete další akce nebo konkrétní informace, dejte mi vědět.

vytvor event handler pro nalezene hrozby za posledni 2 hodiny

A

Event Handler pro detekci nalezených škodlivých stránek za poslední 2 hodiny byl úspěšně vytvořen.

Detaily Event Handleru

- **Název:** Malicious Websites Detection
- **Popis:** Detekce a sledování škodlivých webových stránek za poslední 2 hodiny
- **MITRE Technique ID:** T1071.001 (Application Layer Protocol)
- **Pravidlo:**
  - **Název:** Malicious Websites Log Monitoring
  - **Skupina:** appcat
  - **Filtrované kategorie:** Malicious Websites za poslední 2 hodiny
  - **Typ logu:** Web Filter

Pokud budete potřebovat další akce nebo informace, dejte mi vědět.

nastav aby v pridade detekce danym eventhandler byly zablokovany souvisejici cilove adresy

A

Event Handler pro detekci nalezených škodlivých stránek s automatickou karanténou souvisejících cílových adres byl úspěšně vytvořen.

Detaily Event Handleru

- **Název:** Malicious Websites Detection and Quarantine
- **Popis:** Detekce a sledování škodlivých webových stránek za poslední 2 hodiny a automatická karanténa souvisejících cílových adres
- **MITRE Technique ID:** T1071.001 (Application Layer Protocol)
- **Pravidlo:**
  - **Název:** Malicious Websites Log Monitoring and Quarantine
  - **Skupina:** appcat
  - **Filtrované kategorie:** Malicious Websites za poslední 2 hodiny
  - **Typ logu:** Web Filter

Při detekci bude nyní automaticky prováděna karanténa souvisejících cílových adres. Pokud máte další požadavky nebo potřebujete další informace, dejte mi vědět.

Kdy nasadit FortiAnalyzer? Úplně VŽDY!

Každý zákazník s FortiGatem

- Nabízet i pro malé instalace FortiAnalyzer VM Free Trial licenci (3 zařízení, 2 ADOMy, 1GB/den)
- Trial obsahuje i 1 roční IOC licenci a SOC funkce
- Bez technické podpory

Pro pokrytí logování nejen Fortinet porfolia

- FortiGate, FortiClient, FortiAP, FortiSwitch, Cisco IOS, Aruba, CheckPoint, Palo Alto, Sophos, Juniper, Zscaler, Windows, Ubuntu, Syslog…atd.
- V základě rychlý přehled aktuální situace, vyhledávání, analýza, archivace logu a pokročilý reporting

Pro začínající SOC

- Odlehčené SIEM funkce – Incident a Event management, korelace, parsery, event handlery
- Základní SOAR Automatizace – vzorové playbooky na karanténu, blokaci, alerting,…atd.
- Umělá inteligence – FortiAI

FortiAnalyzer: MSSP režim

ISP provozuje logování jako službu pro své zákazníky

- Jednoduchá implementace – 1 IP adresa z pohledu zákazníka

- Zákazník získá:
  - Spolehlivě centrálně uložené logy, přehledy, pravidelný reporting
  - Volitelně možnost náhledu na logy
  - SOC funkce a automatizaci
  - Blokace IP na FortiGatu, karanténa klienta – FortiClient, FortiSwitch, FortiAP
  - Automatické notifikace emailem nebo zprávou na MS Teams, Slack

- Typicky VM rešení – onprem VMware, Hyper-V, KVM
- Jednoduché licencování a škálovatelnost – GB/day licenční model

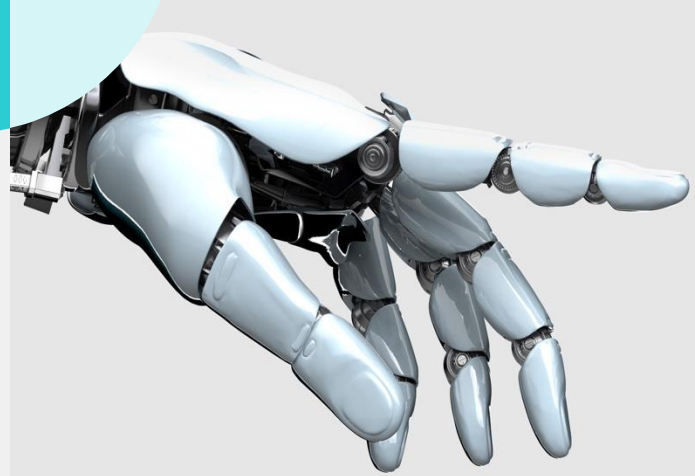
FortiAnalyzer: Licencování

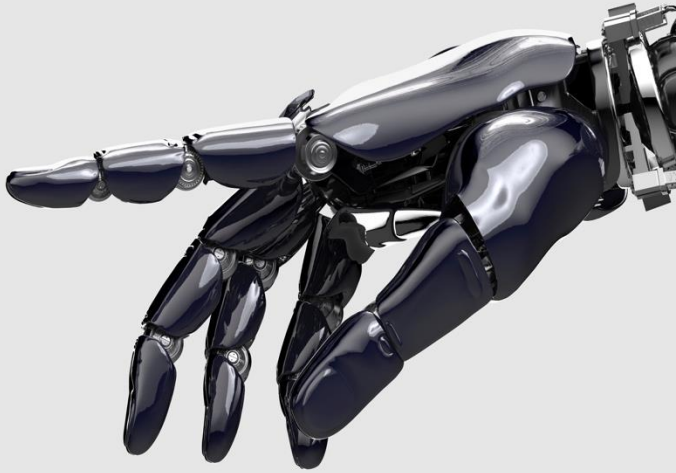
- Platforma VM, Cloud, HW box
- GB/day licenční model
- VM - perpetual nebo subskripce

Nejvýhodnější je VM subskripce obsahuje přehledy, logy, reporting, IOC + SOC funkce

- GB/day
- IOC & Outbreak Detection,
- Security Automation Service
- FortiCare Premium Support
- Pouze 5 ADOM, další možno dokoupit

Představení: 24/7 Security Monitoring





Více proaktivních schopností pro zdokonalování vašich bezpečnostních operací a zmírnění obav z napadení a kompromitace

24/7 Bezpečnostní monitoring s FortiGuard SOCaaS

Fortinet Security Experts

AI-Powered Technologies

FortiGuard Labs

Predictable Pricing

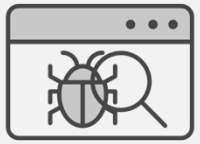
Rapid Deployment

Alert Acknowledgment	Triage Critical Alerts	Average
2.5	**5-12**	**15**
Minutes	Minutes	Minutes MTTR

Detekce

Nechte Fortinet monitorovat a analyzovat výstrahy a upozornění z FortiGatu v režimu 24/7. Upozorníme vás pouze, když je něco důležitého a vyžaduje pozornost.

Odpověď

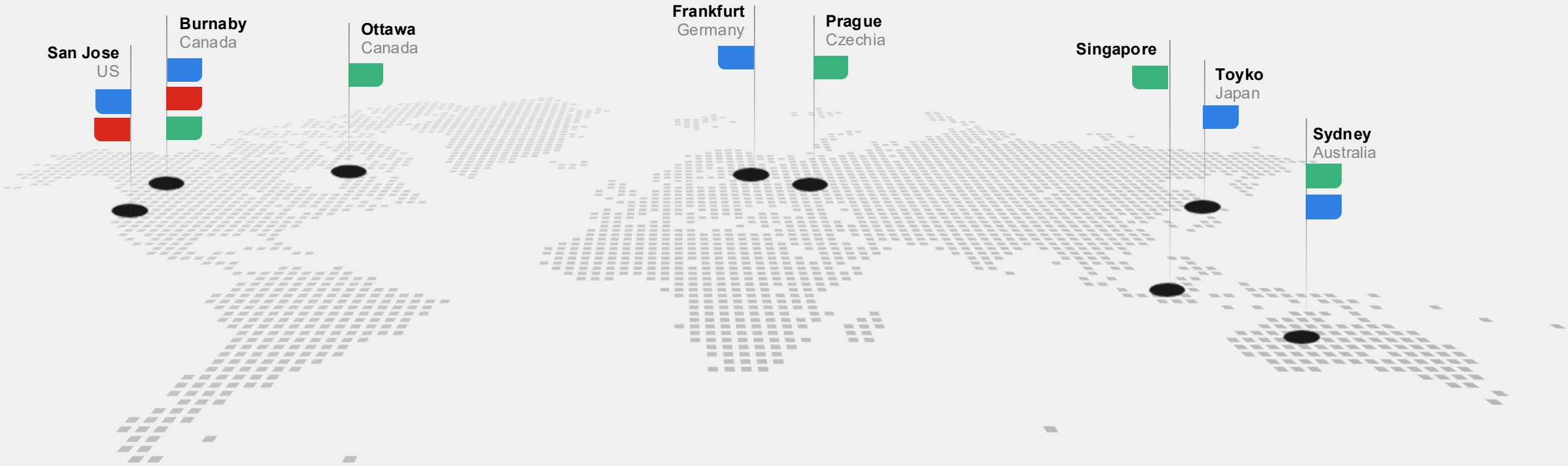


Bezpečnostní experti Fortinetu reagují již za 15 minut a poskytnou informace o tom, co se stalo, proč se to stalo a jaké kroky podniknout k nápravě incidentu.

Zlepšení

Cloudový portál s intuitivním přehledem, zprávami na vyžádání a pravidelnými čtvrtletními schůzkami s odborníky na zabezpečení společnosti Fortinet.

FortiGuard SOCaaS: Global Security Operation and Data Centers



Global Response Teams

- SOC
- Data Center
- Disaster Recover

Critical Escalation Times

P1, Priority 1: 15 minutes

P2, Priority 2: 45 minutes

P3, Priority 3: 90 minutes

P4, Priority 4: 6 hours

99.99%
Availability

24x7x365
Service Hours

Unlimited
Log Capacity

FortiGate & Security Fabric logs
Ingest Log Data

Fast & Simple
Onboarding

FortiGuard SOCaaS: Fortinet Experti, Technologie a Threat Informace

Automatizovaná reakce na incidenty

Incident Monitoring Management

Logy
FortiGate, FortiSASE, FortiClient, FortiEDR a telemetrická data

Bezpečnostní události
Mapování na MITRE a detekční pravidla v cloudové FortiAnalyzeru

Korelace výstrah
FortiSOAR vedoucí platforma orchestrace a automatizace pro snížení false positive

Analýza
Fortinet experti analyzují a eskalují incidenty

Incident
Notifikace zákaznického SOCu

DETECTIONS
- Botnet/C&C
- Compromised Hosts
- Unauthorized Access
- Lateral movement
- Malware
- Outbreak Alerts

RESPONSE
- Self Remediate
- Request Assistance
- MFGS Engagement
- FCT Forensics

RECOVER
- QBRs
- Outbreak Report
- Posture Assessment
- Compliance Reports
- Trainings

FortiGuard SOCaaS: Komunikace v reálném čase s Fortinet experty

Reakce když je potřeba

Rychlá odezva

Eskalace potvrzených problémů již za 15 minut s upozorněním na telefon, e-mail a cloudový portál SOCaaS

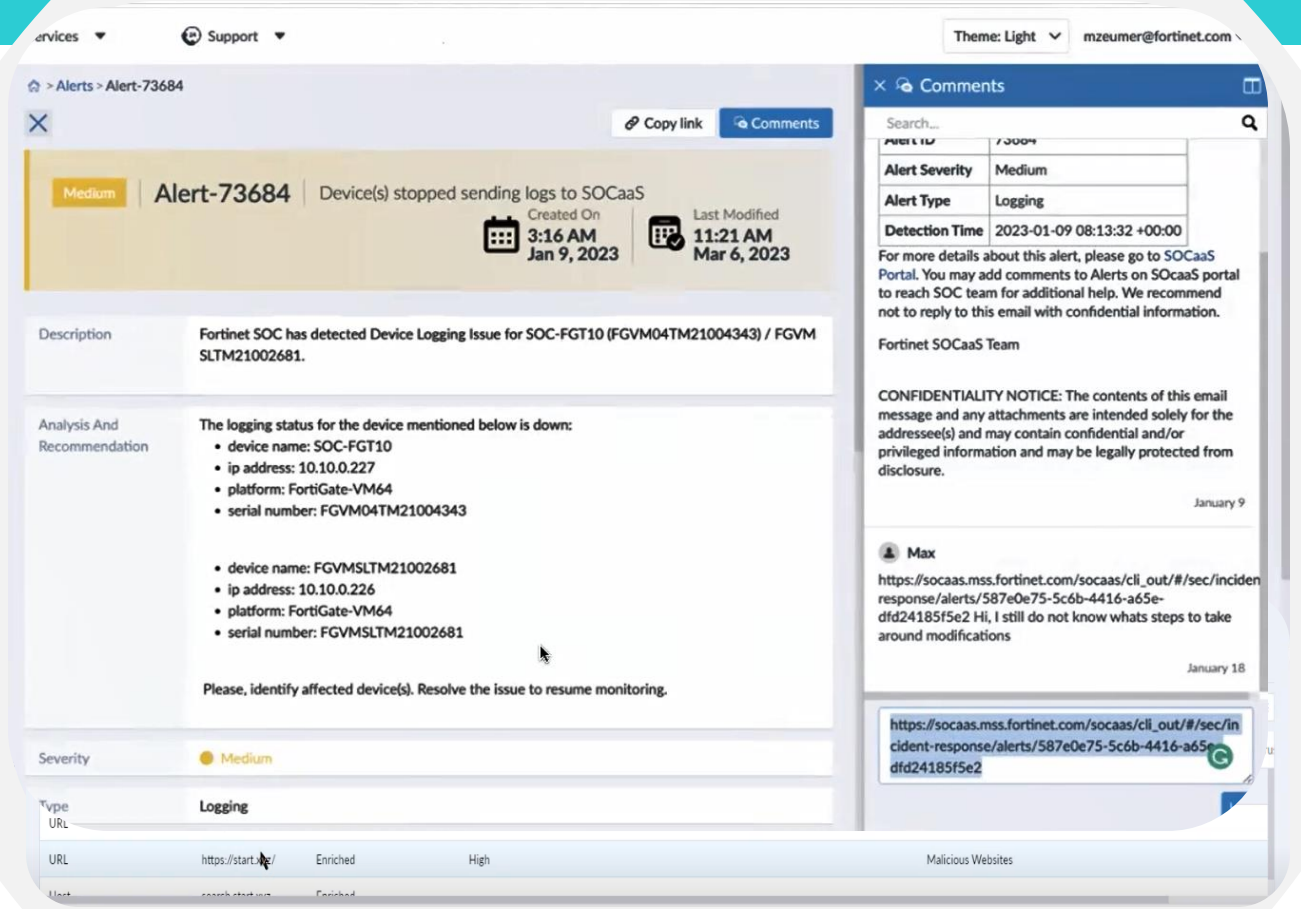
Spolupráce s Fortinet odborníky

Podrobné instrukce krok za krokem:

- Co se stalo – Proč – Dopad – Kroky k nápravě

Komunikace v reálném čase

24/7 podpora pro jakékoliv dotazy



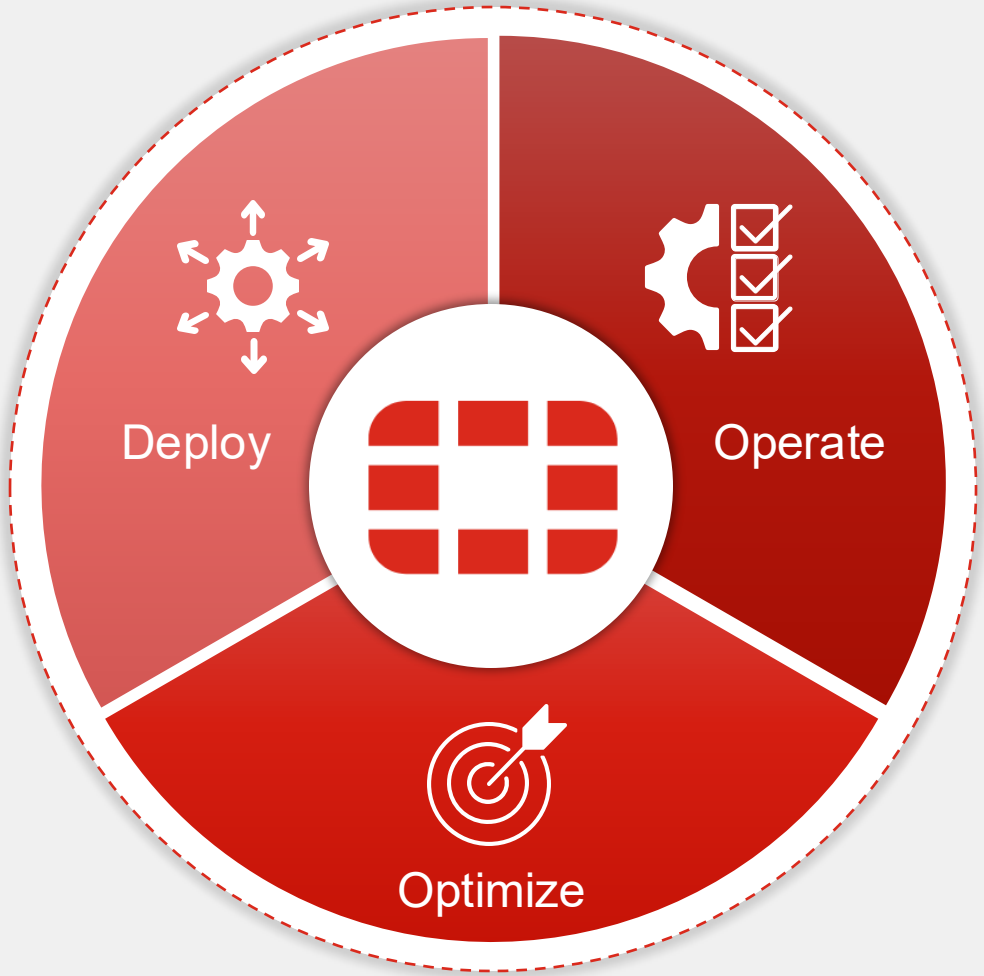
FortiGuard SOCaaS: Pravidelné týdenní reporty

Snadné sledování všeho na čem se pracuje nebo pracovalo

ID	TENANT	CREATED ON	RESOLVED DATE	NAME	STATUS	TYPE	SEVERI...	DESCRIPTION	CLOSURE NOTES
								Malware detection in [redacted] Sandbox detected Malware Action = quarantinefailed	
7208	[redacted]	03/11/2022 06:15 PM	03/15/2022 02:44 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	File Name = C:\Users\[redacted]\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\28\Attachments\Ваш счет пополнен. - DzMNa37mTnCxobr4jeFDRqcguByVAhdSEl86wfkIZYPW1UJKiX[2639].xhtml	BYOD PC has been ban from [redacted] network
7109	[redacted]	03/02/2022 06:18 PM	03/15/2022 02:19 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	Malware detected on host [redacted]	ran full malware scan, no malware detected.
7068	[redacted]	02/23/2022 09:12 PM	03/15/2022 02:17 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	Unhandled malware detections for files in [redacted]	ran full malware scan, no malware detected, PC is clean
6742	[redacted]	01/09/2022 11:18 PM	03/11/2022 10:45 AM	FCT detected unhandled malware from [redacted]	Closed (Risk Accepted)	Malware	High	FCT detected unhandled malware from [redacted]	user was not connected to ems (possibly why the file failed to quarantine) confirmed with user that file is no longer there full av scan results are clean
7274	[redacted]	03/18/2022 06:30 PM	03/21/2022 03:20 PM	Malware Activity detected from [redacted]	Closed (Resolved)	Malware	High	Unhandled malware declared in [redacted]	file was quarantined and removed
7054	[redacted]	02/22/2022 07:54 PM	03/16/2022 10:22 AM	Malware Activity detected from [redacted]	Closed (Resolved)	Malware	High	Quarantine failed for [redacted]	manual scan via EMS came clean, archiving the case.
7275	[redacted]	03/18/2022 07:03 PM	03/21/2022 04:37 PM	High Risk Traffic detected from [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	CryptoMiner detected on [redacted]	this is FGD one time event
7270	[redacted]	03/18/2022 12:57 AM	03/21/2022 09:14 AM	Malicious Email detected from [redacted]	Closed (Risk Accepted)	Malicious Email	Mediu...	Virus detected in mail from [redacted]	was a test
7259	[redacted]	03/16/2022 04:06 PM	03/22/2022 12:11 PM	High Risk Traffic detected from [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	Potential dataexfil from [redacted]	was a test
7228	[redacted]	03/14/2022 05:51 PM	03/17/2022 12:15 PM	High Risk App Usage detected from [redacted]	Closed (Risk Accepted)	High Risk App	Mediu...	Tor app detected	The traffic is being blocked by our FW. We are not able to find the owner of this IP.
7198	[redacted]	03/10/2022 11:36 PM	03/15/2022 02:41 PM	Botnet traffic detected to CnC server: [redacted] related to [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	Fortinet SOC has repeatedly detected Botnet traffic attempts Sunburst from [redacted] to [redacted]	Endpoint Quarantine, ongoing investigation

Managed FortiGate Service

- Specializovaný tým odborníků je k dispozici 24/7
- Zjednodušení a optimalizace síťové správy a aktivit.



Managed FortiGate Service: Co všechno za vás uděláme?

Device Provisioning

- NGFW Deployment
- Security Fabric Setup
- Secure SD-WAN
- ZTNA
- Remote Access
- LAN Edge

Change Management

- Evaluation / Implementation / Verification of change requests
- FSBP and ITIL methodology

System Hardening

- System Audit
- Security Posture Review
- PSIRT Advisories Response
- Fortiguard Outbreak Response
- SOCaaS Incident Remediation

FortiSIEM Platform

SaaS, Virtual Appliance and Hardware Appliance

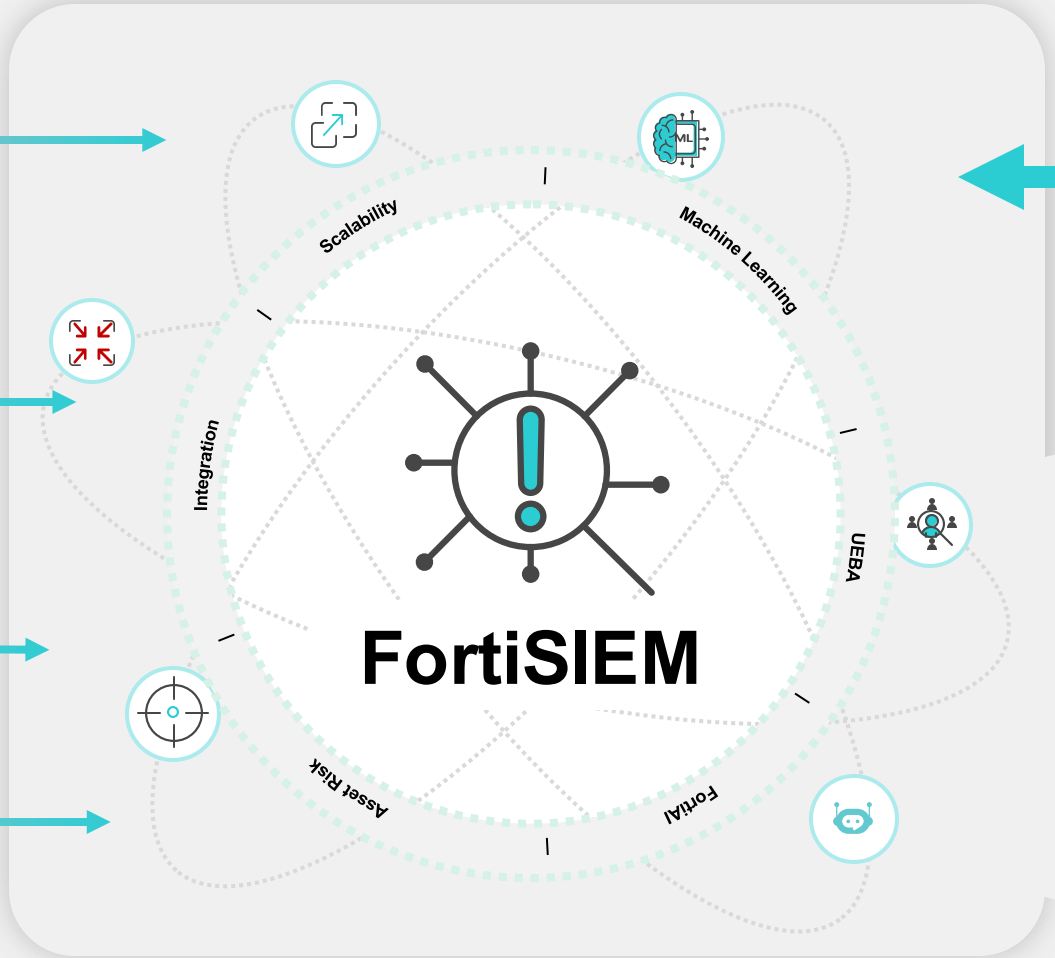
300+

3rd Party Devices, CIP, SaaS, Applications, Windows, Linux and more

Fortinet Fabric
FortiAnalyzer & Direct Integration

FortiNDR
Network Detection & Response

FortiEDR
Endpoint Protection



FortiSOAR
SOC Automation

Real-Time Incident Detection

Visibility - NOC & SOC

Investigation - Security Data Lake

Enterprise & MSSP Platform


FORTINET