



Automatizácia odozvy na bezpečnostné incidenty

Zsolt Géczi, CEH, regional account manager, Slovakia

zgeczi@fortinet.com



KTO JE FORTINET?

Fortinet je globálnym lídrom v oblasti kybernetickej bezpečnosti a ponúka široký, integrovaný a automatizovaný systém zabezpečenia, ktorý zákazníkom umožňuje urýchliť cestu digitalizácie.

\$3.09B

FY2020 Billing

Financially Stable

38.9B+ Market Cap (as of 7.31.21)
Nasdaq: FTNT

S&P 500

BBB+ Baa1

Security Investment Grade Rating

Leading the Cybersecurity Industry

50

Integrated Fabric Products

Broadest Attack Surface Coverage

530,000+
Customers Worldwide

Massive Customer Input

660,000+

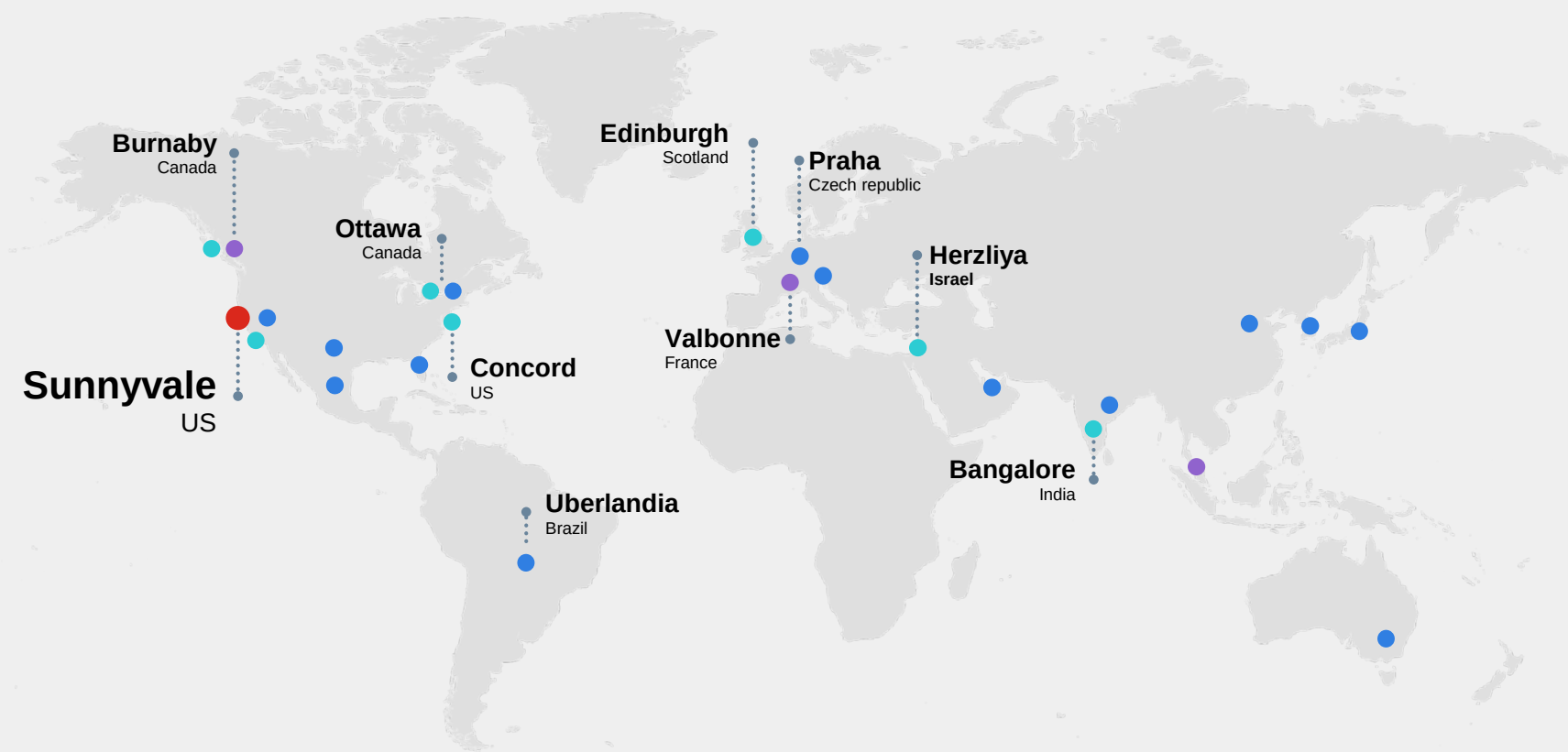
NSE Certifications

WEF Cybersecurity Founders



Široké globálne pokrytie - vyvážený globálny rast

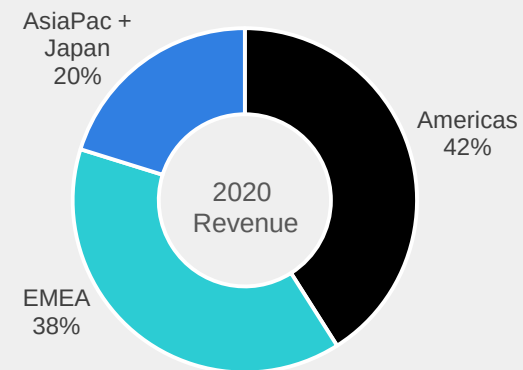
Obrovské investície do výskumu a vývoja na podporu organického rastu



9,000+
zamestnancov

530,000+
zákazníkov po celom svete

785
registrovaných patentov



● Headquarters

● Dev Centers

FortiCare

● Support Centers

● Centers of Excellence



Fortinet je ocenený v 6 Gartner magických kvadrantoch

Fortinet recognized as a Leader in **2** Magic Quadrants



Network Firewalls



WAN Edge Infrastructure

Fortinet recognized as a Visionary in **2** Magic Quadrants



Wired and WLAN



SIEM

Fortinet recognized as a Challenger or Niche in **2** Magic Quadrants



Web Application Firewall



Endpoint Protection Platforms*

Fortinet mentioned in **2** Magic Quadrants



Secure Web Gateway



Indoor Location Services

And Fortinet is listed in **8** Gartner Market Guides



EDR



IDPS



Email



NAC



NDR



ZTNA



OT



SOAR

Fortinet Security Fabric

Široký

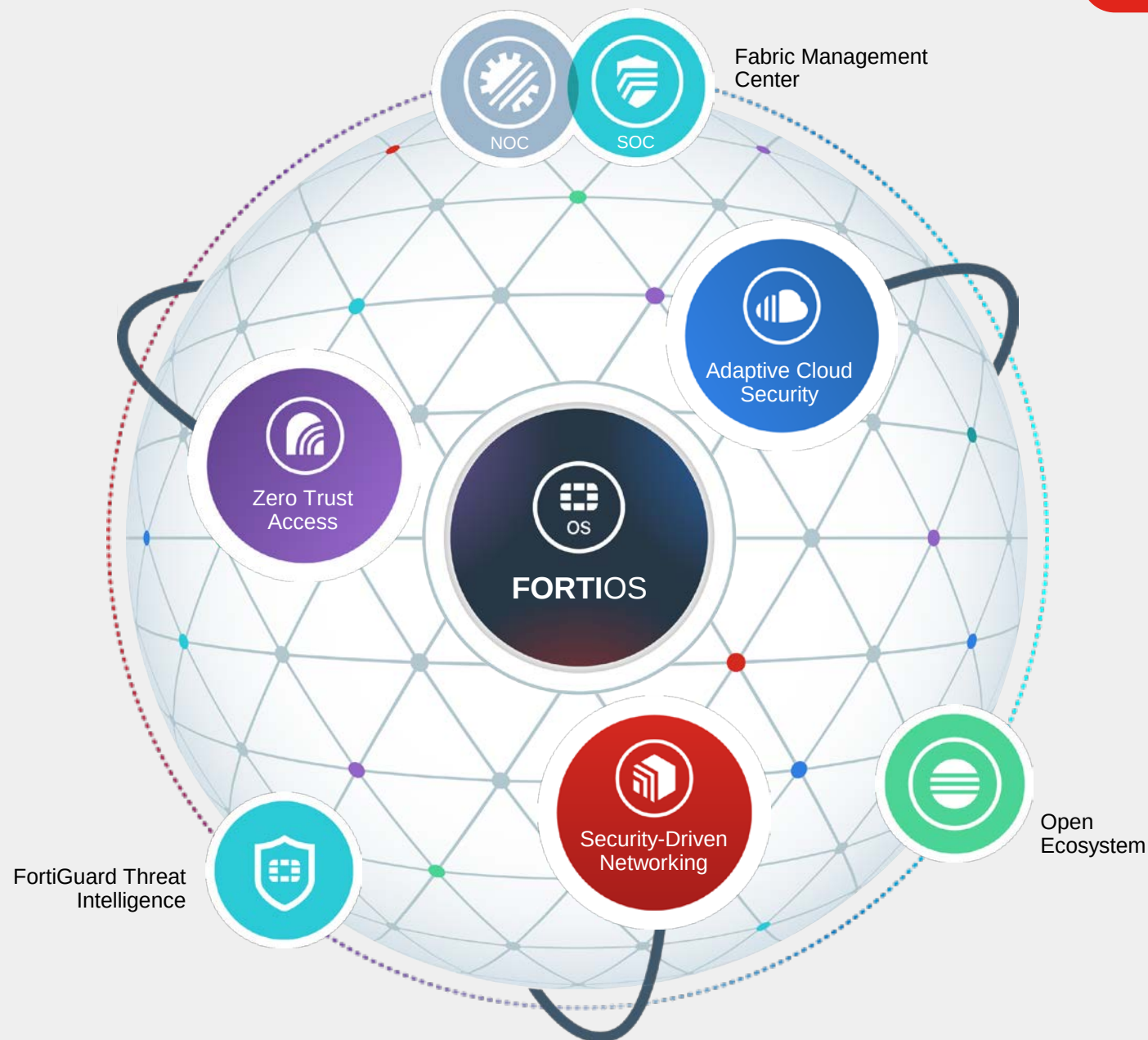
viditeľnosť a ochrana celého digitálneho útočného priestoru s cieľom lepšie riadiť riziká.

Integrovaný

riešenie, ktoré znižuje zložitosť správy a zdieľa informácie o hrozbách

Automatizovaný

samoregeneračné siete so zabezpečením založeným na umelej inteligencii pre rýchlu a efektívnu prevádzku



Fortinet Security Fabric umožňuje digitálne inovácie

Platforma kybernetickej bezpečnosti naprieč Koncovými Bodmi, Sieťou a Cloudom

Zero-trust Network Access



Identifikácia a zabezpečenie
používateľov a zariadení v sieti aj
mimo nej

Security-driven Networking



Zabezpečenie a zrýchlenie
sieťe a používateľského
prostredia

Dynamic Cloud Security



Zabezpečenie a kontrola
cloudovej infraštruktúry a
aplikácií

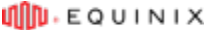
AI-powered Security Operations



Automatická prevencia, detekcia a
reakcia na kybernetické hrozby

Otvorený Fabric Ekosystém

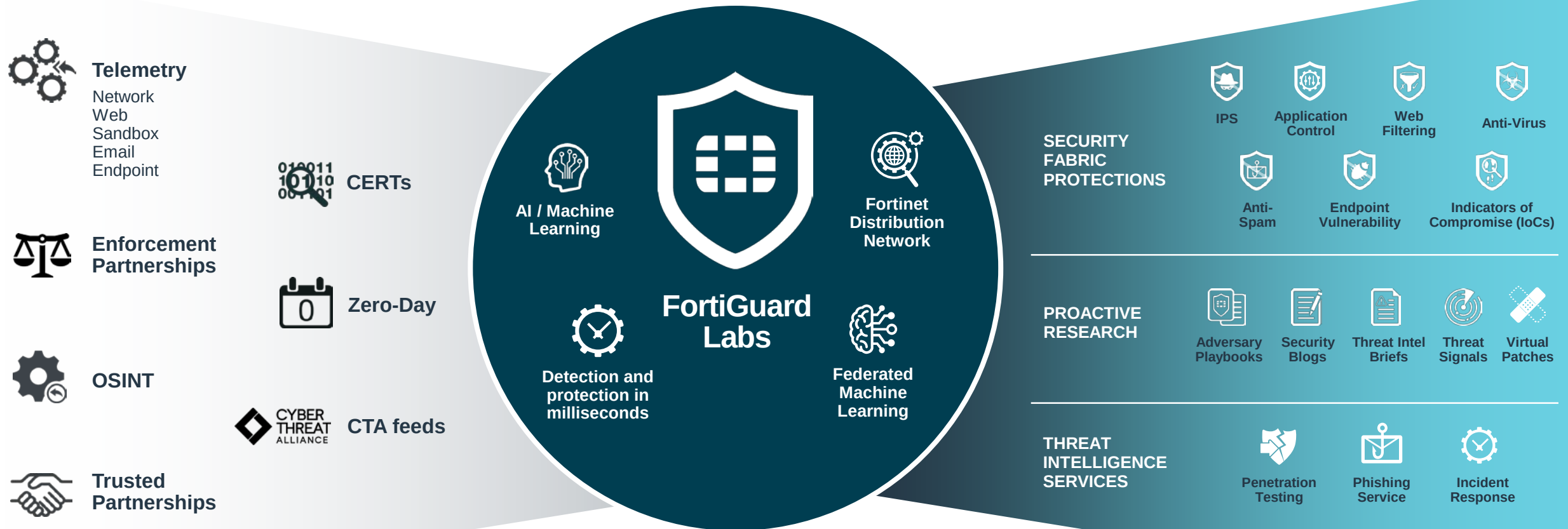
Najlepšie integrované riešenia vo svojej triede na komplexnú ochranu

 SECURITY-DRIVEN NETWORKING	 ADAPTIVE CLOUD SECURITY	 AI-DRIVEN SECURITY OPERATIONS	 ZERO TRUST ACCESS
 	 	 	 
 	 	 	 
 	 	 	 
 	 	 	 
 	 	 	 
 	 	 	 
 	 	 	 
 	 		
 			

450+ integrácií ekosystémov na urýchlenie a zabezpečenie digitálnych inovácií

FortiGuard Labs

VISIBILITY → **INNOVATION** → **ACTIONABLE THREAT INTELLIGENCE**





15 Million

Botnet C&C attempts

TW HARTED

PER MINUTE



462,217

Malicious Website

ACCESSES

Blocked Per Minute





5.3 Million
NETWORK INTRUSION
ATTEMPTS
resisted per minute

136,173 PHISHING

BLOCKED PER MINUTE





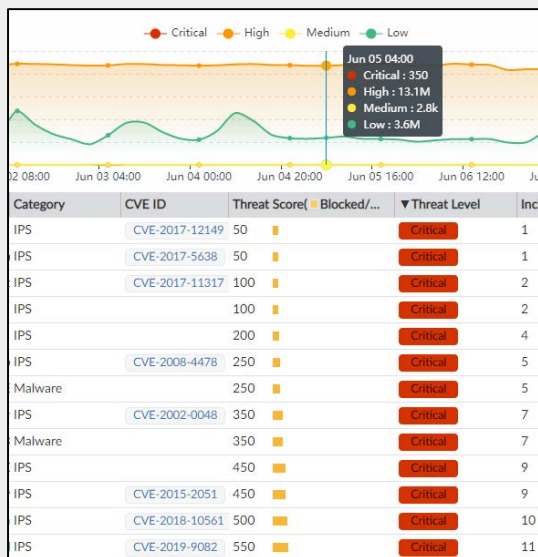
903,860

MALWARE PROGRAMS
Neutralized Per Minute

UDALOSTÍ za deň?

31,395,240,000

SOC Výzvy



Preťaženie výstrahami

- Množstvo detekčných technológií
- Obrovský objem údajov



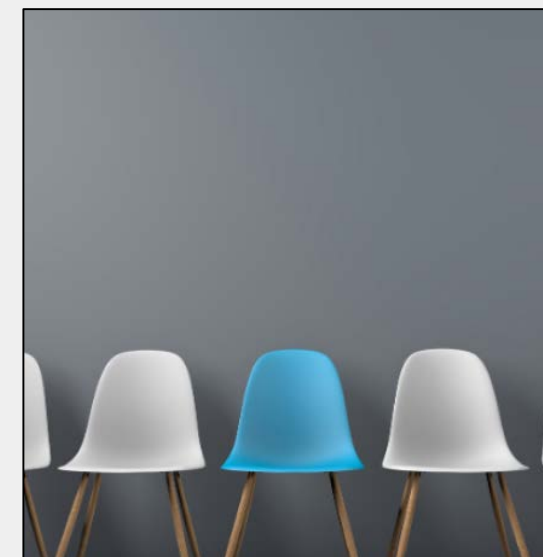
Rôzne nástroje

- Viaceré konzoly ako SIEM, Threat Intels, EDRs, Sandboxes ...
- Limitované integrácie



Manuálne procesy

- Slabá dokumentácia
- Analytici sa neriadia procesmi



Nedostatok talentov

Globálny nedostatok pracovníkov v oblasti kybernetickej bezpečnosti 1,8 milióna do roku 2022

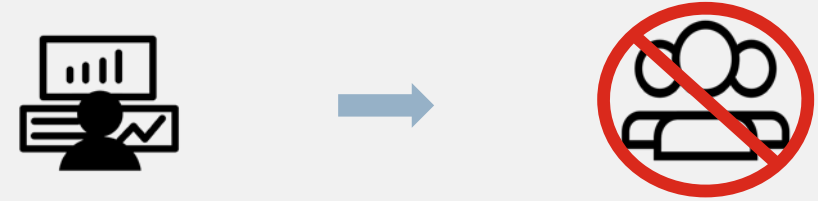
Trendy komplexnosti ekosystémov spomaľujú reakciu SOC

Objem upozornení a zdĺhavé manuálne procesy



Množstvo výstrah na vyšetrovanie maskuje hrozby a je navrstvené s nespočetnými manuálnymi pracovnými postupmi, čo spôsobuje **pomalé reakcie, zvýšenú zraniteľnosť a únavu z výstrah**.

Nedostatok zručností a tímovej spolupráce



Organizácie majú problémy s udrжанím a získavaním zamestnancov na vyššej úrovni - **Tímy kybernetickej bezpečnosti majú problémy so súdržnou spoluprácou**, často kvôli izolácii vytvorenej technológiami.

Výzvy konsolidácie výrobcov



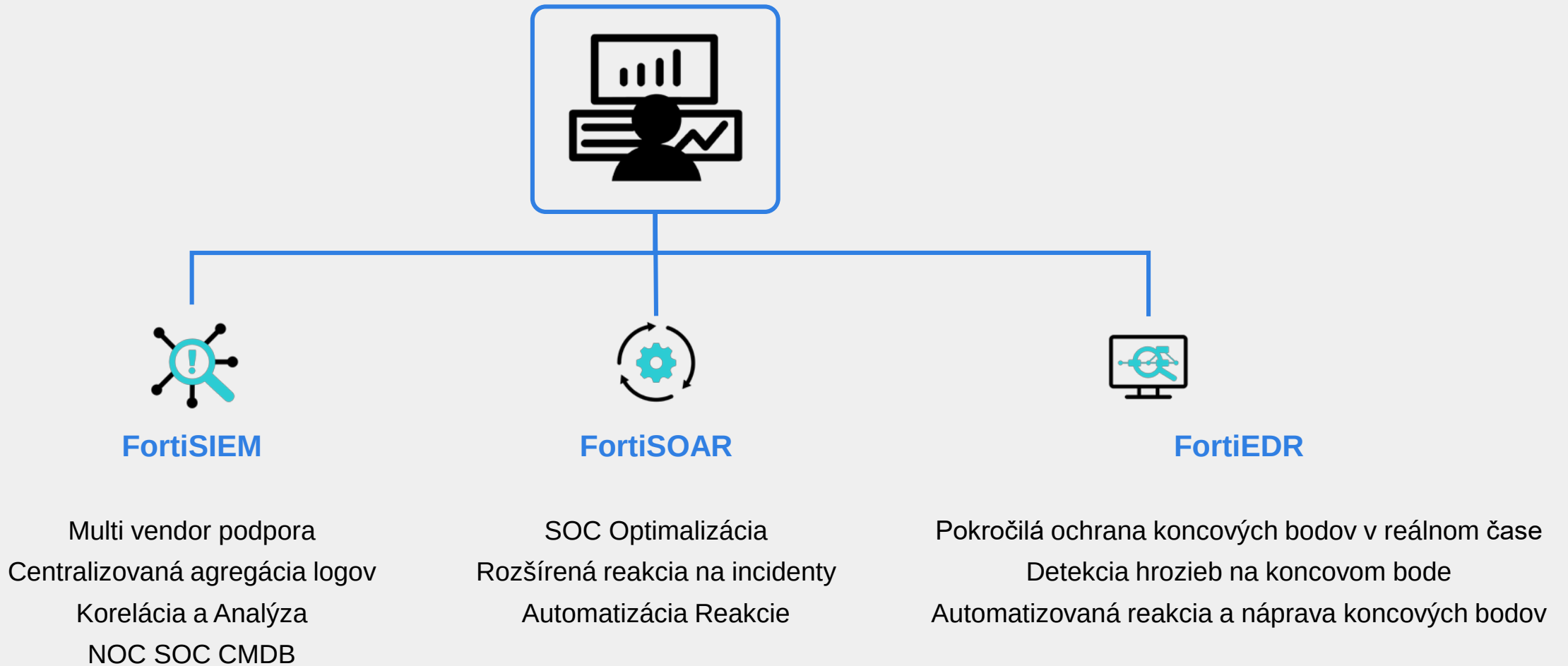
Zavedené technológie na boj proti kybernetickým hrozbám sú často obmedzené pri koordinácii a udržovaní kontroly nad rozsiahlymi bezpečnostnými systémami. To vedie organizácie k **hľadaniu konsolidovaného prístupu**.

Dopyt po automatizácii



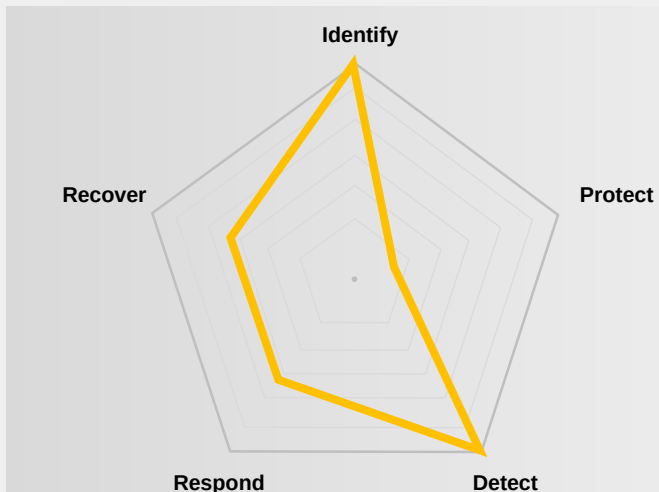
Organizácie, ktoré sa stretávajú so zložitými problémami, potrebujú strojovú pomoc na zníženie TCO, zlepšenie efektívnosti a bezpečnostnej pozície. **Do roku 2025 bude mať viac ako 90 % podnikov architektu pre automatizáciu**¹

SOC Toolkit – FortiSIEM, FortiSOAR, FortiEDR

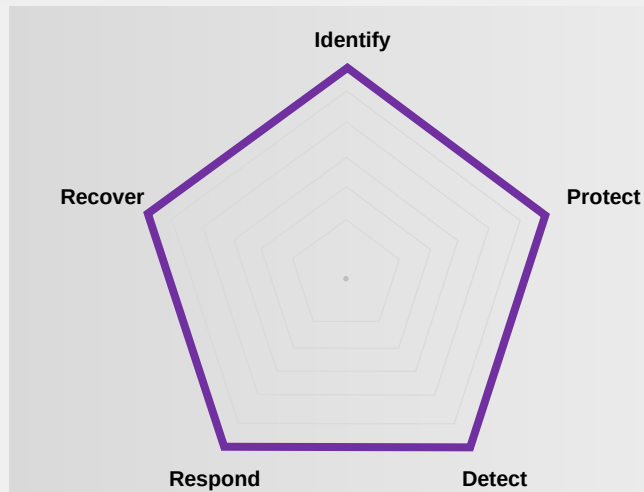


Technické zameranie súboru nástrojov SOC,

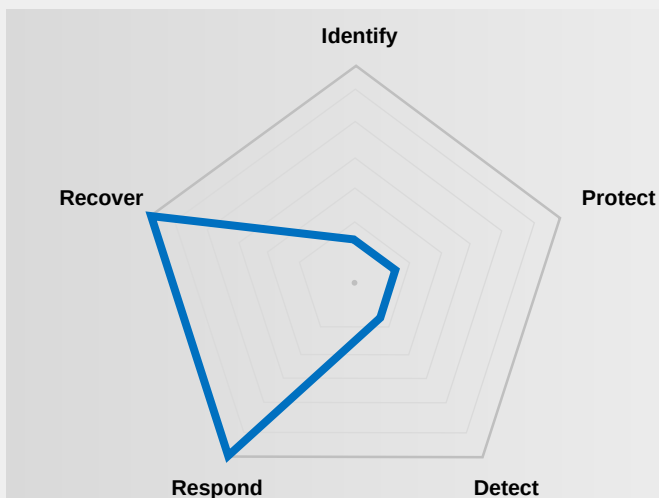
pretože CIEL'OM je riadiť a znižovať riziká kybernetickej bezpečnosti.



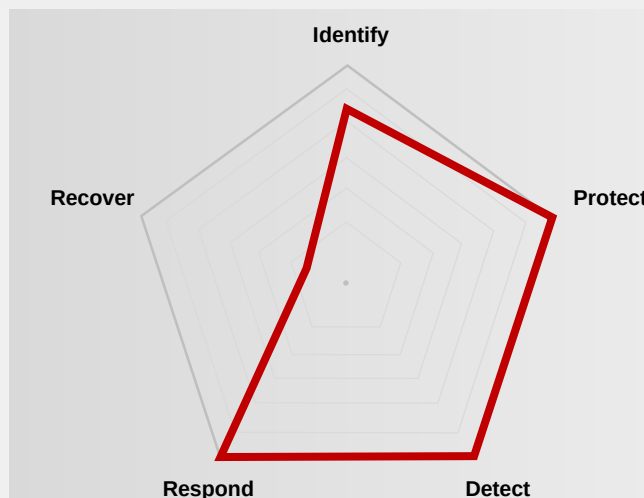
FortiSIEM



**FortiEDR
(endpoint)**



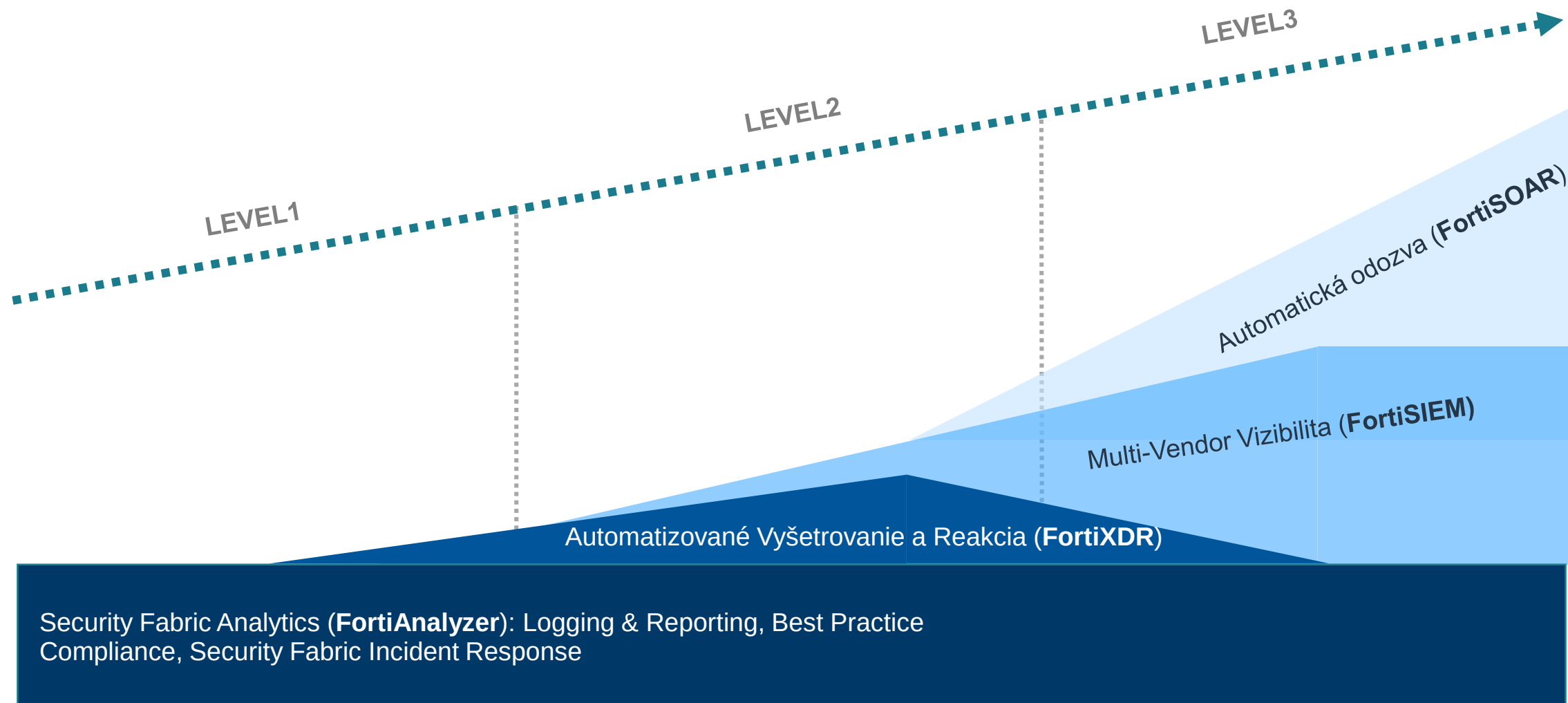
FortiSOAR



**Advanced Network Security
(E.g. Fortinet Security Fabric)**

Automatizujte Bezpečnostné Operácie

Vyberte si riešenie, ktoré je v súlade s vašou SOC vyspelosťou





FORTINET®