FortiDeceptor

a jeho integrace do Fortinet Security Fabric

Jakub Kačer, Systems Engineer, Fortinet

Průměrná doba od detekce k nápravě

Zdroj: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, October 2022.

Jaké jsou příčiny?

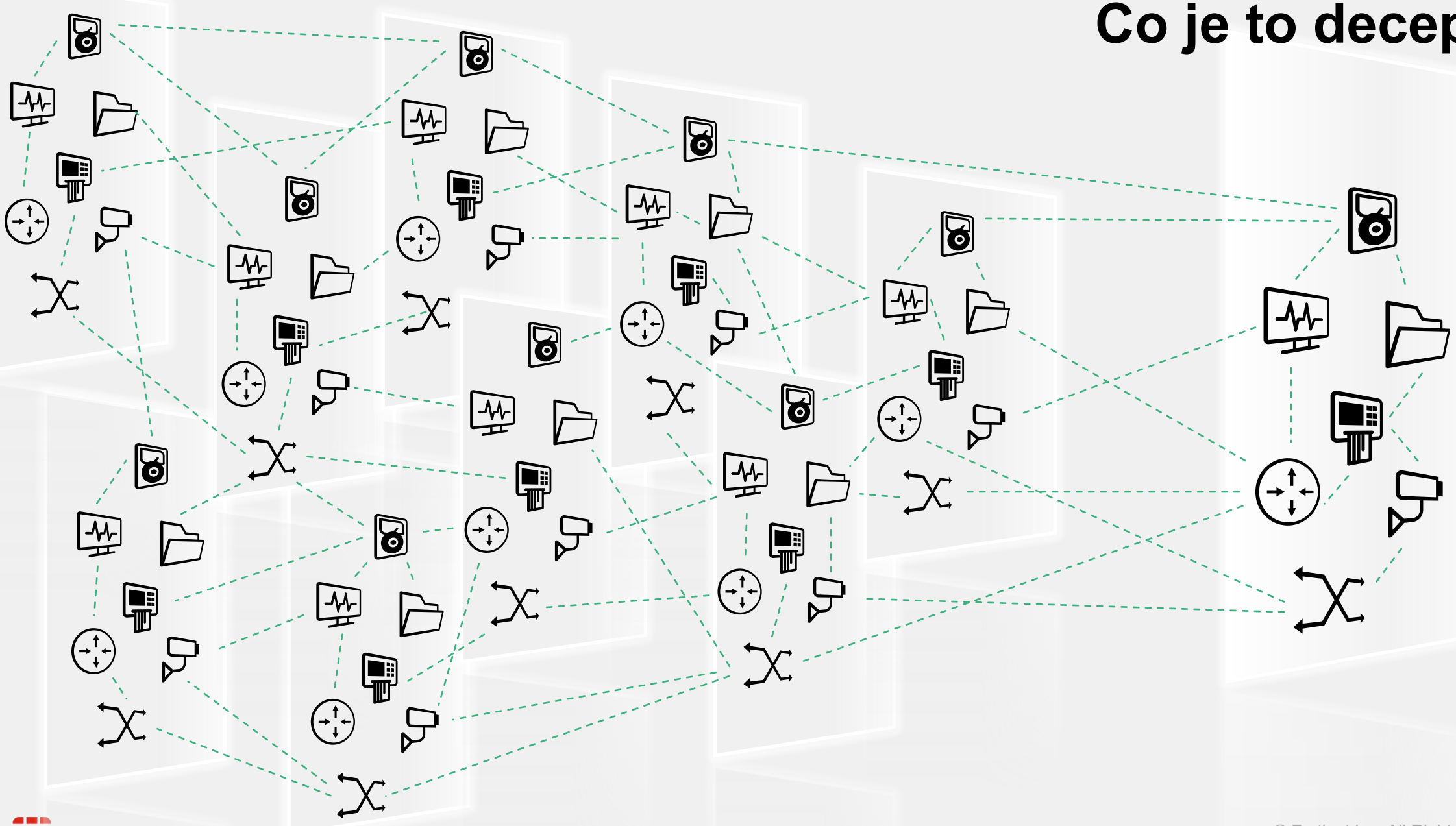
Výzvy zákazníků

- Nedostatek personálu
- Nedostatek znalostí systému
- Absence Zero-Day ochrany
- Velké množství logů

Výzvy výrobců

- Absence integrací
- Vysoká komplexita systémů
- Zastaralé detekční mechanismy
- Příliš mnoho false-positives

Co je to decepce?



Co je to decepce?

Odklánění útočníků na falešná aktiva k ochraně skutečných aktiv v síti

Návnady (Decoys)
Honeypoty, falešná aktiva, falešná síťová zařízení, falešné aplikace a falešné služby

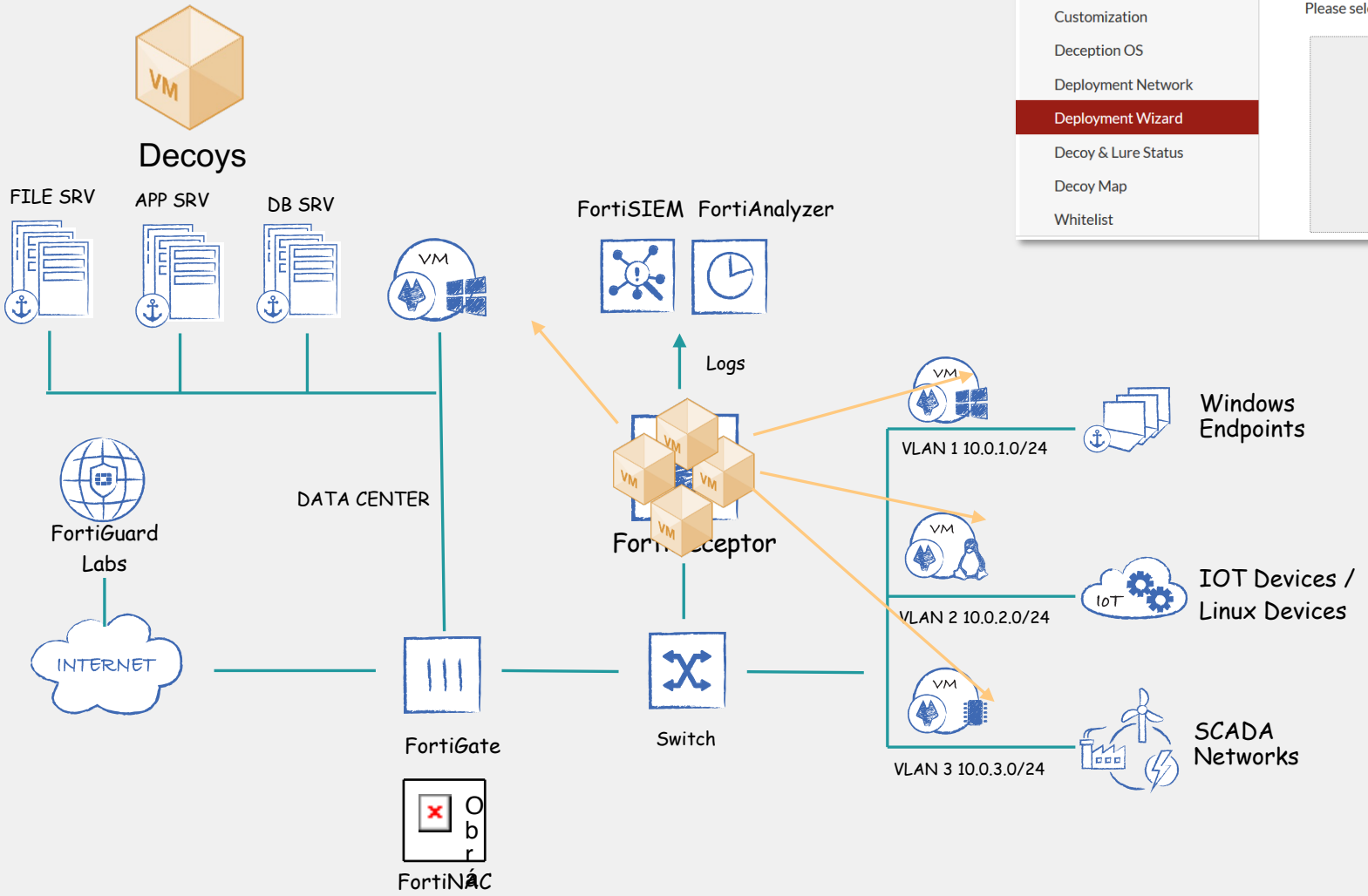
Služby (Lures)
Falešné služby aktivní na návnadách

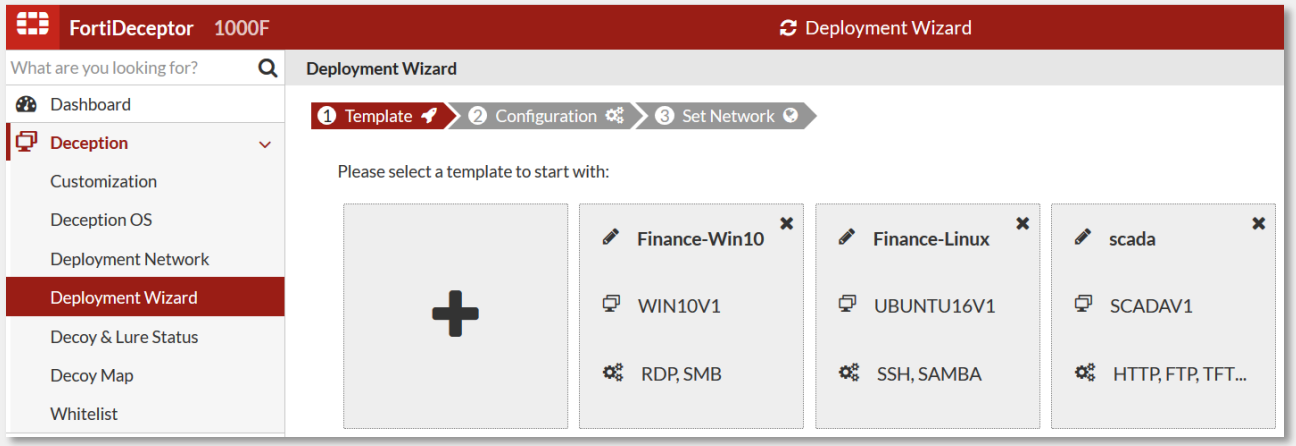
Síťový provoz (Network traffic)
Falešné síťové signalizace (SMB, CDP, UPnP a další)

Střípky (Tokens)
Falešné soubory, konfigurace a informace umístěné na skutečných IT aktivech směřující na falešné návnady

FortiDeceptor - nasazení

Nalákání | Odhalení | Eliminace

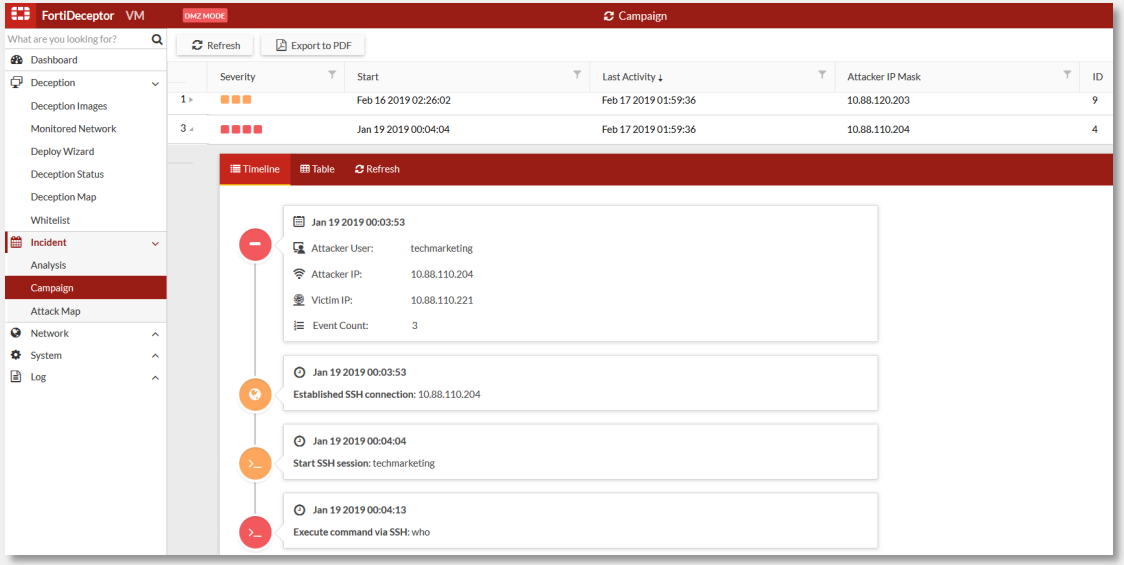


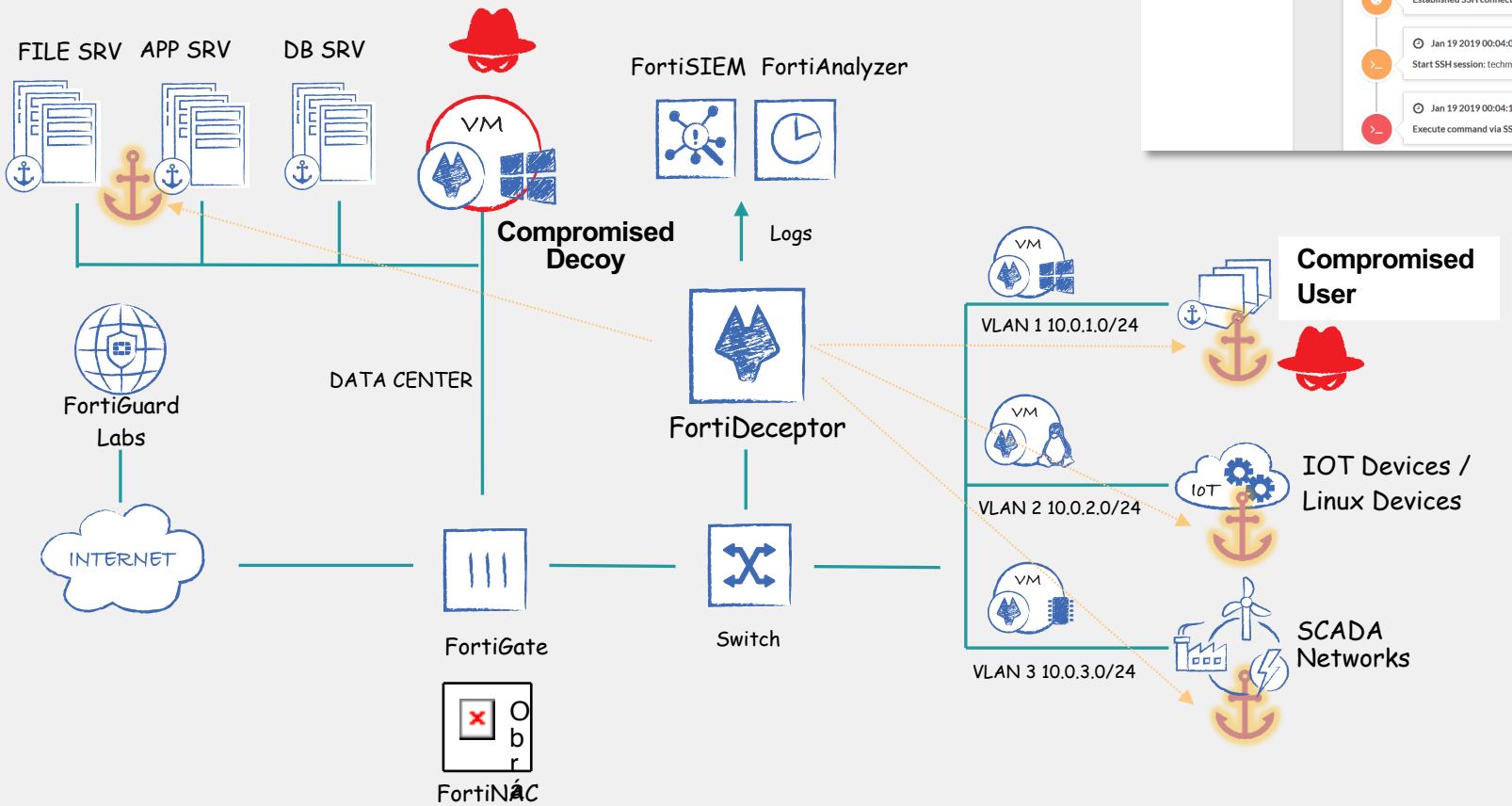


- Nalákání útočníka na návnady, které jsou k nerozeznání od skutečných IT aktiv a jsou vysoce interaktivní
- Centrální správa a automatizace nasazení virtuálních počítačů (Windows, Linux, ICS/SCADA) a generování návnad (data, aplikace/služby)
- Nasazení tokenů na klientská PC

FortiDeceptor - nasazení

Nalákání | Odhalení | Eliminace

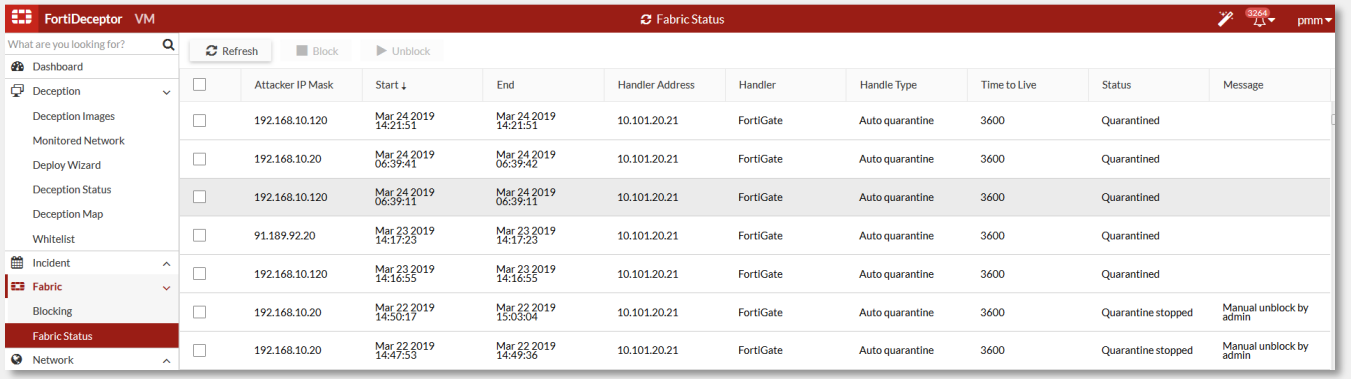


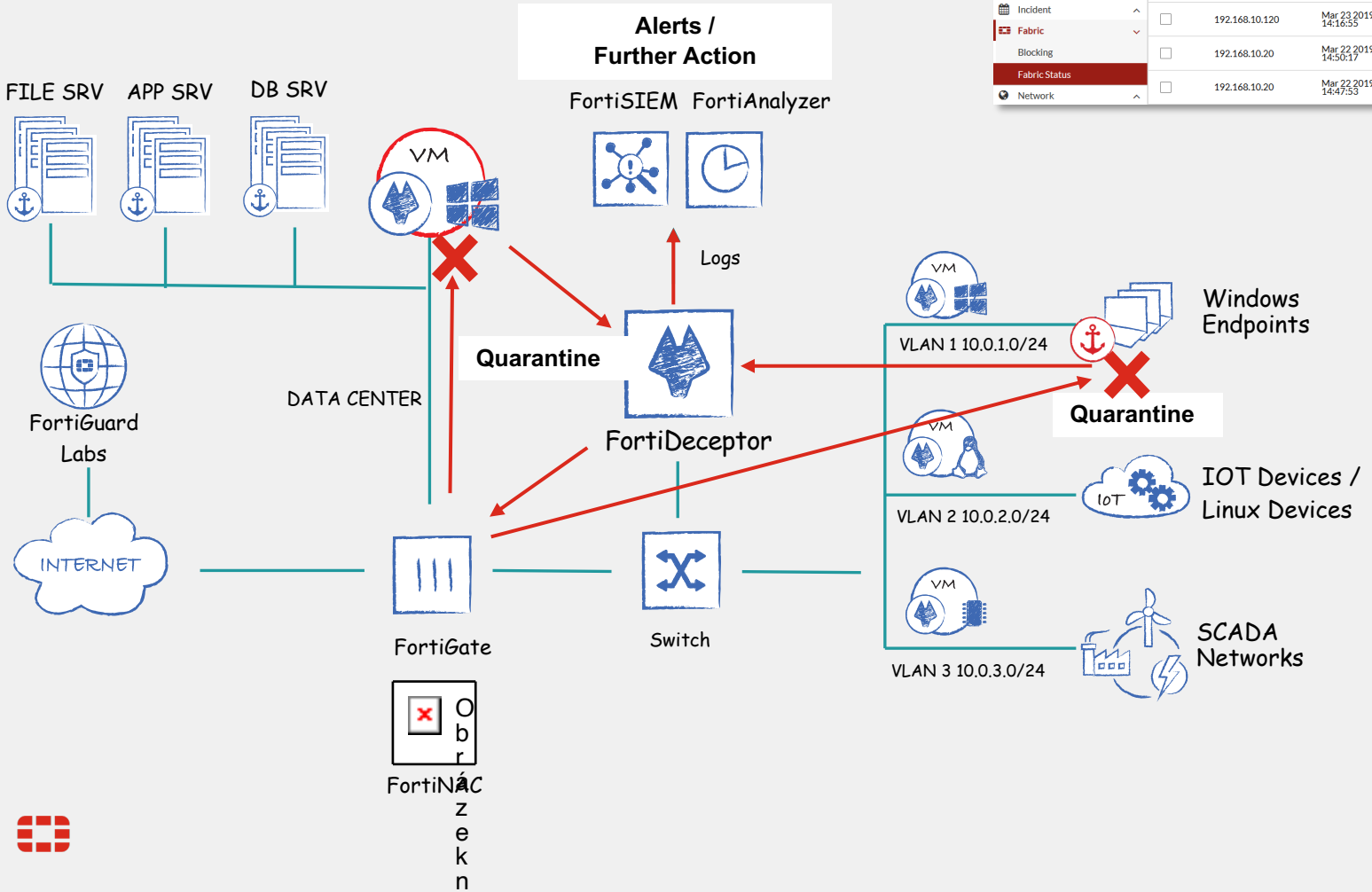


- Systém včasného varování, který generuje výstrahy ke kontrole a analýze
- Konsolidace detekce a korelace aktivit externích i interních útočníků do jediného panelu pro zobrazení celé kampaně

FortiDeceptor - nasazení

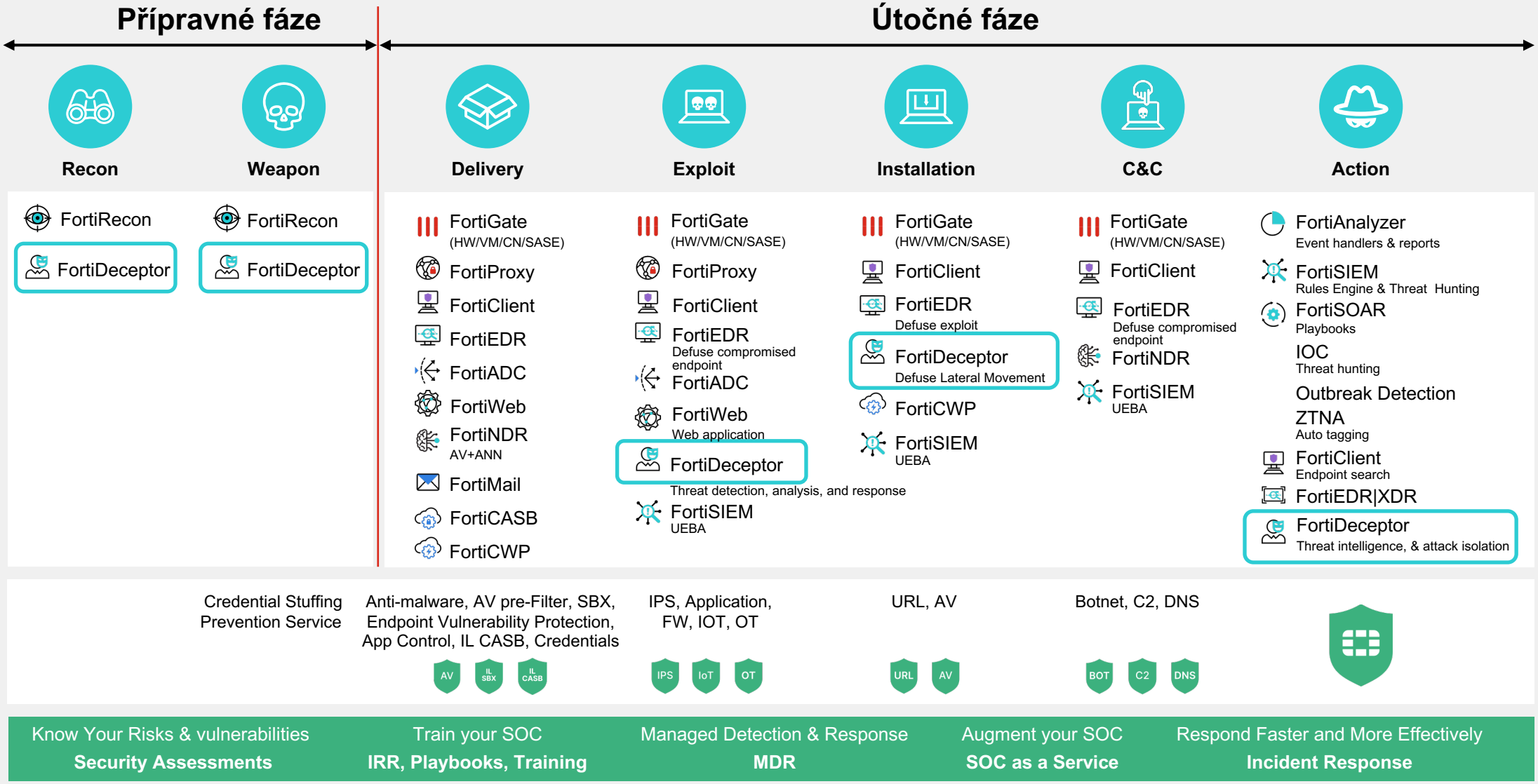
Nalákání | Odhalení | Eliminace





- Včasné ruční/automatické blokování útočníků na základě závažnosti předtím, než dojde ke skutečné škodě
- FortiGate: karanténa interních i externích IP adres
- FortiNAC: izolace zařízení
- Externí konektor pro integrace technologií třetích stran

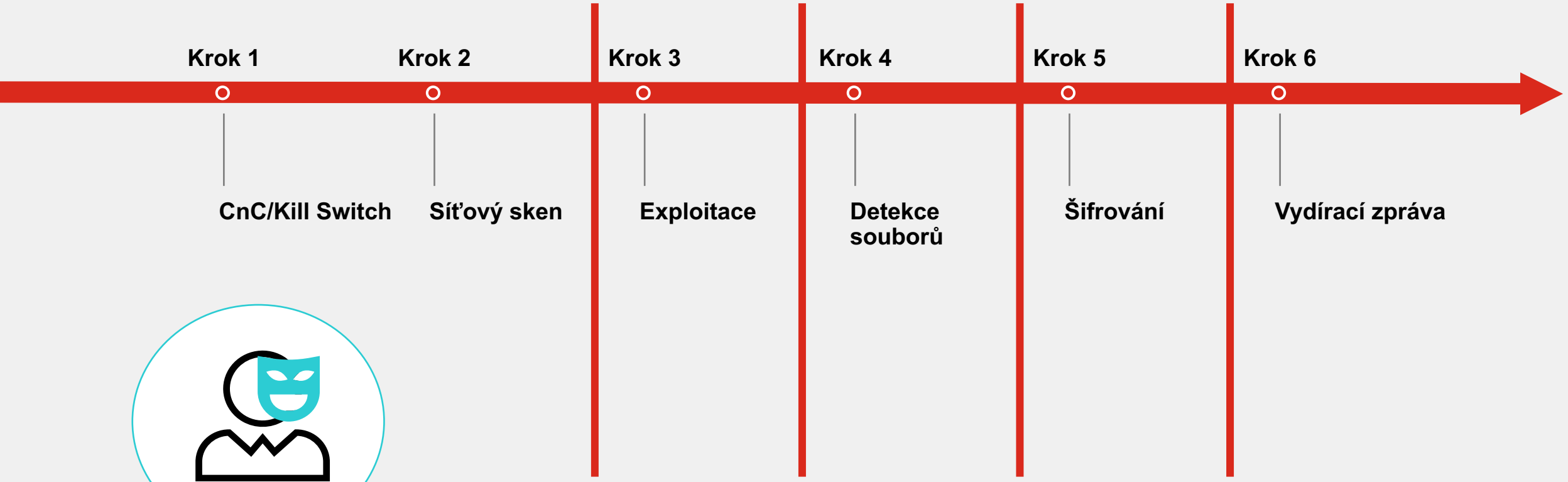
Jak přerušit sekvenci útoku?



WannaCry Ransomware

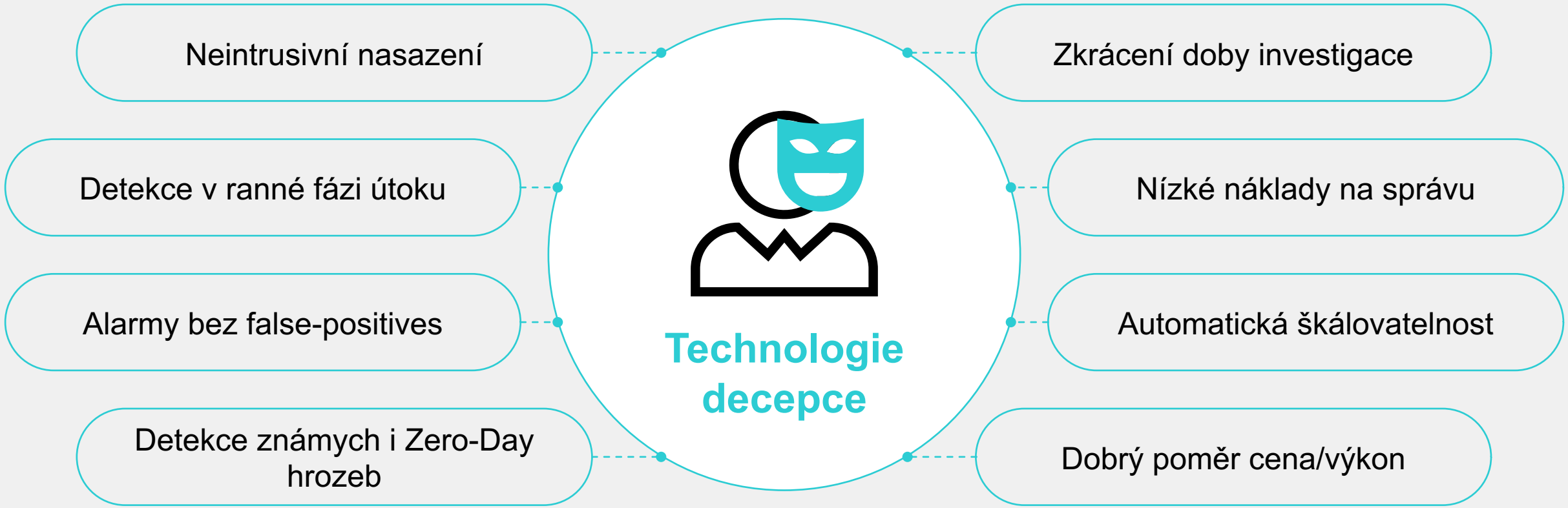
Krok 1	Krok 2	Krok 3	Krok 4	Krok 5	Krok 6
CnC/Kill Switch	Síťový sken	Exploitace	Detekce souborů	Šifrování	Vydírací zpráva

WannaCry Ransomware



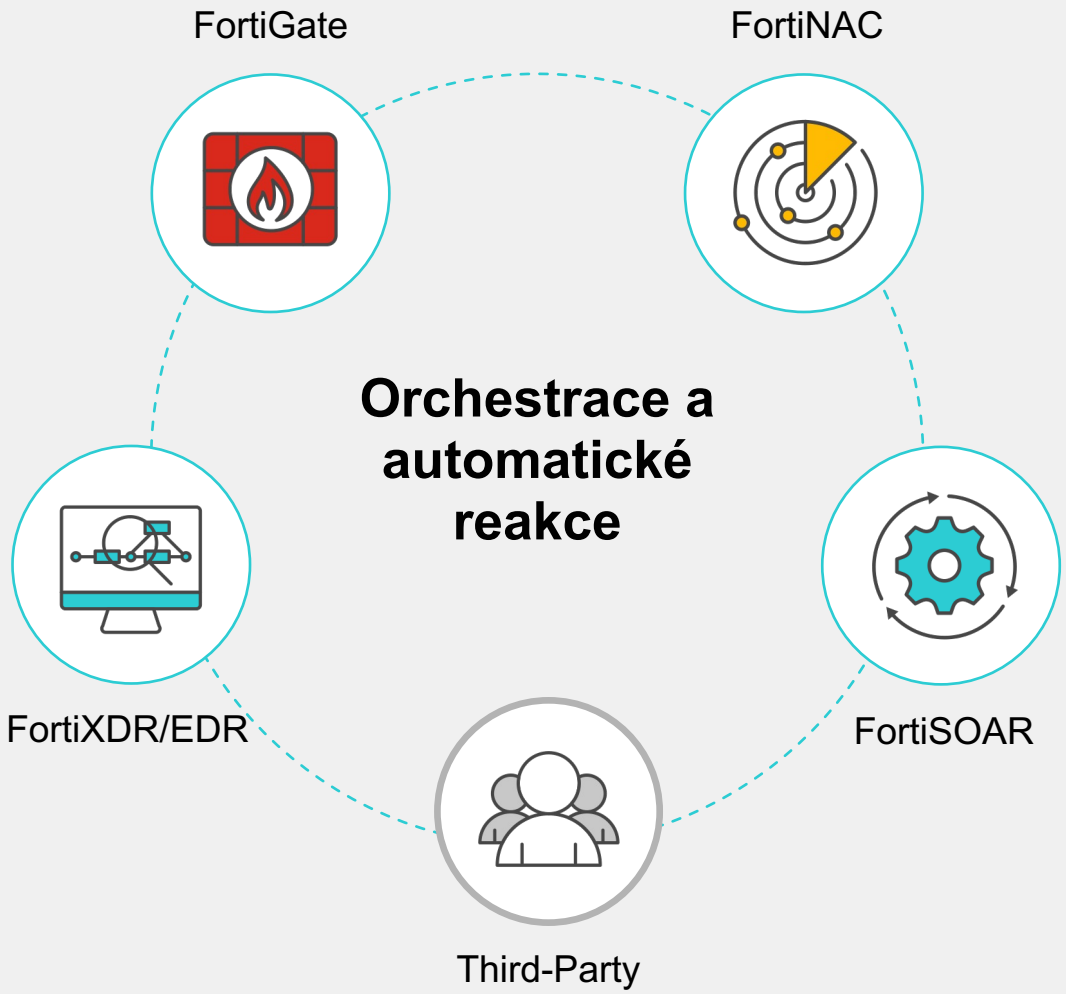
FortiDeceptor

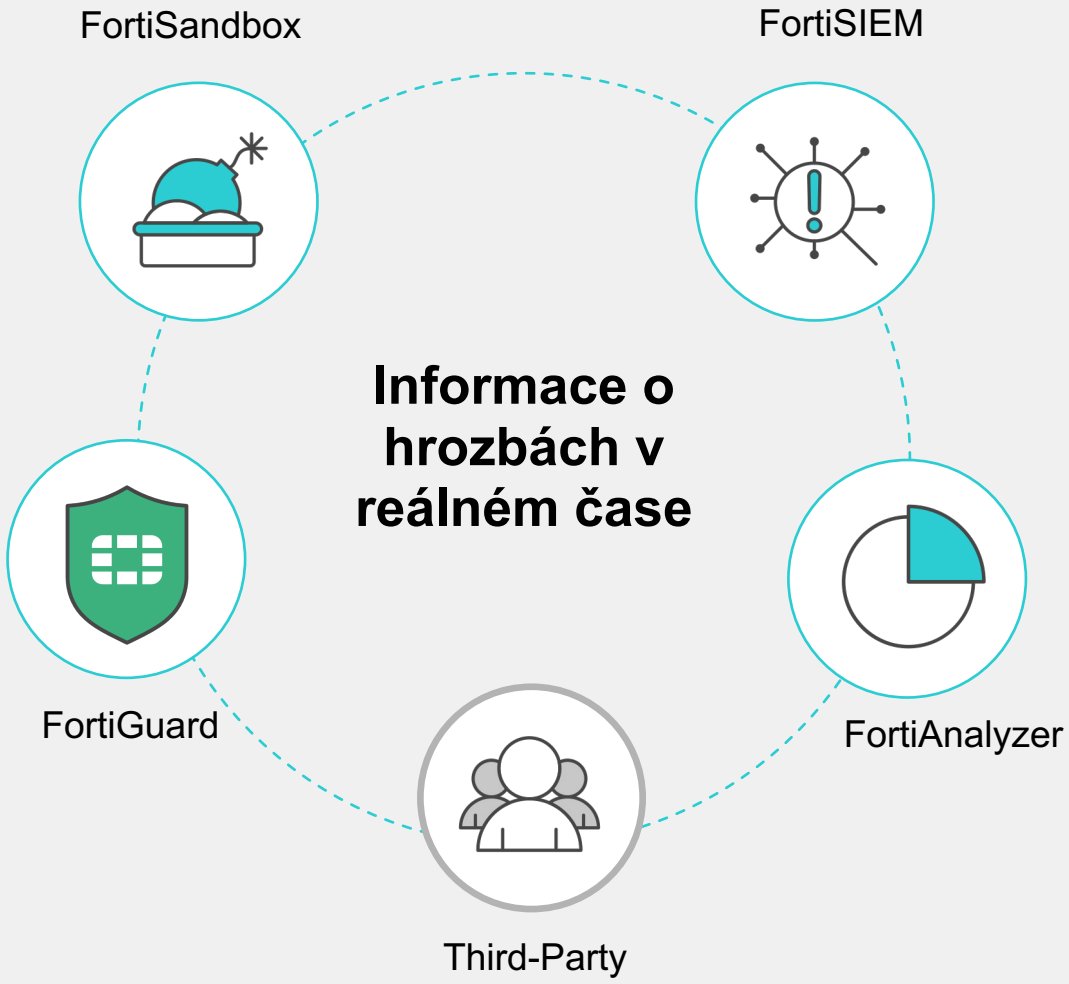
Proč by měl každý využívat decepci



Integrace s Fortinet Security Fabric

Obohacené informace o hrozbách, automatizovaná reakce





Fortinet Security Fabric

Robustní

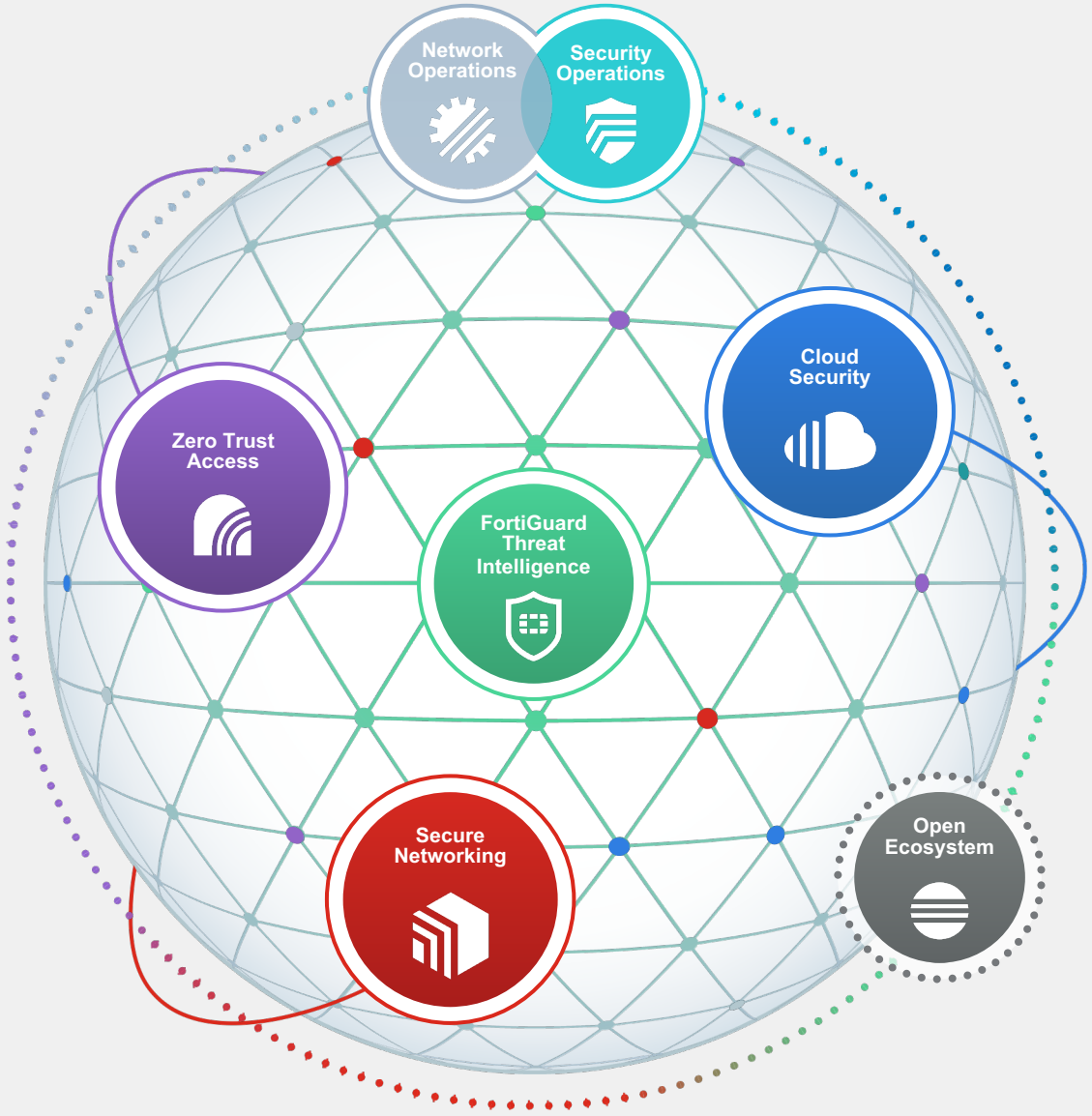
Viditelnost a ochrana celého digitálního prostoru pro lepší zvládání rizika

Integrovaná

Řešení, které snižuje komplexitu a sdílí informace o hrozbách

Automatizovaná

Samonápravná sít s AI řízenou bezpečností pro rychlý a efektivní provoz



Appliance

Virtual

Hosted

Cloud

Agent

Container

Thank You