POSÍLENÍ OBRANY KYBERNETICKÉHO PROSTORU PROSTŘEDNICTVÍM XDR

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

sales@corpus.cz
+420 241 020 333
www.corpus.cz

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4

Agenda

- Corpus Solutions a.s.
- Tradiční přístup budování SOC
- eXtended Detection and Response (XDR)
- Umělá inteligence a strojové učení v XDR
- Využití XDR v procesu SOC

CORPUS SOLUTIONS A. S.

- Konzultační a technologická společnost
- Aplikovaná kybernetická bezpečnost
- Založena 1992
- Česká společnost
- Čeští akcionáři
- 75 zaměstnanců
- Určeni jako provozovatel KII

TF-CSIRT
Trusted Introducer
Accredited
since 24 Oct 2018

AFCEA

Corpus = Cybersecurity Experts

PŘEDSTAVENÍ

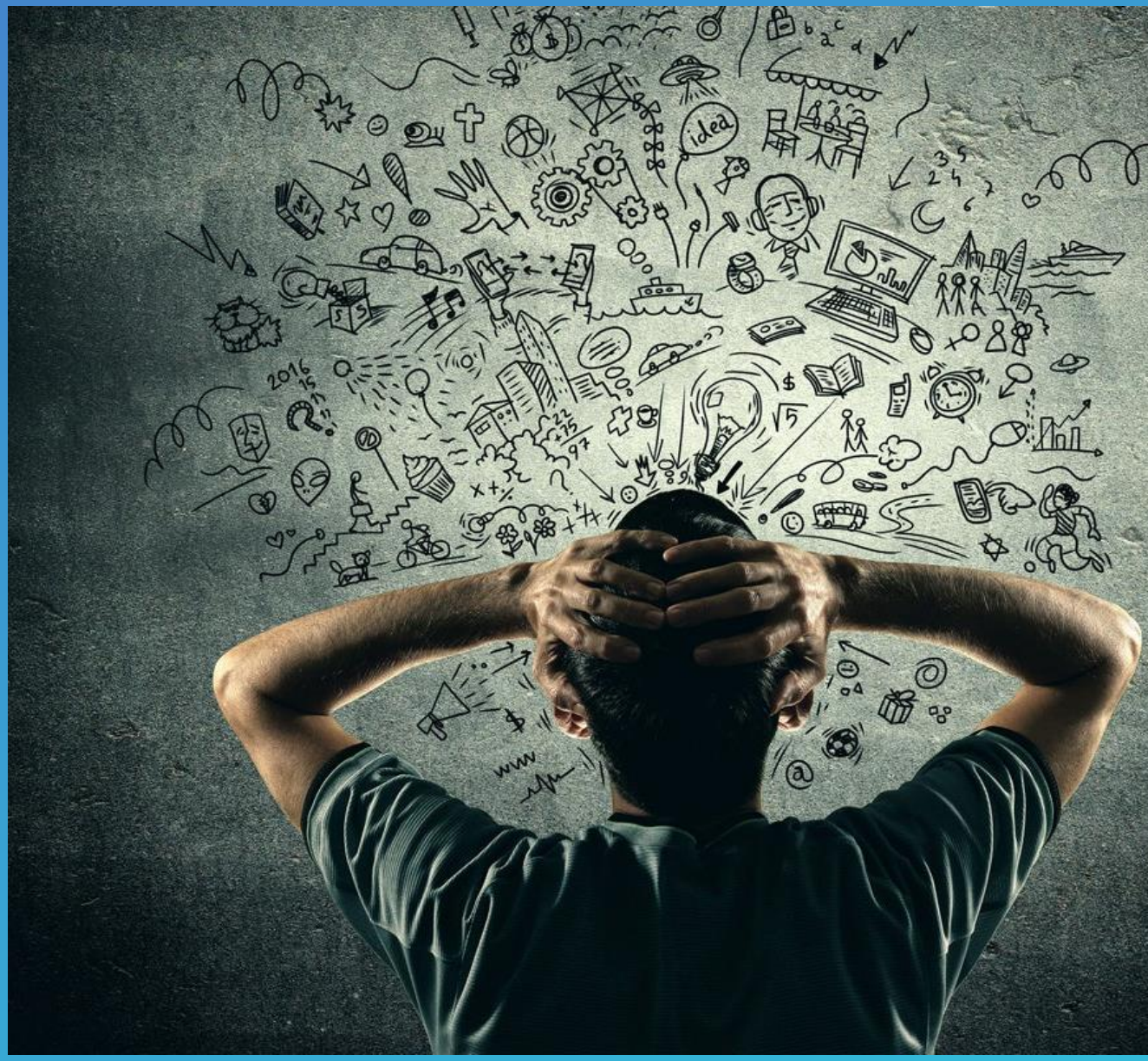
Pavel Klimeš

- Ředitel rozvoje bezpečnostních produktů v Corpus Solutions a.s.
- Zakladatel Offensive Security v Corpus Solutions a.s.
- Architekt efektivní kybernetické obrany u zákazníků.
- Praktické zkušenosti s detekcí a zvládáním kybernetických útoků.
- Autor tréninkového konceptu Cyber Defense Academy.
- 25 let praxe v oboru kybernetická bezpečnost.

pavel.klimes@corpus.cz

TRADIČNÍ PŘÍSTUP BUDOVÁNÍ SOC

Od SIEM Driven Security k XDR



TRADIČNÍ KYBERNETICKÁ BEZPEČNOST

SIEM DRIVEN SECURITY

Projekty začínají výběrem platformy SIEM její instalací a konfigurací a průběžnou správou:

- Integrace zdrojů dat – s agenty nebo bez instalace agentů
- Sběr dat – přenos dat od cílového systému do LM/SIEM
- Normalizace dat – sjednocení rozdílných formátů logů
- Parsing – syntaktická analýza, tedy porozumění obsahu dat
- Detekce a korelace – příprava a neustálá údržba pravidel
- Ukládání a indexace – umožnění rychlého vyhledávání a archivace

Nezbytnou činností je neustálá údržba zdrojů dat, tedy řízení životního cyklu (vznik, modifikace a zánik).

Implementace SIEM trvá v závislosti na připravenosti zákazníka 0,5 – 3 roky.

TRADIČNÍ KYBERNETICKÁ BEZPEČNOST

PROČ POSKYTOVATEL SOC PŘEMÝŠLÍ O VHODNOSTI XDR?

Zákazník

- Portfolio bezpečnostních nástrojů je zaměřeno převážně na prevenci a neposkytuje potřebná data pro detekci projevů kybernetických hrozeb.
- Absence nástrojů se schopností detekovat kybernetické hrozby.
- Specialisté IT provozu nemají dostatek volných kapacit na řešení kybernetické bezpečnosti (*součinnost při implementaci SIEM + podpora vyšetřování a reakce*).

Poskytovatel

- Zavedení služby SOC závislé jen na implementaci SIEM je neefektivní.
  - Jen zavedení technologie SIEM trvá 0,5 - 3 roky.
  - Spuštění služby SOC není možné dříve, než je SIEM adekvátně implementován.
  - Chybí automatizace vyšetřovacích postupů.
  - Chybí automatizace nebo podpora reakčních postupů.

Je třeba najít řešení, které umožní rychle chránit organizace a poskytne čas na budování robustního SIEM popř. SOAR.

eXtended Detection and Response (XDR)

Platforma pro detekci, vyšetřování a zvládání kybernetického ohrožení

eXtended Detection and Response (XDR)

Co je XDR?

eXtended Detection and Response je bezpečnostní řešení, které poskytuje rozšířenou detekci, analýzu a reakci na kybernetické hrozby napříč prostředím chráněné organizace.

- XDR integruje více bezpečnostních nástrojů, jako jsou:
  - Ochrana koncových zařízení (EDR)
  - Ochrana sítě (NDR)
  - Ochrana e-mailového a webového provozu
  - Ochrana prostředí pomocí návnad a SANDBOXu
- Vzájemná integrace nástrojů, jednotný formát metadat a vzájemná podpora procesů detekce, vyšetřování a reakce tvoří řešení XDR.

eXTENDED DETECTION AND RESPONSE (XDR)

eXtended Detection and Response (XDR)

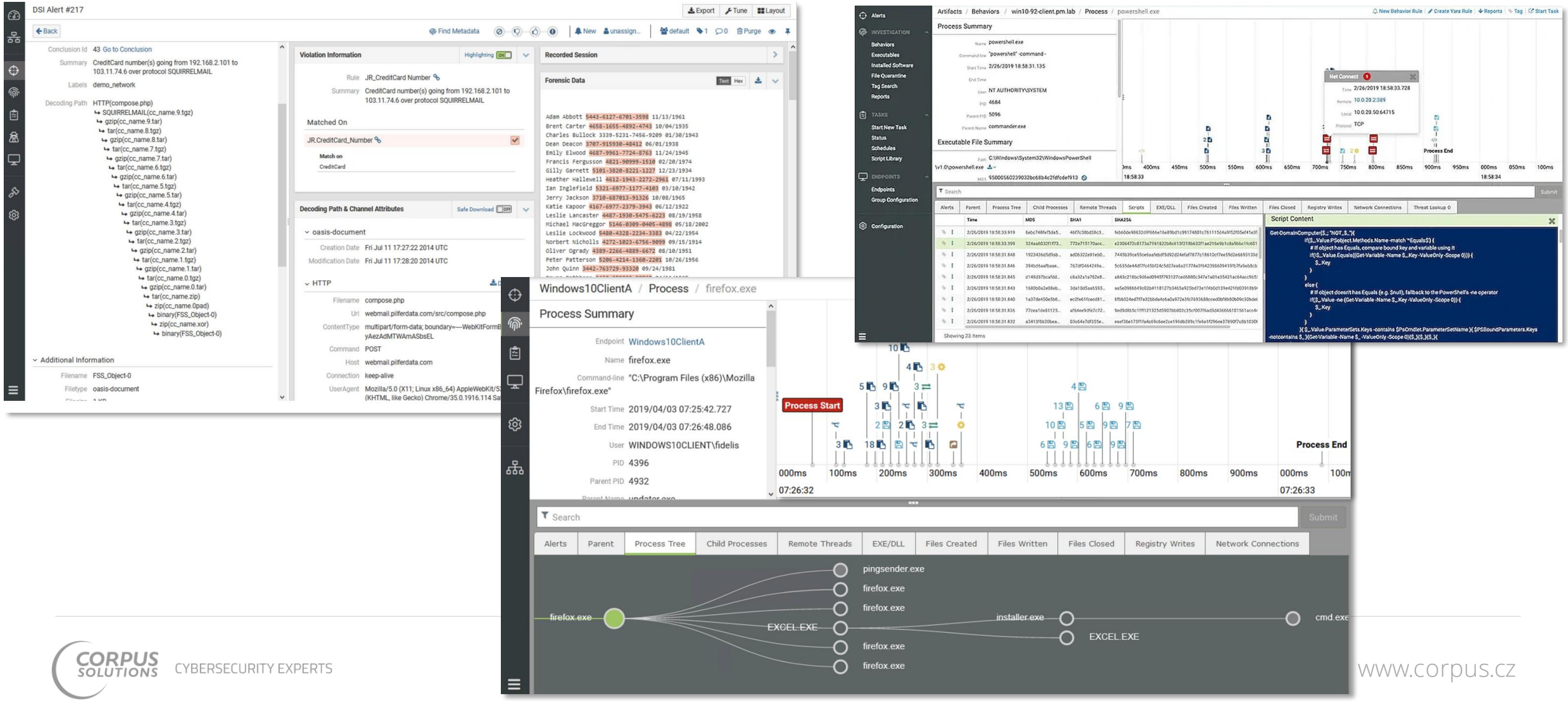
Pre-Infection		Post-Infection	
Prevence: • Signatury • Heuristika • Block-listy **Block**	**Sběr dat:** • Záznam metadat o veškerém chování sítě a koncových bodů **Collect**	**Detekce:** • Strojové učení • Threat hunting • Bezp. analýzy Analýzy: a) Bahaviorální b) Retrospektivní c) Souvislostní **Detect**	**Reakce:** • Zastavení šíření • Vyšetřování • Obohacení • Zotavení • Návrat do provozu • Důkazy a IoC **Respond**

eXTENDED DETECTION AND RESPONSE (XDR)

Co nám technologie XDR přináší?

ZVÝŠENÍ SCHOPNOSTI DETEKCE A VYŠŠÍ EFEKTIVITA SOC

eXTENDED DETECTION AND RESPONSE (XDR)



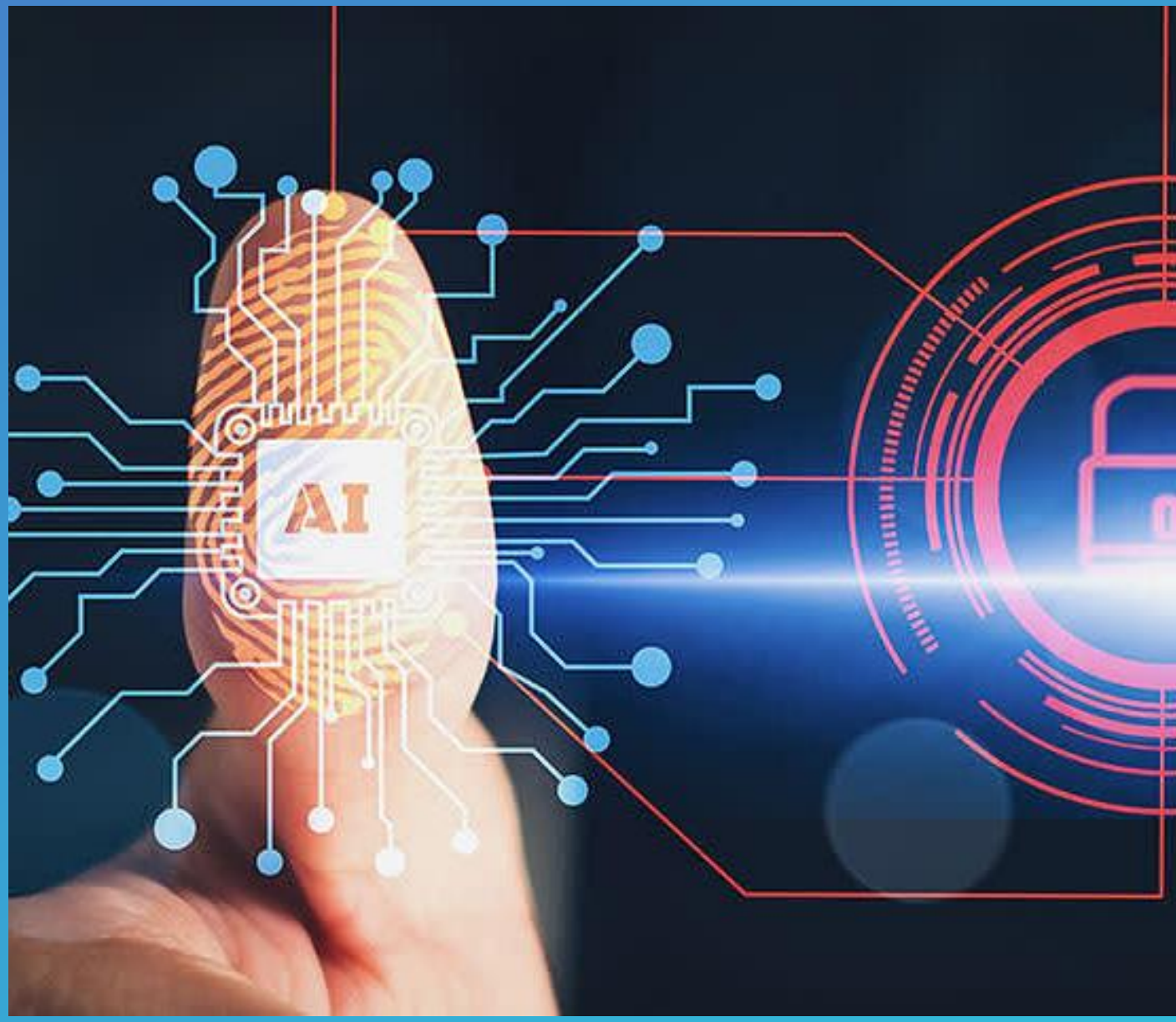
eXtended Detection and Response (XDR)

Pozor na rozdíly mezi XDR nástroji

- On-premise nebo CLOUD řešení – někteří výrobci nabízejí pouze CLOUD řešení XDR
  - Zpracovávají omezené množství dat
  - Nástroj není funkční při zasažení organizace útokem DDoS
- Neselektivní nebo jen vybraná metadata – aby výrobce snížil zátěž na analýzu dat, tak ukládá pouze taková metadata, která náleží detekovaným událostem (+/- 5min)
- Integrované nebo integrovatelné – je mnoho výrobců, kteří nemají vlastní integrované XDR řešení, ale pouze své NDR nebo EDR řešení umí integrovat na produkty 3. stran.

Vyberte takové řešení, které odpovídá reálným požadavkům SOC !

UMĚLÁ INTELIGENCE A STROJOVÉ UČENÍ V XDR



UMĚLÁ INTELIGENCE A STROJOVÉ UČENÍ V XDR

PŘÍKLADY UŽITÍ AI A ML V PLATFORMÁCH XDR

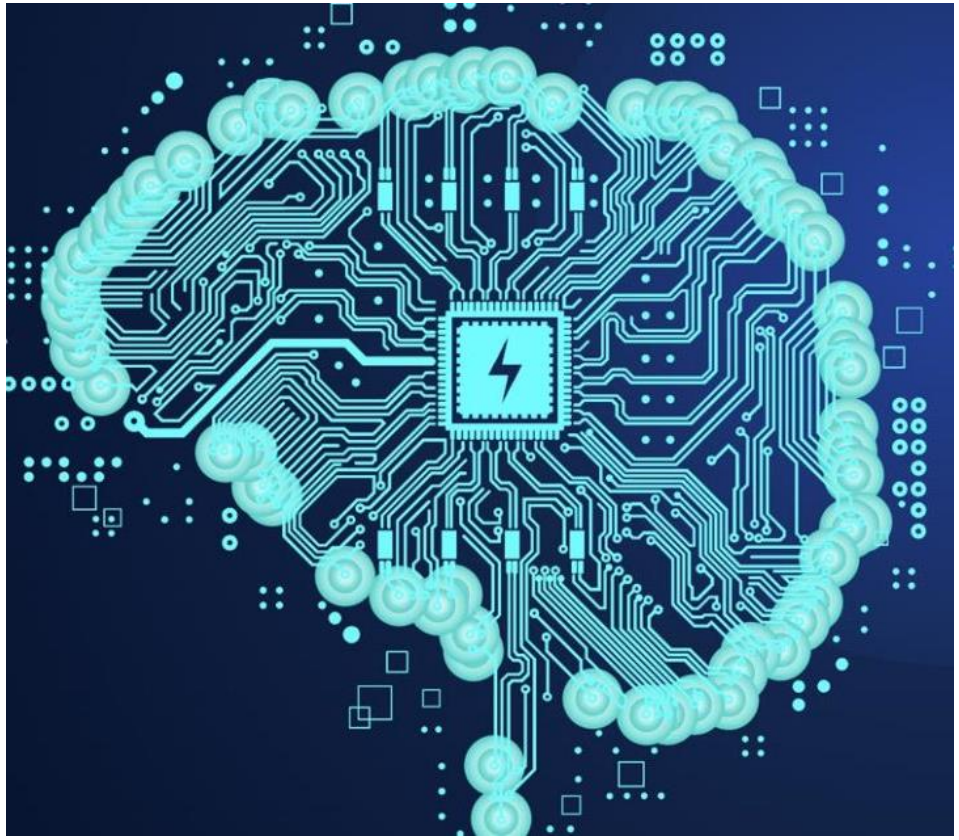
- Detekce kybernetických hrozeb
  - Analýza chování identit a aktiv (definice baseline)
  - Pokročilá detekce malware
  - Real-time Threat hunting (anomálie)

Pro	Proti
Vysoká rychlost blížící se real-time detekci.	Často se jedná jen o statistické modely, které jsou prodávané jako AI nebo ML.
Rychlá detekce znamená možnost včasné reakce a předcházení ztrát minimalizací dopadů.	Výrobci neposkytují vlastní AI modely mimo prostředí svých CLOUD platforem. Nutí klienty zasílat svá data do jejich prostředí.
Schopnost zpracování aktuálních i historických dat v souvislostech. Odhalení vektoru průniku, označení paciten-0, modelování dopadu.	Časté chyby (algoritmická **ne**přesnost), které z exaktní detekce dělají spíše hypotézy vyžadující další šetření.

UMĚLÁ INTELIGENCE A STROJOVÉ UČENÍ V XDR

PŘÍKLADY UŽITÍ AI A ML V PLATFORMÁCH XDR

- Automatizace postupů pracoviště SOC
  - Obohacení vyšetřování o související informace nezbytné pro rychlé rozhodování
  - Decoy deployment, tedy automatická distribuce návnad do prostředí (dle charakteru prostředí, dle vývoje hrozeb)
  - Reakce na incident dle rozhodovacích stromů v playbooku, kde AI/ML umí poskytnout optimální cestu na základě intenzity hrozby.

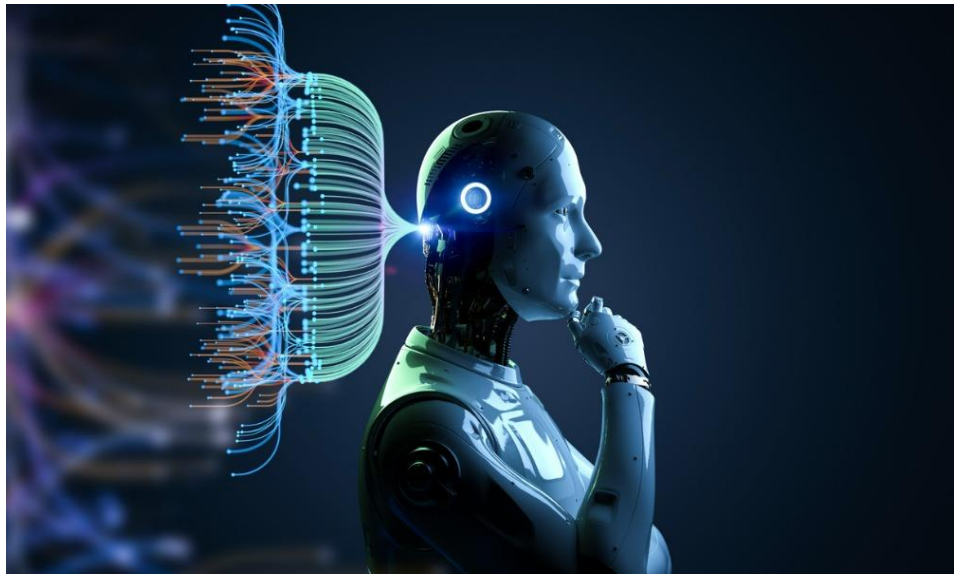


Pro	Proti
Významné urychlení celého vyšetřovacího postupu, analytik dostává všechny dostupné související důkazy od systému XDR.	Zcela logicky stále nepanuje důvěra v automatické reakce, které mají významné provozní dopady do chráněné organizace. - Izolace zasaženého aktiva - Aktivace blokačních pravidel EDR / NDR
Reakce na vývoj hrozeb, nebo na incident samotný zahrnuje i dynamické změny v infrastruktuře díky návnadám.	

UMĚLÁ INTELIGENCE A STROJOVÉ UČENÍ V XDR

A CO RIZIKA SAMOTNÉ AI V KYBERNETICKÉ BEZPEČNOSTI

- Závislost na zdroji kvalitních dat – evidence identit a aktiv, popis procesů, ohodnocení rizik a dopadů, systematická evidence zranitelností. Přesto, že tyto informace jsou nezbytné pro správné rozhodování, často chybí.
- Sofistikované útoky na umělou inteligenci – není složité AI oklamat tím, že bude cíleně dostávat podvržená data, která ovlivní rozhodující procesy použitých algoritmů.
- Bezpečnostní rizika v modelech AI - chyby v modelech AI nebo zranitelnosti v jejich implementaci představují rizika, která mohou vést ke zneužití kybernetickými útočníky.
- Oslabení lidských dovedností - silné spoléhání na umělou inteligenci by mohlo snížit kritické myšlení a dovednosti odborníků na kybernetickou bezpečnost.



Nedostatek kvalifikace v oblasti implementace a řízení AI.

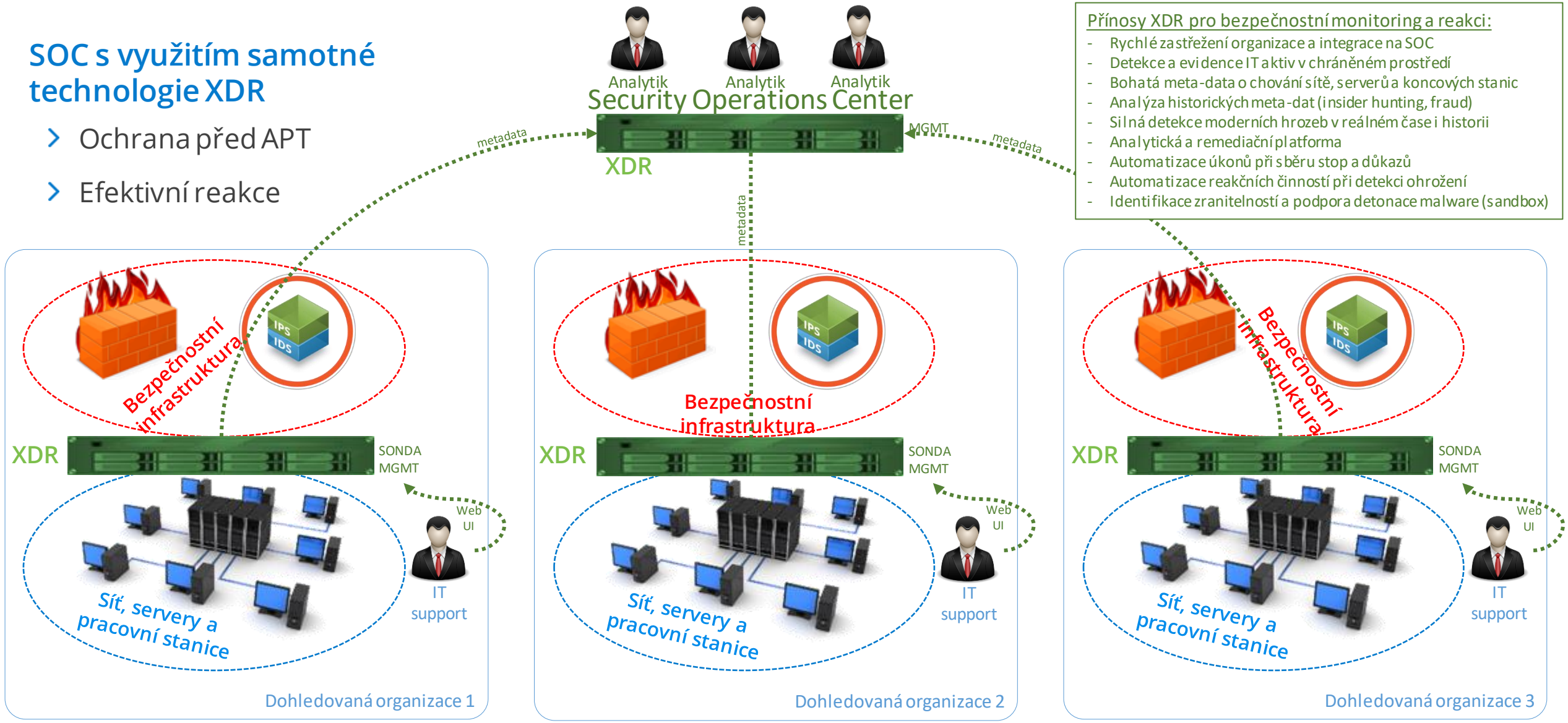
Využití XDR v procesu SOC

Security Operations Center

eXTENDED DETECTION AND RESPONSE (XDR)

SOC s využitím samotné technologie XDR

- Ochrana před APT
- Efektivní reakce



Přínosy XDR pro bezpečnostní monitoring a reakci:

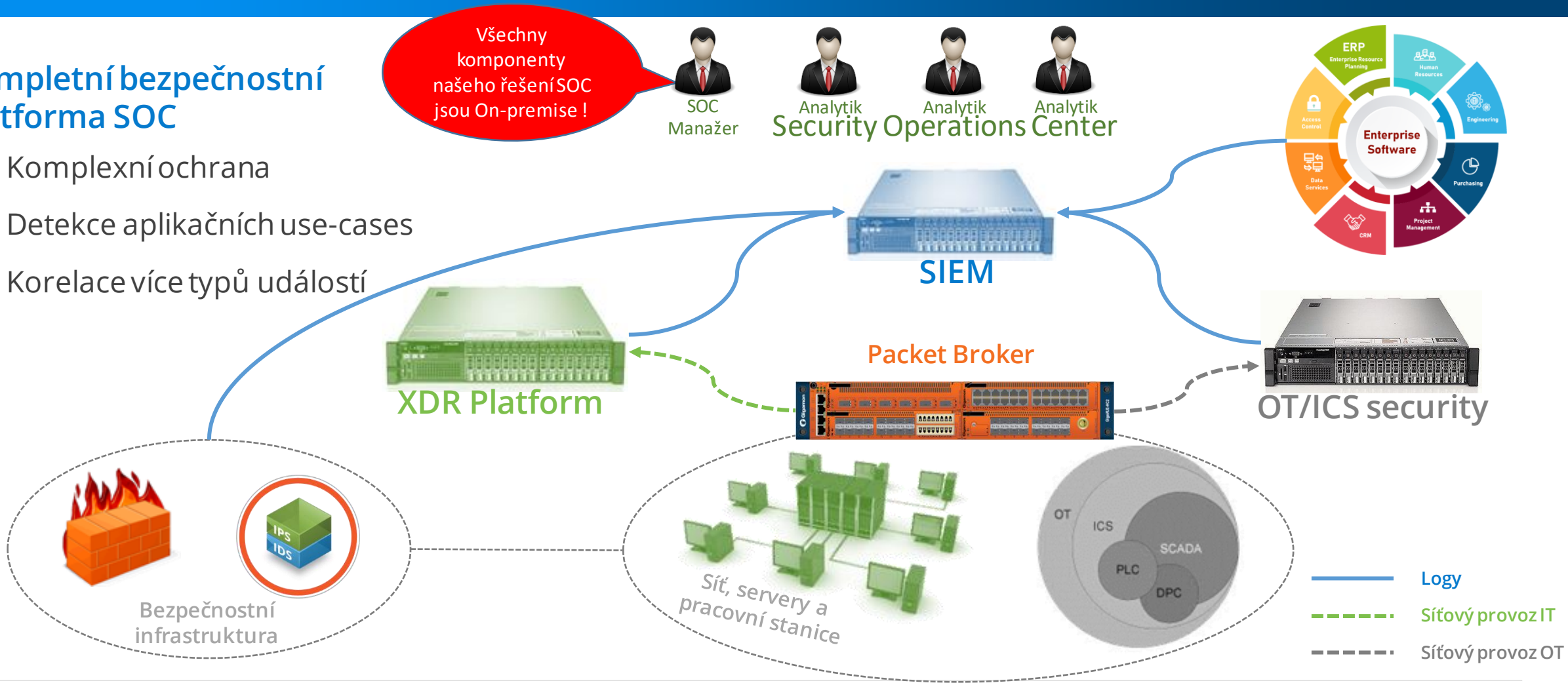
- Rychlé zastřežení organizace a integrace na SOC
- Detekce a evidence IT aktiv v chráněném prostředí
- Bohatá meta-data o chování sítě, serverů a koncových stanic
- Analýza historických meta-dat (insider hunting, fraud)
- Silná detekce moderních hrozeb v reálném čase i historii
- Analytická a remediační platforma
- Automatizace úkonů při sběru stop a důkazů
- Automatizace reakčních činností při detekci ohrožení
- Identifikace zranitelností a podpora detonace malware (sandbox)

eXTENDED DETECTION AND RESPONSE (XDR)

Moderní nástroje pro efektivní zastřežení prostředí OT/IoT

Kompletní bezpečnostní platforma SOC

- Komplexní ochrana
- Detekce aplikačních use-cases
- Korelace více typů událostí



CORPUS SOLUTIONS

Průzkum → Zbrojení → Doručení → Exploitace → Instalace → C&C → Cíl

eXTENDED DETECTION AND RESPONSE (XDR)

KDY POUŽÍT JAKOU TECHNOLOGII?

- SIEM je ideální pro organizace, které potřebují komplexní dohled nad bezpečnostními daty, auditování a splnění regulatorních požadavků.
- XDR je vhodnější pro organizace, které hledají integrované řešení schopné rychle detekovat a reagovat na hrozby v reálném čase a mají zájem o snížení komplexity svého bezpečnostního prostředí.

Každá technologie nabízí jedinečné výhody a nejlepší volba závisí na specifických bezpečnostních potřebách organizace.

Ideální je, když se obě technologie společně doplňují.

SECURITY OPERATIONS CENTER