ROLE INTELIGENTNÍCH PASTÍ V KYBERNETICKÉ OBRANĚ

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

CORPUS SOLUTIONS A. S.

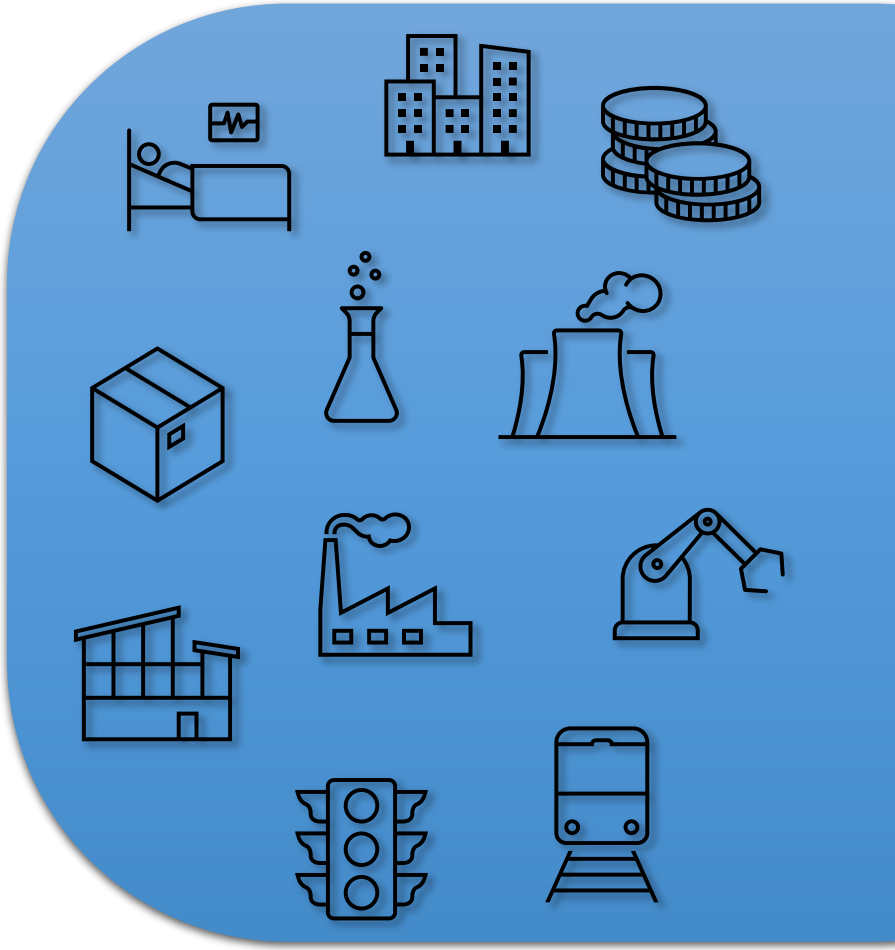
- Konzultační a technologická společnost
- Obor aplikovaná kybernetická bezpečnost
- Založena 1992
- Česká společnost
- Čeští akcionáři
- Dvě pobočky
- 60 zaměstnanců
- Určeni jako provozovatel KII

TF-CSIRT
Trusted Introducer
Accredited
since 24 Oct 2018

Corpus = Cybersecurity Experts

Security Operations Center – Corpus Solutions a.s.

SECURITY OPERATIONS CENTER
provided by Corpus Solutions



Security Operations Center – Corpus Solutions a.s.

Soustřeďme se na to podstatné

- Pro organizace vybíráme relevantní kybernetické hrozby mířící na klíčová aktiva (dle BIA, AR, GDPR, NÚKIB, …).
- Z procesu Vulnerability managementu (pen-testů) navíc nabíráme informace o neošetřených slabinách.
- Provádíme modelování kybernetických hrozeb vůči organizaci a převádíme je na známé útočné techniky (dle MITRE).
- Pro každou identifikovanou hrozbu a vektor ohrožující zranitelnost, definujeme tzv. **bezpečnostní scénáře**:
  - Hrozba, MITRE technika, relevantní aktiva, zdroje detekce
  - Metriky pro reporting

Bezpečnostní scénáře definují požadavky na:

- Bezpečnostní infrastrukturu
- Bezpečnostní detekční politiku
- Intenzitu a způsob logování
- Určení vlastníků
- Určení technických garantů
- Parametry pro reakce a reporting

Security Operations Center – Corpus Solutions a.s.

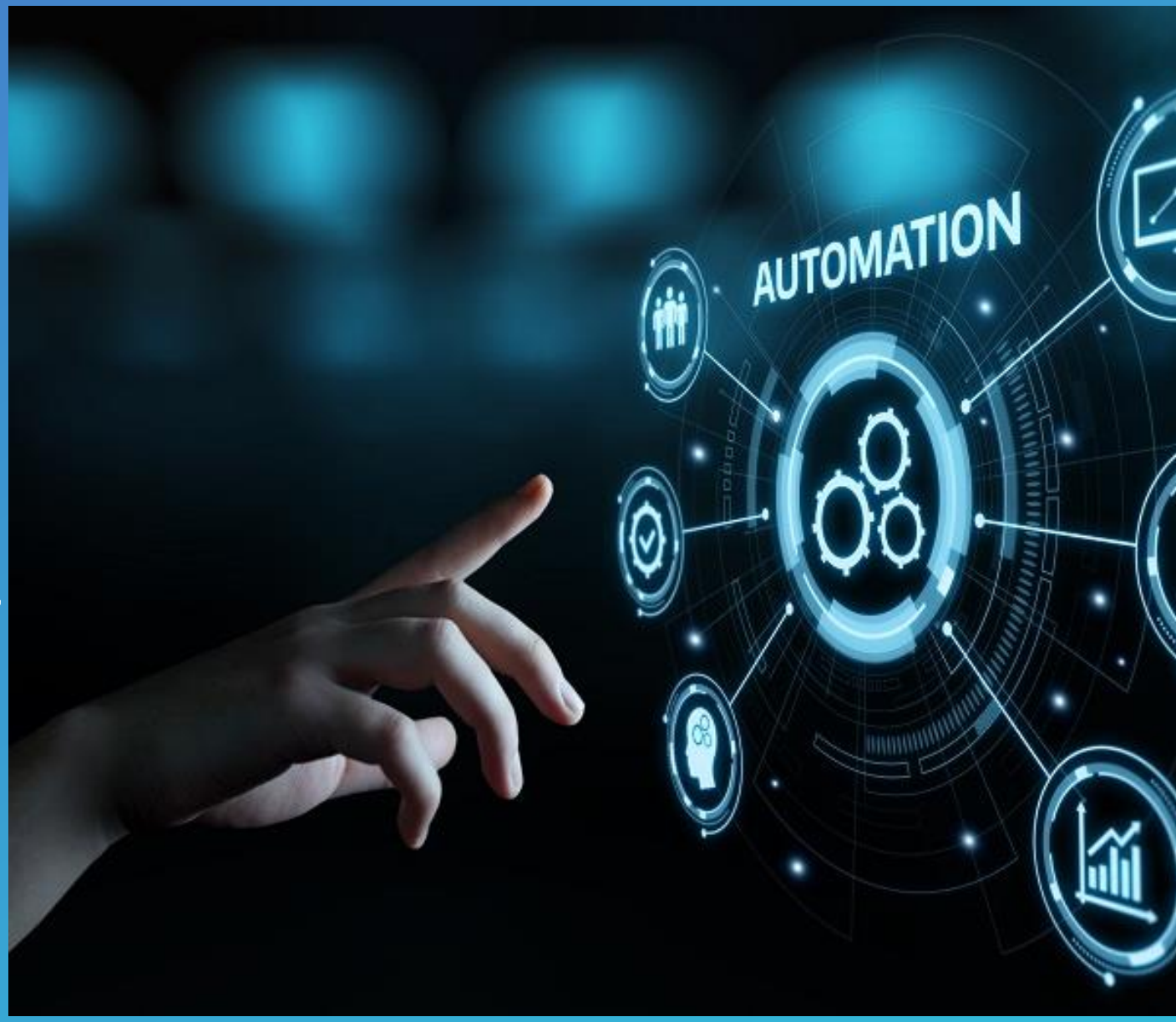
Efektivita zavádění některých bezpečnostních scénářů

- Pro naplnění některých bezpečnostních scénářů je třeba doplnit specifické detekční, vyšetřovací a reakční schopnosti do infrastruktury.
- Moderní přístup využívá technologie z kategorií ADR/XDR, IT/OT anomaly detection, user behavioral analysis, SOAR, …
- Tyto technologie zároveň umožňují výrazné urychlení implementace SOC a výrazně snižují zátěž na IT provoz.

Nelze spoléhat jen na SIEM, ale je potřeba přístup zrychlit a zjednodušit.

Automated Detection and Response

Moderní platforma pro detekci, vyšetřování a zvládání kybernetického ohrožení



AUTOMATED DETECTION AND RESPONSE

Co nám technologie ADR přináší?

ZVÝŠENÍ SCHOPNOSTI DETEKCE A VYŠŠÍ EFEKTIVITA SOC

Rychle nasaditelné a na ostatních technologiích nezávislé bezpečnostní řešení.

Provede zmapování ICT infrastruktury z hlediska ICT aktiv a jejich atributů.

Přináší schopnost detekovat moderní kybernetické útoky.

Minimalizuje požadavky na IT při implementaci i šetření detekovaných událostí.

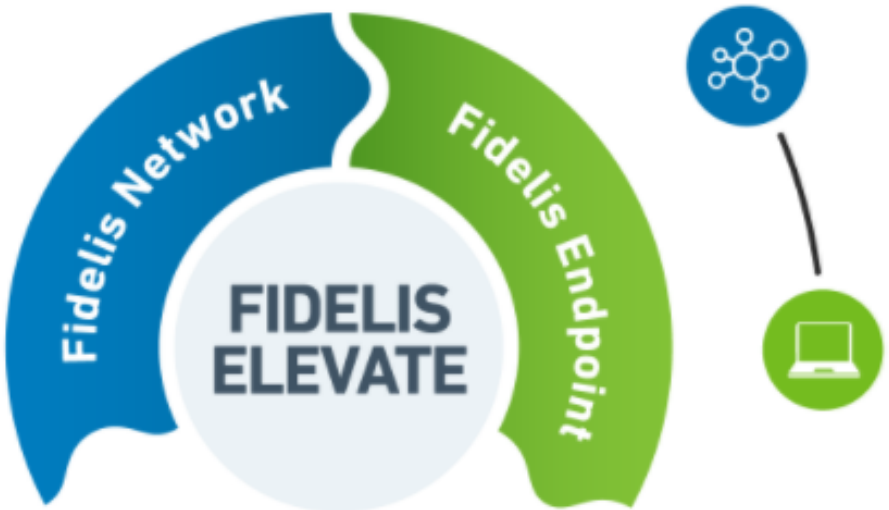
Umožňuje vyšetřovat celý průběh bezpečnostního incidentu, nikoli jen projevy jeho poslední fáze.

Dodává nástroje pro podporu reakčních a nápravných opatření.

AUTOMATED DETECTION AND RESPONSE

Představení platformy Fidelis Elevate

The Fidelis Elevate™ Platform Automates Detection & Response to Improve SOC Efficiency and Effectiveness



Fidelis Network®

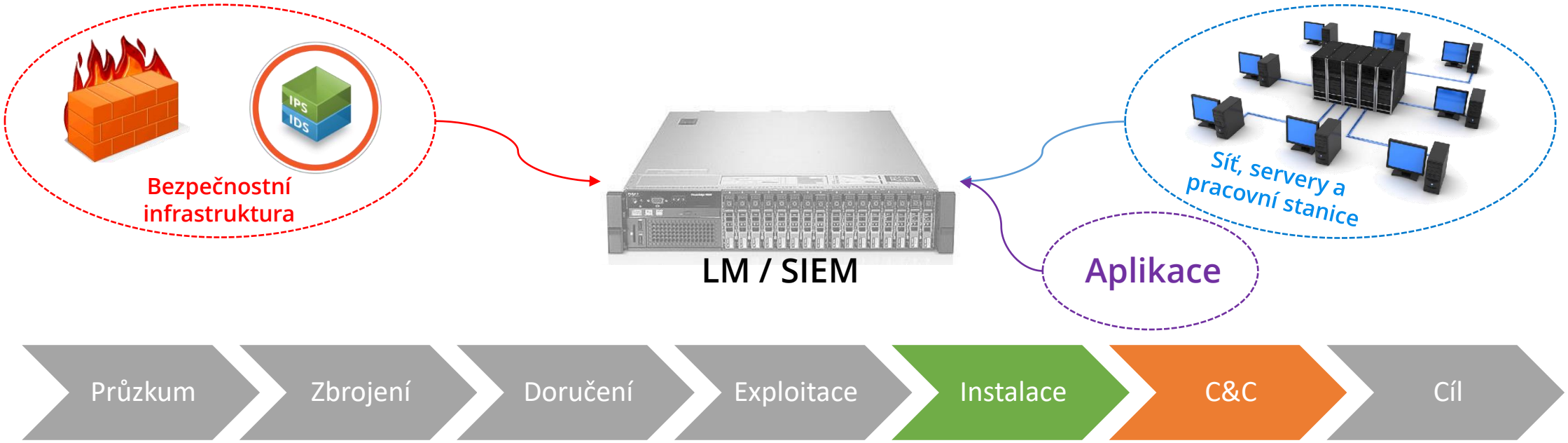
Gain Deep Visibility into Sessions, Packets and Content and Automate Breach Detection for Faster Response

Fidelis Endpoint®

Increase Visibility and Reduce Response Time with Endpoint Detection and Response

AUTOMATED DETECTION AND RESPONSE

Představení platformy Fidelis Elevate



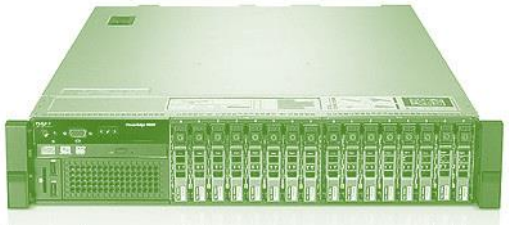
AUTOMATED DETECTION AND RESPONSE

Představení platformy Fidelis Elevate

Detekční *use-cases* vycházející z analýzy rizik a best practice

Reakční *playbooks* pro rychlé zvládání útoků

2 – 20 týdnů

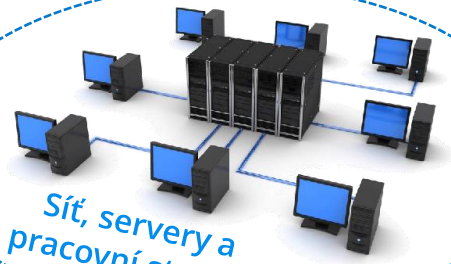


ADR – network & endpoint

Bezpečnostní infrastruktura

LM / SIEM

role konsolidace logů pro scénáře compliance a aplikační bezpečnost

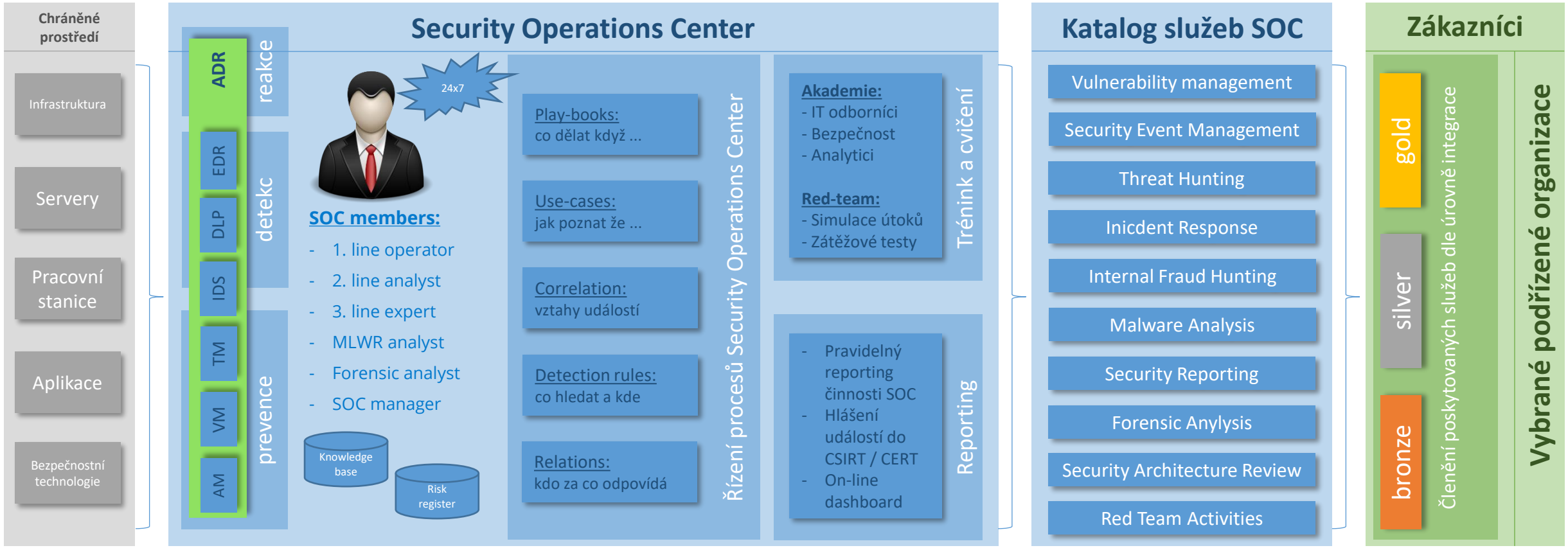


Síť, servery a pracovní stanice

Aplikace

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

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST



IT Risk management - legislativa - regulace – nařízení - povinnosti

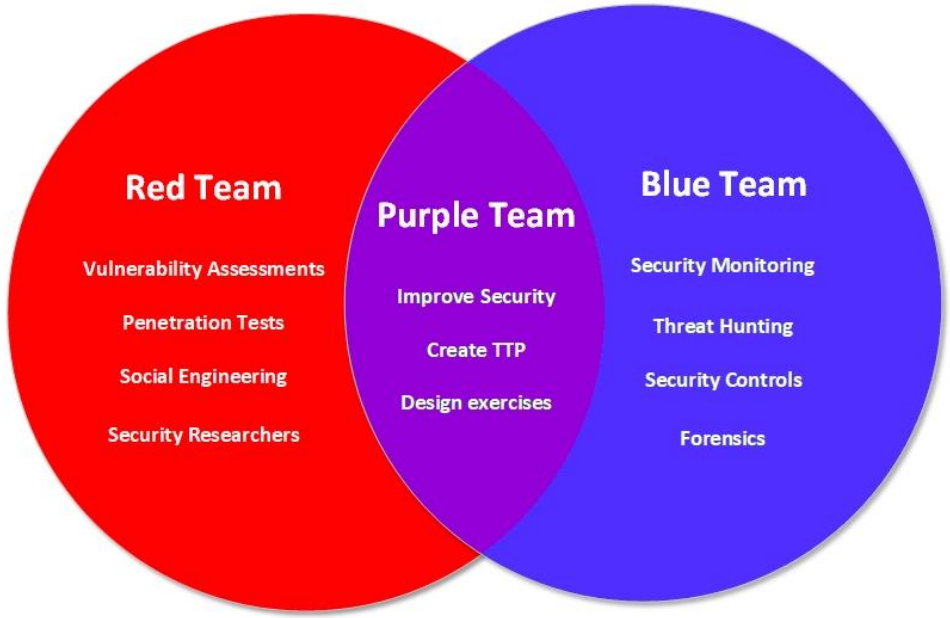
JAKÝ JE PROSTOR PRO DALŠÍ ZVÝŠENÍ ÚČINNOSTI OBRANY?

POSILOVÁNÍ KYBERNETICKÉ OBRANY

EFEKTIVITU POMÁHÁ POVYŠOVAT NÁŠ PURPLE TEAM

- Neustálé zvyšování účinnosti našich bezpečnostní scénářů pro SOC zajišťujeme díky znalosti nových útočných technik
- Nové útočné techniky aplikujeme ve vlastní Cyber Aréně
  - Definice nových TTP
- Učíme se novým způsobům budování kybernetické obrany
- Zejména budováním nových detekčních schopností

Purple Team CS – spojením dovedností útočných s obrannými posilujeme efektivitu týmu SOC.



POSILOVÁNÍ KYBERNETICKÉ OBRANY

ROZŠIŘOVÁNÍ MONITORINGU CHRÁNĚNÉHO PROSTŘEDÍ

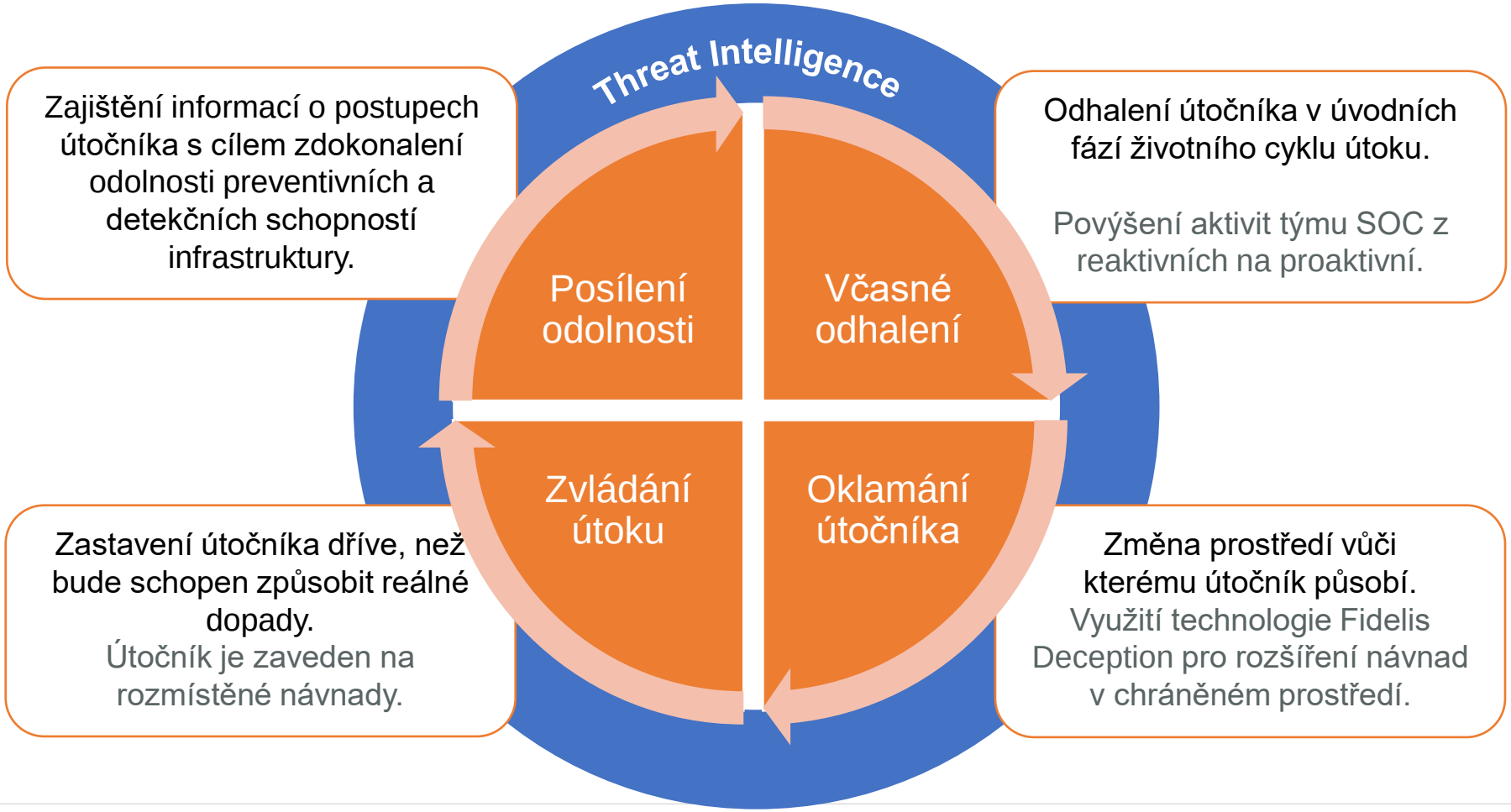
Často nacházíme nepokrytá místa:

- Nedostatečný vhled do šifrovaných komunikací
  - SSL, TLS, SSH, …
  - Dešifrování pro účely monitoringu není schválené
- Nemožnost sledovat provoz v sítích s mohutným provozem (v řádech 10 Gbps – 400 Gbps) – zrcadlení není dnes problém, ale monitoring je finančně enormně nákladný
- Cloudové infrastruktury
- Koncové body, které nejsou podporovány nástroji EDR
  - Zastaralé verze OS, zařízení (tiskárny, kamery, IoT, OT prvky, routery, …)

FIDELIS DECEPTION

Rozšíření obrany o řešení inteligentních pastí/návnad

FIDELIS DECEPTION



Zajištění informací o postupech útočníka s cílem zdokonalení odolnosti preventivních a detekčních schopností infrastruktury.

Odhalení útočníka v úvodních fází životního cyklu útoku.

Povýšení aktivit týmu SOC z reaktivních na proaktivní.

Zastavení útočníka dříve, než bude schopen způsobit reálné dopady.
Útočník je zaveden na rozmístěné návnady.

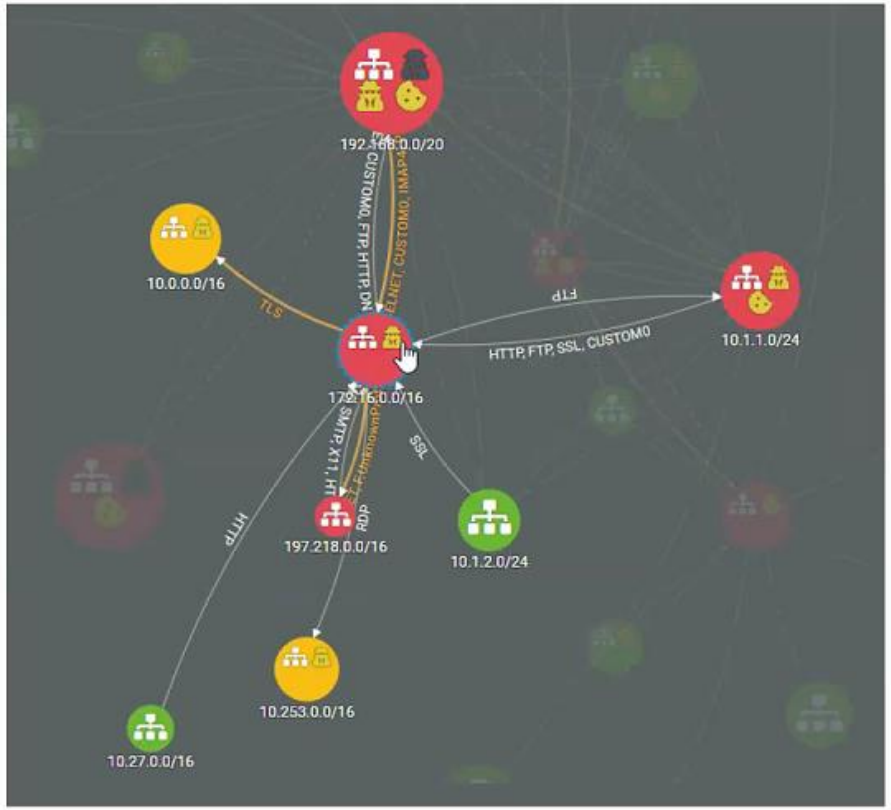
Změna prostředí vůči kterému útočník působí.
Využití technologie Fidelis Deception pro rozšíření návnad v chráněném prostředí.

Proaktivní obranná strategie: odhalit, oklamat a odrazit nepřítele dříve, než způsobí škody

Fidelis Deception

Komponenty systému inteligentních pastí

- **Decoys** – návnady, které se chovají jako reálná IT/OT/IoT aktiva
- **Credentials** – falešní uživatelské a servisní účty
- **Breadcrumbs** – Stopy poukazující na existenci návnad v síti
- **Network deception** – Broadcast, multicast, ARP poisoning
- **Data deception** - RealOS, struktury souborových složek, webové stránky, certifikáty
- **AD Deception** – falešné uživatelské účty, servisní účty, účty počítačů návnad a zajištění interakce mezi návnadami a MS AD



FIDELIS DECEPTION

KLÍČOVÉ PŘÍNOSY

- Umožňuje rychlé nasazení stovek návnad do prostředí
- Návnady jsou emulované procesy, které útočník nemůže využít k vlastnímu prospěchu při realizaci útoku
- Účinně ochraňuje taková prostředí, kde není možné nasadit EDR agenty – IoT/OT prostředí, Shadow IT a zastaralé systémy
- Provádí průběžné automatické profilování chráněného prostředí a navrhuje odpovídající druhy návnad k nasazení
- Detekuje laterální pohyb útočníka a jeho útočné techniky aplikované vůči návnadám rozmístěným v síti
- V případě, že se útočník pokouší nahrát vlastní soubory do návnad, tak ty jsou prověřeny v SANDBOX nástroji

Fidelis Deception

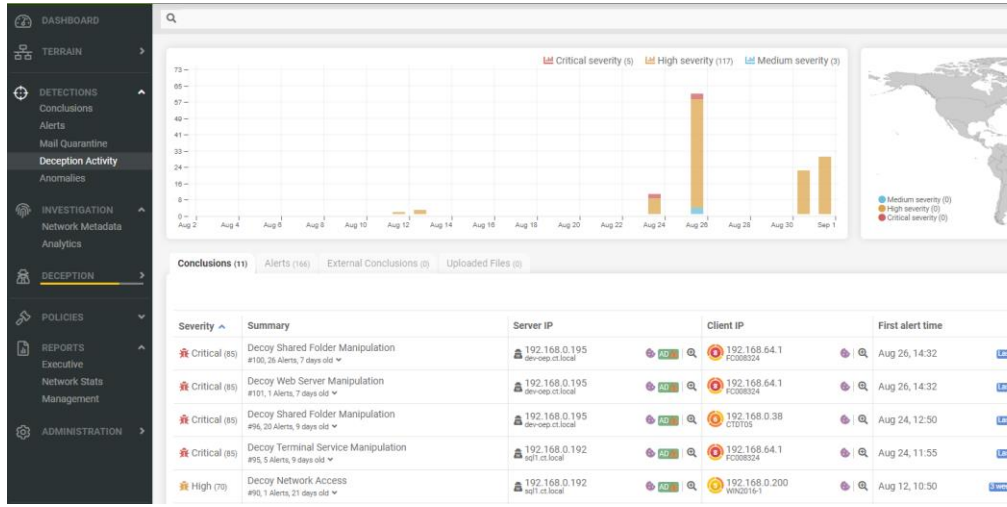
Každá návnada se chová tak, jako by měla

- Vlastní operační systém, souborový systém a služby
- Otevřené komunikační porty / protokoly
- Data – webové stránky, uvítací bannery síťových služeb
- MAC Addresy výrobců běžných v chráněném prostředí
- Certifikáty
- Odpovídající záznamy v MS AD
- Aktivity falešných uživatelů vůči návnadám

FIDELIS DECEPTION

KAŽDÁ NÁVNADA ROZŠIŘUJE SCHOPNOST DETEKCE A PODPORUJE VYŠETŘOVÁNÍ

- Návnada vygeneruje bezpečnostní ALERT ihned, jakmile dojde k přístupu na jakékoli její rozhraní
  - Skenery zranitelností, nebo dohledové nástroje je možné přidat do výjimek (zamezení False Possitive)
- Alerty jsou bohaté informace:
  - Parametry návnady
  - Přistupující aktivum a použité přístupové údaje
  - Údaje o službě, která byla využita k přístupu do návnady
  - Soubory nahrávané na návnadu včetně výsledků SANDBOX analýzy
    - Soubory jsou přístupné pro pozdější analýzu
  - Příkazy vykonávané útočníkem v prostředí návnady

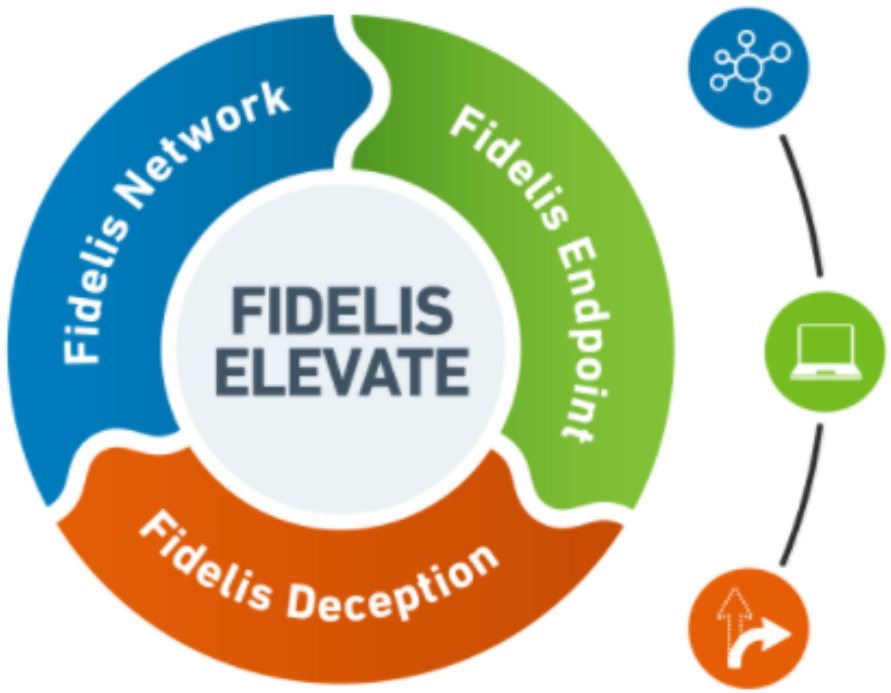


- Alerty jsou spojovány do tzv. CONCLUSIONS v kontextu ostatních detekovaných událostí nástroji NDR a EDR
- Všechny informace potřebné k vyšetřování kybernetických útoků má analytik dostupné v jednom rozhraní

AUTOMATED DETECTION AND RESPONSE

Představení platformy Fidelis Elevate

The Fidelis Elevate™ Platform Automates Detection & Response to Improve SOC Efficiency and Effectiveness



Fidelis Network®

Gain Deep Visibility into Sessions, Packets and Content and Automate Breach Detection for Faster Response

Fidelis Endpoint®

Increase Visibility and Reduce Response Time with Endpoint Detection and Response

Fidelis Deception™

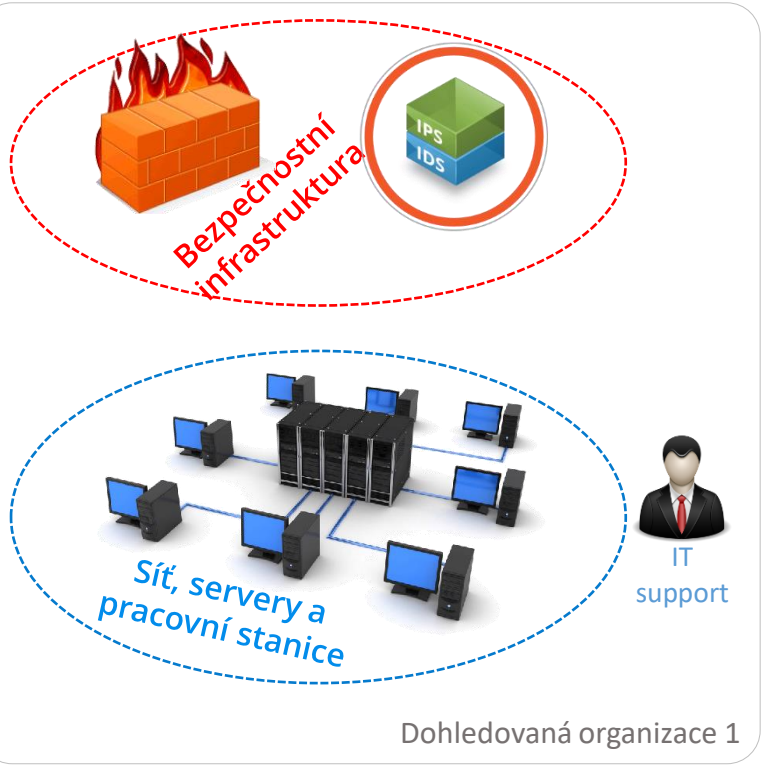
Detect and Defend Against Threats in Your Network and Cloud with Active Decoys

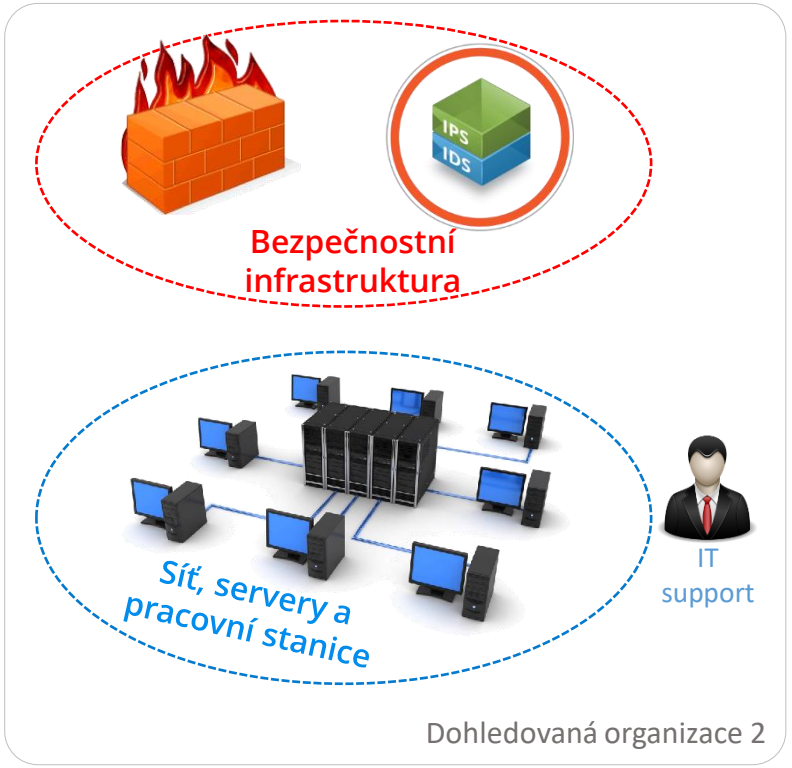
Security Operations Center

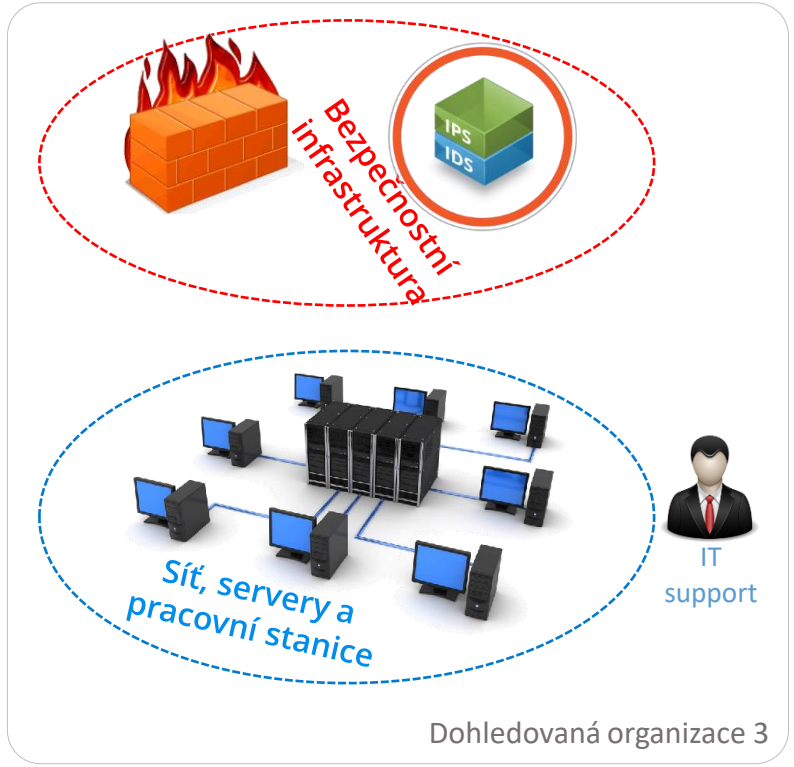
SOC Driven přístup

ARCHITEKTURA SOC V HIERARCHICKÉM PROSTŘEDÍ

STÁVAJÍCÍ PROSTŘEDÍ

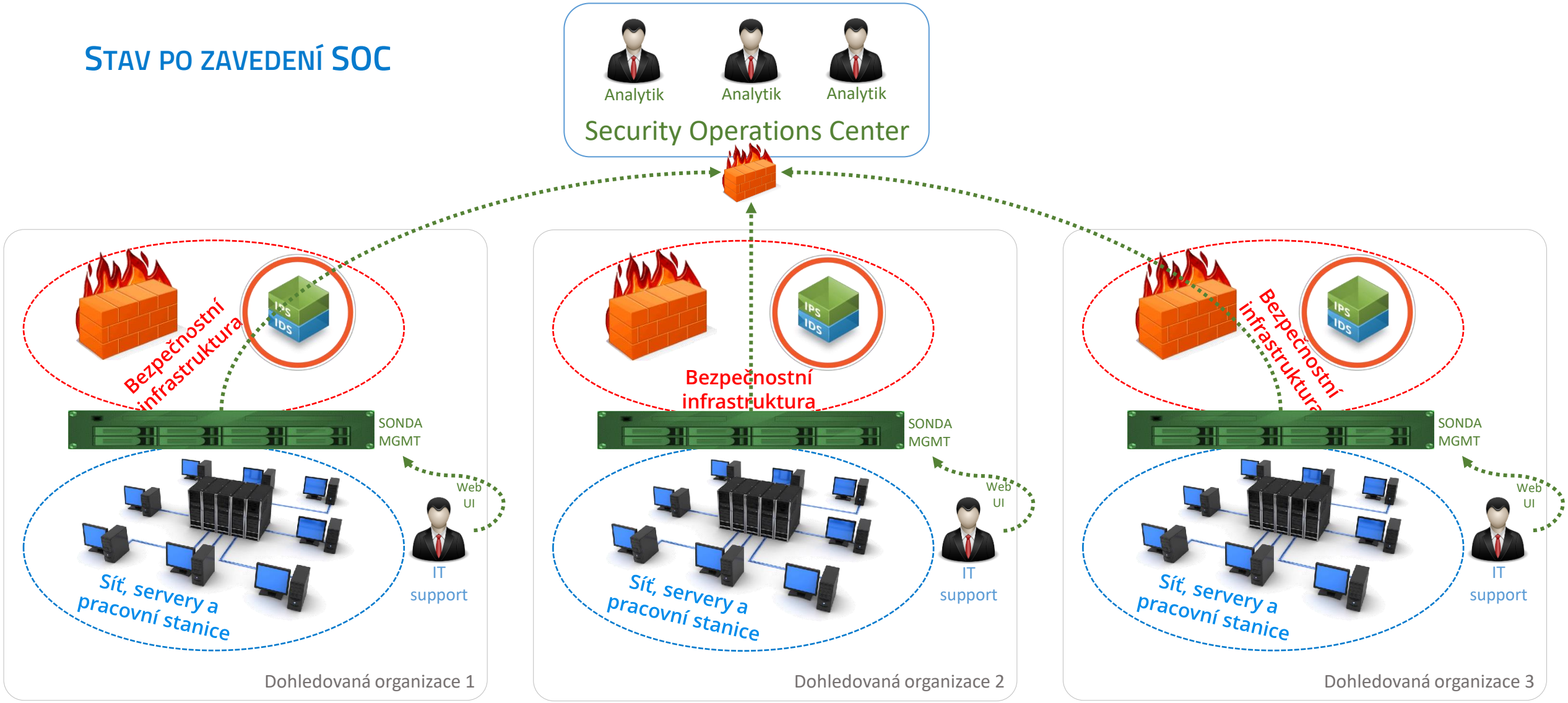






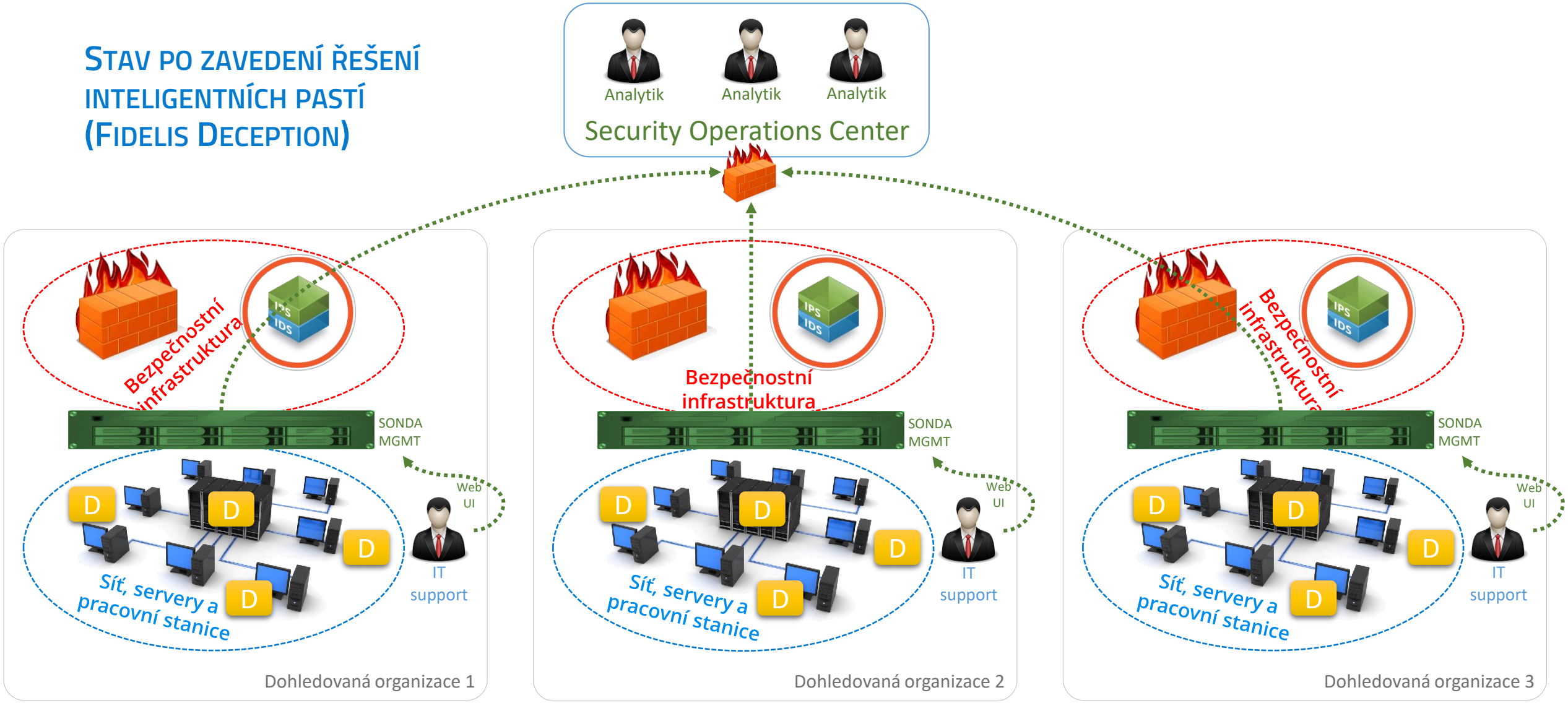
ARCHITEKTURA SOC V HIERARCHICKÉM PROSTŘEDÍ

STAV PO ZAVEDENÍ SOC

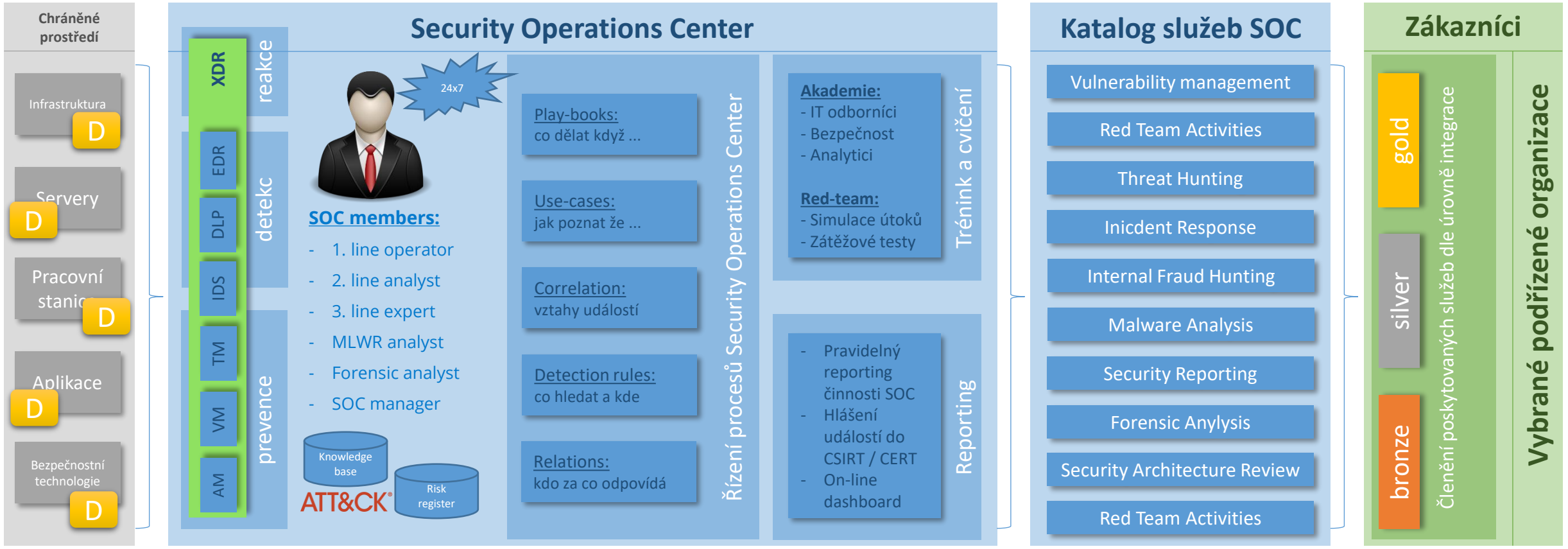


ARCHITEKTURA SOC V HIERARCHICKÉM PROSTŘEDÍ

STAV PO ZAVEDENÍ ŘEŠENÍ INTELIGENTNÍCH PASTÍ (FIDELIS DECEPTION)



Security Operations Center



IT Risk management - legislativa - regulace – nařízení - povinnosti

SOC Driven kybernetická bezpečnost

Na jakých principech je SOC driven přístup postaven

- Přesná definice chráněného prostředí
- Klasifikace cílů (*každý cíl chráním s jinou intenzitou*)
- Modelování hrozeb (*na každé prostředí působí různé hrozby*)
- Definování obranných scénářů
  - Určím co chci detekovat (*SOC use-cases*)
  - Co potřebuji abych mohl vyšetřovat
  - Jak budu na ohrožení reagovat (*SOC playbooks*)
- Určení požadavků na jednotnou bezpečnostní platformu pro detekci, vyšetřování a nápravu pro prostředí IT/OT

SOC Driven kybernetická bezpečnost

Naše nabídka

- Roadmapa náběhu služeb SOC pro jednotlivé subjekty
- Rychlé zastřežení (síť a koncové body v IT a OT), základní vizibilita prostředí (klíčová aktiva), generické hrozby
- Dopracování scénářů specifických hrozeb pro organizaci
- Zapojení SIEM pro tvorbu pokročilých scénářů (např. aplikačních)
- Precizování procesu Incident Management

Organizace je po celou dobu chráněna před vlivem generických kybernetických hrozeb.

Prezentací provázel

Pavel Klimeš

- Ředitel rozvoje bezpečnostních produktů v Corpus Solutions a.s.
- Vedoucí týmu „Offensive Security“
- Praktické zkušenosti s detekcí a zvládáním kybernetických útoků
- Autor tréninkového konceptu „Cyber Defense Academy“
- Lektor kybernetické bezpečnosti pro IT a OT pracovníky
- 22 let praxe v oboru kybernetická bezpečnost

pavel.klimes@corpus.cz