FIDELIS CYBERSECURITY

TECHNOLOGICKÁ PLATFORMA PRO ÚČINNÝ BEZPEČNOSTNÍ DOHLED NEMOCNIC

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

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

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

NÁŠ CÍL

Podpora nemocnic v zavádění centralizovaného modelu poskytování služeb Security Operations Center

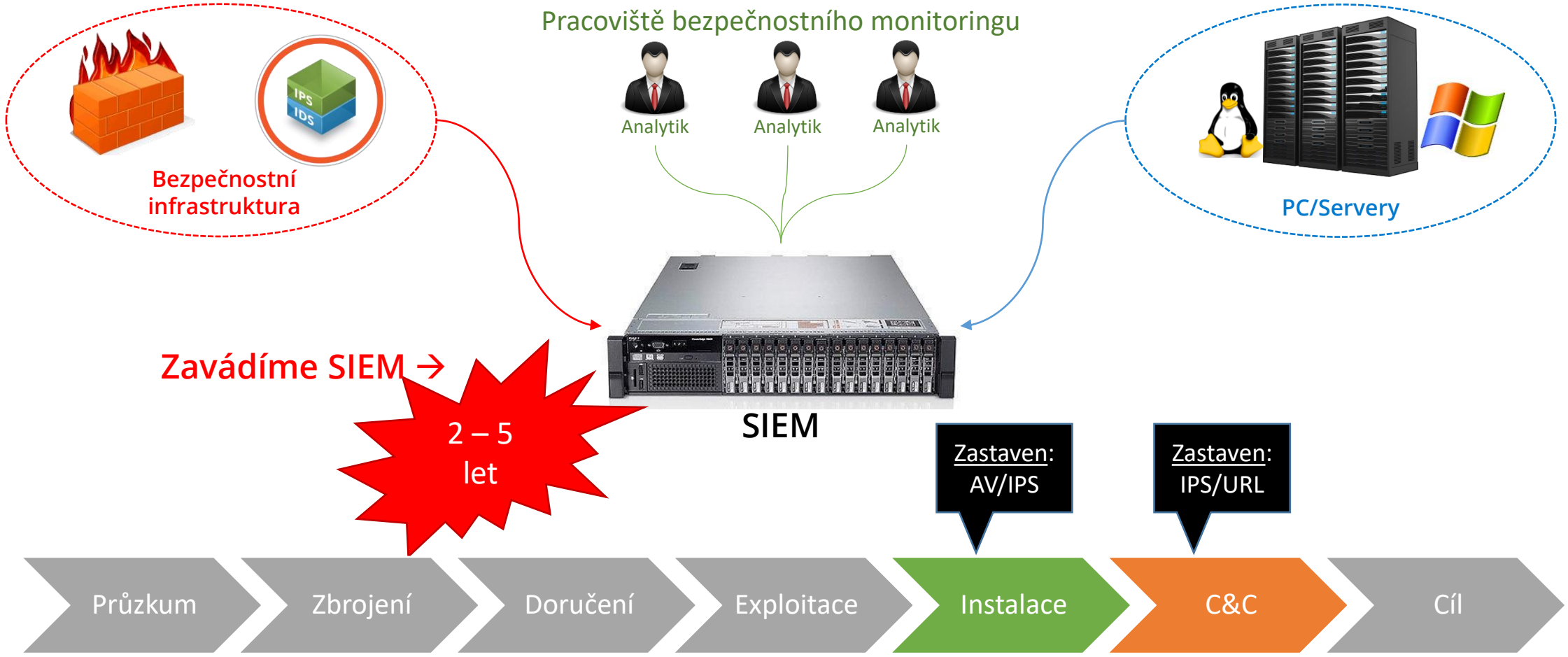
např. hSOC a jiné centralizované služby.

JAKÝM VÝZVÁM ČELÍME PŘI STŘEŽENÍ NEMOCNIC?

JAKÝM VÝZVÁM ČELÍME?

- Každá nemocnice má různou úroveň kvality kybernetické obrany (prevence – detekce – analýza – reakce)
  - Opatření jsou zaváděna bez ohledu na reálné potřeby AR/BIA
  - Opatření nasazována pod taktovkou výrobců
- Chybí schopnost rozpoznat moderní kybernetické útoky a jejich projevy pokud již jsou přítomny v infrastruktuře
- Je obrovský nedostatek kvalifikovaných odborníků na kybernetickou bezpečnost
- Specialisté IT provozu nemají dostatek volných kapacit na řešení a podporu procesů kybernetické bezpečnosti

TRADIČNÍ KYBERNETICKÁ BEZPEČNOST



KYBERNETICKÁ BEZPEČNOST

SOC Driven s využitím ADR

SOC Driven – kybernetická bezpečnost

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.

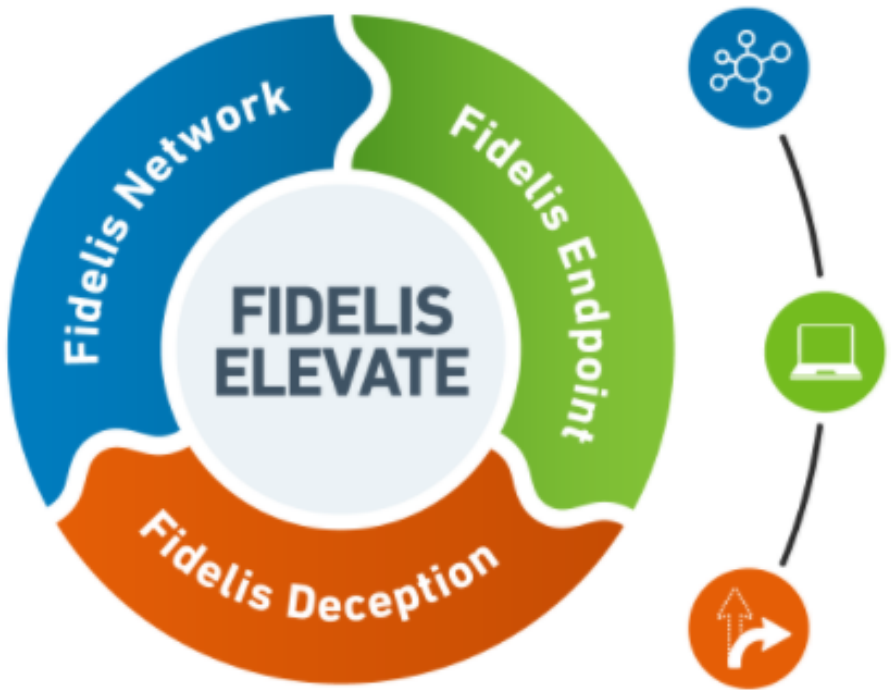
Umožňuje vyšetřovat celý průběh bezpečnostního incidentu, nikoli jen projevy jeho poslední fáze.

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®

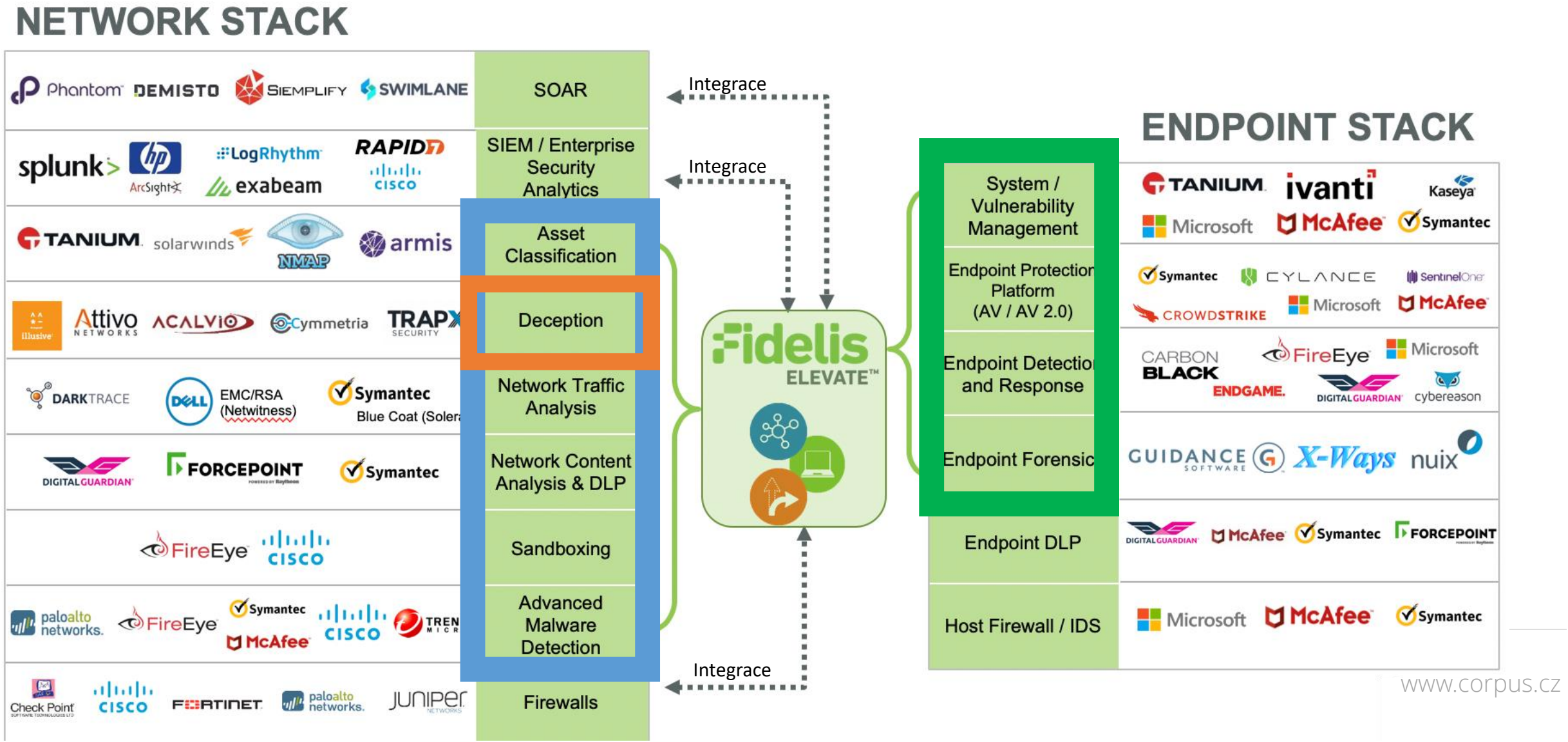
Increase Visibility and Reduce Response Time with Endpoint Detection and Response

Fidelis Deception™

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

AUTOMATED DETECTION AND RESPONSE

Představení platformy Fidelis Elevate



SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST

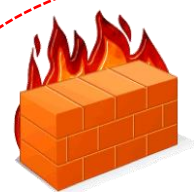
Automated Detection and Response

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

Reakční *playbooks* pro rychlé zvládání útoků

2 – 20 týdnů

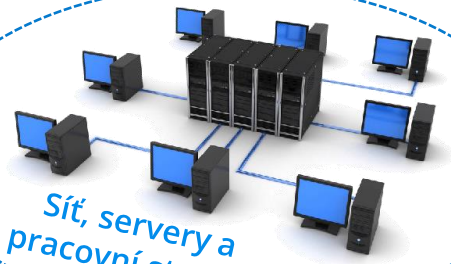
ADR – network & endpoint



Bezpečnostní infrastruktura

LM / SIEM

role konsolidace logů pro scénáře compliance a aplikační bezpečnost

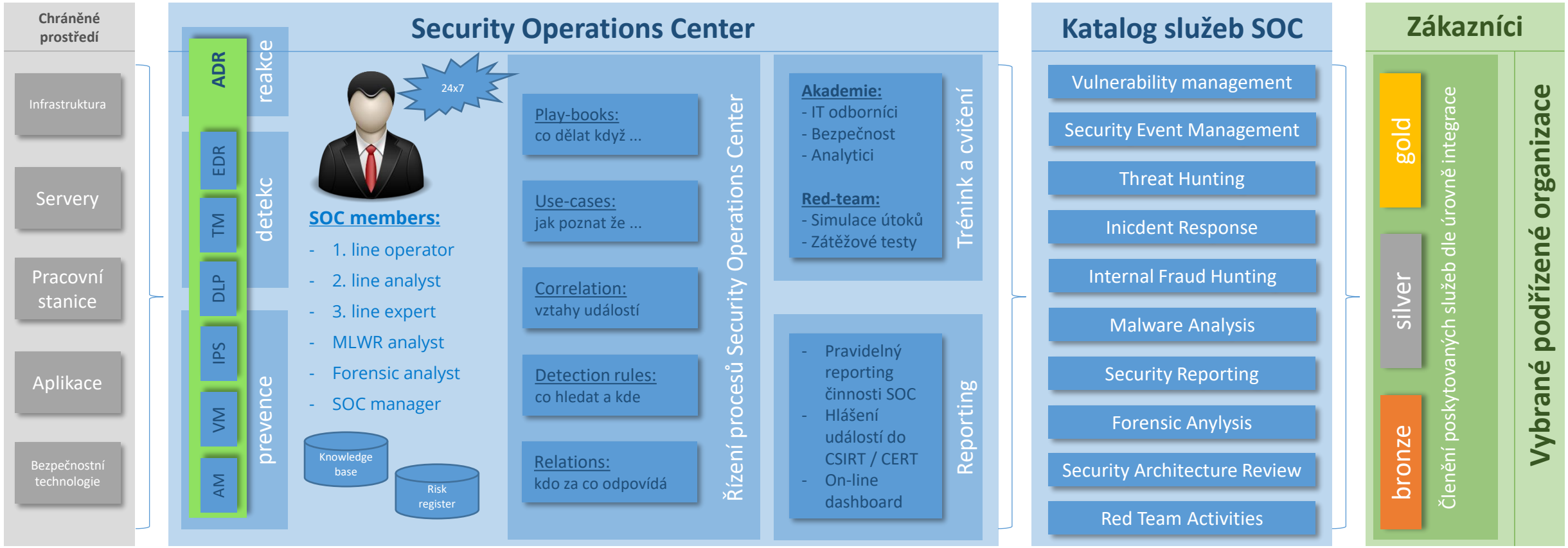


Síť, servery a pracovní stanice

Aplikace

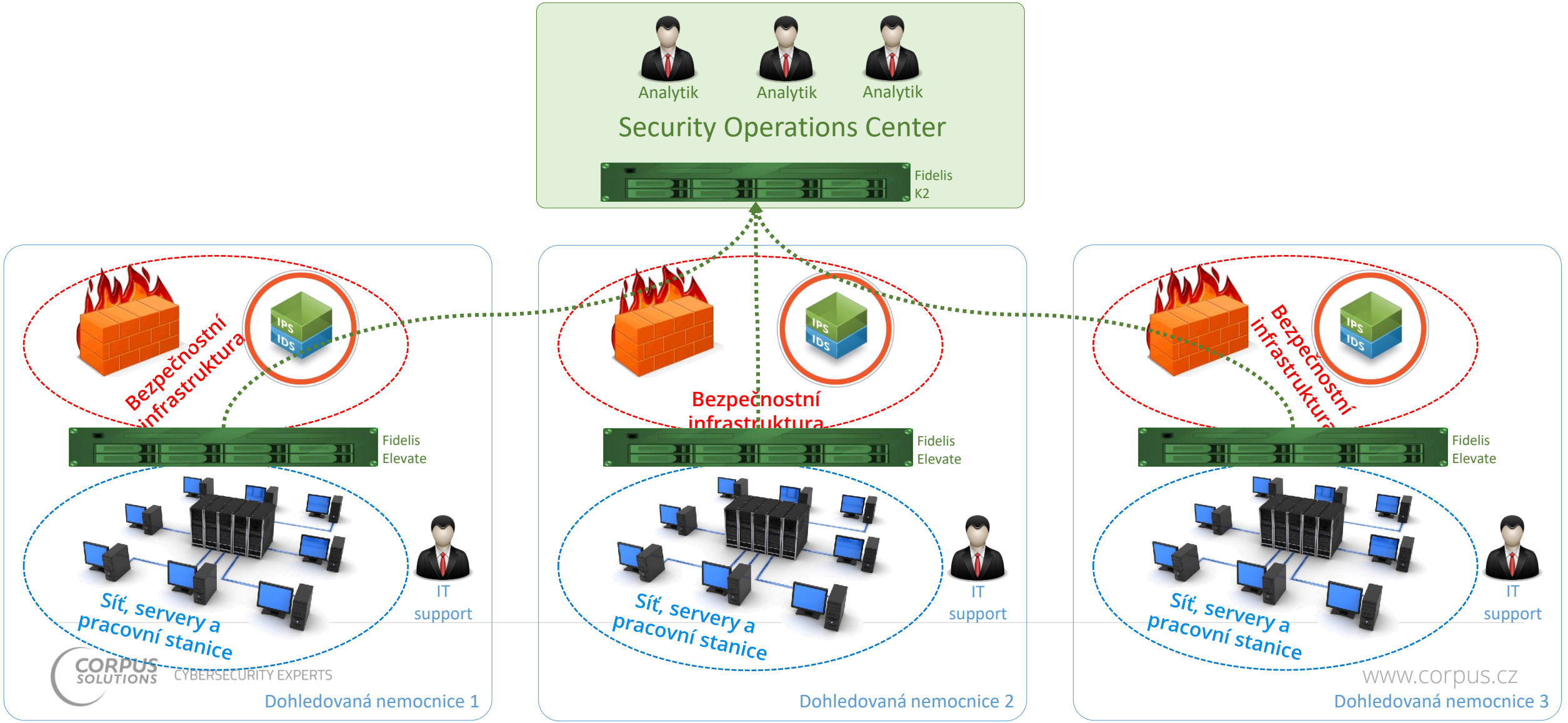
Průzkum → Zbrojení → Doručení → Exploitace → Instalace → C&C → Cíl

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST



IT Risk management - legislativa - regulace – nařízení - povinnosti

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST



Automated Detection and Response – PoC

4 týdny

Připojení ADR nástroje do prostředí organizace

- Do sítě
  - Pomoci určit vhodná přípojná místa
  - Zajistit SPAN/mirror rozhraní
  - Zajistit prostor pro umístění technologie (rack space, napájení, IP adresaci, konektivitu)
- Na koncové body
  - Distribuci agentského SW na vybrané endpointy
- Umožnit vzdálené připojení z prostředí SOC pro správu nástroje ADR
- Poskytnout informace o infrastruktuře za účelem správného určení chráněného prostředí
- Asistovat týmu SOC při průběžném vyšetřování detekovaných událostí – *pokud je součástí projektu*

PŘEDNÁŠEJÍCÍ

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