

PRAKTICKÉ ZKUŠENOSTI S PROVEDENÍM BEZPEČNOSTNÍHO AUDITU V NEMOCNICÍCH



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



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

AGENDA

- Něco málo o Corpus Solutions a.s.
- Trendy a výzvy pro kybernetickou bezpečnost
- Zkušenosti z projektů Security Assessment
- Řešení pro ochranu organizací nemusí být tak složité



CORPUS SOLUTIONS A. S.

- › Konzultační a technologická společnost
- › Obor aplikovaná kybernetická bezpečnost
- › Založena 1992
- › Česká společnost
- › Čeští akcionáři
- › Dvě pobočky Praha - Olomouc
- › Cca 60 zaměstnanců
- › Určení jako provozovatel KII



Corpus = Cybersecurity Experts

CORPUS SOLUTIONS A. S.

Pavel Klimeš

- Ředitel rozvoje bezpečnostních produktů v Corpus Solutions a.s.
- Nastavuje strategie efektivní kybernetické obrany u zákazníků
- Praktické zkušenosti s detekcí a zvládáním kybernetických útoků
- Autor tréninkového konceptu Cyber Defense Exercise
- 21 let praxe v oboru kybernetická bezpečnost



pavel.klimes@corpus.cz

TRENDY A VÝZVY V KYBERNETICKÉ BEZPEČNOSTI

JAKÉ JSOU TRENDY V KYBERNETICKÉ BEZPEČNOSTI

VÝVOJ V POPULARITĚ TÉMAT KYBERNETICKÉ BEZPEČNOSTI

- Covid-19 a urychlená digitální transformace
 - Vzdálené přístupy, BYOD, Cloud služby
 - **Nárůst aktivit útočníků:** Phishing/Malware, Ransom, Fraud
 - Nespokojenost ve společnosti => hacktivismus
- Přejít od preventivní bezpečnosti k proaktivní
 - Definice chráněného prostředí
 - Vizibilita chování klíčových aktiv
 - Proaktivní monitoring (garantované scénáře pro detekci)
 - Hunting (chytáme insidery)
 - Retrospektivní analýza
 - Definice a řízení procesu zvládání kyberútoků



JAKÝM VÝZVÁM ČELÍME

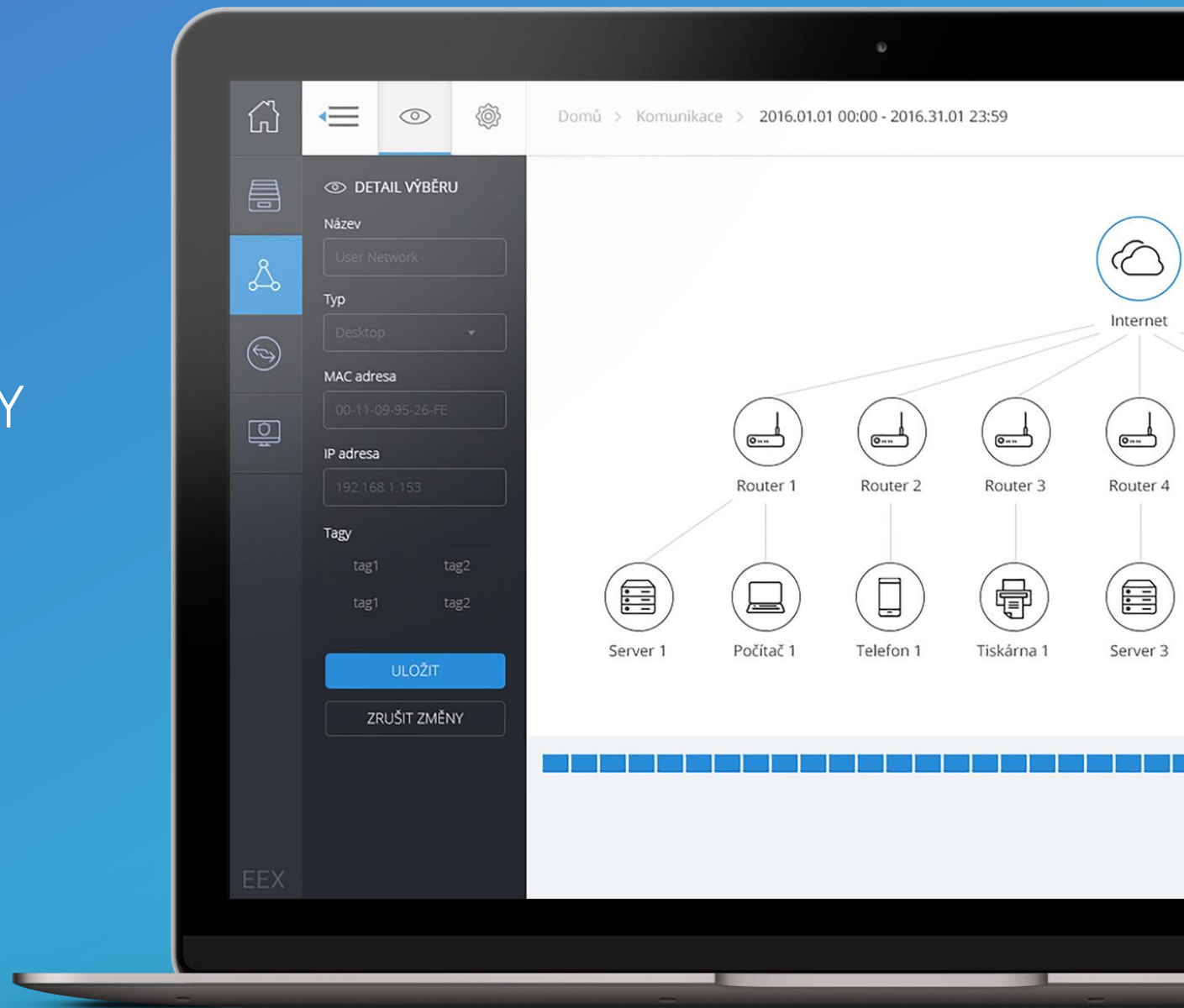
OBECNÉ VÝZVY

- Každá organizace má různou úroveň kvality kybernetické obrany (prevence – detekce – analýza – reakce)
- Chybí schopnost rozpoznat moderní kybernetické útoky a jejich projevy pokud již jsou přítomny v infrastruktuře
- Je obrovský nedostatek kvalifikovaných odborníků na kybernetickou bezpečnost
- Specialisté podporující IT provoz nemají dostatek volných kapacit na řešení a podporu procesů kybernetické bezpečnosti



Jaká je tedy reálná úroveň zabezpečení v organizacích?

ZKUŠENOSTI Z PROJEKTŮ SECURITY ASSESSMENT



PROČ ZROVNA SECURITY ASSESSMENT?

V RÁMCI PROJEKTU „SA“ PŘINÁŠÍME

- Posouzení účinnosti současné bezpečnostní ochrany organizace
- Rychlé zmapování chráněného prostředí
 - Aktiva, služby, komunikační matice, zranitelnosti, identifikaci slabých míst v infrastruktuře
- Účinnou detekci projevů tradičních i moderních hrozeb
- Vyšetření detekovaných událostí a řízení nápravných činností
- Tvorba registru rizik a návrh efektivních opatření

V průběhu projektu je zákazník vybaven technologiemi s předdefinovanými detekčními a reakčními scénáři.



**„SA“ provádíme v prostředích IT i OT.
Realizace je typicky dokončena za 45 dní.**

VÝSLEDKY „SA“ UKAZUJÍ NA STÁLE SE OPAKUJÍCÍ PROBLÉMY

TECHNICKÉ NÁLEZY SECURITY ASSESSMENTU:

- Neznámá aktiva v síti – shadow IT
- Neřízené uploady dat do internetu a napojení na známé C&C
- Četné výskyty zranitelných systémů a služeb
- Z internetu dostupná administrační rozhraní systémů
- Nízká míra segmentace vnitřních sítí ... snadný laterální pohyb
- Nedostatečná ochrana elektronické pošty
- Používání slabých a dlouho platných hesel

Zcela chybějící nebo neúčinné technické prostředky pro detekci, vyšetřování a zvládání tradičních a moderních kybernetických hrozeb (IPS, SIEM, PIM, DLP, EDR, ...) a jejich zavedení může trvat i 5let.



VÝSLEDKY „SA“ UKAZUJÍ NA STÁLE SE OPAKUJÍCÍ PROBLÉMY

PROCESNÍ A ORGANIZAČNÍ NÁLEZY SECURITY ASSESSMENTU:

- Personálně nejsou organizace připravené čelit kybernetickému ohrožení
 - Nedostatek kapacit
 - Chybí specializace na kybernetickou bezpečnost
- Omezený přístup k know-how
 - Organizace nemají zkušenosti s identifikací, vyšetřováním a se zvládáním kybernetických útoků
 - Neexistují zavedené postupy pro krizové situace
- Chybí bezpečnostní požadavky na dodavatele
 - Hardening, bezpečný vývoj, využívání standardů
 - Řízení kyberbezpečnosti v celém životním cyklu dodaného díla



VÝSLEDKY „SA“ UKAZUJÍ NA STÁLE SE OPAKUJÍCÍ PROBLÉMY

REKAPITULACE - AŽ Z TOHO MRAZÍ V ZÁDECH

- Téměř každý projekt Security Assessment zachytí probíhající kybernetický útok.
 - Často jsou nalezeny post-infikační artefakty.
 - Zákazník nemá o zaznamenaných nebezpečných jevech ponětí.
 - Důvěra v tradiční bezpečnostní perimetr je nabourána.
-
- Naše detekční nástroje jsou provozovány v síti zcela pasivně.
 - Při použití SW agentů na koncové stanice a servery jsme kompatibilní a nekolizní se současnými nástroji.



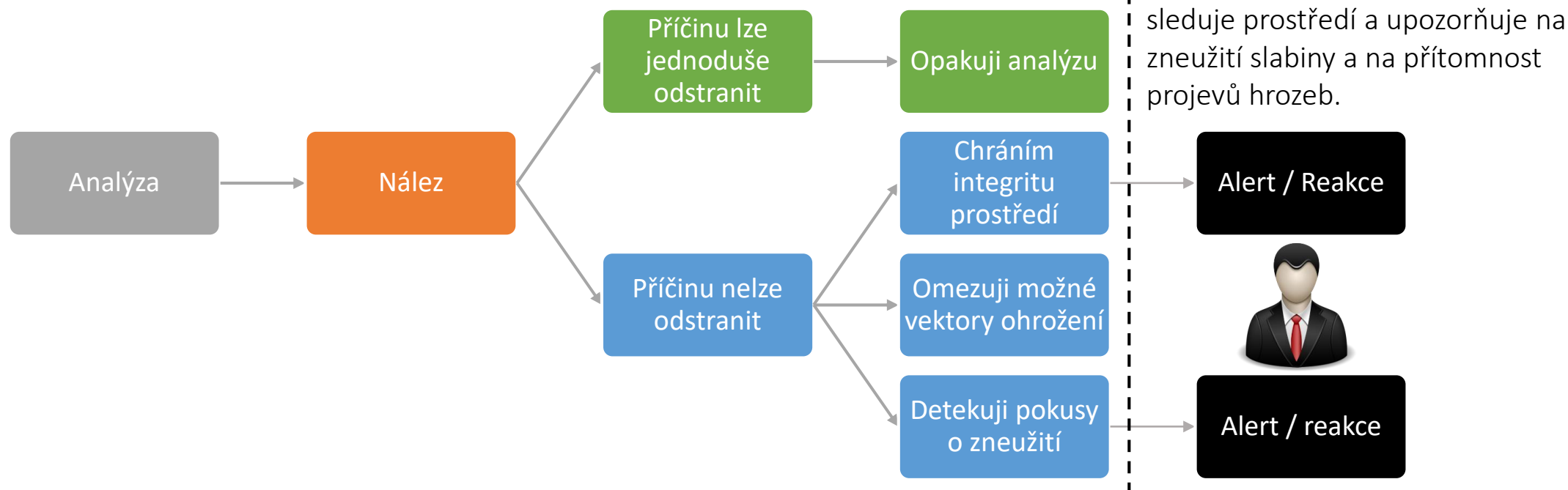
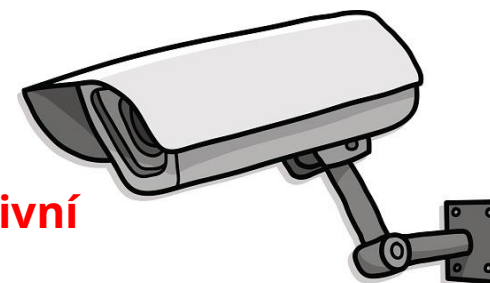
ŘEŠENÍ PRO OCHRANU
ORGANIZACÍ NEMUSÍ BÝT SLOŽITÉ

SOC Driven - kybernetická bezpečnost

ZPRACOVÁNÍ NÁPRAVNÝCH OPATŘENÍ

STRATEGIE VYPOŘÁDÁNÍ IDENTIFIKOVANÝCH NÁLEZŮ

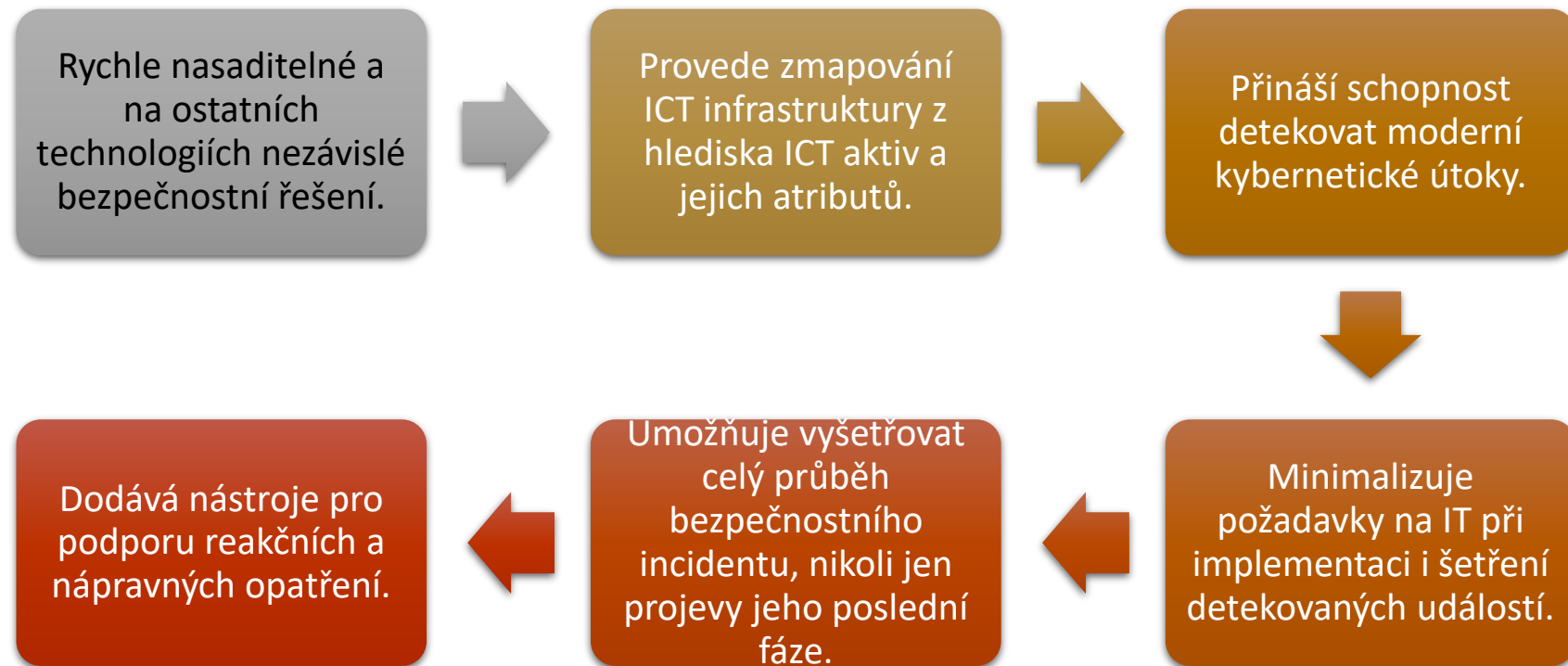
- > U některých nálezů **je odstranění příčin nákladné, špatně vynutitelné, časově neefektivní**
- > Proto doporučujeme zavedení proaktivního dohledu s **využitím účinných nástrojů**
 - > Typicky zajišťuje Security Operations Center (SOC)
 - > Reakce koordinována s provozním týmem zákazníka



SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST

Systémy automatické detekce a reakce

ZVÝŠENÍ SCHOPNOSTI DETEKCE A VYŠŠÍ EFEKTIVITA SOC



Pouze detekovat nestačí. Pro rychlé vypořádání incidentu jsou nezbytné nástroje pro podporu rychlé reakce.

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST

Systémy automatické detekce a reakce

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

Reakční *playbooks* pro
rychlé zvládnutí útoků

2 – 20
týdnů

ADR – network & endpoint

Bezpečnostní
infrastruktura

Sít', servery a
pracovní stanice

Aplikace

LM / SIEM

role konsolidace logů pro scénáře
compliance a **aplikační bezpečnost**

Průzkum

Zbrojení

Doručení

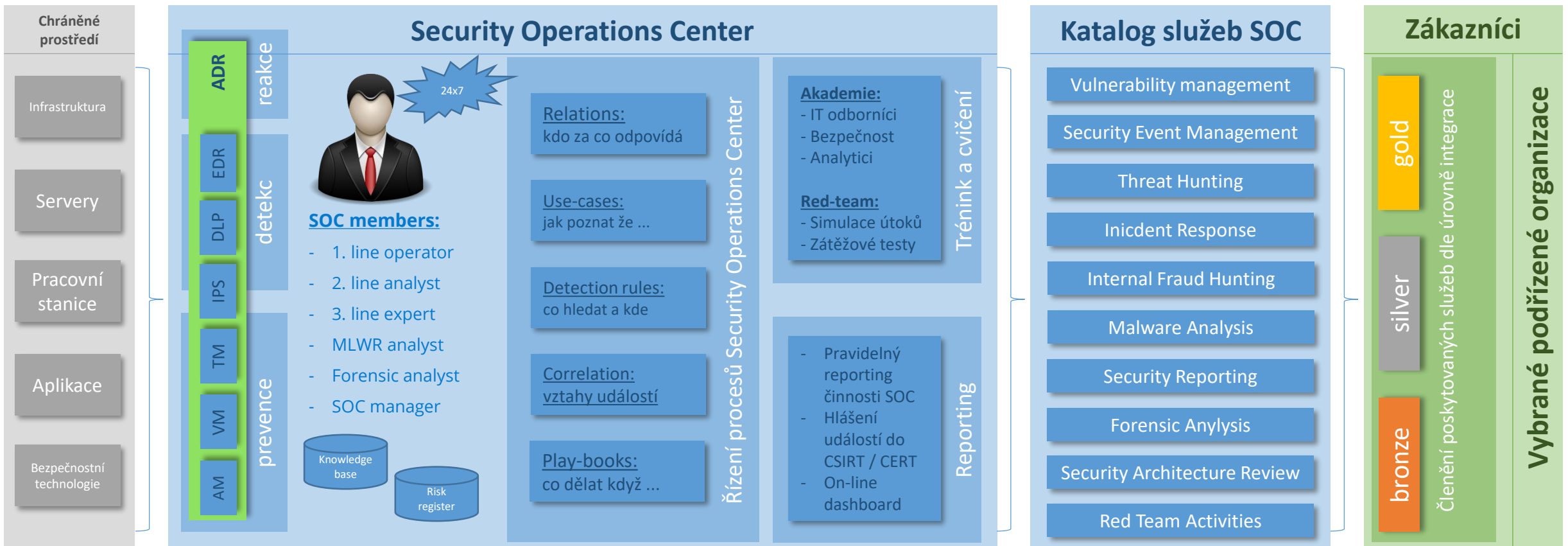
Exploitace

Instalace

C&C

Cíl

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST



IT Risk management - legislativa - regulace – nařízení - povinnosti

SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST

Budme si jisti, že dosavadní alibistický „compliance“ přístup některých organizací k bezpečnosti nevede.

Je tu čas na změnu:

- Ochranu můžete svěřit odborníkům
- Rychlé zavedení proaktivní obrany
- Účinnost již za 2 - 20 týdnů
- Instantní čerpání unikátního know-how
- Postupná edukace organizací a rychlé zvýšení jejich odolnosti

The Hacker News



A Patient Dies After Ransomware Attack Paralyzes German Hospital Systems

September 21, 2020 Ravie Lakshmanan

German authorities last week disclosed that a ransomware attack on the University Hospital of Düsseldorf (UKD)...