# Cyber Defense Center

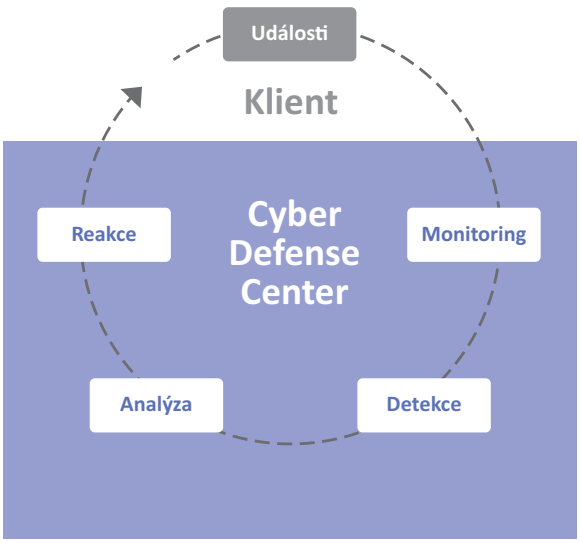

AEC

Zajištění důvěrnosti, integrity a dostupnosti dat v moderním podnikání zahrnuje mnoho úkolů, od řízení systémů, změnového a konfiguračního managementu až po kybernetickou bezpečnostní strategii. Účinná strategie musí zahrnovat, mimo jiné, i detekci a reakci na bezpečností incidenty, bez které se neobejde žádná společnost zpracovávající citlivá data. Úroveň detekčních a reakčních schopností přímo souvisí se znalostmi, zkušenostmi a kvalitou bezpečnostních nástrojů a právě tyto ingredience v našem Cyber Defense Centru máme a jsme připraveni vám je poskytnout.

## Náš tým

Chod CDC zajišťuje tým zkušených analytiků a SIEM administrátorů s **praxí z globálních SOC**, zkušenostmi s nasazením špičkových technologií a **řešením rozsáhlých incidentů i APT útoků** na lokální i globální úrovni.

## CDC proces




**www.aec.cz**

# Cyber Defense Center

## Služby CDC

- **Log Management** – sběr, normalizace a uchovávání logů (retence volitelná).
- **Security Monitoring** – nasazení a rozvoj detekčních pravidel, analýza bezpečnostních událostí a incidentů.
- **Incident Response** – doporučení postupu pro řešení bezpečnostních incidentů a pomoc při řešení.
- **Threat Hunting** – aktivní vyhledávání nových hrozeb a podezřelých anomálií nad shromážděnými událostmi z klientských prostředí.
- **Threat Intelligence** – detekčních pravidla jsou obohacována o IOC z externích informačních zdrojů/feeds.
- **Pokročilá detekce a ochrana aktiv** – agentní řešení s unikátními prevenčními a zejména detekčními schopnostmi s reakčními funkcemi, které umožňují incidenty vzdáleně na koncovém zařízení i řešit.
- **Cyber Brand Protection** – monitoring externích informačních zdrojů s cílem podchycovat úniky definovaných citlivých informací z prostředí klientů (přihlašovací údaje, interní dokumenty apod.).
- **Malware a Forenzní Analýza** – rozbor a analýza chování a možných dopadů škodlivého kódu, forenzní sběr a analýza dat s postupy a výstupy akceptovatelnými v soudních řízeních.
- **Professional Services** – analýza dopadů, návrh a podpora při implementaci nápravných opatření po rozsáhlých kybernetických incidentech či APT útocích (analýza dopadů podmíněná instalaci agentů na koncová zařízení).

## Formy poskytování služby

- **Kompletní outsourcing** – získáváte kompletní servis, v němž jsou zahrnuty krom služeb CDC i ceny potřebných licencí a HW. CDC SIEM je provozován v tzv. multi-tenantním prostředí, kdy jsou události od jednotlivých klientů striktně odděleny. Pokud trváte na ukládání logů v rámci své vlastní infrastruktury, lze úložiště provozovat na vaší, zákaznické straně.
- **Hybridní model** – vy vlastníte licence pro SIEM a hardware, my dodáme služby.

## Přínosy našeho řešení

### Cyber Defense Center poskytuje vyšší ochranu s menšími starostmi a nižšími náklady

- **Významná redukce rizik** – Nadstandardní úroveň ochrany klienta díky kontinuálnímu monitoringu a neustálému rozvoji detekčních pravidel. CDC tým s rozsáhlými zkušenostmi řeší detekované události samostatně a efektivně.
- **Nižší náklady** – CDC služba představuje pro klienta při vysoké kvalitě nižší náklady než interní provoz. Odpadají starosti s hledáním, zapracováním a retencí expertních zaměstnanců.
- **Špičkové technologie** – využívané nástroje se řadí mezi TOP produkty na trhu (SIEM, EDR, Threat Inteligence). Sledujme kontinuálně vývoj produktů a nabízíme důkladně otestované a prověřené funkcionality.
- **Špičkové technologie** – používané nástroje se řadí mezi TOP produkty na trhu (SIEM, EDR, Threat Intelligence). Kontinuálně sledujeme vývoj produktů, dodáváme důkladně otestované a prověřené funkcionality.

### Využíváme dlouholeté zkušenosti a spolupracujeme napříč všemi divizemi AEC

- **Security Assessment Division** – využíváme zkušeností našich pentesterů z reálných prostředí a přizpůsobujeme tomu skladbu korelačních pravidel a pravidelně testujeme naše detekční schopnosti včetně práce našich analytiků.
- **Risk & Compliance Division** – spolupracujeme s procesními specialisty při tvorbě a dokumentaci procesů mezi zákazníky a CDC.
- **Security Technologies Division** – naši kolegové nám pomáhají s odstraňováním problémů detekovaných na bezpečnostních řešeních u zákazníka (konfigurace FW, IDS/IPS, DLP apod.).

## Chcete si být jisti svou volbou? Vyzkoušejte si nás!

- **Nabízíme CDC službu na zkoušku.**
- **Na vašem zvoleném aktivu předvedeme naše špičkové detekční i reakční schopnosti. Odhalíme např.:**
  - infikované servery a stanice ve vaší síti,
  - závadnou komunikaci z vašich koncových zařízení do internetu na Command and Control servery (Botnet apod.),
  - spojení na Bitcoin minery z vaší sítě,
  - zneužití privilegovaných účtů.
- **Ukážeme vám reálná rizika, kterým čelíte a navrhneme jak je redukovat.**

## Maturity assessment

- **Provedeme rychlý maturity assessment vašeho SIEM/SOC.**
- **Posoudíme úroveň vašich detekčních i reakčních schopností.**

AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283