AEC

CYBER DEFENSE CENTER
Powered by AEC

Cyber Defense Center

Kybernetická bezpečnost bez růžových brýlí

Institucionální pohled

NSCI: Czech Republic in **??Top ten??** countries best prepared against cyber attacks

Proč jsme tam, kde jsme?

Špatný management –– nemáme vhodné lidi –– neumíme vybrat vhodné nástroje ani využít jejich potenciál – méně detekujeme – nevíme co se děje

Vše začíná u lidí

Interně

- Rozvoj a vzdělávání
- Expertní leader
- Mzdy

Hledáme na trhu

- Dostupnost expertů
- Cena
- Udržitelnost
- Řízení potřeb týmu

ZÁŽITEK

Hledání SOC L3 EXPERTA v EU

1000 oslovených

70 pohovorovaných

4 nabídky

0 přijatých

AEC

CYBER DEFENSE CENTER

Tým zkušených expertů

CDC tým má bohatou praxi z globálních SOC, zkušenostmi s nasazením špičkových technologií napříč kontinenty a řešením rozsáhlých incidentů i APT útoků na lokální i globální úrovni.

AEC

CYBER DEFENSE CENTER

CDC Služby

Klient

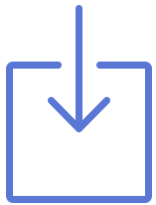
Cyber Defense Center

- SIEM & Log Management
- Security monitoring
- Incident Response
- Threat Hunting
- Threat Intelligence
- Cyber Brand Protection
- Advanced Asset Protection
- Malware & Forensics Analysis
- Professional Services

Formy nasazení CDC

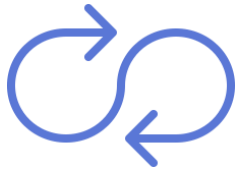
Kompletní outsourcing

- 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,
- Legislativa GDPR nezakazuje outsourcing SOC služeb.



Hybridní model

- Služby CDC jsou poskytovány při využití vašeho SIEM řešení, vy vlastníte SIEM licence a je provozován na vašich HW prostředcích. Možná je i varianta přeposílání relevantních eventů z vašeho SIEM řešení do CDC SIEM. Všechny následné operace jsou prováděny v prostředí CDC.
- Pokud trváte na sběru a ukládání logů v rámci své vlastní infrastruktury, lze log processor instalovat na vaší straně a přihlašovat se vzdáleně prostřednictvím centrální konzole,



AEC

CYBER DEFENSE CENTER

Chcete si být jisti svou volbou? Vyzkoušejte si nás!

Stojíme za kvalitou našich služeb a jsme připraveni Vám to prokázat!

Mějte kvalifikované informace před tím, než se rozhodnete!

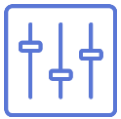
CDC na zkoušku

- Nabízíme CDC službu na zkoušku,
- Na Vašem zvoleném aktivu předvedeme naše špičkové detekční i reakční schopnosti např.:
    - Infikované servery a stanice ve vaší síti,
    - Závadná komunikace z vašich koncových zařízení do internetu,
    - Identifikace spojení na Bitcoin minery z vaší sítě.
- 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.

Klíčové benefity při využití služeb CDC



Významné snížení rizik

- Široká paleta vlastních detekčních pravidel monitoruje bezpečnost prostředí klienta
- Klient ví co se v jeho prostředí skutečně děje a naši experti mu pomáhají zvolit ideální řešení

Nižší náklady

- Kompletní služba CDC obsahuje i cenu HW a SW a stojí zákazníka výrazně méně než poskytování obdobné kvality interními zdroji
- Odpadají starosti s hledáním, zapracováním a retencí expertních zaměstnanců
- Není třeba investovat čas a prostředky do hledání a testování vhodných technologií

Špičkové zdroje

- Tým expertů s letitou globální praxí (budování SOC i následný provoz a řešení rozsáhlých incidentů)
- Využívané nástroje se řadí mezi TOP produkty na trhu (SIEM, EDR, Threat Intelligence)
- Sledujeme vývoj na trhu nástrojů a stále hledáme to nejlepší pro klienty
- Nabízíme důkladně otestované a prověřené funkcionality

Detekce

- Díky dlouholetým zkušenostem dokážeme detekovat i rozsáhlé útoky a APT
- Nadstandardní úroveň ochrany klienta díky kontinuálnímu rozvoji detekčních pravidel

Zkušenosti AEC

28

Let na trhu

80

Expertů ve 4 divizích

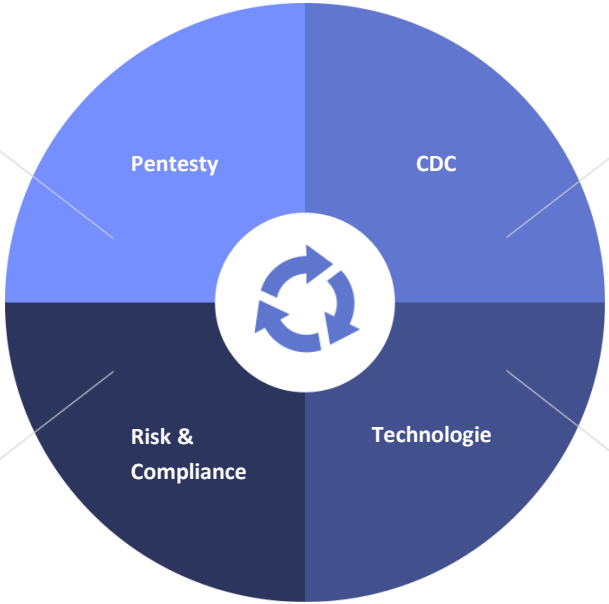
100%

Komplexní cybersecurity portfolio služeb

Úzce spolupracujeme napříč divizemi

Využíváme pentestery při konstrukci pravidel a hlídáme bdělost analytiků CDC

Rozsáhlé portfolio znalostí a služeb napříč divizemi



Využíváme analytiky R&C při designu a formalizaci procesů mezi zákazníkem a CDC

Společně navrhujeme řešení problémů detekovaných u zákazníka (konfigurace FW, IDS/IPS, DLP)

Využijte program CDC start 20

Nezapomeňte na AEC Konferenci SECURITY 2020

Zeptejte se, jsme tu pro Vás

Tomáš Filip AEC
tomas.filip@aec.cz