Cyber Defense Center

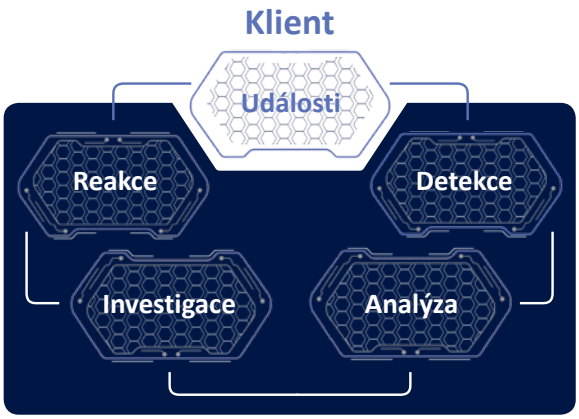
SOC as a Service

AEC

Monitorujte svou infrastrukturu a předejděte kybernetickým útokům

Cyber Defense Center (CDC) řeší kybernetické bezpečnostní události a incidenty za naše zákazníky. Toto řešení pomáhá incidentům předcházet, případně je včas detekovat, eliminovat či zmírnit jejich dopad a vést o nich evidenci. V centru jsou používány nejnovější technologie a praxí osvědčené techniky a taktiky pro bezpečnost 24/7.

Centrum stojí na pilířích detekce, analýzy, investigace, reakce a aktivit po incidentu. Kontinuálním monitoringem v reálném čase identifikujeme, případně přijmeme notifikaci o potenciálně škodlivém chování v chráněné infrastruktuře (detekce). Určíme, zda se jedná o bezpečnostní incident, který může mít negativní dopad na námi chráněnou infrastrukturu, nebo o falešný poplach a je nezbytné upravit detekční mechanismy (analýza). Zkoumáním vyhodnocených bezpečnostních incidentů zjistíme konkrétní dopady a cestu, kterou se útočníkovi podařilo proniknout do infrastruktury (investigace). Okamžitou reakci minimalizujeme dopad bezpečnostních incidentů (reakce). Po úspěšné reakci zajistíme poučení se z incidentu, kontrolu zavedení nápravných opatření a reporting pro evidenci a zvýšení informovanosti (aktivity po incidentu).



Cyber Defense Center

www.aec.cz

Cyber Defense Center – SOC as a Service

Náš tým

Chod centra zajišťuje tým zkušených a certifikovaných bezpečnostních analytiků a administrátorů s praxí z globálních Security Operations Center, kteří disponují zkušenostmi s nasazením špičkových technologií a řešením bezpečnostních událostí a incidentů na lokální i globální úrovni.

Služby CDC

- Bezpečnostní monitoring sleduje a řeší bezpečnostní události a incidenty v reálném čase. Klíčovou schopností je rozpoznání incidentů od událostí či falešných poplachů, reakce na incidenty či návrh úpravy detekčních mechanismů.
- CSIRT, který v případě incidentu je schopen zasáhnout přímo v místě jeho vzniku, případně poskytnou vzdálenou koordinaci při jeho řízení.
- Řízení zranitelností, kdy detekujeme, vyhodnocujeme, prioritizujeme a dodáváme doporučení, jak řešit zranitelnosti v zákaznícké infrastruktuře, kterým se věnovat neprodleně a které mohou počkat do dalšího patch cyklu.
- Ochrana značky, kde zkoumáme dark web a hledáme náznaky útoků na naše zákazníky.
- Forenzní analýza do hloubky bezpečnostních incidentů, které se již staly a je nezbytné k nim zajistit důkazní materiál případně je více došetřit.
- Konzultace v oblasti bezpečnosti jsou největší přidanou hodnotou AEC, kdy jsme schopni pokrýt téměř celé portfolio kybernetické bezpečnosti.
- Výstavba SOC na míru přímo v prostředí zákazníka dle jeho potřeb a požadavků.

Důvody k pořízení SOC

- Snížení reakční doby na incident (zvýšení efektivity) a tudíž zmírnění dopadu incidentu (snížení nákladů na obnovu).
- Centralizace bezpečnosti do jednoho bodu.
- Znalost bezpečnostní situace v infrastruktuře v reálném čase.
- Snížení nákladů na lidský faktor (bezpečnostní analytici jsou součástí dodávané služby).
- Minimalizace možnosti pochybení operátorů (automatizace bezpečnosti) díky předem definovaným postupům řešení incidentů.
- Pokrytí komplexního portfolia bezpečnostních hrozeb, reflexe aktuálních, ale i nově vznikajících.

Naše přednosti

- Patříme mezi zavedené české firmy, na trhu úspěšně působíme již déle než 30 let a po celou dobu působení se zaměřujeme na oblast bezpečnosti informací.
- Disponujeme týmem zkušených a certifikovaných bezpečnostních konzultantů a specialistů.
- Naši specialisté jsou schopni integrovat široké portfolio technologií do jednoho bodu a nad těmito technologiemi vytvořit a nastavit procesy a komplexní detekční a korelační pravidla k zajištění správné funkčnosti a visibility navrženého řešení.
- Námi nabízené řešení je přímo optimalizované na zákazníkovu infrastrukturu a reflektuje její podobu, aktuální bezpečnostní hrozby a trendy v oblasti kybernetické bezpečnosti.
- Naslouchame klientům a přizpůsobujeme řešení jejich potřebám, požadavkům a možnostem.
- Disponujeme referencemi od velkých zákazníků napříč sektory (banky, energetika u utility, telekomunikace, výrobní podniky, média a obchod, pojišťovny a veřejný sektor).

Využíváme dlouholeté zkušenosti a spolupracujeme napříč AEC

Security Assessment Division
využíváme zkušeností našich penetračních testerů z reálných prostředí a přizpůsobujeme tomu skladbu detekčních a korelačních pravidel. 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 a s jejich rozvojem (konfigurace NGFW, IDS/IPS, DLP, EDR a další).

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