Cyber Defense Center

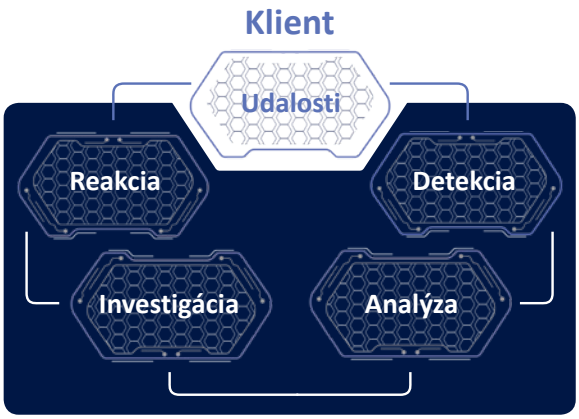
SOC as a Service

AEC

Monitorujte svoju infraštruktúru a predídete kybernetickým útokom

Cyber Defense Center (CDC) rieši kybernetické bezpečnostné udalosti a incidenty za našich zákazníkov. Toto riešenie pomáha incidentom predchádzať, prípadne ich včas detegovať, eliminovať či zmierniť ich dopad a viesť o nich evidenciu. V centre sú používané najnovšie technológie a praxou osvedčené techniky a taktiky pre bezpečnosť 24/7.

Centrum stojí na pilieroch detekcie, analýzy, investigácie, reakcie a aktivít po incidente. Kontinuálnym monitoringom v reálnom čase identifikujeme, prípadne prijmeme notifikáciu o potenciálne škodlivom správaní v chránenej infraštruktúre (detekcia). Určíme, či ide o bezpečnostný incident, ktorý môže mať negatívny dopad na nami chránenú infraštruktúru, alebo o falošný poplach, a je nevyhnutné upraviť detekčné mechanizmy (analýza). Skúmaním vyhodnotených bezpečnostných incidentov zistíme konkrétne dopady a cestu, ktorou sa útočníkovi podarilo preniknúť do infraštruktúry (investigácia). Okamžitou reakciou minimalizujeme dopad bezpečnostných incidentov (reakcia). Po úspešnej reakcii zaistíme poučenie sa z incidentu, kontrolu zavedenia nápravných opatrení a reporting pre evidenciu a zvýšenie informovanosti (aktivity po incidente).



Cyber Defense Center

www.aec.sk

Cyber Defense Center – SOC as a Service

Náš tím

Chod centra zaisťuje tím skúsených a certifikovaných bezpečnostných analytikov a administrátorov s praxou z globálnych Security Operations Centier, ktorí disponujú skúsenosťami s nasadením špičkových technológií a riešením bezpečnostných udalostí a incidentov na lokálnej aj globálnej úrovni.

Služby CDC

- Bezpečnostný monitoring sleduje a rieši bezpečnostné udalosti a incidenty v reálnom čase. Kľúčovou schopnosťou je rozpoznanie incidentov od udalostí či falošných poplachov, reakcia na incidenty či návrh úpravy detekčných mechanizmov.
- CSIRT, ktorý je v prípade incidentu schopný zasiahnuť priamo v mieste jeho vzniku, prípadne poskytnúť vzdialenú koordináciu pri jeho riadení.
- Riadenie zraniteľností, keď detegujeme, vyhodnocujeme, prioritizujeme a dodávame odporúčania, ako riešiť zraniteľnosti v zákazníkovej infraštruktúre, ktorým sa venovať neodkladne a ktoré môžu počkať do ďalšieho patch cyklu.
- Ochrana značky, kde skúmame dark web a hľadáme náznaky útokov na našich zákazníkov.
- Forenzná analýza do hĺbky bezpečnostných incidentov, ktoré sa už stali a je nevyhnutné k nim zaistiť dôkazný materiál, prípadne ich viac došetriť.
- Konzultácie v oblasti bezpečnosti sú najväčšou pridanou hodnotou AEC, keď sme schopní pokryť takmer celé portfólio kybernetickej bezpečnosti.
- Výstavba SOC na mieru priamo v prostredí zákazníka podľa jeho potrieb a požiadaviek.

Dôvody na obstaranie SOC

- Zníženie reakčného času na incident (zvýšenie efektivity) a teda zmiernenie dopadu incidentu (zníženie nákladov na obnovu).
- Centralizácia bezpečnosti do jedného bodu.
- Znalosť bezpečnostnej situácie v infraštruktúre v reálnom čase.
- Zníženie nákladov na ľudský faktor (bezpečnostní analytici sú súčasťou dodávanej služby).
- Minimalizácia možnosti pochybenia operátorov (automatizácia bezpečnosti) vďaka vopred definovaným postupom riešenia incidentov.
- Pokrytie komplexného portfólia bezpečnostných hrozieb, reflexia aktuálnych, ale aj novovznikajúcich.

Naše prednosti

- Patríme medzi zavedené české firmy, na trhu úspešne pôsobíme už vyše 30 rokov a po celý čas pôsobenia sa zameriavame na oblasť bezpečnosti informácií.
- Disponujeme tímom skúsených a certifikovaných bezpečnostných konzultantov a špecialistov.
- Naši špecialisti sú schopní integrovať široké portfólio technológií do jedného bodu a nad týmito technológiami vytvoriť a nastaviť procesy a komplexné detekčné a korelačné pravidlá na zaistenie správnej funkčnosti a vizibility navrhnutého riešenia.
- Nami ponúkané riešenie je priamo optimalizované na zákazníkovu infraštruktúru a reflektuje jej podobu, aktuálne bezpečnostné hrozby a trendy v oblasti kybernetickej bezpečnosti.
- Počúvame klientov a prispôsobujeme riešenia ich potrebám, požiadavkám a možnostiam.
- Disponujeme referenciami od veľkých zákazníkov v rámci sektorov (banky, energetika a utility, telekomunikácie, výrobné podniky, médiá a obchod, poisťovne a verejný sektor).

Využívame dlhoročné skúsenosti a spolupracujeme v rámci AEC

Security Assessment Division
Využívame skúsenosti našich penetračných testerov z reálnych prostredí a prispôsobujeme tomu skladbu detekčných a korelačných pravidiel. Pravidelne testujeme naše detekčné schopnosti vrátane práce našich analytikov.

Risk & Compliance Division
Spolupracujeme s procesnými špecialistami pri tvorbe a dokumentácii procesov medzi zákazníkmi a CDC.

Security Technologies Division
Naši kolegovia nám pomáhajú s odstraňovaním problémov detegovaných na bezpečnostných riešeniach u zákazníka a s ich rozvojom (konfigurácia NGFW, IDS/IPS, DLP, EDR a ďalšie).

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