Security Operations Centre (SOC)

AEC

Security Operations Centre (SOC) je riešenie zaisťujúce komplexnú centralizáciu riadenia bezpečnostných udalostí a incidentov v jednom bode, s cieľom minimalizácie reakčnej doby na incident a škôd z nej vyplývajúcich.

Centrum stojí na pilieroch detekcie, analýzy, investigácie, reakcie a post incident aktivít. Kontinuálnym monitoringom v reálnom čase identifikujeme, prípadne prijmeme notifikáciu o potenciálne škodlivom chovaní, v chránenej infraštruktúre (detekcia). Určíme, či sa jedná o bezpečnostnú udalosť alebo o bezpečnostný incident, ktorý môže mať negatívny dopad na nami chránenú infraštruktúru (analýza). Skúmaním daného bezpečnostného incidentu zistíme konkrétne dopady a cestu, ktorou sa útočníkovi podarilo preniknúť do infraštruktúry (investigácia). Okamžitou reakciou minimalizujeme dopad bezpečnostných incidentov (reakcia). Po úspešnej reakcii zaistíme ponaučenie z incidentov (kontinuálne zlepšovanie), kontrolu zavedenia nápravných opatrení a reporting zistených skutočností na zvýšenie informovanosti (post incident). A to všetko vďaka silnej kombinácii procesov, technológií a ľudských zdrojov priamo optimalizovaných podľa potrieb zákazníka.

www.aec.sk

Security Operations Centre (SOC)

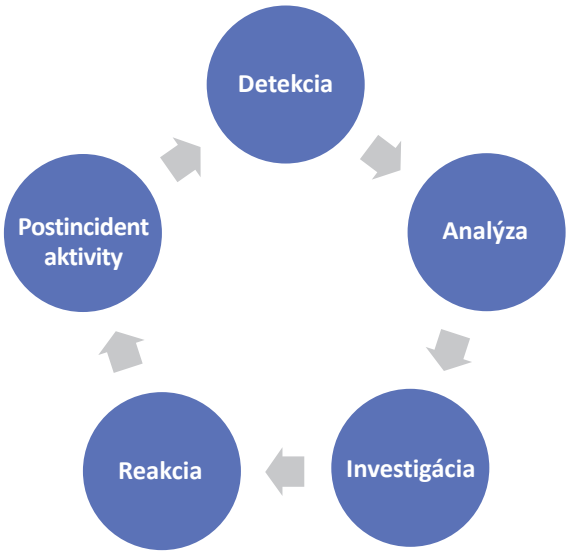
AEC môže ponúknuť dva varianty Bezpečnostného Operačného Centra – onsite a as a service. Onsite SOC je kompletne vybudovaný a spravovaný na strane zákazníka. Rola AEC v takomto type SOCu je postavená najmä na Supportnej zmluve, kde môžu byť niektoré kľúčové bezpečnostné prvky spravované zo strany AEC. SOC as a service je naopak prevádzkovaný v infraštruktúre AEC a zákazník je do nej pripojený. AEC v tejto oblasti ďalej ponúka aj „Professional Services“ ako sú: Cybersecurity Incident Response Tím, Analýza Malware, Brand Protection, Cyber Threat Intelligence, Security Awareness, Continual Security Advisor a konzultačné služby v rôznych oblastiach bezpečnosti.

Čo môže byť dôvod na zaobstaranie SOC?

- Zníženie reakčnej doby na incident (zvýšenie efektivity) a teda zmiernenie dopadu incidentu (zníženie nákladov na obnovu)
- Centralizácia bezpečnosti do jedného bodu
- Real-time znalosť bezpečnostnej situácie v infraštruktúre
- Zníženie nákladov na ľudský faktor (operátori SOC namiesto technikov na jednotlivé technológie)
- Minimalizácia možnosti pochybenia operátorov (automatizácia bezpečnosti) vďaka vopred definovaným postupom riešenia incidentov
- Pokrytie komplexného portfólia bezpečnostných hrozieb
- Reflexia aktuálnych aj novo vznikajúcich hrozieb

Kľúčové prínosy

- Priamo optimalizovaný na zákazníkovu infraštruktúru
- Reflektuje aktuálne bezpečnostné hrozby a trendy v oblasti Cybersecurity
- Zvyšuje úroveň bezpečnosti
- Znižuje reakčný čas na incident
- Poskytuje prehľad o bezpečnostnej situácii v infraštruktúre
- Priamo optimalizovaný podľa potrieb zákazníka



Prečo zvoliť AEC?

- Disponujeme tímom skúsených bezpečnostných konzultantov a špecialistov
- Naši špecialisti sú schopní integrovať široké portfólio technológií do jednotného bodu a nad týmito technológiami vytvoriť a nastaviť procesy k zaisteniu správnej funkčnosti navrhnutého riešenia
- Sme schopní celé navrhnuté riešenie a jeho funkčnosť otestovať penetračnými testami
- Sme lokálna firma s kmeňovými zamestnancami a preferujeme osobný prístup ku každému zákazníkovi
- Disponujeme referenciami od veľkých zákazníkov
- Takmer 30 rokov skúseností v oblasti bezpečnosti informácií naprieč sektormi (banky, energetika a utility, telekomunikácie, výrobné podniky, média a obchod, poisťovne, verejný sektor)

AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
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