Security Operations Centre (SOC)

AEC

Security Operations Centre (SOC) je řešení zajišťující komplexní centralizaci řízení bezpečnostních událostí a incidentů v jednom bodě s cílem minimalizace reakční doby na incident a škod z něj plynoucích.

Centrum stojí na pilířích detekce, analýzy, investigace, reakce a post incident aktivit. Kontinuálním monitoringem v reálném čase identifikujeme, případně přijmeme notifikaci o potenciálně škodlivém chování v chráněné infrastruktuře (detekce). Určíme, zda se jedná o bezpečnostní událost, nebo o bezpečnostní incident, který může mít negativní dopad na námi chráněnou infrastrukturu (analýza). Zkoumáním daného bezpečnostního incidentu zjistíme konkrétní dopady a cestu, kterou se útočníkovi podařilo proniknout do infrastruktury (investigace). Okamžitou reakcí minimalizujeme dopad bezpečnostních incidentů (reakce). Po úspěšné reakci zajistíme poučení se z incidentu (kontinuální zlepšování), kontrolu zavedení nápravných opatření a reporting zjištěných skutečností pro zvýšení informovanosti (post incident). A to vše díky silné kombinaci procesů, technologií a lidských zdrojů přímo optimalizovaných dle zákazníkových potřeb.

www.aec.cz

Security Operations Centre (SOC)

AEC

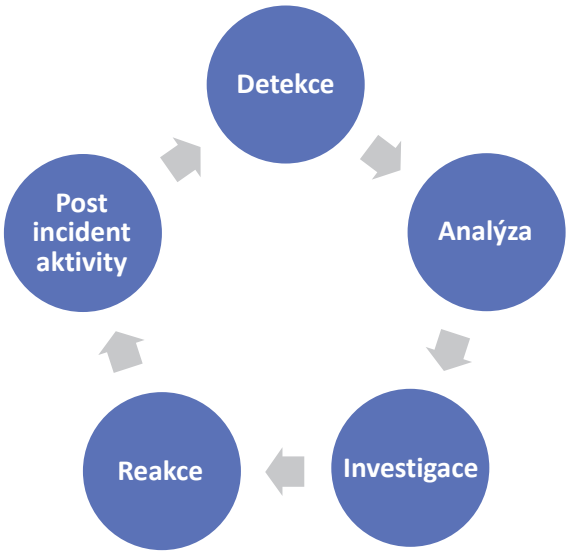
AEC může nabídnout dvě varianty Bezpečnostního Operačního Centra – onsite a as a service. Onsite SOC je kompletně vybudován a spravován na straně zákazníka. Role AEC v takovémto typu SOCu je postavena zejména na Supportní smlouvě, kde mohou některé klíčové bezpečnostní prvky být spravovány na straně AEC. SOC as a service je provozován v infrastruktuře AEC a zákazník je do něj připojen. AEC v této oblasti dále nabízí „Professional Services“ jako jsou: Cybersecurity Incident Response Tým, Analýza Malware, Brand Protection, Cyber Threat Intelligence, Security Awareness, Continual Security Advisor a konzultační služby v různých oblastech bezpečnosti.

Co může být důvod k pořízení SOC?

- Snížení reakční doby na incident (zvýšení efektivity) a tudíž zmírnění dopadu incidentu (snížení nákladů na obnovu)
- Centralizace bezpečnosti do jednoho bodu
- Rreal-time znalost bezpečnostní situace v infrastruktuře
- Snížení nákladů na lidský faktor (operátoři SOC namísto techniků pro jednotlivé technologie)
- Minimalizace možnosti pochybení operátorů (automatizace bezpečnosti) díky předem definovaným postupům řešení incidentů
- Pokrytí komplexního portfolia bezpečnostních hrozeb
- Reflexe aktuálních, ale i nově vznikajících hrozeb

Klíčové přínosy

- Přímo optimalizovaný na zákazníkovu infrastrukturu
- Reflektuje aktuální bezpečnostní hrozby a trendy v oblasti Cybersecurity
- Zvyšuje úroveň bezpečnosti
- Snižuje reakční čas na incident
- Poskytuje přehled o bezpečnostní situaci v infrastruktuře
- Přímo optimalizovaný dle potřeb zákazníka



Proč zvolit AEC?

- Disponujeme týmem zkušených bezpečnostních konzultantů a specialistů
- Naši specialisté jsou schopni integrovat široké portfolio technologií do jednotného bodu a nad těmito technologiemi vytvořit a nastavit procesy k zajištění správné funkčnosti navrženého řešení
- Jsme schopni celé navržené řešení a jeho funkčnost otestovat penetračními testy
- Jsme lokální firmou s kmenovými zaměstnanci a preferujeme osobní přístup ke každému zákazníkovi
- Disponujeme referencemi od velkých zákazníků
- Téměř 30 let zkušeností v oblasti bezpečnosti informací napříč sektory (banky, energetika a utility, telekomunikace, výrobní podniky, média a obchod, pojišťovny, veřejný sektor)

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