Cyber Defense Center

S naším SOC as a Service, ktorý sme nazvali Cyber Defense Center, sa môžete sústrediť na rozvoj svojho podnikania, zatiaľ čo my sa postaráme o vašu kybernetickú bezpečnosť.

Poskytneme vám konečné riešenie na riadenie udalostí a incidentov v oblasti kybernetickej bezpečnosti vo forme služby, ktorá okrem iného zabezpečí minimalizáciu reakčného času na bezpečnostné udalosti alebo incidenty, a tým zníži potenciálne škody.

Prostredníctvom Cyber Defense Centra vám poskytneme služby pozostávajúce z nepretržitého zberu, detekcie, analýzy a investícií do bezpečnostných udalostí a incidentov. Okrem toho ponúkame aj riešenia v podobe reakcie a post incident aktivít vrátane evidencie a oznamovania nielen vnútroštátnym orgánom.

Prečo by ste si mali zaobstarať náš bezpečnostný dohľad?

- Poskytujeme komplexné bezpečnostné riešenia bez ohľadu na to, či ste alebo nie ste pod útokom.
- Sme tu pre vás 24 hodín denne, 7 dní v týždni, 365 dní v roku.
- Máme nezávislé odborné znalosti a skúsenosti.
- Monitorujeme a reagujeme v reálnom čase.
- Ponúkame pomoc a partnerstvo, keď si neviete rady.
- Flexibilná a škálovateľná architektúra riešenia presne podľa vašich potrieb a požiadaviek.
- Dodávame presne to, čo potrebujete, nie univerzálne balíky.

Sledujeme

Neustále monitorujeme a identifikujeme anomálie a nežiaduce alebo škodlivé správanie v chránenej infraštruktúre v reálnom čase. Všetky získané údaje alebo informácie navzájom korelujeme pomocou odborných technologických riešení. Pomôžeme vám odhaliť nielen bezpečnostné incidenty, ale aj chybné konfigurácie a slabé miesta kybernetickej bezpečnosti.

Analyzujeme

Určíme, či ide o falošný poplach, bezpečnostnú udalosť alebo bezpečnostný incident, ktorý môže mať negatívny vplyv na nami chránenú infraštruktúru. Z falošných poplachov vytvárame podnety na zvýšenie bezpečnosti. Bezpečnostné udalosti a incidenty ďalej odovzdávame na investigáciu.

Vyšetrujeme

Podrobným preskúmaním bezpečnostného incidentu zistíme, čo presne sa stalo, identifikujeme vplyv a cestu, ktorou sa útočníkovi podarilo preniknúť do infraštruktúry, a zhromaždíme všetky potrebné informácie, aby sme mohli určiť presné a primerané reakčné opatrenia.

Reagujeme

Okamžitou reakciou minimalizujeme dopad bezpečnostných incidentov. Pomáhame tiež koordinovať celú reakciu a vysielame náš Cyber Security Incident Response Tím (CSIRT), aby incident riešil priamo na mieste, alebo len poskytujeme pomocnú ruku a usmernenie, ako incident riešiť.

Zlepšujeme

Po úspešnej reakcii sa z incidentu učíme a iniciujeme sériu nápravných opatrení, ktoré následne reportujeme podľa zistených skutočností na zvýšenie informovanosti. Incident evidujeme a pomáhame pri jeho oznamovaní zainteresovaným stranám a vnútroštátnym orgánom.

Medzi naše hlavné služby patrí:

- Cyber Security Incident Response Tím (CSIRT),
- služba nepretržitého monitorovania bezpečnosti (SOC as a Service),
- bezpečnostné technológie a infraštruktúra ako súčasť služby,
- Vulnerability Management ako služba,
- štruktúrovaný, neštruktúrovaný, situačný alebo entitou riadený Threat Hunting,
- konzultačné služby v oblasti kybernetickej bezpečnosti.