Cyber Defense Center

S naším SOC as a Service, který jsem pojmenovali Cyber Defense Center se můžete plně soustředit na svůj podnikový růst, zatímco my se vám postaráme o kybernetickou bezpečnost.

Poskytneme vám konečné řešení pro řízení kybernetických bezpečnostních událostí a incidentů v podobě služby, která vám mimo jiné zajistí minimalizaci reakční doby na bezpečnostní události či incidenty a tím i sníží případné škody.

Prostřednictvím Cyber Defense Centra vám dodáme služby spočívající v kontinuálním sběru, detekci, analýze a investigaci bezpečnostních událostí a incidentů. Společně s tím nabízíme i řešení v podobě reakce a post incident aktivit včetně evidence a komunikace nejen na národní autority.

Proč byste si měli pořídit náš bezpečnostní dohled?

- Poskytujeme komplexní bezpečnostní řešení ať už jste, nebo nejste pod útokem.
- Jsme tu pro vás 24 hodin denně 7 dní v týdnu a 365 dní v roce.
- Disponujeme nezávislými expertními znalostmi a zkušenostmi.
- V reálném čase monitorujeme i reagujeme.
- Nabízíme pomoc a partnerství pro případy, kdy si nevíte rady.
- Flexibilní a škálovatelná architektura řešení přesně podle vašich potřeb a požadavků.
- Dodáváme přesně to, co potřebujete, ne univerzální krabičky.

Sledujeme

V reálném čase nepřetržitě monitorujeme a identifikujeme anomálie a nežádoucí či škodlivé chování v chráněné infrastruktuře. Veškerá získaná data či informace korelujeme mezi sebou, a to prostřednictvím expertních technologických řešení. Pomůžeme vám nejen odhalit bezpečnostní incidenty, ale i chybnou konfiguraci či nedostatky v kybernetické bezpečnosti.

Analyzujeme

Určíme, zda se jedná o falešný poplach, bezpečnostní událost, nebo bezpečnostní incident, který může mít negativní dopad na námi chráněnou infrastrukturu. Z falešných poplachů vytváříme podněty ke zlepšení bezpečnosti. Bezpečnostní události a incidenty dále postupujeme investigaci.

Vyšetřujeme

Detailním zkoumáním bezpečnostního incidentu zjistíme, co přesně se stalo, identifikujeme dopad a cestu, kterou se útočníkovi podařilo proniknout do infrastruktury a shromáždíme veškeré nezbytné informace, abychom byli schopni stanovit přesné a adekvátní reakční kroky.

Reagujeme

Okamžitou reakcí minimalizujeme dopad bezpečnostních incidentů. Pomáháme rovněž i koordinovat celou reakci, vysíláme náš Cyber Security Incident Response Tým (CSIRT), který incident vyřeší na místě, nebo jen poskytujeme pomocnou ruku a návodné postupy, jak se s incidentem vypořádat.

Zlepšujeme

Po úspěšné reakci se z incidentu učíme a spustíme série nápravných opatření, která následně reportujeme dle zjištěných skutečností pro zvýšení informovanosti. Incident evidujeme a pomáháme s jeho komunikací na zainteresované subjekty a národní autority.

Mezi naše hlavní služby patří:

- Cyber Security Incident Response Tým (CSIRT),
- služba kontinuálního bezpečnostního monitoringu (SOC as a Service),
- bezpečnostní technologie a infrastruktura jako součást služby,
- Vulnerability Management jako služba,
- strukturovaný, nestrukturovaný, situační nebo entitou řízený Threat Hunting,
- konzultační služby v oblasti kybernetické bezpečnosti.