Security Operations Center (SOC)

Od roku 2010 patříme k průkopníkům kybernetické bezpečnosti, máme tým expertů s dlouholetými zkušenostmi.

Rychlost detekce a reakce je pro nás zásadním parametrem kybernetické obrany.

Každé riziko něco stojí

Kolik vás bude stát ztráta dobrého jména? Spočítali jste si jakým rizikům byste vystavili své zákazníky a akcionáře v případě úspěšně provedeného kybernetického útoku, kterému jste mohli zabránit?

Ochrana 24/7/365

V dnešní době nelze zavírat oči před kybernetickými útoky, dějí se všude kolem nás. Snažíte se ochránit vaši organizaci, váš business, citlivá data či know-how. Investujete do technologií, nastavujete procesy a najímáte odborníky. Víte kolik vás to bude stát za rok, za tři nebo třeba v pětiletém horizontu? Vynakládáte tyto investice účelně?

Máme expertní tým

Potřebujete experty na kybernetickou bezpečnost? Kde je vzít, jak je zaplatit a hlavně, jak je udržet? Jsou nakoupené technologie opravdu správně využívány? Opravdu víte, co a jak chránit? Co jsou pro vaši organizaci opravdu kritická rizika? Reagujete jen na vzrůstající množství incidentů a máte problém se v tom vyznat nebo řešíte bezpečnost proaktivně?

„Klíčový je čas a expertní tým a ten můžeme našim klientům poskytnout.“

Irena Hýsková,
CEO

Díky Security Operations Center (SOC) vyřešíme vzrůstají množství bezpečnostních incidentů. Najdeme a zpracujeme prioritně ty nejdůležitější.

Opakující se problémy řešíme automaticky s využitím strojového učení (Machine learning) a inteligentních playbooků.

Na kritické zranitelnosti reagujeme s předstihem, využíváme informace z několika nezávislých zdrojů, monitorujemeinternet.

Díky pokročilým nástrojům využíváme umělé inteligence (AI) k prohledání skrytých anomálií a pokusů o zcizení citlivých dat.

Retence historických dat není problém, objevíme možné útoky i několik let dozadu.

Pracujeme podle mezinárodních standardů MITRE ATT&CK a splňujeme všechny požadavky dané Zákonem o kybernetické bezpečnosti a GDPR.

Rychle a efektivně dokážeme spojit kybernetickou bezpečnost v libovolném hybridním prostředí, ať máte data aplikace v cloudech, vlastních datacentrech či přímo na lokálních serverech.

Monitoring bezpečnostních incidentů

Poskytujeme monitoring bezpečnostních incidentů v režimu 24/7/365, provádíme kontrolu, prioritizaci a korelaci údajů na základě standardizované metodiky a definovaných pravidel a zároveň proaktivně reagujeme na události podle požadavků klienta, na základě kterých jsou vytvářeny specifické bezpečnostní kontroly.

Prostřednictvím zákaznického portálu poskytujeme přístup k detailnímu reportingu, který umíme přizpůsobit požadavkům zákazníka.

Proaktivní detekce a reakce

Security Operations Center (SOC) poskytuje proaktivní bezpečnostní dohled napříč lokální infrastrukturou zákazníka a zároveň monitoruje využívaná cloudová prostředí. Analytici sledují jednotlivé komunikační systémy, aplikace, chování uživatelů a vyhodnocují probíhající bezpečnostní incidenty.

Analýza událostí (Logs and Event Analysis) umožňuje zákaznický přístup k bezpečnostním událostem přes grafické webové rozhraní. Součástí je např. možnost podle potřeby spouštět jak vlastní dotazy nebo pohledy, tak připravené „best practices“. Se souhlasem zákazníka lze automaticky provádět reaktivní opatření s cílem zastavit kybernetický útok nebo zabránit úniku dat. Činnost obsahuje auditovaný záznam veškeré činnosti analytiků SOC.

Auditní záznam a monitoring činností

Ke každé činnosti operátora pořizujeme auditovaný záznam veškeré činnosti operátorů a analytiků SOC. Aktivity je možné v případě potřeby zobrazit a uskutečnit jejich audit.

Korelační pravidla a hledání anomálií

Na základě MITRE ATT&CK metodiky, identifikace slabých míst a dlouhodobé analýzy provozu naši experti vydefinují základní bezpečný model komunikace, který dále optimalizujeme. Díky tomuto modelu jsme schopni velmi rychle detekovat i dovedně skryté anomálie a latentní útoky a zero-day zranitelnosti. Díky použité technologii mají naši experti přístup k více jak 300 pokročilým detekčním pravidlům, automatizovaným playbookům a dalším informačním zdrojům, které zrychlují a zpřesňují detekci kybernetických útoků.

thein.security
Security Operations Center

www.theinsecurity.eu