Proč využít 24/7/365 Security Operations Center?

TRVALÝ BEZPEČNOSTNÍ DOHLED SNIŽUJE RIZIKO ZTRÁT

KYBERNETICKÉ ÚTOKY NEČEKAJÍ NA PRACOVNÍ DOBU

K mnoha úspěšným útokům nedochází proto, že by selhalo technologické zabezpečení, které by nenahlásilo pokus o prolomení bezpečnosti. Ale proto, že upozornění buď nebylo pro velké množství sledovaných dat adekvátně vyhodnoceno, bylo přehlédnuto nebo na ně nebylo reagováno dostatečně rychle. A při tom RYCHLOST DETEKCE A REAKCE je při probíhajícím kybernetickém útoku klíčová pro jeho zastavení a zamezení dalšího šíření. Často jde o minuty a sekundy, ne o hodiny a dny. Útočníci si k průniku záměrně vybírají čas předpokládané nižší pohotovosti v nočních hodinách nebo v časech pracovního klidu. V běžném pracovním režimu bez trvalého monitoringu je pak nemožné zajistit odpovídající ochranu.

TRVALÝ DOHLED OBTÍŽNÝ NA ZAJIŠTĚNÍ

U téměř dvou třetin společností funkci bezpečnosti zastávají IT zaměstnanci, kteří bezpečnost nemají jako svůj hlavní úvazek. A další čtvrtina společností, které už vyčlenily bezpečnostní specialisty na plný úvazek, jich nemá dostatečný počet na to, aby pokryli nepřetržitý provoz a zajistili 24/7/365 monitoring.

HON NA KVALIFIKOVANÉ SPECIALISTY

Firmy mají dlouhodobě neobsazené cybersecurity pozice a nalezení vhodného kandidáta často trvá déle než několik měsíců. Navíc specialisté kybernetické bezpečnosti, kteří změnili zaměstnavatele, často uvádí, že důvodem změny bylo přetažení jinou společností a nabídnuté vyšší finanční ohodnocení, což ukazuje na riziko další fluktuace.

ŘÍZENÁ BEZPEČNOST JAKO SLUŽBA

Problém se zajištěním stálého bezpečnostního dohledu a s nedostatkem odborně školených specialistů může pomoci vyřešit externí **Security Operations Center (SOC)** jako nadstavba nad interními systémy kybernetické bezpečnosti. Stane se prodlouženou rukou vlastního IT a bezpečnostního týmu.

SNADNÉ NASAZENÍ

Odpadá dlouhodobé ladění a ruční nastavování korelací. Řešení je schopno už v krátkém čase po nasazení začít poskytovat výsledky.

EXPERTNÍ TÝM

Denní zapojení do bezpečnostní operativy, sledování dění v oboru i průběžné profesní vzdělávání a zvyšování kvalifikace operátorů přispívá k udržení schopnosti adekvátní reakce.

EFEKTIVNÍ VYUŽITÍ TECHNOLOGIÍ

Zapojení „Managed Service“ nadstavby zvyšuje úroveň využití už pořízené bezpečnostní infrastruktury na její plný potenciál.

PROVOZNÍ NÁKLADY

Náklady na řešení zůstávají předvídatelné i při zachování možnosti rozšiřování a škálovatelnosti rozsahu plnění podle aktuálních potřeb.

S VYUŽÍTÍM SOC-AS-A-SERVICE JE MOŽNO V TŘÍLETÉM HORIZONTU DOSÁHNOUT AŽ 8,8KRÁT NIŽŠÍCH NÁKLADŮ V POROVNÁNÍ S PROVOZOVÁNÍM 24/7/365 BEZPEČNOSTNÍHO DOHLEDU INTERNĚ. [1]

[1] *Zdroj: A Frost & Sullivan SOC-as-a-Service versus DIY SOC Report, 2018.*

BEZPEČNOSTNÍ DOHLED OD THEIN SECURITY

V **Security Operations Center** poskytujeme proaktivní bezpečnostní dohled v libovolném hybridním prostředí, ať máte svoje data a aplikace v lokální infrastruktuře, ve vlastních datacentrech nebo ve veřejných cloudech. Vyřešíme vzrůstající množství bezpečnostních incidentů. Najdeme a zpracujeme prioritně ty nejdůležitější. Opakující se problémy řešíme automaticky s využitím strojového učení a inteligentních playbooků. Na kritické zranitelnosti reagujeme s předstihem, sledujeme několik nezávislých zdrojů.
Pracujeme podle mezinárodně uznávaných standardů, postupujeme v souladu s MITRE ATT&CK metodologií.
Splňujeme požadavky dané normou ISO/EIC 27001 a zákonem č. 181/2014 Sb. o kybernetické bezpečnosti. Činnost našich operátorů se soustředí na několik **hlavních funkcí:**

- **DETEKCE**
  Monitorování a správa bezpečnostních událostí
- **REAKCE**
  Odvrácení a/nebo zmírnění dopadu incidentu
- **PREVENCE**
  Identifikace a proaktivní kroky odhalování kybernetických hrozeb, testování zranitelností
- **PREDIKCE**
  Upozornění na anomálie ve standartním chování uživatelů a v provozu sítě, analýza trendů

VE VÝSLEDKU...

zapojení **Security Operations Center** přináší

- **přidání řízeného dohledu** s **24/7/365 monitoringem** jako nadstavbou nad činností interního IT a bezpečnostního týmu
- **zrychlení detekce a reakce** na zjištěné incidenty a v případě útoku možnost jeho zastavení už v jeho počátečních fázích, což značně omezuje následné dopady a ztráty
- **využití už pořízených bezpečnostních technologií** v jejich plném potenciálu
- **snížení personálních a časových nároků** na průběžnou správu bezpečnostních systémů
- **ochranu investic** a **omezení nákupu a údržby** další softwarové a hardwarové **infrastruktury,** které by jinak byly nutné k dosažení proaktivního přístupu při omezování bezpečnostních hrozeb

PROČ BYSTE SI MĚLI VYBRAT PRÁVĚ NAŠE ŘEŠENÍ.

Používáme inovativní technologie a dosahujeme vyšší efektivity v pracovních postupech, což mohou následně jako přidanou hodnotu využít naši zákazníci.

„V IT ODDĚLENÍ JSME TADY S KOLEGOU DVA. A MÁME NA STAROSTI I BEZPEČNOST. NEMÁME ČAS V SECURITY SYSTÉMECH SLEDOVAT A LADIT ÚPLNĚ VŠECHNO. SOC PRO NÁS Z MILIÓNŮ LOGŮ A TISÍCŮ BEZPEČNOSTNÍCH HLÁŠENÍ VYFILTRUJE 15 ESKALACÍ MĚSÍČNĚ, KTERÝM SE POTOM PODROBNĚJI VĚNUJEME. NEUMÍM SI PŘEDSTAVIT LEPŠÍ ÚSPORU ČASU.“

IT ŘEDITEL, PRÁVNÍ A ADVOKÁTNÍ KANCELÁŘ

PRO NAŠE ZÁKAZNÍKY GARANTUJEME KVALITU

Vyhýbáme se laciným řešením. Dbáme na fyzickou přítomnost česky mluvících operátorů a možnost přímého kontaktu s našimi zákazníky. Spolupracujeme s předními poskytovateli a světovými lídry v oboru kybernetické bezpečnosti a udržujeme vysokou úroveň kvalifikace našeho expertního týmu včetně nezbytných certifikací.
Uplatňujeme principy zaměřené na neustálé zvyšování kvality poskytovaných služeb a produktů s cílem dosahovat maximální úrovně spokojenosti a loajality svých zákazníků i spolupracujících partnerů.

CERTIFIKACE

ZKUŠENOSTI I MODERNÍ OCHRANA PROTI NOVODOBÝM HROZBÁM

Thein Security patří od roku **2010** k průkopníkům v oblastech **prevence úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**.

V současnosti se zaměřujeme především na **ochranu moderní síťové infrastruktury** proti novodobým typům útoků. Poskytujeme služby pro technologie **hybridních prostředí** (on prem / cloud) a specializujeme se na zavádění **Zero Trust přístupu**.

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Pro více informací o Security Operations Center a Službách řízené bezpečnosti kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, T +420 226 531 832. e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546

www.theinsecurity.eu