axians

The best of ICT with a human touch

SECURITY OPERATIONS CENTER

Nenechte kyberzločince ohrozit Vaši společnost. Náš SOC tým je první linií obrany, vybavený pokročilými nástroji a zkušeným týmem odborníků na kybernetickou bezpečnost.

Náš SOC (Security Operations Center)

- Mezinárodní expertní tým
- Vyšetřování a analýzy
- 24/7 provoz
- 10 x SOC v Evropě
- Zkušenost s 6 SIEM/SOC platformami

Naše silné stránky

- Axians provozuje **10 SOC** center v rámci Evropy
- Důraz na **identifikaci incidentů** a **hrozeb** a jejich včasné **řešení**
- Zkušenost s nejrozšířenějšími SIEM/SOC platformami
- Integrace s HR systémy, CMDB, tiketovacími nástroji, Asset a Risk Management nástroji
- Integrace nástrojů fyzické bezpečnosti a přístupových systémů v kombinaci se zdroji IT
- Nastavení detekce podvodů v aplikacích
- Integrace s **Threat Intel platformou** a průběžné vylepšování detekčních schopností

Víte, že?

- 43 % kybernetických útoků je zaměřeno na malé podniky, ale pouze 14 % je připraveno se bránit
- 43 % všech průniků jsou hrozby zevnitř, ať už úmyslné nebo neúmyslné
- 66 % malých podniků zažilo v posledních 12 měsících kybernetický útok
- 95 % narušení kybernetické bezpečnosti je způsobeno lidskou chybou
- 54 % společností tvrdí, že jejich IT oddělení nejsou dostatečně vyspělá na to, aby zvládla pokročilé kybernetické útoky
- Přibližně 70 % všech útoků bylo motivováno finančně, zatímco méně než 5 % bylo motivováno špionáží
- Téměř 40 % útoků bylo způsobeno phishingem, asi 11 % malwarem a 22 % hackováním

Security Operation Center

BALÍČEK SLUŽEB

SLUŽBY SOC

Klíčové charakteristiky služby

- 8x5 nebo 24x7 (web, telefon, e-mail)
- Přístup k odborníkům (L1 až L3) v ceně
- Počáteční nastavení a integrace SIEM
- Předpřipravené konektory
- Definice korelačních pravidel
- Plán reakce na incidenty

Přidaná hodnota

- Pomoc s monitorováním zabezpečení a reakcí na straně zákazníka
- Proaktivní monitorování a přizpůsobení se změnám infrastruktury
- Vytváření scénářů na základě zkušeností

Služba rovněž zahrnuje

- Vstupní analýzu před nasazením
- Incident Response Playbooks
- Příprava reportů na míru
- Identifikace incidentů a hrozeb
- Identifikace kritičnosti incidentu
- Komunikaci odpovědnému týmu
- Měsíční zprávu o incidentech, hrozbách, trendech a sadu doporučení
- Ladění falešně pozitivních událostí

Fixní cena [měsíční platba]

DOPLŇKOVÉ SLUŽBY

Automatizace

- Vývoj konektorů na míru
- Obohacení logů

SIEM optimalizace

- Optimalizace použitých licencí
- Optimalizace ukládání a zálohování
- Optimalizace úrovně logování
- Optimalizace využití kapacity síťového provozu

Doplňky

- Změny v architektuře a designu
- Projekty migrace
- Integrace na míru
- Integrace s tiketovacími nástroji
- Analýza aplikací pro integraci do SIEM
- Posouzení souladu s regulatorními požadavky a integrace do SIEM
- Další integrace prostřednictvím API

Variabilní cena [hodinová sazba]

IBM Security SentinelOne FORTINET Microsoft Defender HUNTERS wazuh.

Kontakt:

Kryštof Oczadlý
Head of Sales
tel.: +420 720 761 981
e-mail: krystof.oczadly@axians.com

David Tůma
Sales Manager
tel.: +420 731 441 783
e-mail: david.tuma@axians.com

VINCI ENERGIES