IXPERTA

SIEM Security Operations

zajištění kompletního bezpečnostního monitoringu a managementu

Je pro vás IT bezpečnost prioritou, ale raději se věnujete svému byznysu?

Pak je služba SIEM SecOps (SIEM Security Operations) pro vás tím pravým řešením. Zajistíme pro vás na míru všechny činnosti bezpečnostního monitoringu a managementu, na které nechcete alokovat vaše cenné interní zdroje. Díky integrovanému Security Operation Center získáte okamžitý přehled o bezpečnostních událostech a incidentech ve vaší společnosti.

Co Vám SIEM SecOps přinese?

- Dodá vašemu byznysu odborné činnosti IT bezpečnosti s jasně definovanými parametry služby (SLA).
- Uvolní odborné lidské zdroje pro Vaše primární podnikové aktivity.
- Zajistí plnění Vašich specifických bezpečnostních požadavků. Sami si určíte, jaké výstupy potřebujete a řídíte si požadované kontrolní mechanizmy.
- Jednoduše si naplánujete rozpočet na základě strukturovaných konstantních nákladů služby.
- Služba je flexibilní - rozšiřování nebo změna rozsahu služeb je velmi snadné.

IXPERTA s.r.o.
Lihovarská 1060/12
190 00 Praha - Libeň

IČ: 27599523
DIČ: CZ27599523
Datová schránka: kp6z92b

IXPERTA infolinka
t: +420 266 061 111
e: info@ixperta.com

www.ixperta.com

IXPERTA

Nastavte si bezpečnostní monitoring a management podle svých potřeb

Jaké služby může IXPERTA SIEM SecOps obsahovat a co přináší?

Zajištění rutinních činností SOC

Rutinní vyhodnocování zjištěných událostí, předávání potencionálních incidentů k řešení, předávání výsledků zákazníkovi v požadovaném formátu, požadovaným informačním kanálem (např. reporting), pravidelná review výsledků se zákazníkem.

Zajištění expertních činností SOC

Analýza potenciálních bezpečnostních incidentů, nalezení příčiny, zajišťování důkazů, rozpoznání false-positives, předávání výsledků v požadovaném formátu určeným informačním kanálem (např. reporting), pravidelná review výsledků se zákazníkem.
Podpora při odezvě na incident.

Zajištění expertních činností SIEM

Odborná kontrola a rozvoj správné funkce SIEM, prohledávání systémových a bezpečnostních logů a zavádění nových zajímavých atributů pro pohledy, reporty a hlášení porušení, reflexe identifikovaných změn ve zdrojích logů / toků, odstranění nalezených chyb ve zpracování.

Technologické integrace SIEM s IT prostředím

Začlenění specifických zdrojů logů nad rámec možností SIEM, možné použití na míru vyvinutých datových pump, vlastních normalizérů a parserů, začleňování dalších zdrojů dat (informací), např. data identitních systémů, skenerů zranitelností, reputačních služeb, pravidelné ověřování jejich správné funkce k obohacení výstupů SIEM.

Aplikační rozšíření SIEM

Doplnění nové aplikační funkcionality do produktu SIEM, využití SIEM API, tvorba doplňkových aplikací. Aplikační úpravy v grafickém rozhraní.
IXPERTA má vlastní vývojové centrum (R&D).

Propojování s procesy informační bezpečnosti

Kontrola a rozvoj procesů ve vazbě na SIEM, sladění reálného nastavení technologie s formální bezpečnostní dokumentací, pravidelná verifikace a aktualizace postupů proti realitě, podněty pro zlepšování, návrhy na zavedení a zlepšení IT kontrol. Vazba na ZKB a ISMS.

Komunikační platforma služby

- Využití zákaznických servisdeskových a kooperačních platforem, pokud je požadováno.
- Vlastní servisdesková a kooperační platforma IXPERTA (na základě produktu Atlassian Jira & Confluence) zajištěná pro tuto službu.
- Tradiční komunikační kanály a výstupy (např. reporting) pro organizace, které nechtějí využívat moderní kooperační platformy.

Platební flexibilita služby

Pravidelné jednotné měsíční / roční platby ve stejné výše za vybrané služby (OPEX).
Úvodní akontace (CAPEX), která pokryje úvodní nasazení produktu SIEM a dalších podpůrných nástrojů, následně pravidelné jednotné měsíční / roční platby za vybrané služby (OPEX).

Se SIEM SecOps získáte špičkový SIEM produkt IBM QRadar, na který je SIEM SecOps navázán.

IXPERTA je certifikovaným partnerem IBM specializovaným na implementaci QRadar.

IBM Silver Business Partner™

Divize Bezpečnosti

Tým Bezpečnostní služby

FILIP FIALA
Division Leader
filip.fiala@ixperta.com
+420 602 596 689

VLADISLAV ŠAFRÁNEK
Team Leader
vladislav.safranek@ixperta.com
+420 266 062 371

MILAN ŠEREDA
Security Consultant
milan.sereda@ixperta.com
+420 603 459 854