

***Projektová dokumentace***

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU  
KOLÍN - zpracování projektové dokumentace“***

***TECHNOLOGICKÁ ČÁST JCE IB***

***D.1.4.9. Technologie a řešení JCE IB***

***D.1.4.9.19. SLUŽBA SECURITY OPERATIONS CENTER  
(SOC) - ŠKOLA***

**Zpracoval:**

Petr Lacina

## 19 SLUŽBA SECURITY OPERATIONS CENTER (SOC) - ŠKOLA

---

### 19.1 POPIS

V rámci projektu bude pro zajištění monitoringu kybernetické bezpečnosti využito služeb bezpečnostního dohledového centra.

Služby zajistí monitoring nad stávajícími informačními systémy a nově dodanými technologiemi NDR a EDR a tím eliminují rizika spojená s nedostatečnou personální kapacitou na úrovni pracovníků Školy.

V rámci služeb SOC dojde k napojení současných IS do dohledového centra a zajištění dohledu v režimu 8 x 5.

Součástí ceny je pronájem licenci SIEM, napojení EDR + NDR a provozování služby SOC po dobu 5 let.

## 19.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

### 19.2.1 Obecné funkční požadavky na rozsah technologií a technologických vlastností v dohledovém centru

Požadovaná funkcionalita	Specifikace minimálních požadavků
Řešení je plnohodnotné – tedy služba, která obsahuje všechny technologie, procesy SOCu a lidi v SOCu.	
Řešení obsahuje z pohledu technologií LM, SIEM, Security Ticketing, Security Dashboard a SOAR. Monitoring Netflow je technologicky zajišťován zadavatelem, dodavatel provádí sběr z této technologie.	Prokažte, jakým způsobem a jakými produkty bude toto splněné.
SOC bude poskytovaný jako externí outsourcovaná služba – všechny technologie jsou provozované v prostředí zadavatele, dodavatel potřebné logy / data z těchto technologií vyhodnocuje ve svém prostředí	V případě potřeby kolektoru, bude tento kolektor realizován v rámci virtuální infrastruktury
Všechna data budou přenášena do SOC-u v zabezpečené zašifrované formě a musí být chráně vůči neoprávněným změnám/zásahům	
Provozu SOCu je zajišťován v režimu 8x5, dle stanovených SLA parametrů.	
Součástí SOC jsou služby certifikovaného CSIRT.	
Je požadovaná vysoká dostupnost služby SOC provozovaná minimálně ve 2 geograficky oddělených lokalitách pro vykrytí případného výpadku.	
CSIRT je certifikovaný minimálně na stupeň "Accredited".	
Provozovatel SOC je certifikovaný na ISO 27000.	
Všechny aktivity specialistů SOCu jsou auditované na úrovni detailních aktivit (pohyby myši, práce s klávesnicí, obsah obrazovky), které vůči zadavateli vykonávají. Daný nástroj na zajištění této auditní stopy je součástí technického řešení dodavatele.	
Řešení SOCu jako služby musí být v souladu se zákonem 181/2014 Sb o kybernetické bezpečnosti (ZoKB).	
Součástí řešení bude real-time provozní monitoring dostupnosti informačních systémů, kritických aplikací a síťových prvků s cílem zjistit výpadky procesů a funkčnosti systémů, narušení dostupnosti, včasného identifikování bezpečnostních incidentů, resp. omezení účinnosti bezpečnostních opatření.	
Řešení musí vědět zpracovat i dočasné zvýšený přenos dat (peak) na síti bez jeho zahození/ignorování.	
Řešení musí umožňovat rozšíření výkonnosti anebo připojení monitorovaných zdrojů jen licenčním vypořádáním (škálovatelnost). Popište ji.	

Řešení bude dostupné 99,9 %.	
<b>Výkonový rozsah licence pro LM/SIEM je minimálně 250 EPS.</b>	
<b>Požadovaný čas ukládání dat pro ONLINE vyhledávání je minimálně 100 dní.</b>	
<b>Požadovaný čas ukládání dat pro OFFLINE archive je minimálně dalších 200 dní.</b>	
Řešení je postavené jako otevřené pro zadavatele, zadavatel má přístup do všech částí/technologie minimálně v rozsahu READ ONLY.	
Součástí služby jsou specialisté bezpečnostního monitoringu v rozsahu L1, L2, L3.	
Součástí SOC sú pravidelné schůzky/status meetingy aspoň 1x do měsíčně.	
Součástí SOC je tvorba Knowledge Base a tvorba RUNBOOKS pro efektivní řešení bezpečnostních událostí.	
Součástí SOCu je specializovaný portál, kde jsou dostupné všechny informace na jednom místě v podobě DASHBOARDU. Tento portál poskytuje dashboards na míru (možnost konfigurace specialisty dodavatele), kde je možné zobrazit informace ze všech komponent SOCu.	
Součástí SOCu jsou služby forenzní analýzy bezpečnostního incidentu ve formě rámcové smlouvy.	
Řešení bude schopné monitorovat, analyzovat a vyhodnocovat bezpečnostní události, hrozby, útoky a anomálie na základě netflow, pomocí přímého monitoringu v reálném čase a to aj na aplikační vrstvě ISO/OSI, resp. TCP/IP. Technologicky řešení monitoringu netflow zajistí zadavatel. Po provozovateli SOC požaduje jeho napojení do dohledu a konzultace speciality certifikovaného na tuto technologii.	
Řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy).	
Řešení musí umožňovat automatické korelování událostí z více zdrojů, vyhodnocení incidentů a následné generování alertů, a to všechno v reálném čase.	
Řešení musí primárně využívat bez-agentový sběr logů. Ten typ sběru je preferovaný. Instalace agenta bude umožněna jen v odůvodněných případech Např. pokud není technologicky možné zajistit sběr logů jiným způsobem.	
Databáze musí být zabezpečená proti manipulaci, tak aby nebylo možné narušit integritu uložených záznamů.	
Řešení bude podporovat napojení různých zdrojů obohacujících informací (DNS, IDM, LDAP, ap.).	
Řešení nesmí způsobit omezení funkcionality, kvality a narušení bezpečnosti jiných zařízení / systémů v síti.	
Řešení bude podporovat možnosti vícenásobné notifikace jednoho alertu.	

Řešení musí podporovat filtraci a agregaci už na úrovni sběru logů v prostředí zadavatele.	
Řešení zabezpečí normalizaci logů z různých zdrojů a formátů do jednotného formátu.	
Řešení bude schopné zaznamenávat a vyhodnocovat minimálně následující detaily bezpečnostních událostí: typ nebo akce, datum a čas, ID systému, který událost zaznamenal, ID systému, kde k události došlo a ID uživatele nebo systému, který akci vyvolal.	
Řešení SOC využívá SOAR techniky a procesy pro orchestraci a zrychlení threat detection a incident response.	
Řešení je na úrovni Alertingu provázané s technikami popsanými v knowledge base MITRE ATT&CK.	
Součástí služby SOCu je měsíční KPI reporting na míru zákazníka.	
Samotný poskytovatel SOCu musí nabízet RestAPI (nebo podobné API) rozhraní pro výměnu informací o svých aktivitách, minimálně na úrovni ticketing nástroje.	
Služba SOCu musí obsahovat funkcionality THREATS EXCHANGE, minimálně na úrovni MISP.	