Úvod

Předmětem zakázky je zajištění kybernetické obrany formou dodávky SW produktu pro sběr, analýzu a detekci kybernetických bezpečnostních událostí (SIEM). Cílem je vytvoření systému zajišťujícího bezpečnostní dohled ICT aktiv na Univerzitě J. E. Purkyně v Ústí nad Labem (dále jen „Objednatel“) a to pomocí implementovaných technologií, které zajistí:

* sledování datového provozu informační infrastruktury
* detekci útoků na prostředky ICT ve sítích Objednatele,
* odhalování případných interních a externích útočníků
* detekci nestandardního chování

Záměr Objednatele v oblasti systému bezpečnostního monitoringu

Objednatel očekává zavedení bezpečnostní platformy, která umožní detekovat kybernetické bezpečnostní hrozby a podpoří budoucí vznik procesů Security Operations Center.

Požadovaná bezpečnostní platforma musí umožnit detekci nebezpečných projevů v síťovém provozu, jehož analýzu bude řešení provádět sběrem logů a jejich vyhodnocováním.

Řešení musí umožňovat nebo pomocí rozšíření funkcionality umožňující automatizaci mnoha kroků a procesů v rámci vyšetřování a reakcí na incident s cílem snížit zatížení specialistů, kteří by jinak museli pracovat s mnoha bezpečnostními technologiemi zvlášť a tím by byla snížena jejich efektivita. Řešení tudíž musí obsahovat vnitřní integraci (on-prem) s automatizačním bezpečnostním systémem SOAR (Security Orchestration, Automation and Response) od stejného výrobce jako je dodavatel SIEMu (SOAR není součástí této poptávky).

Požadované řešení by mělo zajistit rychlé detekce na stoupající nebezpečí napadení organizace Objednatele kybernetickým útokem realizovaným externím či interním útočníkem, a to minimálně tím, že bude splňovat níže specifikované funkcionality nebo vlastnosti:

* Zajišťovat sběr, ukládání, analýzu a korelaci logů z různých zdrojů v IT infrastruktuře prostřednictvím nástroje Log management a nástroje pro management a analýzu bezpečnostních událostí a logů (SIEM).
	+ sběr logů z různých zdrojů (servery, aplikace, síťové prvky, bezpečnostní zařízení) do jednoho centralizovaného úložiště;
	+ Pokročilá analýza a korelace, identifikace souvislostí mezi událostmi a detekce komplexních bezpečnostních hrozeb pomocí korelací a analytických pravidel;
	+ Real-time monitoring a alerting, monitorování událostí v reálném čase a automatické upozorňování na podezřelé aktivity;
	+ Podpora pro forenzní analýzu, dlouhodobá retence logů a nástroje pro efektivní vyhledávání a analýzu pro účely forenzní analýzy;
	+ Generování reportů o bezpečnostních událostech a dodržování regulatorních požadavků.

Předmět plnění veřejné zakázky

Předmětem veřejné zakázky je dodávka, implementace a podpora řešení systému Log management a nástroje pro management a analýzu bezpečnostních událostí a logů (SIEM).

Nástroje Log Management a SIEM poskytují sdruženou funkcionalitu vycházející ze správy logů (Log Management) a správy bezpečnostních informací a událostí (Security Information and Event Management), přičemž obě tyto funkcionality jsou vzájemně úzce integrovány a poskytují své schopnosti v rámci jednotného uživatelského rozhraní a dalších vzájemných integrací, které podporují činnosti bezpečnostních týmů, ať už se jedná o Security Operations Center (SOC), nebo o interní IT oddělení. Log Management zajišťuje centralizovaný sběr, ukládání, normalizaci a vyhledávání v logovacích datech z různých zdrojů IT infrastruktury. SIEM pak nad těmito daty provádí pokročilou analýzu, korelaci událostí, detekci anomálií a generování bezpečnostních upozornění, čímž umožňuje proaktivní detekci a reakci na bezpečnostní incidenty.

Objednatel očekává nabídku na technické řešení, které bude do jeho prostředí naimplementováno a po implementaci provozováno **po dobu 3 let**, přičemž po celou dobu bude řešení pokryto potřebnou licencí, technickou podporou výrobce a budou aktivovány všechny předplatné výrobce nezbytné k zajištění chodu řešení a splnění požadovaných funkcionalit.

Dodávané řešení musí splňovat funkcionality – Log management a SIEM

* Log Management (Správa logů):
	+ Centralizovaný sběr logů probíhá z heterogenních zdrojů, jako jsou servery, aplikace, síťová zařízení a bezpečnostní prvky, do jednoho centrálního úložiště;
	+ Indexace a vyhledávání zajišťuje efektivní indexaci logů pro rychlé vyhledávání a filtrování dat;
	+ Dlouhodobá retence logů ukládá logy po definovanou dobu pro účely auditu, forenzní analýzy a plnění regulatorních požadavků;
	+ Komprese a archivace logů optimalizuje úložný prostor pomocí komprese a archivace starších logů;
	+ Správa životního cyklu logů zahrnuje automatizované procesy pro archivaci, mazání a správu logů dle definovaných politik;
	+ Import a export logů umožňuje import logů z různých formátů a export pro další zpracování;
	+ Monitorování integrity logů zajišťuje integritu logů proti neoprávněným změnám.
* SIEM (Security Information and Event Management):
	+ Korelace událostí identifikuje souvislosti mezi událostmi z různých zdrojů a detekuje komplexní útoky;
	+ Detekce anomálií identifikuje neobvyklé chování a odchylky od normálního provozu;
	+ Analýza chování uživatelů a entit profiluje chování uživatelů a entit a detekuje podezřelé aktivity;
	+ Real-time monitoring a alerting monitoruje události v reálném čase a automaticky upozorňuje na podezřelé aktivity;
	+ Správa bezpečnostních pravidel a korelací umožňuje definování a správu pravidel pro detekci bezpečnostních incidentů;
	+ Vizualizace dat a dashboardy graficky zobrazují data a klíčové metriky pro lepší přehled a analýzu;
	+ Reportování a reporting generuje reporty o bezpečnostních událostech a dodržování regulatorních požadavků;
	+ Threat intelligence integrace umožňující získávat informace z databáze hrozeb pro detekci známých útoků;
	+ Forenzní analýza poskytuje nástroje pro efektivní vyhledávání a analýzu logů pro účely forenzní analýzy;
	+ Audit a compliance podporuje plnění regulatorních požadavků a auditů.

Všechny komponenty řešení Log management a SIEM požaduje Objednatel provozovat v režimu on-premise (tedy ve své vlastní infrastruktuře). Tento požadavek vychází z potřeby nepřetržité možnosti sbírat logy, ukládat je a vyhodnocovat bezpečnostní události i v situaci, kdy je vlivem provozní nedostatečnosti nebo působením kybernetické hrozby nedostupná internetová konektivita.

Přípustná integrace s online / CLOUD službami je pouze pro aktualizační služby a získávání informací o hrozbách. V případě nedostupnosti internetové konektivity umožní řešení manuální dodání aktualizací pro Log management a SIEM (řešení musí umožňovat fungování v tzv. režimu Air-Gap).

Není přípustné předávat data z prostředí Objednatele ke zpracování k výrobci nabízeného řešení, pokud tuto aktivitu manuálně a pouze pro konkrétní vyšetřování neiniciuje pracovník Objednatele nebo SOC.

Parametry poptávaných komponent bezpečnostního řešení

Požadavky na technické funkcionality řešení

Všechny parametry požadované v tomto dokumentu jsou pro dodavatele závazné a Objednatel vyžaduje jejich naplnění.

Požadavky na vybrané funkcionality poptávaného řešení, které Objednatel vyžaduje splnit technickými prostředky, a u nichž dodavatel musí popsat způsob, kterým jím nabízené řešení naplní daný požadavek, jsou specifikovány v tabulce, která tvoří přílohu zadávací dokumentace. Nedílnou přílohou Zadávací dokumentace je dotazník „Priloha 4\_SIEM\_technicka\_specifikace\_v2.xlsx“, ve kterém dodavatel potvrdí připravenost nabízeného řešení splnit vybrané požadavky a vyplní způsob, kterým je každý požadavek naplněn (žlutě označená pole).

Objednatel upozorňuje, že nesplnění kteréhokoliv požadavku na technické funkcionality řešení povede k vyloučení dodavatele ze zadávacího řízení. V případě, že bude nesplnění takového požadavku odhaleno až v průběhu provádění plnění, bude to považováno za hrubé porušení povinností a bude důvodem pro odstoupení od této smlouvy.

Požadavky na plnění

Objednatel očekává dodávku komplexního řešení, která bude sestávat z jednorázových projektových činností, dodávky nástroje se souvisejícími technickými komponenty a průběžných služeb dodavatele řešení.

Jednorázové projektové činnosti

Jednorázové projektové činnosti jsou nedílnou součástí dodávaného řešení, jsou zahrnuty mezi akceptační milníky a je k nim vázána etapizace dodávky a fakturace.

Před-implementační analýza

Před-implementační analýza popisuje způsob a podmínky nasazení řešení do prostředí Objednatele. Dokument musí popisovat charakteristiku dodávaného technického řešení, popis jednotlivých jeho komponent, navrhovaný způsob zapojení do prostředí Objednatele a samozřejmě způsob vzájemné integrace komponent.

Dokument musí mít charakter detailní technické specifikace pro všechny uvažované implementační postupy, na jejichž předběžném schválení závisí umožnění provádět technické zásahy do prostředí Objednatele.

Výstupem tohoto kroku bude dokument obsahující alespoň:

* Popis dodávaného SW řešení a jeho komponent
* Návrh architektury dodávaného řešení v prostředí Objednatele
* Detailní popis implementačních kroků
* Detailní technická specifikace:
	+ Síťové segmenty pro správu technologie
	+ IP adresace
	+ HW požadavky na virtualizační platformu Objednatele (HW platformu pro běh poptávaného řešení zajišťuje Objednatel)
	+ Požadavky na síťové prostupy
	+ Požadavky na přístup do internetu
	+ Požadavky na vzdálený přístup pro správu technologie
* Postup vzájemné integrace komponent řešení
* Požadované součinnosti na Objednatele
* Návrh akceptačních testů
* Specifikace kroků, součinností dodavatele a jejich rozsah v MD, při ukončení projektu (exit plán), které budou součástí poskytované služby
* Detailní harmonogram implementace řešení

Instalace a konfigurace řešení

V této části projektu dojde k dodání, instalaci a konfiguraci všech komponent SW řešení, které naplní požadavky předmětu veřejné zakázky a naplní specifika projektu uvedená v dokumentu před-implementační analýza.

Výstupem tohoto kroku bude funkční SW řešení, které bude:

* Obsahovat všechny potřebné licence, předplatné a technické podpory výrobce.
* V souladu se schválenou architekturou.
* Zcela funkční pro výkon požadovaných funkcí LM/SIEM, tak jak Objednatel požaduje v této technické specifikaci.
* Schopno vyhovět definovaným akceptačním testům v rozsahu specifikovaném v před-implementační analýze.

Napojení dat

Do SIEMu musí být napojeny minimálně definované zdroje dat a to v takové kvalitě aby nat těmito zdroji bylo možné provádět jednotné vyhledávání (nezávisle na zdroji dat dohledat přihlášení uživatele jedním unifikovaným dotazem nad všemi systémy, změna nastavení systému,…)

* Cisco Tacacs+
* Cisco Switch s IOS
* Cisco Router s IOS
* Eset Era
* FreeRadius
* Linux
* Microsoft Windows
* OpenLDAP
* OpenVpn
* Shibboleth
* Sysmon for Windows
* XCP-ng

Optimalizace bezpečnostní / detekční politiky řešení

V této části projektu bude dodavatelem provedeno vyhodnocení účinnosti nasazeného řešení, upravena bezpečnostní / detekční politika a zdokumentovány všechny provedené konfigurační úpravy, které vedou k vyšší efektivitě detekce pro budoucí analytický tým SOC Objednatele.

Výstupem tohoto kroku bude funkční SW řešení, které bude mít upravenu bezpečnostní / detekční politiku tak, že bude minimalizován objem falešných detekcí (false positive). Objednatel požaduje provedení alespoň následujících činností:

* Zohlednění reálných dostupných IP adresací Objednatele v detekčních politikách.
* Upřesnění konkrétních druhů validních aktiv Objednatele zaznamenaných v komunikacích, které jsou důležité pro fungování detekčních pravidel (DNS, SMTP, WEB, NTP, PROXY, MS AD).

Aplikace výjimek, které doporučí Objednatel.

* Zajistit všechny potřebné licence, předplatné a technické podpory výrobce.
* Zajistit soulad se schválenou architekturou.
* Dodat zcela funkční řešení pro výkon požadovaných funkcí LM a příjem logů ze Zadavatelem specifikovaných zdrojů dat, tak jak Zadavatel požaduje v této technické specifikaci.
* Dodat zcela funkční řešení, které je schopno vyhovět definovaným akceptačním testům v rozsahu specifikovaném v před-implementační analýze.

Součástí dodání je 50+ odladěných relevantních korelačních pravidel které pracují nad zadanými zdroji dat a 1000+ dalších pravidel které je možné v systému aplikovat (nemusí být nutně aplikovatelné na zadané zdroje dat)

Výrobce systému musí v pravidelném intervalu min 1\* za měsíc aktualizace na existující korelace a vytvářet nové korelace.

### Dokumentace řešení

Zadavatel požaduje, aby součástí dodávky byla ucelená a úplná dokumentace dodaného řešení. Dokumentace musí být dodána v českém jazyce (nebo v angličtině s výslovným souhlasem zadavatele) a musí být předána v elektronické podobě ve formátu PDF, případně v jiném otevřeném formátu dle dohody se zadavatelem.

Dokumentace bude sloužit pro účely provozu, správy a dalšího rozvoje řešení v prostředí zadavatele a musí obsahovat zejména následující části:

* Detailní přehled architektury dodaného řešení, popis jednotlivých komponent, jejich funkcionality a vzájemných vazeb.
* Podrobný popis konfigurace jednotlivých částí řešení v prostředí virtualizační platformy zadavatele. Dokumentace musí být přizpůsobena použité virtualizační technologii zadavatele.
* Popis možností a postupů pro integraci nástroje se systémy zadavatele – např. zdroje logů, SIEM systémy, identity management, e-mailové notifikace apod.
* Doporučené postupy pro zabezpečení jednotlivých komponent systému, včetně síťové komunikace, uživatelských přístupů a uchovávání dat.
* Seznam běžných provozních scénářů a nejčastějších problémů včetně postupů pro jejich identifikaci a řešení.

Všechny upravené konfigurace budou zdokumentovány a předány jako výstup této části projektu.

### Školení

Dodavatelem projektu bude provedeno zaškolení technického servisního týmu Zadavatele. Cílem je přenesení znalostí o správě dodaných nástrojů a předání rutinní správy na tým Zadavatele.

Výstupem tohoto kroku bude realizované školení se zaměřením na využívání a správu technického řešení Log management a SIEM:

* Prezenční školení servisního týmu Zadavatele, který nominuje maximálně 5 pracovníků a bude požadovat naplnění časové dotace alespoň 4 MD.
	+ Administrátor systému:
		- komponenty systému;
		- konfigurační parametry komponent;
		- ladění výkonnostních a kapacitních parametrů řešení;
		- troubleshooting; a
		- update a upgrade.
	+ Uživatel systému:
		- práce se systémem;
		- prohledávání dat;
		- vytváření reportů; a
		- obohacování dat.

Konzultace nad rámec specifických požadavků ZD

Dodavatel poskytne pro Objednatele služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 10 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb Objednatele. Jedná se o rozvojové aktivity, které budou souviset především ve změnami v prostředí Objednatele, které mohou mít dopad na provoz řešení LM/SIEM.