Příloha č. 4 – Technická specifikace

Popis stávajícího stavu

Z důvodu kompatibility celkového řešení uvádí zadavatel stručný přehled současných HW a SW technologií, přehled aplikací a podstatné informace o již instalovaných i očekávaných řešeních v rámci již proběhnuvších zakázek, ale i zakázek, které jsou ve stádiu realizace, nebo které se připravují.

Network Core LAN: Cisco C6800/HA, Core DC: Nexus9300/HA, 5xC4500, 11xC9400, 10xC3650

Network lokality (14+): 70+ Cisco C3650PoE (v procesu realizace), 10+ Cisco 2960PoE

Internet: ASR1001X/HA, ASA5585X/HA, 2x C3850 (stack DMZ)

WiFi: WLC5520/HA, 100+ AP (80+ AIR LAP 1142, 20+AIR LAP 2702)

VPN: C5515/HA, MS Certifikační autorita pro VPN a WiFi navázaná na MS AD (2008R2)

Network management: zkonfigurován 802.1X – vazba na MS AD, Cisco ISE/HA, Cisco Prime Infrastructure

SAN: 2x Brocade 6520, BNA

Disková pole:

- blokový přístup: 2x IBM Storwize V7000 (3tier)
- souborový přístup: 2x IBM Storwize V5000 (1tier) + 5 NAS serverů pro CES služby s GPFS

Virtualizace:

- 2x IBM p740 (11 virtuálních LPAR, AIX, 2x Oracle Standard Edition RAC, 9x Oracle Standard Edition single instance, 3x Oracle Enterprise Edition single instance), ver 11g
- VMware interní: 8x DL380G9, 120+ virtuálních serverů (80+ Microsoft, ostatní Linux, z aplikací: MS SQL DB cluster, MS Exchange 2010 - 2x CAS, 2x HUB)
- VMware externí: 2x DL380G8, 10+ virtuálních serverů
- 2x Fujitsu Siemens M10, Solaris, Oracle HSM

Backup:

- VEEAM backup and replication Enterprise: VMware
- IBM Spectrum Protect: ostatní Linux/Unix systémy

Doména:

- MS AD, DC 2008R2, FS na 2012R2
- 1900 klientů¨

Antivir:

- TrendMicro – Enterprise Security for Endpoints Light, Damage Cleanup Services, Mobile Security

Antispam:

- Symantec Messaging Gateway

Vlastní dohled: 2x Zabbix instalace, Cisco Prime Infrastructure

Centrum sítě ve stadiu rekonstrukce/2018 - původní řešení, postavené na Cisco 6509/VSS s přístupovými switchi C3560G a C6506 a C2960PoE je nahrazováno centrem rozděleným na část serverovou (DC), založenou na technologii Cisco Nexus 9300 v HA s FEX moduly a část přístupovou (LAN) s Cisco Catalyst 6880/VSS, na kterou jsou připojeny patrové rozvaděče se switchi C9400 a C4500, doplněné ve 3 patrech pro zvýšení dostupnosti o switche C3650.

Připojení do internetu (dvě nezávislá vedení na jednoho providera) je řešeno dvojicí routerů ASR1001X oddělených od vnitřní sítě dvojicí firewallů ASA5585X, ke kterým je připojena DMZ na stacku switchů C3850.

WiFi je realizováno na dvou kontrolerech Cisco WLC5520 s 100+ AP Cisco 1142 a 2702, které budou postupně nahrazovány novějšími a výkonějšími typy 28XX.

WAN síť 16 lokalit je realizována jako full mesh přístupem z CE boxů umístěných v ČRo na PE boxy poskytovatele veškerá infrastruktura je zdvojená (technologie Cisco).

LAN sítě v regionech jsou většinou realizovány na switchích Cisco 3560G a 2960PoE, které budou postupně nahrazovány (část v 2018 a zbytek v následujícím roce) typem C3650 s PoE+ a dvěma zdroji pro zajištění vyšší dostupnosti. V regionech je umístěno cca 70+ switchů.

Základní přehled SW a HW vybavení zadavatele

V této části je uveden přehled základního vybavení zadavatele z hlediska používaných SW a HW technologií používaných zadavatelem příp. předpokládaných.

Oblast využití	Platforma	Popis
Operační systémy SW pracovní stanice	Microsoft Windows 7, Windows 10 Apple macOS 10.x	Většina konc. Stanic W7 (1800+), nové nákupy W10 (100+), pro práci se zvukem Mac (50+)
Operační systémy – servery	Microsoft Windows Server 2008, 2012, 2016, Standard/Datacenter Linux RedHat, CentOS, Debian IBM AIX 7.X Oracle Solaris 11.3	Většina WS Datacenter ve Vmware 8xhw prostředí, AIX na virtualizovaném 2xhw pro konsolidované prostředí Oracle aplikací, Solaris pro 2xhw HSM archiv
Operační systémy – virtualizace	VMware 5.5, 6.0, 6.X AIX 7.X	Interní 8xhw a externí 2xhw (DMZ), AIX LPAR virtualization na 2xhw
Databáze	Oracle Standard Edition 11.2 Oracle Enterprise Edition 11.2 MS SQL 2010, 2012, 2016 Postgres	V AIX prostředí, EE pro SAP/R3, MS SQL HA ve VMware pro 8 aplikací Monitoring zabbix
Integrace ESB	Talend	Pro integraci EDMS s ostatními systémy
Portálová řešení Redakční systém	Drupal iNews/ 2019 nahrazován OpenMedia	Intra / extranet
Řízení přístupu	MS AD, DC Cisco ISE, 802.1X	Sdílení dat, Exchange, VPN, WiFi,
Zálohování Snapshoting	IBM Spectrum Protect VEEAM	Centrální zálohování, Zálohy ve VMware prostředí

Oblast využití	Platforma	Popis
Firewall, router	Cisco ASA5585X, ASR1001X, Cisco 2811,2911, Cisco 819 ISR	2x v HA, 2 cesty k poskytovateli (BGP), Voice gw pro ICT, Pro dočasné přenosy (WiFi, 3G/4G)
Antivirová ochrana	Trend Micro, Symantec Brightmail	EPP, antispam v DMZ
Servery	HP Proliant DL3xxG[6-9], IBMp740, Fujitsu-Siemens M10,	
Aktivní prvky LAN	Cisco Nexus 9300, Cisco Catalyst 6880, Cisco 450x, 94xx, 3650PoE, 2960XPoE, 3560X, 3850	Core v HA: 2x N9300, 2x C6880, Patra: C450x, C94xx, C3650X (vše PoE) Regiony: C3650X PoE
SAN	Brocade 6520	HA – 2xhw
Diskové pole	IBM V7000, IBM V5010 + GPFS Synology RSxxxx	Block storage Tier0-2 2xhw v hyperswap File storage Tier-2, GPFS (CIFS, NFS, FTP)/10G 2xhw, mirror
Tape	IBM TS4500, Oracle SL-150	Virtualizace TS4500 - Centrální backup IBM Spectrum Protect, HSM část přes Oracle HSM
Doména	MS AD, 2008R2, FS 2012, 2016	Microsoft Active Directory, DNS, DHCP
Mail	MS Exchange 2010	mailový systém
ICT	Cisco CUCM/HA, UCCX/HA, VGW 2811/HA, VGW 2911/HA, 2RING	IP telefonie, kontaktní centrum, tarifikace
ERP aplikace	SAP/R3, AIX LPAR, Oracle EE	produkce, vývoj, test
CRM aplikace	is.USYS.net, AIX LPAR, Oracle SE, RAC	produkce, test
DMS aplikace	vm, WS 2012, MS SQL 2016/HA	EDMS produkce, test
AIS aplikace	AIX LPAR, Oracle SE, RAC	vlastní vývoj – podpora vysílání, archivy, produkce, vývoj, test
DI aplikace	vm, VARS, MS SQL 2016	podpora dopravního vysílání
Redakční systém	vm, WS 2012, OpenMedia	náhrada redakčního systému 2019
Vysílací systém	vm, DALET Plus	vysílání
Redakční systém	hw, RHEL, iNews/AVID	starý redakční systém

Zadavatel si vyhrazuje právo případné změny ve vybavení ICT nebo změny týkající se zvýšení dostupnosti a bezpečnosti.

Zadavatel používá pro umístění ICT a aplikační infrastruktury lokalit DC, kdy je podporováno při výpadku zpracování v primární lokalitě zajistit zpracování v záložní lokalitě. Vysoké dostupnosti zpracování se rovněž dosahuje prostřednictvím serverové virtualizace, kde se zpracování realizuje na virtuálních serverech. Součástí implementační analýzy bude i popis celkového dodávaného řešení ICT pro zajištění funkčnosti systému včetně dodávaných a využívaných technologií (infrastruktura), popisu dodávky, montáže a instalace, implementace, harmonogramu, záručního a pozáručního servisu, SLA.

Zadavatel na výše uvedené technologie má proškolené pracovníky. V případě dodávky rozdílných technologií vyžadujeme dodávku včetně školení výrobcem zařízení a SW a kompletní dokumentaci!

Využitelnost ICT vybavení zadavatele

Zadavatel podporuje nastavení standardního prostředí Systému pomocí technologií MS. Pro uvedená SW prostředí disponuje zkušenými administrátory s možností instalace a administrace, a může

poskytnout licence v rámci smlouvy Enterprise Agreement pro účely zajištění Projektu. V této souvislosti může poskytovatel využít následující licence:

- MS Windows Server DataCenter/SA
- VEEAM Backup and Replication Enterprise
- VMware 6.x
- IBM Spectrum Protect

Uvedené licence jsou pro uchazeče využitelné. Zadavatel nepoptává licence VMware při volbě SW řešení SIEM, protože v současné době licenčně pokrývá dostatečné zdroje ve virtualizaci.

Pokud poskytovatel dodá zadavateli další technologie nad rámec technologií MS jakožto standardu, je potřeba, aby zajistil a dodal jejich licenci s podporou, administrací a zajistil zadavateli odpovídající počet certifikovaných administrátorských školení (úrovně základní školení, pokročilá školení) a zajistil kompletní produktovou originální dokumentaci (např. instalační, uživatelskou, administrátorskou, školící dokumentaci) ve vyčerpávajícím rozsahu a další vhodnou a dostupnou dokumentaci k takovým produktům.

Předmětem výběrového řízení je komplexní řešení bezpečnostního monitoringu kybernetického prostoru zadavatele, které dokáže detekovat neobvyklé chování, případně upozornit i na hrozbu v organizaci zadavatele. Tento systém bezpečnostního dohledu a správy umožní shromažďovat informace o proběhlých událostech, zranitelnostech a síťových tocích z různých systémů a zdrojů logů (firewall, HW, AD, switche, IDS/IPS, DLP, EDP, zálohování, skenery, interní aplikace, atd.), sjednocovat je do jednoho místa a následně je korelačně vyhodnocovat v kontextu organizace a s obohacením o externí zdroje threat intelligence. Platforma a její rozšíření musí umožňovat bezpečnostní dohled a integraci všech technologií, sběr logů a jejich vyhodnocení s následnou korelací na jednom místě. Řešení bezpečnostního monitoringu bude doplněno o komplexní nástroj pro monitoring databázových aktivit.

Tato příloha obsahuje podrobné vymezení předmětu veřejné zakázky. Požadavky specifikované v přiložených tabulkách této přílohy považuje zadavatel za minimální a na jejich splnění zadavatel trvá.

Požadavky jsou rozděleny po oblastech plnění zakázky.

<u>Předmět veřejné zakázky se skládá z následujících částí:</u>

A. **Dodávka SW licencí řešení bezpečnostního monitoringu a monitoringu databází**

B. **Implementace řešení bezpečnostního monitoringu a monitoringu databází**

C. **Poskytování služeb technické podpory provozu a správa řešení bezpečnostního monitoringu a monitoringu databází**

<u>Jednotlivé etapy předávání díla</u>

Dílo bude realizováno a předáváno po etapách. Etapy vycházejí z hrubého harmonogramu, který je uveden v ZD. Začátek každé etapy je vázán protokolárním převzetím předchozí etapy zadavatelem na základě akceptačního protokolu.

a) První etapa zahrnuje:

- detailní definici architektury systému a identifikování platforem pro integraci - zadání implementace
- vypracování implementačního plánu na základě architektury hrubého harmonogramu

- dodávku SW řešení bezpečnostního monitoringu dle technických požadavků v článku C této Přílohy, včetně podpory výrobce na 3 roky
- akceptaci první etapy

b) Druhá etapa zahrnuje:

- implementaci řešení - viz článek B této Přílohy
- akceptaci a převzetí implementované části díla do provozu

c) Třetí etapa zahrnuje:

- provoz a podporu systému po dobu 3 let
- konzultační postupný rozvoj řešení

A. Dodávka a implementace řešení bezpečnostního monitoringu a monitoringu databází a souborových systémů

a. Shrnutí základních požadavků řešení na dodávku bezpečnostního monitoringu a monitoringu databází a souborových systémů

Řešení bezpečnostního monitoringu postavené na Security Information and Event Management systému (dále jen „SIEM“) je jedním ze základních stavebních prvků, který zajišťuje nutné bezpečnostní informace pro plnění povinností vyplývajících ze Zákona o kybernetické bezpečnosti a příslušných vyhlášek. Bez SIEM nástroje nelze reálně splnit požadavek na detekci bezpečnostní události a následného hlášení kybernetického bezpečnostního incidentu dle § 7 a § 8 zákona 181/2014 Sb.

Poptávané řešení bezpečnostního monitoringu bude dodáno jako ucelená platforma pro sběr a vyhodnocování bezpečnostních událostí. Poptávané řešení poskytne log management, event management, reporting a analýzy chování pro sítě a aplikací a uživatelů. Součástí řešení musí být doplňující moduly pro rozšíření funkcionality a zpřesnění detekce a správy zranitelností, pro efektivní práci a korelaci zranitelností.

Řešení pro monitoring databází bude dodáno jako samostatný systém pro monitoring databázových aktivit s možností automatického zastavení nežádoucí akce. Jeho smyslem je zajistit kvalitní a maximálně dostupný audit klíčových databází s minimálním dopadem na výkon vlastních databází. Řešení bude v rámci implementace integrováno s řešením pro bezpečnostní monitoring do jednoho celku.

Poptávaná implementace má za cíl zavést řešení bezpečnostního monitoringu a integrovat platformy až na úroveň aplikací, tedy databáze, operační systémy a infrastrukturu. Integrace samotných aplikací není součástí tohoto zadání a bude realizována postupně v rámci konzultačního rozvoje řešení.

b. Řešení bezpečnostního monitoringu

- Zákazníky prověřené řešení, hodnocené jako leader v Gartner Magic Quadrant pro SIEM řešení

- Podpora řešení na 3 roky

- Shromažďování logů o událostech ze zařízení a aplikací na síti

- Komplexní zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase

- Monitorování chování v síti, tvorba přehledných reportů a přístup ke všem informacím z webové konzole
- Identifikace a kategorizace zranitelností
- Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak zranitelnost odstranit.
- Možnost forenzního šetření a analýzy nad událostmi z mnoha typů zdrojů a zařízení
- Možnost filtrováni nalezených zranitelností a jejich prioritizace
- Možnost vytvářet pravidla pro korelaci nad filtry zranitelností
- Automatizovaná korelace událostí a následná reakce na identifikované problémy
- Zajištění souladu s regulatorními a legislativními požadavky
- Zajištění požadavků Zákona o kybernetické bezpečnosti
- Efektivní identifikace incidentů (snížení nákladů na jejich identifikaci)
- Techniky detekce hrozeb APT a "Zero-Day" útoků, včetně behaviorální analýzy
- Přístup k knowledge-base – rozšiřující informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak zranitelnost odstranit
- Podpora operačních systémů Windows/Linux, AIX, Solaris, síťových zařízení předních světových výrobců (switche, routery, firewally CISCO), databází (Oracle, MS SQL, Postgres), webových serverů (Apache, MS IIS), mail serverů (MS Exchange), DNS, DNSSEC
- Monitorování přístupu k datům, jejich modifikaci a umožnění aktivního zásahu proti neoprávněné činnosti.

c. Řešení pro monitoring databázových a souborových aktivit

- monitorování všech běžně komerčně používaných databází a BigData platforem, zejména Oracle (včetně ASO/SSL), Oracle RAC (včetně ASO/SSL), Microsoft SQL, IBM DB2 (Linux, Unix), PostgreSQL
- pravidelná detekce zranitelností (chybějící aktualizace, chyby v nastavení a další rizika), jejich prioritizace a doporučení, jak zranitelnosti odstranit
- klasifikace dat v souborových systémech
- tvorba přehledných reportů a přístup ke všem informacím z webové konzole
- zajištění souladu s regulatorními a legislativními požadavky
- podpora na 3 roky
- podpora operačních systémů Windows/Linux, AIX, Solaris
- integrace se SIEM systémem, LDAP

d. Základní architektura řešení

Zadavatel požaduje nasazení formou virtuálních/softwarových All-in-One appliance včetně síťové sondy pro sběr síťového provozu a generování síťových toků pro zpracování v řešení bezpečnostního monitoringu. Sonda bude dodaná také jako virtuální/softwarová pro možnost nasazení na HW zadavatele.

Řešení bezpečnostního monitoringu musí licenčně poskytovat dostatečné kapacity pro monitoring prostředí Zadavatele:

- 1 000 EPS (událostí za sekundu) a 120 GB dat za den
- 50 000 flow/min (síťových obousměrných toků)
- samostatná sonda pro sběr a zpracování síťového provozu a generování síťových toků
- neomezený počet logujících zařízení

Řešení monitoringu databází musí licenčně poskytovat dostatečné kapacity pro monitoring prostředí Zadavatele:

- 4 databáze Oracle (2x Oracle RAC)
- detekce zranitelností pro 4 databáze
- klasifikace dat v souborových systémech

Obě Řešení musí dále splňovat všechny požadavky z tabulky sekce C

B. Pravidla pro vyplňování technických parametrů řešení

Uchazeč vyplní v následujících kapitolách pouze všechny žlutě označené části.

Tato příloha slouží k uvedení názvu / typu konkrétního nabízeného řešení či zařízení a dále **k vymezení minimálních technických požadavků zadavatele na řešení a osvědčení jejich splnění uchazečem**. Požadavky zadavatele jsou uvedeny ve sloupci 1. Následná smlouva s vybraným uchazečem může být v této části upravena tak, aby obsahovala uchazečem nabídnuté zařízení a jeho technické parametry.

V níže uvedené tabulce (sloupci 1) jsou uvedeny veškeré povinné minimální parametry kladené na celý systém SIEM. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

C. Technická specifikace bezpečnostního monitoringu a monitoringu databází

Výrobce / název / typ zařízení / řešení: ……..……

Výrobce / název / typ zařízení / řešení: ……..……

Výrobce / název / typ zařízení / řešení: ……..……

Minimální technické požadavky			**„Popis jak bude požadavek splněn/řešen“**
1	Nabízené řešení musí být včetně podpory na 3 roky: nové verze, základní podpora		……

2	Nabízené řešení musí být postaveno na technologii od výrobce uvedeného v sekci leaders "Magic Quadrant for Security Information and Event Management" společnosti Gartner. Nabízené řešení musí tuto technologii obsahovat jako hlavní funkční celek a může její funkce dále rozšiřovat pro pokrytí všech požadavků zadavatele. Tento fakt musí být prokázán potvrzením výše v tomto bodě zmíněného výrobce.		……
3	Nabízené řešení musí být dodáno formou virtuální appliance se zárukou a maintenance dodavatele na appliance jako celek.		……
4	Nabízené řešení v případě, že je nabízeno jako All-in-One řešení, musí umožnit později upgrade na distribuovanou architekturu se zachováním stávajících licencí a HW.		……
5	Musí zahrnovat všechny komponenty pro Log Management, Event management, Flow Management, Korelace, příjem a sběr logů a síťového provozu, centrální správu a reporting a to včetně nestandardizovaných logů.		……
6	Licencování nabízeného řešení může být na počet událostí za sekundu (EPS) nebo na celkový objem dat za časový úsek.		……
7	Licence musí pokrývat zpracování min. 1 000 EPS a 50 000 flow/min (obousměrné toky).		……
8	Nabízené řešení musí podporovat neomezený počet zdrojů logů.		……
9	Nabizené řešení musí podporovat zpracování 120 GB událostí za den.		……
10	Nabízené řešení musí obsahovat databázi pro uložení dat (události, toky, korelované událsotí a další data) po dobu minimálně 6 měsíců. Využití externí databáze nedodávané uchazečem v rámci dodávky není akceptovatelné.		……
11	Nabízené řešení musí umožnit zálohování a archivaci dat (konfigurace, událostí, toků) mimo dodávané řešení.		……
12	Nabízené řešení musí umožnit zpracování krátkodobých špiček (60 min objemu událostí přesahující licenci, tak aby nedošlo k zahození událostí ale maximálně k prodlevě ve zpracování.		……
13	Nabízené řešení musí umožňovat volně definovat několik retenčních politik ukládaných logů na základě libovolných atributů.		……
14	Nabízené řešení musí uchovávat logy i flows jak v normalizovaném formátu, tak i v „raw“ formátu.		……
15	Nabízené řešení musí mít otevřený protokol a kompletní uživatelské rozhraní SIEM dostupné z webového browseru. Musí být jednotné, nevyžadovat více různých		……

	podpůrných technologií, pluginů nebo tlustého klienta. Rozhraní nesmí být postaveno na technologii flash.		
16	Nabízené řešení musí umožňovat definici vlastního atributu (číselného i textového) v událostech, do kterého je automaticky doplňována aktuální hodnota z logu nebo dopočítaná hodnota.		.....
17	Vlastní atribut nabízeného řešení musí být použitelný pro filtraci, drilldown i definice korelací napříč celým SIEMem		.....
18	Nabízené řešení musí umožnit rozšíření o doplňující informace pro účely reportingu, vyhledávaní nebo korelací. Tyto informace mohou přicházet z různých zdrojů jako jsou nejrůznější reputační databáze nebo interní doplňující informace.		.....
19	Nabízené řešení musí být dodáno spolu s IP reputační databází.		.....
20	Nabízené řešení musí obsahovat jednoduchý editor pro definici/správu korelačních pravidel bez znalosti programování či skirptovaní.		.....
21	Veškerá konfigurace a definice zdrojů logů nabízeného řešení musí probíhat z grafického rozhraní SIEM.		.....
22	Uložiště logů bude realizováno na externím diskovém úložišti, které zajistí zadavatel.		.....
23	Nabízené řešení musí umožnit zpětný import archivních či zálohovaných dat a jejich zpracování / vyhodnoceni.		.....
24	Řešení musí podporovat zpracování událostí minimálně ve formě: příchozího syslog (UDP/TCP/TLS), SNMP, log file, auditní tabulka v databázi, RPC/WMI pro Windows Events		.....
25	Řešení musí podporovat autodetekci zasílaných logů pomocí syslog		.....
26	Řešení musí poskytovat out-of-the box konektory pro široké spektrum systémů, minimálně: síťové prvky Cisco, Brocade, OS Windows, OS Unix/Linux, MS SQL, Oracle, Postgres. Tyto konektory musí být podporovány výrobcem SIEM a v rámci podpory pravidelně updatovány.		.....
27	Řešení musí podporovat oddělený sběr událostí a flow (Netflow/IPFIX)		.....
28	Sběr z prostředí MS Windows musí probíhat bez nutnosti instalace agenta na vlastní zdroj logů		.....
29	Řešení musí obsahovat průvodce "wizard" pro vytváření a editování reportů		.....
30	Řešení musí poskytovat oddělené rozhraní pro práci s vygenerovanými potencionálními incidenty - výstupy korelace.		.....
31	Řešení musí poskytovat klíčovou SIEM funcktionalitu - sběr logů, jejich vyhodnocení, kategorizaci a zpracování korelačním enginem, který na základě definovaných korelačních pravidel identifikuje potencionální incidenty a prezentuje je uživateli.		.....

32	Řešení musí být schopné korelovat nad raw daty. Například vytvořit incident na základě řetězce v payload logu.		……
33	Řešení musí podporovat korelaci s řetězením pravidel. Například pokud nastane incident a více korelačních pravidel vyhodnotí, že se jedná o incident, tak se v rámci řešení založí pouze jeden potencionální incident.		……
34	Řešení musí ve výchozím nastavení (tzv. out-of-the box) obsahovat předdefinovaná pravidla pro identifikaci základních typů hrozeb, útoků a incidentů (tj. získání informací, činnost botnetů, DoS a DDoS útoky, autentizace, exploit, malware a podezřelé aktivity a anomálie).		……
35	Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu. Alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků).		……
36	Součástí řešení musí být modul, který umožní prioritizaci zranitelností na základě reálných komunikací v infrastruktuře. Například závažnost zranitelnosti bude zvýšena, pokud sever komunikuje aktivně do internetu.		……
37	Součástí řešení musí mít samostatný modul integrovaný do GUI pro vyhodnocování chování uživatelů - UBA.		……
38	Řešení musí podporovat right-click rozšíření. Například po "najetí" na IP adresu se pomocí pravého tlačítka zavolá skript, který zobrazí dodatečné informace z externí databáze či online služby.		……
39	Řešení musí obsahovat otevřené API pro integraci se systémy třetích stran. Minimálně pro vyhledávání v datech, správu tabulek, práci s alerty a zařízeními.		……
40	Řešení musí obsahovat funkcionalitu obohacení logů s cílem obohatit vybrané příchozí nebo uložené logy o chybějící informace, jedná se především o doplnění IP adresy do logu, kde je pouze hostname a naopak, dále pak doplnění jména reálného uživatele k username.		……
41	Nabízené řešené musí poskytovat možnost integrace generovaných alertů na ticketovací/helpdeskový interní systém ve formou automatického i manuálního založení ticketu v rámci GUI řešení, včetně konfigurace takové integrace v GUI. Jednotlivé alerty musí být možné přidělit konkrétním uživatelům/řešitelským skupinám na základě druhu/jména alertu.		……
42	Nabízené řešení musí provádět kompletní audit administrátorské aktivity v rámci řešení (konfigurace pravidel, změna konfigurace) a musí umožnit v rámci GUI tyto auditní záznamy provázat s manuálně zadanými komentáři administátora tak, aby každá aktivita byla dokumentovaná a bylo zřejmé, proč byla prováděna.		……
43	Nabízené řešení musí umožnit automatické vytváření historické databáze identit na základě příchozích zpráv tak, aby bylo možné v jakémkoliv historickém okamžiku dohledat identitu uživatele ke konkrétní IP adrese, MAC adrese nebo hostname. Řešení umožní integrovat data z různých databází za účelem vytvoření jednotné databáze identit a k nim přiřazených uživatelských identifikátorů (AD username, lokální username, email, certifikát…).		……

44	Nabízené řešení musí v grafickém rozhraní umožnit vyhledávat v historii identit podle konkrétní IP adresy, MAC adresy, hostname a podle konkrétní uživatelské identity v čase.		……
45	Řešení musí obsahovat aktivní modul pro sdílení informací o aktuálních bezpečnostních hrozbách tzv. cyber threat intelligence, automatické aktualizace tohoto modulu musí být zahrnuty v ceně licence.		……
46	Řešení musí obsahovat modul pro management zranitelností, kterým lze ovládát (spouštět) skenovací úlohy skenerů třetí strany, importovat zranitelnosti k aktivům v SIEM a umožňovat jejich přidělení uživateli.		……
47	Řešení pro monitoring databází musí mít minimální dopad na výkon monitorovaného databázového serveru (max. navýšení zátěže o 5%)		……
48	Licence musí pokrývat monitoring pro 4 databáze včetně klasifikace dat v těchto databázích		……
49	Licence musí pokrývat funkcionalitu klasifikace dat v souborových systémech a připojených discích v celém interním prostředí zadavatele pro identifikaci citlivých informací		……
50	Licence musí pokrývat vyhledávání zranitelností na 4 databázových serverech v pravidelně se opakujícím intervalu		……
51	Řešení musí umožňovat vytváření vlastních klasifikačních pravidel dle a) regulárních výrazů, b) porovnání se slovníkem, c) programovatelného API rozhraní		……
52	Řešení pro monitoring databází musí být schopné archivovaná data ukládat v šifrované podobě		……
53	Řešení musí tvořit jeden logický celek a jednotlivé komponenty musí být vzájemně propojitelné, zejména monitoring databází a monitoring bezpečnostních událostí musí být vzájemně integrované		……
54	Řešení musí být schopno analyzovat databázová data v reálném čase a poskytovat možnost aktivního blokování dle IP adresy zdroje a cíle, uživatelského jména , databáze, tabulky, sloupce nebo typu databáze		……
55	Řešení musí umožňovat vyhledávání dalších databází v infrastruktuře		……

56	Auditní záznamy musí být možné ukládat, pořizovat a přistupovat k nim tak, aby nebyla možná jejich modifikace ze strany databázového správce, případně dalších privilegovaných uživatelů		……
57	Řešení musí umožňovat dle nastavených politik maskovat citlivá databázová data, například pro potřeby testování		……
58	Řešení musí obsahovat modul pro zhodnocení zranitelností databází, který bude pokrývat minimálně: - CVE identifikaci - konfigurační zranitelnosti a slabiny dle CSI a STIG standardů - identifikaci nadměrných oprávnění a překryv oprávnění		……
59	Řešení musí poskytovat informace od DNS (dotaz i odpověď) provozu ze sítě a exportovat je ve formátu síťového toku (NetFlow, IPFIX nebo obdobné)		……
60	Řešení musí umět zobrazit profily provozu ve tvaru počet bajtů, paketů a komunikujících stran o všech aplikacích, portech, protokolech, hrozbách a každém monitorovaném místě sítě		……
61	Řešení musí podporovat rozpoznávání aplikací jinak, než jen pomocí portů. Systém musí podporovat identifikaci aplikace používající jiné než obecně používané porty nebo aplikaci tunelující se na jiných portech (např. HTTP jako transportní protokol pro IM messenger by měl být rozpoznán jako Instant messenger, nikoliv jako HTTP)		……
62	Řešení musí detekovat “zero-day” události		……
63	Řešení musí mít schopnost dynamického učení běžných norem chování a odhalit změny vůči těmto normám		……
64	Řešení musí detekovat DoS a DDoS útoky		……
65	Řešení musí detekovat hrozby v síti a prezentovat veškerý provoz související s těmito hrozbami. Popište typy detekovaných hrozeb a možnosti jejich zobrazení		……
66	Řešení musí profilovat provoz podle TCP a UDP portů.		……
67	Řešení musí identifikovat provoz potenciálně riskantních aplikací (např sdílení souborů, P2P, atd.)		……

68	Řešení musí profilovat a prezentovat informace v různých časových rámcích. Musí být dostupné týdenní, denní a hodinové profily. Uveďte minimální a maximální časové rámce dostupné pro profilování a analýzu.		……
69	Řešení musí umět profilovat komunikaci přicházející z/odcházející do internetu podle geografické lokace (IP geolokace) v reálném čase		……
70	Řešení musí rozlišovat lokální provoz a provoz z/do internetu		……
71	Řešení musí umožnit uživateli vytvářet vlastní profily a pohledy s využitím libovolných síťových toků, logů, zdrojů dat anebo už z profilovaného provozu.		……
72	Řešení musí podporovat profilování provozu na základě IP adresy, skupiny IP adres, dvojice zdrojové a cílové IP adresy, atd.		……
73	Řešení musí podporovat sběr a analýzu dat zachycených paketů		……
74	Řešení musí mít schopnost extrahovat specifické, uživatelem definované položky paketového záchytu a využít tato data v korelačních pravidlech		……
75	Řešení musí být schopné analyzovat síťový provoz uvnitř virtuálního prostředí (VMware)		……
76	Pokud je součástí agentní řešení, musí agenti podporovat instalaci na tyto OS: Windows Server 2008, 2012, 2016 Red Hat Enterprise Linux 4, 5, 6, 7 Oracle Linux 4, 5, 6, 7 SuSE Enterprise Linux 11, 12 AIX 7.1, 7.2 Solaris 11.3		……

D. Požadavky na implementaci řešení

Implementace se skládá z následujících fází:

1. Úvodní analýza nasazení
   - Diskuze a určení metody sběru logů pro jednotlivé platformy
   - Příprava tabulky zdrojů logů určených k integraci (tabulka slouží pro evidenci stavu integrovaných systémů a je klíčovým dokumentem implementace)
   - Výběr metody sběru logů z prostředí MS Windows (WinCollect agent, jiné...)
   - Návrh metod zálohování a archivace dat
2. Příprava dokumentace a návodů pro nastavení zdrojů logů zaměstnanci Zadavatele

3. Instalace virtuálních appliances řešení do infrastruktury Zadavatele, základní napojení, integrace bezpečnostního monitoringu a řešení monitoringu databází
4. Instalace agentů řešení pro monitoring databází na požadované DB
5. Nastavení zdrojů logů uvedených v tabulce zdrojů logů (odpovědnost Zadavatele), napojení na řešení bezpečnostního monitoringu, tvorba nezbytných konektorů, kontrola správnosti parsování, nastavení sběru NetFlow
6. Vytvoření uživatelských rolí, profilů a účtů; integrace ověřování proti AD
7. Analýza požadavků na korelace – use cases
   - Poskytnutí best practice use cases a dizkuze jejich vhodnosti pro Zadavatele
   - Zapracování Zadavatelových požadavků na korelace formou use cases
   - Vytvoření finální tabulky use cases pro implementaci formou reportů a pravidel
8. Nastavení pravidel a reportů dle analýzy use cases
   - Úprava přednastavených pravidel a reportů
   - Tvorba specifických pravidel a reportů
   - Příprava dashboardů
   - Konfigurace neuzbytných rozšíření pro pokrytí use cases
9. Fine-tuning pro nízká false positive hlášení
10. Školení pracovníků Zadavatele v rozsahu 2 dnů
11. Celková dokumentace implementace:
    - Provozní dokumentace (Administrátorská příručka),
    - Uživatelská dokumentace,
    - Bezpečnostní dokumentace

E. Poskytování služeb technické podpory provozu a maintenance řešení bezpečnostního monitoringu

Poskytovatel bude poskytovat Objednateli služby spočívající v zajištění podpory řešení bezpečnostního monitoringu (dále jen „Služby“).

Povinnost Poskytovatele zahrnuje:

1. Služby servisní podpory
   - Poskytování nových verzí SIEM a opravných patchů dle aktuální technologické úrovně,
   - Podpora certifikovaného bezpečnostního konzultanta,
   - Poskytování služeb monitoringu a dohledových služeb nad řešením bezpečnostního monitoringu i řešení po monitoring databází
   - Poskytování služby HotLine/Helpdesk včetně servisní technické podpory SIEM dle parametrů SLA sjednaných touto Smlouvou.
   - Odezva další pracovní den (NBD) na incident
   - Služba dostupná 8x5 (9.00 – 17.00) v pracovní dny (po-pá)
   - Servisní podpora pokrývající celé implementované řešení

2. Konzultační služby
   - Školení dle požadavků Objednatele nad sjednaný rozsah
   - Analýza logování aplikací na základě obecných požadavků
   - Tvorba konektorů, napojování aplikací
   - Konzultační podporu v rozsahu, ve kterém si to Objednatel objedná.
   - Součinnost při řešení systémových problémů a při implementaci systémů třetích stran.
   - Spolupráce při tvorbě koncepce a při koordinaci budování SIEM Objednatele.
   - Úpravy a funkční doplnění SIEM dle požadavků Objednatele.
   - 12 předplacených člověkodní na rok

Služby budou poskytovány po dobu 3 let.