Příloha č. 1
Specifikace předmětu plnění

Kvalita návrhu plnění 16

TECHNICKÁ SPECIFIKACE 20

Kvalita návrhu plnění

Zhotovitel předkládá popis řešení dílčích funkcionalit tak, jak bude splněn nabízeným produktem/řešením. Specifikace je pro dodavatele závazná zároveň zahrnuta do smlouvy na plnění veřejné zakázky jako její příloha (příloha č. 1 návrhu smlouvy o dílo).

1. **způsob řešení platformy pro řešení incidentů** - v rámci tohoto subkritéria bude jako nejvhodnější hodnoceno řešení umožňující, poté co platforma SIEM zachytí a vyhodnotí bezpečnostní událost, vygenerovaní procesu následující reakce – řešení incidentu s nejvyšší mírou automatizované orchestrace vyřešení incidentu a dynamické obohacení o informace z reputačních zdrojů či lokálních zdrojů (např. Active Directory), před řešeními vyžadujícími manuální řešení pomocí lidského faktoru,

Popis způsobu řešení:

Produktové řešení naplňující požadovanou funkcionalitu:

IBM Security QRadar SIEM, IBM Resilient IRP

Popis jak je daná funkcionalita řešena:

Pro řešení bezpečnostních incidentů nabízíme nástroj IBM Resilient Incident Response Platform (IRP). Tento nástroj umožňuje snadno řídit lidské zdroje, procesy a technologie tak, aby incidenty byly řešeny co nejrychleji, standardizovanou cestou a co nejvíce automatizovaně. Resilient poskytuje řešitelům informace vedoucí k jejich rychlému vyšetření a uzavření, a to pomocí obohacení incidentů integracemi s dalšími nástroji a podnikovými systémy. Založení incidentů probíhá několika způsoby - většina incidentů vzniká integrací se QRadar SIEM systémem, ale protože některé incidenty nejsou detekovány QRadar SIEM systémem (např. ztráta notebooku či hlášení podezření o úniku dat atd.) existují i další způsoby, jako např. integrace s IT service management nástroji, pomocí e-mailu či manuálním zadáváním. Incidenty jsou poté automaticky či na vyžádání obohacovány dalšími informacemi ze QRadar SIEM systému (např. kontrolní součty souborů či související incidenty), informacemi z externích security feedů, Active Directory či LDAPu, správy koncových bodů - BigFixu či dalších systémů. Integrace rovněž umožňují automatické či manuální akce, např. spuštění nebo ukončení procesu na koncovém bodu či jiné akce na externích systémech. Informace jsou mezi QRadarem a Resilientem neustále synchronizovány - v případě přidání nových informací k offensu (např. nová IP adresa) je tato informace přidána k incidentu v Resilientu, stav a poznámky mezi offensy a incidenty mohou být rovněž synchronizovány.

2. **počet typů chráněných databází** - v rámci tohoto subkritéria bude jako nejvhodnější hodnoceno řešení, které podporuje automatizovanou ochranu největšího počtu různých typů databází, a které zároveň umožňuje na jednom místě monitorovat aktivitu nad všemi firemními databázemi. Uchazeč do nabídky uvede počet a úplný výčet typů chráněných databází.

Popis způsobu řešení:

Produktové řešení naplňující požadovanou funkcionalitu:

IBM Security Guardium Data Protection for Databases

Popis jak je daná funkcionalita řešena:

IBM Security Guardium Data Protection for Databases poskytuje centralizovaný monitoring, ochranu (včetně možnosti blokace), automatickou analýzu dat a jejich kategorizaci, vysokou škálovatelnost, vytváření a uchovávání auditních záznamů v reálném čase bez vysokých výkonových nároků na databázový server. Konkrétně je na databázový server nainstalován agent, který monitoruje vše, co se na databázi děje a tato data poté odesílá do Guardium appliance, kde se data analyzují a korelují. Výhodou tohoto přístupu je to, že Guardium dokáže odhalit i útoky od privilegovaných uživatelů, kteří se mohou do databáze připojit přímo a nepřistupují k ní přes aplikaci nebo přes síť. Pro monitoring a analýzu citlivých údajů, jsou připraveny vzorové politiky zaměřené na normy jako GDPR, PCI atd.

Celkový počet a úplný výčet typu chráněných databází:

Počet: 20 databází

Typy databází: Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, IBM PureData, IBM Netezza, MySQL, SAP Sybase, SAP HANA, PostgreSQL,
MongoDB, MariaDB, MemSQL, Teradata, Cloudera, Aster, Cassandra,CouchDB, Greenplum DB a Horton Works.

3. **kontrolní mechanismy vyhledávání zranitelností** - v rámci tohoto subkritéria bude jako nejvhodnější hodnoceno řešení, které poskytne nejširší škálu mechanismů vnitřní kontroly: například, řešení by mělo poskytovat (i) modul pro vyhledávání zranitelností, což bude centralizovaná platforma pro řízení rizik spojených s datovou infrastrukturou. Řešení bude umožňovat provádění pravidelného skenování prostředí a hledání chybějících aktualizací, slabých hesel, známých chyb v nastavení a dalších bezpečnostních rizik, přičemž tato bude zaznamenávat do jednotného místa nástroje SIEM (ii) a zároveň bude na tato rizika upozorňovat formou notifikací v mnoha různých formátech jako například. PDF, Syslog, CSV a další. Zadavatel preferuje řešení, které umožní automaticky odesílat (iii) reporty zainteresovaným osobám a automatizovat tím auditní proces.

Popis způsobu řešení:

Produktové řešení naplňující požadovanou funkcionalitu:

IBM Security QRadar SIEM, QRadar Vulnerability and Risk Manager

Popis jak je daná funkcionalita řešena:

Jedná se o integrované řešení QRadar SIEM a Vulnerability Manager a Risk Manager.

QRadar SIEM slouží jako centrální komponenta pro práci a integraci těchto řešení.

QRadar Vulnerability Manager umožnuje aktivně skenovat a vyhledávat zranitelnosti a známá slabá hesla na zařízeních v sítí, třídit je, prioritoziovat a samozřejmě reportovat o nálezech. Report může být buď na vyžádání a manuálně nebo plně automatizovaně, kdy uživatel dostane report přímo do emailu. Informace o výsledku skenování můžou být doručeny konkrétním osobám jako je třeba definovaný vlastník zařízení nebo jinak definovaný seznam. Podporovány jsou různé formáty jako HTML, XML PDF, RTF a XSL.

IBM Security Qradar Risk Manager (QRM) je součástí IBM QRadar Security Intelligence Platform kde

zastává roly pre-exploit řešení. QRM není určen k odhalení nebo zablokování probíhajících útoků, ale zaměřuje se na jejich předcházení. K předcházení útokům dochází pomocí identifikace chybně nastavených pravidel u aktivních prvků síťové infrastruktury, jako jsou firewally, routery, switche nebo IPS.

Qradar Risk Manager slouží jako přídavný modul pro IBM Qradar SIEM, jenž obohacuje o nástroje, které jsou nepostradatelné při předcházení budoucích útoků na počítačovou infrastrukturu.

IBM Qradar Risk Manager umožňuje analyzovat síťovou topologii a porovnávat seznam všech zranitelností s aktuální topologií v síti. Výsledkem této analýzy je seznam všech zařízení, které mohou být zranitelné a jsou například dostupné z internetu, nebo mohou komunikovat s napadeným zařízením.

Lze vytvářet vlastní Policies pro vyhledávání a určovat jim Risk Score dle kterého lze zobrazovat ty nejzávažnější hrozby, které jsou například na kritických systémech, před těmi méně závažnými.

O nálezech QRadar Risk Manager lze notifikovat syslogem, emailem nebo report zaslat zainteresovaným osobám v preferovaném formátu HTML, PDF nebo RFT na vyžádání nebo automatizovaně.

4. **Zranitelnosti a distribuce záplat** - v rámci tohoto subkritéria bude jako nejvhodnější hodnoceno řešení, které je schopno pracovat s výsledky skenu zranitelností z více zdrojů, umožní jejich prioritizaci v kontextu prostředí a události. Řešení se musí také integrovat s nástrojem pro centralizovanou správu a distribuci záplat pro proaktivní ochranu. Uchazeč do nabídky uvede počet a úplný výčet typů skenerů, ze kterých čerpá informace.

Popis způsobu řešení:

Produktové řešení naplňující požadovanou funkcionalitu:

IBM Security QRadar SIEM, IBM Security QRadar Vulnerability Manager, IBM Security BigFix Lifecycle, IBM Security Guardium Vulnerability Assessment for Databases

Popis jak je daná funkcionalita řešena:

QRadar QVM a BigFix tvoří ucelenou platformu pro skenování zranitelností, jejich prioritizaci a distribuci. QVM zasílá do BigFixu informace o nalezených vulnerabilitách a risk score jednotlivých zařízení. BigFix poté dokáže identifikovat odpovídající záplaty, tudíž administrátoři se mohou soustředit na distribuci relevantních záplat. Vulnerability nalezené jinými scannery mohou být konsolidovány pomocí QVM a QRM a rovněž využity v BigFixu. Výsledky procesu distribuce záplat jsou poté zpětně zobrazovány v konzoli QRadaru. QRadar umožňuje import výsledků skenu i z jiných systémů (seznam níže). V případě, že pro danou vulnerabilitu neexistuje žádná záplata, BigFix může být použit pro izolaci počítače od sítě či jiné akce.

Celkový počet a úplný výčet skenerů:

Celkem: 22

Beyond Security AVDS, Digital Defense Inc AVS, eEye, Generic Axis, IBM AppScan Enterprise, IBM Guardium, IBM SiteProtector, IBM BigFix, IBM Tivoli Endpoint Manager, Juniper Profiler NSM, McAfee Vulnerability Manager, Microsoft SCCM, nCircle IP360, Nessus, SecureScout, Nmap, Outpost24 Vulnerability Scanner, Positive Technologies MaxPatrol, Qualys, Rapid7 Nexpose, SAINT, Tenable SecurityCenter

5. **Kontrola nad ztrátou dat** - v rámci tohoto subkritéria bude jako nejvhodnější hodnoceno řešení, které umožní nejen detekovat podezřelé aktivity nad daty v databázích, ale nabídne i blokování

na základě širšího kontextu poskytnutého ze SIEM nástroje. Uchazeč do nabídky uvede princip fungování takového integrovaného řešení.

Popis způsobu řešení:

Produktové řešení naplňující požadovanou funkcionalitu:

IBM Security QRadar, IBM Security Guardium Data Protection for Databases

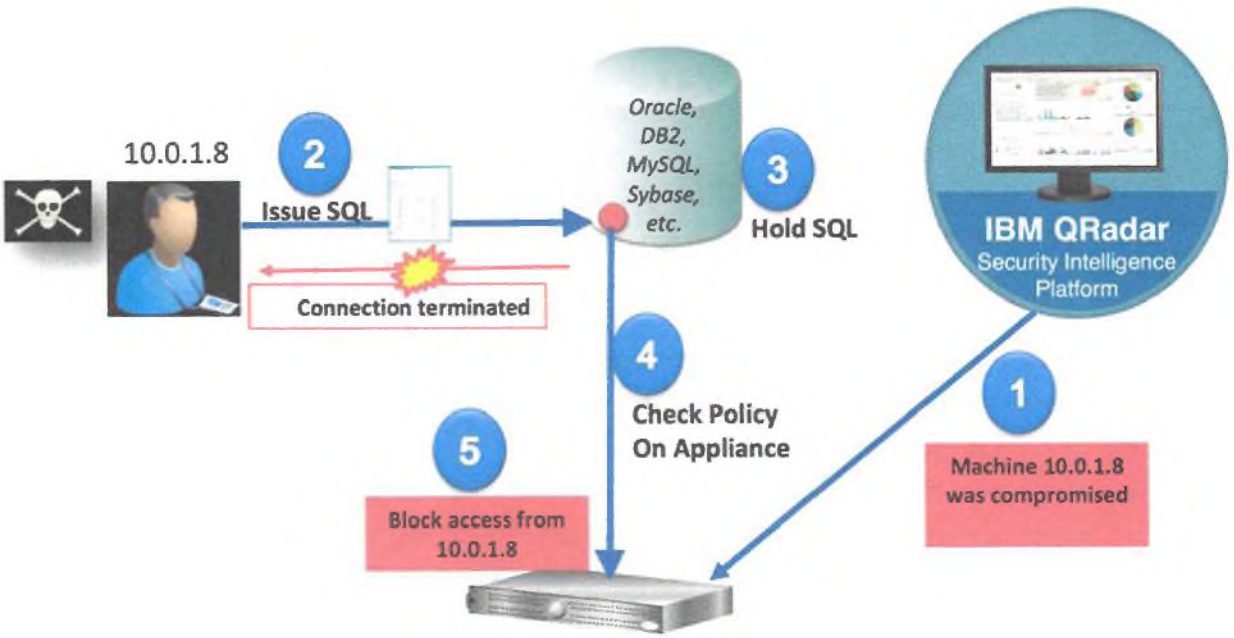
Popis jak je daná funkcionalita řešena:

Daná funkcionalita bude řešena integraci IBM Security QRadar a IBM Security Guardium a možnosti dynamicky upravovat politiky tak, aby v případě ohrožení nemohlo dojít k odcizení dat.

Princip fungování řešení:

IBM Security QRadar SIEM analyzuje informace a je schopen identifikovat podezřelé aktivity, jako například infiltrace uživatelského zařízení malwarem, napadení útočníkem, či zneužití uživatelské identity. Jako reakci na dané zjištění QRadar SIEM zareaguje akcí, které upraví politiky v IBM Security Guardium tak, aby znemožnila danému zařízení nebo uživateli přístup k informacím a nemohlo tak dojít k jejich zneužití.

Viz obrázek:



1. QRadar identifikuje infikované zařízení, aktualizuje politiku v Guardiu
2. Útočník se z infikovaného zařízení snaží o dotaz do databáze
3. Guardium pozdrží dotaz
4. Guardium vyhodnotí politiky
5. Guardium zablokuje požadavek (dotaz)

TECHNICKÁ SPECIFIKACE

Tato příloha je nedílnou součástí zadávací dokumentace veřejné zakázky s názvem

„Implementace a podpora nástroje na vyhodnocování bezpečnostních událostí SIEM z informačních systémů MHMP".

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 na plnění zakázky.

Předmět veřejné zakázky se skládá z následujících částí:

A. **Dodávka a implementace SIEM**
B. **Poskytování služeb technické podpory provozu a maintenance SIEM**

Jednotlivé etapy předávání díla

Dílo bude realizováno a předáváno po etapách. Etapy vycházejí z hrubého harmonogramu, které jsou uvedeny v čl. 3.1. ZD. Začátek každé etapy je vázán protokolárním převzetím předchozí etapy Zadavatelem na základě akceptačního protokolu.

a) V první etapě bude:

- vypracováni detailního návrhu řešení včetně upřesnění dílčích částí hrubého harmonogramu,
- interní oponentura a vypořádání připomínek,
- akceptace a převzetí detailního návrhu řešení.

b) Druhá etapa zahrnuje:

- implementaci systému a požadovanou integraci na základě upřesněného harmonogramu, jež byl akceptován v rámci detailního návrhu řešení
- provedení školení, vypracování dokumentace,
- akceptační zkoušky,
- akceptace a převzetí implementované části díla do zkušebního provozu,

c) Třetí etapa zahrnuje:

- zkušební provoz, v rámci kterého bude prověřena funkčnost díla v rutinním prostředí Zadavatele,
- akceptaci a převzetí díla do rutinního provozu.

d) Čtvrtá etapa představuje:

- rutinní provoz a podporu systému.

Dodávka a implementace SIEM

1. Shrnutí základních požadavků na dodávku SIEM

Security Information and Event Management (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 SIEM bude dodáno jako ucelená platforma pro sběr a vyhodnocování bezpečnostních událostí. Řešení musí umožňovat bezpečnostním analytikům efektivně reagovat na již proběhlé bezpečnostní incidenty, ale dokonce tyto incidenty předvídat a předcházet jim. Jedná se o nadstavbové řešení běžného Log Managementu, který sám o sobě nestačí, ale je potřeba dávat informace do širších souvislosti spolu s informacemi o toku v síti, zranitelnostech a míře rizika pro daný segment nebo zařízení. Poptávané řešení SIEM poskytne log management, event management, reporting a analýzy chování pro sítě a aplikací nebo uživatelů. Důraz na funkcionalitu řešení je kladen, mimo jiné, na komplexní chápání různých zdrojů a relevantních bezpečnostních informací, a to zejména díky univerzální a modulární platformě. Součástí řešení musí být doplňujícími moduly pro rozšíření funkcionality a zpřesnění detekce a správy zranitelností, pro efektivní práci a korelaci zranitelností či nástroj pro řízení rizik umožňující tvorbu "Co – Když" analýz a v neposlední řadě také s modul pro forenzní korelace incidentů, jakožto denní nástroj bezpečnostního analytika ve všech fázích – od detekce potenciálních slabých míst, detekci a následné investigaci chování.

Shrnutí základních vlastností poptávaného SIEM řešení

- Shromažďování logů o událostech ze zařízení a aplikací na síti
- Komplexní zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase
- Pokročilé techniky detekce hrozeb APT a "Zero-Day" útoků, včetně behaviorální analýzy
- Monitorování chování v síti, tvorba přehledných reportů a přístup ke všem informacím z Řešení webové konzole
- Identifikace a kategorizace zranitelností
- Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak mezeru odstranit.
- Možnost filtrováni nalezených zranitelností a jejich prioritizace.
- Možnost nad filtry zranitelností vytvářet pravidla pro korelaci
- Podpora operačních systémů Windows/Linux, mnoha síťových zařízení (routery, firewally), databází, webových serverů, mail serverů, DNS, koncových bodů a mnoha dalších.
- Snížení rizik provozovaných aplikací a možnosti jejich kompromitace
- Detekce kybernetických bezpečnostních událostí a zajištění reakce na incidenty a to zejména:
    - Analýzou prostředí v reálném čase a zajištění včasné reakce na vzniklé události a porušení DAT
    - Požadavek na zavedení SOC
- Možnost forenzního šetření a analýzy nad událostmi z mnoha typů zdrojů a zařízení
- Automatizovaná korelace událostí a následná reakce na identifikované problémy
- Minimalizace rizik včasnou identifikací skutečných útoků
- Zajištění souladu s regulatorními a legislativními požadavky
- Požadavky regulatorních orgánů jestli jsou ve shodě s požadovanými pravidly (nebo vlastními) pro konfiguraci systémů nebo zařízení a vyhodnocování událostí z těchto systémů
- Zajištění požadavků Zákona o kybernetické bezpečnosti
- Efektivní identifikace incidentů zajistí snížení nákladů na jejich identifikaci

Nasazení

Řešení bude nasazeno formou distribuované HW appliance, formou tzv. All-in-One řešení, skládající se z jednotlivých HW/SW modulů. Řešení musí být dodáno jako ucelené tj. od jednoho výrobce, včetně společné management konzole (společné ovládací rozhraní pro všechny moduly). Řešení umožňuje sběr bezagentní z nejrůznějších zdrojů, včetně databázových systémů. Řešení musí disponovat podporou normalizace několika stovek nejrůznějších zařízení napříč dodavateli, zároveň musí být možné velmi snadné rozšíření o další zařízení. Řešení musí též disponovat stovkami předpřipravených korelačních pravidel a reportů, během nasazení se tedy konfigurují zejména nezbytné informace pro kontext (sít, kategorizace serverů,...) a rozšíření o specifická pravidla nebo reporty dle potřeb klienta. Nabízené řešení musí splnit veškeré technické specifikace zařízení na moduly SIEM, řešení incidentů, ochranu databází, správu a detekci zranitelností a ochranu souborů na koncových stanicích a serverech.

1.1. 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 již pouze 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.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Vyjádření ANO/NE" a pokud je požadován i „Popis jak bude požadavek splněn/řešen".

Sloupec „Vyjádření ANO/NE" může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Sloupec „Technická specifikace nabízeného zařízení" a „Popis jak bude požadavek splněn/řešen" bude obsahovat podrobný popis, jak dodavatel požadavek naplní.

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

Výše uvedená pravidla na vyplnění tabulek jsou společné pro kapitoly 1.2 až 1.5.

1.2. Technická specifikace - SIEM

Výrobce / název / typ zařízení: **IBM Security QRadar SIEM**

	Minimální technické požadavky	„Vyjádření ANO/NE“	„Technická specifikace nabízeného zařízení“, pokud je vyžadováno, pak i „Popis jak bude požadavek splněn/řešen“
1	Podporované protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol	ANO	Nabízené řešení podporuje protokoly: Syslog, Windows Events Collection (WinRM/ RPC), FTP, S/TP/SCP, SNMP, ODBC/JDBC, CP-LEA, SDEE, log file protokol.
2	Bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	ANO	Nabízené řešení obsahuje bezagentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém).
3	Licence pro zpracování 10.000 EPS s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 40 000 EPS	ANO	Nabízené řešení obsahuje licence pro zpracování 10.000 EPS s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 40 000 EPS.
4	Licence pro zpracování 200 000 FPM s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 1 000 000 FPM	ANO	Nabízené řešení obsahuje licence pro zpracování 200 000 FPM s možností rozšíření bez nutnosti dodatečného HW, resp. HW upgrade až na 1 000 000 FPM.
5	Licence pro 50 konfigurací síťových prvků.	ANO	Nabízené řešení obsahuje licence pro 50 konfigurací síťových prvků.
6	Počet zdrojů pro sběr logů minimálně 40 000	ANO	Nabízené řešení splňuje minimální počet 40 000 zdrojů pro sběr logů.
7	Možnost sběru logů lokálním kolektorem s přeposíláním do SIEM	ANO	Nabízené řešení obsahuje možnost sběru logů lokálním kolektorem s přeposíláním do SIEM.
8	Možnost záložního uložení logů (rozšiřitelné úložiště neodpovídá tomuto požadavku)	ANO	Nabízené řešení obsahuje možnost záložního uložení logů (rozšiřitelné úložiště

			neodpovídá tomuto požadavku).
9	Centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní	ANO	Nabízené řešení obsahuje centrální management všech komponent a administrativních funkcí ve webovém uživatelském rozhraní.
10	Možnost definovat uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům	ANO	Nabízené řešení obsahuje možnost definovat uživatelům SIEMu přístup k jednotlivým zařízením, jejich skupinám či síťovým segmentům.
11	Automatická identifikace systémů – zdrojů logů	ANO	Nabízené řešení obsahuje možnost automatické identifikace systémů – zdrojů logů.
12	Podpora šifrované komunikace mezi zdroji logů a SIEM	ANO	Nabízené řešení obsahuje podporu šifrované komunikace mezi zdroji logů a SIEM.
13	Integrace s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů	ANO	Nabízené řešení obsahuje integraci s adresářovým systémem (LDAP, Active Directory) pro potřeby autentizace uživatelů.
14	Minimální administrace /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače Cisco a Check Point, F5 Networks, FortiNet, ExtremeNetwork.)	ANO	Nabízené řešení obsahuje minimální administraci /výběr zařízení ze seznamu od výrobce/pro připojení dalších zdrojů událostí (servery Windows, Unix/Linux, přepínače Cisco a Check Point, F5 Networks, FortiNet, ExtremeNetwork.).
15	Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí	ANO	Nabízené řešení obsahuje Log Management s minimální postimplementační administrací. /agregace událostí dle typů, analýza, vyhodnocování/ pro případy jako je zavedení nového zdroje událostí, nastavení pravidel pro sběr dat a archiv událostí.
16	Automatické připojení zařízení výrobců ExtremeNetwork a Cisco	ANO	Nabízené řešení obsahuje automatické připojení zařízení výrobců ExtremeNetwork a

			Cisco.
17	Podpora sběru síťových toků (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, NetFlow sondy)	ANO	Nabízené řešení podporuje sběr síťových toků (NetFlow, JFLow, Sflow) z infrastrukturních prvků (switche, routery, NetFlow sondy).
18	Součástí řešení musí být sonda pro sběr Flow informací ze síťového provozu, včetně exportu až 255 bytů z payloadu pro analýzu v SIEM. Sonda musí mít propustnost: 1 GBPS	ANO	Nabízené řešení obsahuje sondu pro sběr Flow informací ze síťového provozu, včetně exportu až 255 bytů z payloadu pro analýzu v SIEM. Sonda má propustnost 1 GBPS.
19	Řešení musí umožňovat automatické aktualizace	ANO	Nabízené řešení umožňuje automatické aktualizace.
20	Webové uživatelské rozhraní pro management, analýzu a reporting	ANO	Nabízené řešení obsahuje Webové uživatelské rozhraní pro management, analýzu a reporting.
21	Poskytování automatického backup/recovery procesu	ANO	Nabízené řešení umožňuje automatický backup/recovery proces.
22	Poskytovat interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému	ANO	Nabízené řešení poskytuje interní kontroly stavu zařízení (healthcheck) a upozornění uživatele v případě problému.
23	Možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI	ANO	Nabízené řešení poskytuje možnost integrovaného managementu rizik na základě síťových toků a konfigurace aktivních prvků do GUI.
24	Poskytování analytické a korelačních funkcí bez dalších zásahů a činností (out-of-the-box)	ANO	Nabízené řešení poskytuje analytické a korelačních funkce bez dalších zásahů a činností (out-of-the-box).
25	Řešení musí být dodáno jako all-in-one appliance	ANO	Nabízené řešení je poskytováno jako all-in-one appliance.
26	Sběr logů z dalších bezpečnostních a síťových systémů (FlowMon, AFW f5, FW Cisco, AV Symantec, IronPort Cisco)	ANO	Nabízené řešení umožňuje sběr logů z dalších bezpečnostních a síťových systémů (FlowMon, AFW f5, FW Cisco, AV Symantec,

			IronPort Cisco).
27	Výkonová rozšířitelnost Popište, jak je nabízené řešení škálovatelné na požadavky: přidání nových zařízení, lokací, aplikací	ANO	Nabízené řešení je výkonově rozšířitelné. Popis: Řešení umožňuje škálovatelnost přidáním nových komponent do jádra systému, jenž tvoří společná ovládací konzole a výkonost přídáním potřebných licencí a HW výkonu v podobě přídavných Nodů.
28	Možnost rozšíření výběrů o uživatelské položky z obsahu logů	ANO	Nabízené řešení obsahuje rozšíření výběrů o uživatelské položky z obsahu logů.
29	Zajištění integrity nasbíraných dat	ANO	Nabízené řešení zajišťuje integritu nasbíraných dat.
30	Schopnost uchovat nejméně 36 TB dat (v komprimovaném formátu), aniž by vyžadovalo použití externích paměťových zařízení	ANO	Nabízené řešení má schopnost uchovat nejméně 36 TB dat (v komprimovaném formátu), aniž by vyžadovalo použití externích paměťových zařízení.
31	Umožnění nárůstu zdrojů událostí bez nutnosti pořizování dalšího hardware	ANO	Nabízené řešení umožňuje nárůst zdrojů událostí bez nutnosti pořizování dalšího hardware.
32	Near-real-time analýza událostí	ANO	Nabízené řešení obsahuje Near-real-time analýzu událostí.
33	Analýza dlouhodobých trendů událostí	ANO	Nabízené řešení obsahuje analýzu dlouhodobých trendů událostí.
34	Řešení musí být hodnocené v segmentu „leaders“ v Gartner Magic Quadrantu za minulé tři roky	ANO	Nabízené řešení je hodnocené v segmentu „leaders“ v Gartner Magic Quadrantu za minulé tři roky.
35	Pokročilé "drill-down" dohledávání v případě potřeby	ANO	Nabízené řešení umožňuje pokročilé "drill-down" dohledávání v případě potřeby.
36	Možnost agregace události z logů i podle položek které nejsou standardně zahrnuty v	ANO	Nabízené řešení umožnuje agregaci události z logů i podle položek které nejsou

	řešení		standardně zahrnuty v řešení.
37	Podpora a normalizace časových značek z různých časových zón	ANO	Nabízené řešení obsahuje podporu a normalizaci časových značek z různých časových zón.
38	Sběr textových logů ze souborů	ANO	Nabízené řešení obsahuje sběr textových logů ze souborů.
39	Sběr logů z databází pomocí JDBC/ODBC	ANO	Nabízené řešení obsahuje sběr logů z databází pomocí JDBC/ODBC.
40	Sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server	ANO	Nabízené řešení obsahuje sběr log záznamů z prostředí Windows a Linux/Unix/AIX. Sběr Windows EVT záznamů i z Windows Server.
41	Rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů musí nabízet možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd.	ANO	Nabízené řešení obsahuje rozčlenění vyhledaných dat (Drilldown): Vyhledávací rozhraní systému správy logů nabízí možnost rozčlenění vyhledaných dat až na detailní úroveň, IP adresa, typ události, protokol, port atd.
42	Způsob zadávání vyhledávání: Vyhledávací rozhraní systému správy logů musí poskytovat podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy	ANO	Nabízené řešení obsahuje Způsob zadávání vyhledávání jako vyhledávací rozhraní systému správy logů a poskytuje podporu jak pro zadání dotazu s použitím Booleovy logiky, tak pro regulární výrazy.
43	Poskytování alertů na detekované anomálie, změny chování sítě a změny v generování logů a událostí	ANO	Nabízené řešení poskytuje alerty na detekované anomálie, změny chování sítě a změny v generování logů a událostí.
44	Kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně	ANO	Nabízené řešení obsahuje kombinované hledání v indexovaných i neindexovaných datech v systému správy logů s použitím regulárních výrazů a fulltextového vyhledávání v nestrukturovaném textu současně.

45	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy	ANO	Nabízené řešení obsahuje korelační modul, který poskytuje již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy.
46	Korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení	ANO	Nabízené řešení obsahuje korelace mezi zařízeními již po instalaci (out-of-the-box). Zjišťování chyb autentizace, chování perimetru a výskytu červů bez potřeby specifikovat typy sledovaných zařízení.
47	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení	ANO	Nabízené řešení poskytuje alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení.
48	Alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení musí poskytovat NBAD (Network Behavior Anomaly Detection) funkcionalitu	ANO	Nabízené řešení obsahuje alerting založený na vypozorovaných anomáliích a změnách chování sítě (analýza síťových toků). Řešení poskytuje NBAD (Network Behavior Anomaly Detection) funkcionalitu.
49	Řešení musí poskytnout alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán).	ANO	Nabízené řešení poskytuje alerting porušení bezpečnostních pravidel, založený na stanovené bezpečnostní politice (např. IM provoz je zakázán).
50	Vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript	ANO	Nabízené řešení umožňuje vykonávání akci v závislosti na přijatém logu jako např. zaslat email, notifikaci nebo spustit předem definovaný skript.
51	Schopnost pracovat s IP geolokacemi (botnet kanály atp.)	ANO	Nabízené řešení pracuje s IP geolokacemi (botnet kanály atp.).
52	Generování alertu při výpadku logů z konkrétního zařízení	ANO	Nabízené řešení umožňuje generování alertu při výpadku logů z konkrétního zařízení.
53	Vestavěný mechanismus na klasifikaci systémů podle typu (např. mail server vs.	ANO	Nabízené řešení obsahuje vestavěný mechanismus na klasifikaci systémů podle typu

	databázový server)		(např. mail server vs. databázový server).
54	Vyhodnocení chybějících sekvencí (např. služba přestala běžet)	ANO	Nabízené řešení obsahuje vyhodnocení chybějících sekvencí (např. služba přestala běžet).
55	Schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů	ANO	Nabízené řešení má schopnost monitorovat historii útoků (typů událostí) na kritické komponenty a historii útoků jednotlivých uživatelů.
56	Schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele)	ANO	Nabízené řešení má schopnost korelovat události DHCP, VPN a Active Directory a sledovat průběh uživatelské relace (session) v rámci celé instituce (přesná identifikace uživatele).
57	Schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů)	ANO	Nabízené řešení má schopnost korelovat data o událostech se statickými a dynamickými seznamy označujícími položky, které mají či nemají být v síti povoleny (tj. seznam nezabezpečených protokolů).
58	Poskytování rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy	ANO	Nabízené řešení poskytuje rozhraní pro reporting, pomocí kterého lze vytvářet nové sestavy bez nutnosti sestavovat SQL dotazy.
59	Nezměněná funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS	ANO	Nabízené řešení poskytuje nezměněnou funkcionalita reportingu i při změně nebo náhradě některé technologie jako např. firewallu nebo IDS.
60	Řešení musí být rozšiřitelné o podporu sběru a analýzy sledovaného síťového provozu až na aplikační vrstvu ISO/OSI modelu, pomocí rozšíření licence	ANO	Nabízené řešení je rozšiřitelné o podporu sběru a analýzy sledovaného síťového provozu až na aplikační vrstvu ISO/OSI modelu, pomocí rozšíření licence.
61	Řešení musí být rozšiřitelné o funkci sledování síťové komunikace v rámci virtualizovaného prostředí, pomocí rozšíření licence	ANO	Nabízené řešení je rozšiřitelné o funkci sledování síťové komunikace v rámci virtualizovaného prostředí, pomocí rozšíření licence.

62	Řešení musí být rozšiřitelné o nástroje pro zachytávání síťového provozu (full packet caputure) a pro forenzní analýzu jako rozšíření bez nutnostni komponent třetích stran	ANO	Nabízené řešení je rozšiřitelné o nástroje pro zachytávání síťového provozu (full packet caputure) a pro forenzní analýzu jako rozšíření bez nutnostni komponent třetích stran.
63	Nabízené řešení musí poskytovat webové uživatelské rozhraní pro správu, analýzy, reportovaní a podobně. Rozhraní by nemělo obsahovat pluginy nebo být založeno na technologiích Java, Flash nebo na bázi tlustého klienta.	ANO	Nabízené řešení poskytuje webové uživatelské rozhraní pro správu, analýzy, reportovaní a podobně. Rozhraní neobsahuje pluginy a není založeno na technologiích Java, Flash nebo na bázi tlustého klienta.
64	Řešení musí obsahovat nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.	ANO	Nabízené řešení obsahuje nativní podporu vysoké dostupnosti (HA) bez rozšiřujících komponent/software třetích stran.
65	HA musí být možné připojit v jakékoliv fázi, bez nutnostni reinstalace a celého řešení.	ANO	Nabízené řešení obsahuje HA a je možné připojit v jakékoliv fázi, bez nutnostni reinstalace a celého řešení.
66	Nabízené řešení musí poskytovat automatické aktualizace řešení bez pomoci profesionálních služeb vendora.	ANO	Nabízené řešení poskytuje automatické aktualizace řešení bez pomoci profesionálních služeb vendora.
67	Nabízené řešení musí umět upozornit na anomálie a změnych chování v siťové vrstvě. Popište jaké alerty jsou již out-of-the-box a jakým způsobem může být řešení obohaceno o uživatelská pravidla pro behaviorální analýzu.	ANO	Nabízené řešení umí upozornit na anomálie a změnych chování v siťové vrstvě. Popis: Řešení IBM QRadar obsahuje více než 200 pravidel out of the box a další obsah je k dispozici v rámci QRadar App Exchange zdarma. Pravidla obsahují alerty na anomálie v sítích, kdy například zařízení komunikuje příliš mnoho protokoly, nové zařízení v sítích nebo komunikace s neznámými státy. Uživatel si může definovat vlastní pravidla bez omezení pomocí grafického editoru, který jej provede celým cyklem.

68	Nabízené řešení musí poskytovat možnost sběru a analýzu informací payloadu paketů v síťové komunikaci. Popište jak řešení splňuje tento požadavek.	ANO	Nabízené řešení poskytuje možnost sběru a analýzu informací payloadu paketů v síťové komunikaci. Popis: Řešení QRadar disponuje komponentou pro analýzu síťového provozu, která generuje informace o tocích v sítích (flow) a umožnuje připojit k této informaci i prvních až 255 bytů.
69	Některá zařízení v síti často mění svou IP adresu. Nabízené řešení musí být schopno udržet databázi zařízení konzistentní i v těchto případech. Popište jak řešení splňuje tento požadavek.	ANO	Nabízené řešení udržuje databázi zařízení konzistentní i v případech, kdy často mění svou IP adresu. Popis: Řešení QRadar sleduje zařízení v síti a tvoří jejich profil. Zařízení s často měnící se IP adresou nejsou problém, neboť QRadar používá několik identifikátorů jako třeba IP adresa, DNS jméno, NetBIOS jméno nebo MAC adresu, kde IP adresa je nejméně deterministická.
70	Nabízené řešení musí zaznamenávat činnost uživatele v čase a to i v případě, že tato informace není bezprostředně obsažena ve všech událostech. Popište, jak tento systém umožňuje korelaci identity, i když nejsou přítomny v datech bezprostředních událostí uživatelská jména.	ANO	Nabízené řešení zaznamenává činnost uživatele v čase a to i v případě, že tato informace není bezprostředně obsažena ve všech událostech. Popis: Řešení QRadar udržuje v tabulce assetů (zařízení) informaci o uživatelích, kteří se v historii přihlásili na dané zařízení. Při drill-down analýze je možné tuto informací vytáhnout v korelaci s dalšími událostmi, které přišly do systém QRadar později. Informace v tabulce zařízení jsou aktualizovány pomocí událostí, které právě nesou identitu.

71	Řešení musí nabízet přístup k datům skrze otevřené REST API pro integraci s dalšími systémy. Popište jak řešení splňuje tento požadavek.	ANO	Nabízené řešení nabízí přístup k datům skrze otevřené REST API pro integraci s dalšími systémy. Popis: Řešení IBM QRadar disponuje REST API pro integraci s dalšími systémy. QRadar nabízí širokou škálu API endpointů pro práci s eventy a flows, pro práci se skenery zranitelností, offenses, správu look up tabulek a mnoho dalších.
72	Řešení musí být navrženo tak, aby bylo schopno pracovat s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti. Popište jak řešení splňuje tento požadavek.	ANO	Nabízené řešení je navrženo tak, aby bylo schopno pracovat s interními překrývajícími se rozsahy adres spolu se síťovými toky, událostmi a zařízeními v síti. Popis: Řešení QRadar podporuje tuto funkcionality a umožnuje rozpoznat různé zdroje dat i případě překrývajících se IP adres a přidělit je to jednotlivých „domén", kde doména je určuje část organizace, kde se rozsahy překrývají. Data lze pak korelovat jak napříč doménami nebo jen v rámci domény. Příslušnost do domény lze určit na základě log source, flow collectoru, event colletoru nebo event custom property či jiné property.
73	Řešení musí být schopno agregovat záznamy o síťovém provozu z obou stran datového toku do jedno zázanamu popisující obousměrnou komunikaci.	ANO	Nabízené řešení je schopno agregovat záznamy o síťovém provozu z obou stran datového toku do jedno zázanamu popisující obousměrnou komunikaci.
74	Řešení musí uchovávat logy i flows jak normalizovaném formátu, tak i „raw" formátu.	ANO	Nabízené řešení uchovává logy i flows jak normalizovaném formátu, tak i „raw" formátu.

75	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.	ANO	Nabízené řešení není licenčně omezeno počtem používaných korelačních pravidel.
76	Řešení nebude licenčně omezeno počtem generovaných reportů	ANO	Nabízené řešení není licenčně omezeno počtem generovaných reportů.
77	Řešení musí umět sledovat síťovoy komunikaci v rámci virtualizovaného prostředí VMware ESX. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí sledovat síťovoy komunikaci v rámci virtualizovaného prostředí VMware ESX. Popis: Řešení IBM QRadar disponuje flow sondou, kterou lze nainstalovat do prostředí VMware a umožnuje sledovat komunikaci uvnitř prostředí VMware a monitorovat komunikaci mezi hosty v rámci ESX.
78	Řešení musí být schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.	ANO	Nabízené řešení je schopno konsolidovat výsledky z několika řešení, jako jsou vulnerability scannery, risk management nástroje a externí vstupy bezpečnostních informací z různých zdrojů.
79	Řešení musí umět aktivně skenovat zařízení v sítí na zranitelnosti. Minimálně pak musí nabízet tyto typy scanarů: discovery scan, patch scan, webový scan, databázový scan. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí aktivně skenovat zařízení v sítí na zranitelnosti. Obsahuje tyto typy scanarů: discovery scan, patch scan, webový scan, databázový scan. Popis: Řešení v základu obsahuje předdefinované politiky pro discovery scan, patch scan, web scan a databázový scan. Předdefinované politiky je možné upravovat nebo definovat vlastní.
80	Nabízené řešení musí umožnit sken z internet pro test DMZ zón. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umožňuje sken z internetu pro test DMZ zón. Popis: Součástí licence řešení QRadar Vulnerability Manager je externí sken pro test DMZ zóny a externích IP z venku. Sken provede IBM X-Force a výsledky zašle do

			platformy.
81	Kontrola zranitelností musí reagovat na pravidly definované události a případě naplnění podmínek (například nové neznámé zařízení) musí spustit automatizovaný scan zranitelností. Popište, jak řešení splňuje tento požadavek.	ANO	Kontrola zranitelností v nabízeném řešení reaguje na pravidly definované události a v případě naplnění podmínek (například nové neznámé zařízení) spustí automatizovaný scan zranitelností. Popis: Řešení IBM QRadar umožňuje jako reakci na slepé pravidlo spustit nějakou akci a také spustit sken pomocí modulu QRadar Vulnerability Manager.
82	Řešení musí prioritizovat výsledky scanu zranitelností na základě dostupných informací o síťové konfiguraci. Například zda-li konfigurace síťové infrastruktury umožňuje takovýto typ útoku. Popište, jak Vaše řešení splňuje tento požadavek.	ANO	Nabízené řešení umí prioritizovat výsledky scanu zranitelností na základě dostupných informací o síťové konfiguraci. Například zda-li konfigurace síťové infrastruktury umožňuje takovýto typ útoku. Popis: QRadar v kombinaci QRadar Vulnerability Manager a Risk manager umí vyhodnocovat a upravovat dopad rizika dané zranitelnosti v kontextu prostředí a možných vektorů útoku. Dotazy pro vyhodnocení dopadu rizika lze uživatelsky upravovat.
83	Řešení musí umožňovat definici vyjímek pro jednotlivé zranitelnosti dle různých kritérií tak, aby se nalezené zranitelnosti nepropagovaly v korelacích nebo v reportech. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umožňuje definici vyjímek pro jednotlivé zranitelnosti dle různých kritérií tak, aby se nalezené zranitelnosti nepropagovaly v korelacích nebo v reportech. Popis: Řešení QRadar Vulnerability Manager umožnuje definici výjimek pro jednotlivé zranitelnosti, kde je možné definovat dobu účinnosti výjimky nebo rozsah výjimky, například na konkrétní zařízení nebo celý

			rozsah subnetu.
84	Řešení musí být schopno na základě historického výsledku scanu a informacích o nových zranitelnostech identifikovat zařízení, který mohou být ohrožena. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení je schopno na základě historického výsledku scanu a informacích o nových zranitelnostech identifikovat zařízení, která mohou být ohrožena. Popis: Řešeni QRadar Vulnerability Manager nabízí funkcionalitu „early warnings", kde na základě známého stavu zařízení je schopno identifikovat potencionálně ohrožená zařízení po aktualizaci databáze se zranitelnostmi.
85	Nabízené řešení musí být schopno v realném čase korelovat zařízení, log/flow a zranitelnost na zařízení, konkrétní port.	ANO	Nabízené řešení koreluje v realném čase zařízení, log/flow a zranitelnost na zařízení, konkrétní port.
86	Nabízené řešení musí být schopno podporovat kontrolu souladu s předpisy (compliance) zařízení v sítí, jako jsou CIS Benchmarks. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení je schopno podporovat kontrolu souladu s předpisy (compliance) zařízení v sítí, jako jsou CIS Benchmarks. Popis: Řešení QRadar v kombinaci s modulem Vulnerability and Risk Manager umožnuje definovat a spouštět CIS benchmark sken.
87	Nabízené řešení musí umět zvyšovat/snižovat riziko na základě kontextu (klasifikace zařízení, subnetu, parametru...) Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí zvyšovat/snižovat riziko na základě kontextu (klasifikace zařízení, subnetu, parametru...) Popis: Modul QRadar Risk Manager umožňuje definovat politky a pravidla na základě kterých může být sníženo nebo zvýšeno výchozí riziko zranitelností na daném zařízení.

88	Řešení musí obsahovat funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru jako jsou STIX nebo TAXII. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení obsahoje funkcionalitu pro výměnu standardizovaných informací informačně bezpečnostního charakteru jako jsou STIX nebo TAXII. Popis: Řešení IBM QRadar obsahuje modul pro práci se STIX/TAXI feedy, aby bylo možné tyto informace pravidelně aktualizovat v řešení a korelovat s událostmi v reálném čase.
89	Řešení musí nabízet bepečnostní informace jako je IP Reputation feed, botnety, zdroje malwaru apod., které jsou pravidelně aktualizované a jsou korelované v realném čase se všemi událostmi. Popište, jaké zdroje nabízené řešení využívá a jak je implementováno v korelačních pravidlech.	ANO	Nabízené řešení nabízí bezpečnostní informace jako je IP Reputation feed, botnety, zdroje malwaru apod., které jsou pravidelně aktualizované a jsou korelované v realném čase se všemi událostmi. Popis: Nativní součástí řešení IBM QRadar je prémiový IP reputation feed z dílny X-Force, který je pravidelně aktualizovaný a korelují se vůči němu události a toky v reálném čase.
90	Řešení musí umožňovat simulovat možné vektory útoku na topologii v síti a upozornit tak na mezery v konfiguraci nebo na kritické assety. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umožňuje simulovat možné vektory útoku na topologii v síti a upozorňuje tak na mezery v konfiguraci nebo na kritické assety. Popis: Řešení s modulem QRadar Risk Manager umožnuje na základě načtené konfigurace tvořit simulace a „Co Když?“ analýzy a simulovat vektory útoku a upozornit tak na mezery v konfiguraci nebo ujištění před jejich změnou
91	Řešení musí umět zálohovat konfigurace síťových prvků. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí zálohovat konfigurace síťových prvků. Popis: Tato funckionalita je k dispozici pro podporována zařízení v rámci modulu QRadar Vulnerability a Risk Manager, kde Risk Manager načítá a uchovává konfigurace

			zařízení.
92	Řešení musí umět porovnávat dvě konfigurace v rámci jednoho zařízení, tak i napříč různými síťové prvky. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí porovnávat dvě konfigurace v rámci jednoho zařízení, tak i napříč různými síťové prvky. Popis: Řešení QRadar a modul Risk Manager umožňuje pro podporovaná zařízení označit dvě zařízení a porovnat jejich konfigurace a zobrazit rozdíly. Obdobně i pro dvě různé konfigurace v rámci jednoho zařízení.
93	Řešení musí umět spojit síťové prvky do logických skupin, pro zjednodušení pohledu na celkovou topologii. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí spojit síťové prvky do logických skupin, pro zjednodušení pohledu na celkovou topologii. Popis: V Risk Managery při pohledu na topologii je možné označit související prvky a sloučit je do logické skupiny, tak aby se zjednodušil pohled na topologii sítě a přitom zůstaly zachovány souvislosti.
94	Řešení musí nabízet grafickou vizualizaci typu a zavažnosti incidentů v čase. Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení nabízí grafickou vizualizaci typu a zavažnosti incidentů v čase. Popis: Řešení QRadar SIEM disponuje širokou škálou rozšíření, které jsou napsané, validované a podporované IBM. Jedním z nich je aplikace „Incident Overview“, která graficky znázorňuje incidenty a jejich rozsah či vazby v čase. Další aplikací pro vizualizaci incidentů je „Pulse“, která je velmi vhodná pro SoC.
95	Řešení musí umět detekovat aplikace na základě protokolu, nikoliv "port matchingem" (Např. SSH/Telnet/FTP/DNS na nestandardním portu). Popište, jak řešení splňuje tento požadavek.	ANO	Nabízené řešení umí detekovat aplikace na základě protokolu, nikoliv "port matchingem" (Např. SSH/Telnet/FTP/DNS na nestandardním portu). Popis: Řešení QRadar SIEM

			spolu se síťovou sondou QFlow Collector, která umí číst i část payloadu v komunikaci, identifikuje aplikaci na základě zachyceného payloadu a identifikuje protokol. Je tak možné identifikovat správně aplikace, které komunikují i na jiných než standardních portech.

1.3. Technická specifikace - Řešení incidentů

Výrobce / název / typ zařízení: **IBM Resilient IRP**

	Minimální technické požadavky	„Vyjádření ANO/NE“	„Technická specifikace nabízeného zařízení“, pokud je vyžadováno, pak i „Popis jak bude požadavek splněn/řešen“
1	Licence pro 6 uživatelů	ANO	Nabízené řešení obsahuje licenci pro 6 uživatelů
2	Systém musí poskytovat různé způsoby zadávání incident do řešení (např. manuálně, automaticky, pomocí e-mailu atd.)	ANO	Nabízené řešení poskytuje různé způsoby zadávání incident do řešení (např. manuálně, automaticky, pomocí e-mailu atd.).
3	Systém musí poskytovat různé identifikace a kategorizace incidentů (např. Typ incidentu, Risk atd.)	ANO	Nabízené řešení poskytuje různé identifikace a kategorizace incidentů (např. Typ incidentu, Risk atd.).
4	Řešení musí poskytovat připravené workflow pro automatizaci různých kategorií incidentů jako např. DDoS útoky, Phishing, Malware útok atd.	ANO	Nabízené řešení poskytuje připravené workflow pro automatizaci různých kategorií incidentů jako např. DDoS útoky, Phishing, Malware útok atd.
5	Řešení musí poskytovat možnost graficky vytvořit workflow a aktivity	ANO	Nabízené řešení poskytuje možnost graficky vytvořit workflow a aktivity.
6	Řešení musí umožnit seskupování aktivit ve workflow podle aktivit podle fází a rovněž určit jejich pořadí	ANO	Nabízené řešení umožňuje seskupování aktivit ve workflow podle aktivit podle fází a rovněž určit jejich pořadí.
7	Systém musí podporovat dynamické úpravy workflow - seznam aktivit se přizpůsobí podle parametrů incidentu	ANO	Nabízené řešení podporuje dynamické úpravy workflow - seznam aktivit se přizpůsobí podle parametrů incidentu.
8	Systém musí podporovat přiřazení incidentů, jejich sekcí nebo aktivit různým řešitelům	ANO	Nabízené řešení podporuje přiřazení incidentů, jejich sekcí nebo aktivit různým řešitelům.
9	Řešení musí notifikovat dotčené osoby (např. zakladatele incidentu, analytika atd.) o průběhu a stavu incidentu (např. při jeho aktualizaci, přiřazení aktivity či zmínce v poznámce)	ANO	Nabízené řešení notifikuje dotčené osoby (např. zakladatele incidentu, analytika atd.) o průběhu a stavu incidentu (např. při jeho aktualizaci, přiřazení aktivity či zmínce v poznámce).

10	Notifikace mohou být zasílány na jednotlivé osoby, skupinu nebo celý tým řešitelů incidentu	ANO	Nabízené řešení zasílá notifikace na jednotlivé osoby, skupinu nebo celý tým řešitelů incidentu.
11	Systém musí umožnit komunikaci celého týmu přiřazeného k incidentu, tato komunikace musí být auditovatelná	ANO	Nabízené řešení umožňuje komunikaci celého týmu přiřazeného k incidentu, tato komunikace musí být auditovatelná.
12	K incidentům musí být možno přiložit dokumenty a další přílohy	ANO	Nabízené řešení umožňuje k incidentům přiložit dokumenty a další přílohy.
13	Systém musí umožnit fulltextové vyhledávání	ANO	Nabízené řešení umožňuje fulltextové vyhledávání.
14	Všechny aktualizace incidentů musí být zobrazovány v reálném čase např. v seznamu aktivit atd.	ANO	Nabízené řešení zobrazuje aktualizace incidentů v reálném čase např. v seznamu aktivit atd.
15	Součástí produktu musí být vestavěný reportovací nástroj a dashboard	ANO	Nabízené řešení obsahuje vestavěný reportovací nástroj a dashboard
16	Reporty musí být auditovatelné	ANO	Nabízené řešení obsahuje reporty, které jsou auditovatelné.
17	Řešení musí umožnit trénování reakcí na vzniklé incidenty pomocí simulovaných incidentů	ANO	Nabízené řešení umožňuje trénování reakcí na vzniklé incidenty pomocí simulovaných incidentů.
18	Systém musí poskytovat integraci se SIEM systémy Qradar, Splunk a HP Arcsight	ANO	Nabízené řešení poskytuje integraci se SIEM systémy Qradar, Splunk a HP Arcsight.
19	Řešení musí mít schopnost atomaticky obohacovat incidenty z interních dat organizace (např. o uživatelích, asetech, rolích atd.)	ANO	Nabízené řešení je schopno atomaticky obohacovat incidenty z interních dat organizace (např. o uživatelích, asetech, rolích atd.).
20	Řešení musí poskytovat integraci na interní a externí poskytovatele bezpečnostních informací (např. Thread intelligence feeds, SIEM nástroje, správu koncových bodů atd.)	ANO	Nabízené řešení poskytuje integraci na interní a externí poskytovatele bezpečnostních informací (např. Thread intelligence feeds, SIEM nástroje, správu koncových bodů atd.).
21	Řešení musí umožnit korelaci incidentů pomocí tzv. Indicators of compromise (IOC) identifikovaných pomocí interního, externího nebo manuálního obohacení (např. IP adresa, kontrolní součet souboru, účet uživatele, atd.)	ANO	Nabízené řešení umožňuje korelaci incidentů pomocí tzv. Indicators of compromise (IOC) identifikovaných pomocí interního, externího nebo manuálního obohacení (např. IP adresa, kontrolní součet souboru, účet uživatele, atd.).

22	Řešení musí podporovat případné odebrání specifické korelace v případě potřeby	ANO	Nabízené řešení podporuje případné odebrání specifické korelace v případě potřeby.
23	Řešení musí poskytovat grafický přehled korelovaných incidentů a jejich korelací	ANO	Nabízené řešení poskytuje grafický přehled korelovaných incidentů a jejich korelací.
24	Řešení musí umožňovat vytváření vlastních typů IOC	ANO	Nabízené řešení umožňuje vytváření vlastních typů IOC.
25	Řešení musí podporovat integrace s identity a access management systémy (např. Active Directory, LDAP, SAML).	ANO	Nabízené řešení podporuje integrace s identity a access management systémy (např. Active Directory, LDAP, SAML).
26	Řešení musí umožňovat orchestraci a automatizaci reakcí na incidenty pomocí integrací s produkty třetích stran	ANO	Nabízené řešení umožňuje orchestraci a automatizaci reakcí na incidenty pomocí integrací s produkty třetích stran.
27	Řešení musí poskytovat plně dokumentované REST API	ANO	Nabízené řešení poskytuje plně dokumentované REST API.
28	Řešení musí poskytovat online API interface pro testování a dotazování	ANO	Nabízené řešení poskytuje online API interface pro testování a dotazování.
29	Řešení by mělo poskytovat uživatelům tlačítka pro spuštění akcí na externích systémech	ANO	Nabízené řešení poskytuje uživatelům tlačítka pro spuštění akcí na externích systémech.
30	Řešení by mělo využívat různé skriptovací jazyky pro integraci a akce (např. Python, Java, C#, bash/powershell, atd.)	ANO	Nabízené řešení využívá různé skriptovací jazyky pro integraci a akce (např. Python, Java, C#, bash/powershell, atd.).
31	Řešení by mělo umožňovat drag&drop konfiguraci GUI (např. polí na incidentu atd.) a workflow jako součást jediného administrátorského rozhraní	ANO	Nabízené řešení umožňuje drag&drop konfiguraci GUI (např. polí na incidentu atd.) a workflow jako součást jediného administrátorského rozhraní
32	Řešení by mělo umožňovat definovat vlastní proměnné u incidentů	ANO	Nabízené řešení umožňuje definovat vlastní proměnné u incidentů.
33	Řešení by mělo umožnovat definici vlastních typů incidentů navíc ke standardně dodávaným	ANO	Nabízené řešení umožňuje definici vlastních typů incidentů navíc ke standardně dodávaným.
34	Řešení by mělo umožňovat vkládat vlastní UI elementy (např. tlačítka, pole, rozbalovací menu, textová pole atd.)	ANO	Nabízené řešení umožňuje vkládat vlastní UI elementy (např. tlačítka, pole, rozbalovací menu, textová pole atd.).

35	Řešení by mělo umožnit jednotlivým týmům snadno vytvořit vlastní workflow	ANO	Nabízené řešení umožňuje jednotlivým týmům snadno vytvořit vlastní workflow.
36	Řešení by mělo poskytovat možnost snadno vytvářet pravidla pro dynamickou aktualizaci incidentů na základě různých podmínek (např. obsah polí incidentu)	ANO	Nabízené řešení poskytuje možnost snadno vytvářet pravidla pro dynamickou aktualizaci incidentů na základě různých podmínek (např. obsah polí incidentu).
37	Řešení by mělo být alternativně dodávané i jako virtuální appliance či jako SaaS verze	ANO	Nabízené řešení je alternativně dodávané i jako virtuální appliance či jako SaaS verze.

1.4. Technická specifikace - Ochrana databází a souborů

Výrobce / název / typ zařízení: **IBM Security Guardium Data Protection for Databases**

	Minimální technické požadavky	„Vyjádření ANO/NE“	„Technická specifikace nabízeného zařízení“, pokud je vyžadováno, pak i „Popis jak bude požadavek splněn/řešen“
1	Řešení podporuje monitoring veškerých sezení (vzdálená nebo lokální).	ANO	Nabízené řešení podporuje monitoring veškerých sezení (vzdálená nebo lokální).
2	Podporované databáze: Oracle, IBM DB2, Microsoft SQL Server, mySQL, IBM Informix, PostgreSQL, MongoDB.	ANO	Nabízené řešení podporuje databáze: Oracle, IBM DB2, Microsoft SQL Server, mySQL, IBM Informix, PostgreSQL, MongoDB.
3	Podpora platforem: Windows, UNIX, Linux.	ANO	Nabízené řešení podporuje platformy: Windows, UNIX, Linux.
4	Řešení identifikuje: časovou značku každé operace, celý příkaz operace, uživatelské jméno, odkazovaný objekt.	ANO	Nabízené řešení identifikuje časovou značku každé operace, celý příkaz operace, uživatelské jméno, odkazovaný objekt.
5	Řešení poskytuje nepřetržitý monitoring používání a toku citlivých dat.	ANO	Nabízené řešení poskytuje nepřetržitý monitoring používání a toku citlivých dat.
6	Řešení musí podporovat monitoring šifrovaných spojení na Oracle, MSSQL a DB2.	ANO	Nabízené řešení podporuje monitoring šifrovaných spojení na Oracle, MSSQL a DB2.
7	Řešení musí analyzovat data v reálném čase.	ANO	Nabízené řešení analyzuje data v reálném čase.
8	Řešení umožňuje aktivní blokování dle: ip adresy zdroje a cíle, uživatelského jména, databáze, tabulky, sloupce nebo názvu souboru, typ database.	ANO	Nabízené řešení umožňuje aktivní blokování dle: ip adresy zdroje a cíle, uživatelského jména, databáze, tabulky, sloupce

			nebo názvu souboru, typ database.
9	Řešení musí korelovat události dle nastavených prahů.	ANO	Nabízené řešení koreluje události dle nastavených prahů.
10	Řešení by se mělo být schopno učit odhalit anomálie, aby identifikovalo: neobvyklé nebo nové aktivity, neobvyklé nebo nové chyby, nové uživatele, nové typy objektů žádaných uživatelem, změnu chování v SQL struktuře, změnu chování v přístupovém čase.	ANO	Nabízené řešení odhaluje anomálie, aby identifikovalo: neobvyklé nebo nové aktivity, neobvyklé nebo nové chyby, nové uživatele, nové typy objektů žádaných uživatelem, změnu chování v SQL struktuře, změnu chování v přístupovém čase.
11	Řešení musí umožňovat zasílat poplachy, událostí, které identifikuje, pomocí: emailu, syslog události (konfigurovatelné pro integraci se SIEM systémy), programovatelného API rozhraní.	ANO	Nabízené řešení zasílá poplachy, událostí, které identifikuje, pomocí: emailu, syslog události (konfigurovatelné pro integraci se SIEM systémy), programovatelného API rozhraní.
12	Řešení musí přístup ke kontrolovaným datům kontrolovat RBAC a to na dvou vrstvách: přístup k systémovým funkcionalitám, přístup k uloženým datům.	ANO	Nabízené řešení přistupuje ke kontrolovaným datům kontrolovat RBAC a to na dvou vrstvách: přístup k systémovým funkcionalitám, přístup k uloženým datům.
13	Analýza SQL proudu by měla pokrývat příchozí a odchozí provoz a generované chyby.	ANO	Nabízené řešení pokrývá analýzu SQL proudu, pokrývá příchozí a odchozí provoz a generované chyby.
14	Řešení musí umět klasifikovat data pro identifikaci citlivých informací v databázích.	ANO	Nabízené řešení umí klasifikovat data pro identifikaci citlivých informací v databázích.
15	Řešení musí podporovat sady pravidel pro požadavky PCI-DSS, SOX a GDPR.	ANO	Nabízené řešení podporuje sady pravidel pro požadavky PCI-DSS, SOX a GDPR.
16	Řešení musí umožňovat vytváření vlastních klasifikačních pravidel dle: regulárních výrazů, porovnání se slovníkem, programovatelného API rozhraní.	ANO	Nabízené řešení umožňuje vytváření vlastních klasifikačních pravidel dle: regulárních výrazů, porovnání se slovníkem, programovatelného API

			rozhraní.
17	Řešení musí umožňovat tvorbu reportů v tabulkové a grafické formě.	ANO	Nabízené řešení umožňuje tvorbu reportů v tabulkové a grafické formě.
18	Řešení musí umožňovat vytváření automatizovaných reportů dle naplánovaného rozsahu.	ANO	Nabízené řešení umožňuje vytváření automatizovaných reportů dle naplánovaného rozsahu.
19	Systém by měl umožnit definovat postup vytváření a distribuce automatických výstrah a zpráv.	ANO	Nabízené řešení umožňuje definovat postup vytváření a distribuce automatických výstrah a zpráv.
20	Řešení musí archivovaná data ukládat v šifrované podobě.	ANO	Nabízené řešení archivovaná data ukládá v šifrované podobě.
21	Řešení musí obsahovat modul pro zhodnocení zranitelností, který pokrývá: CVE identifikaci, konfigurační zranitelnosti a slabiny dle CSI a STIG standard, identifikace nadměrných oprávnění a překryv oprávnění.	ANO	Nabízené řešení obsahuje modul pro zhodnocení zranitelností, který pokrývá: CVE identifikaci, konfigurační zranitelnosti a slabiny dle CSI a STIG standard, identifikace nadměrných oprávnění a překryv oprávnění.
22	Řešení musí být schopno monitorovat konfigurační nastavení a identifikovat změny na: databázové úrovni (SQL, skripty), na úrovni operačního systému (skripty, proměnné prostředí, registry).	ANO	Nabízené řešení monitoruje konfigurační nastavení a identifikovat změny na: databázové úrovni (SQL, skripty), na úrovni operačního systému (skripty, proměnné prostředí, registry).
23	Řešení musí poskytovat aktualizaci definic pro vyhodnocování nejméně každé čtvrtletí.	ANO	Nabízené řešení poskytuje aktualizaci definic pro vyhodnocování nejméně každé čtvrtletí.
24	Řešení musí provádět vyhodnocování opakovaně a automaticky.	ANO	Nabízené řešení provádí vyhodnocování opakovaně a automaticky.
25	Řešení musí umožňovat zasílat výsledky vyhodnocení dle definovatelného postupu a přímo příjemcům.	ANO	Nabízené řešení umožňuje zasílat výsledky vyhodnocení dle definovatelného postupu a přímo příjemcům.

1.5. Technická specifikace - Ochrana a správa koncových bodů

Výrobce / název / typ zařízení: **IBM Security BigFix Lifecycle**

	Minimální technické požadavky	„Vyjádření ANO/NE“	„Technická specifikace nabízeného zařízení“, pokud je vyžadováno, pak i „Popis jak bude požadavek splněn/řešen“
1	Systém by měl konzolidovat správu a zabezpečení koncových bodů do jediného systému, serveru, agenta a konzole	ANO	Nabízené řešení konsoliduje právu a zabezpečení koncových bodů do jediného systému, serveru, agenta a konzole.
2	Licence pro 2500 pracovních stanic (nebo laptopů) a 500 serverů	ANO	Nabízené řešení obsahuje licenci pro 2500 pracovních stanic (nebo laptopů) a 500 serverů.
3	Vyhodnocování a náprava bezpečnostních politik na úrovni agenta, ne na serveru	ANO	Nabízené řešení obsahuje vyhodnocování a náprava bezpečnostních politik na úrovni agenta, ne na serveru
4	Kontinuální vyhodnocování bezpečnostních politik (ne plánovaně za definované období, třeba jednou denně)	ANO	Nabízené řešení kontinuálně vyhodnocuje bezpečnostní politiky (ne plánovaně za definované období, třeba jednou denně).
5	Agent by měl zabírat méně než 10 MB v paměti počítače a měl by umožnit nastavení maximální hodnoty vytížení CPU (zabránění ohrožení běhu kritických aplikací)	ANO	Nabízené řešení obsahuje agenta, který zabírá méně než 10 MB v paměti počítače a umožňuje nastavení maximální hodnoty vytížení CPU (zabrání ohrožení běhu kritických aplikací).
6	Agent musí plnohodnotně fungovat i bez konektivity na server	ANO	Nabízené řešení obsahuje agenta, který plnohodnotně funguje i bez konektivity na server.
7	Agent se musí při přístupu na server autentizovat, aby bylo zabráněno přístupu neautorizovaným počítačům	ANO	Nabízené řešení obsahuje agenta, který se musí při přístupu na server autentizovat, aby bylo zabráněno přístupu neautorizovaným počítačům.

8	Systém musí umožnit nastavit zatížení sítě (např. při distribuci balíčků) podle jejího aktuálního stavu	ANO	Nabízené řešení umožňuje nastavit zatížení sítě (např. při distribuci balíčků) podle jejího aktuálního stavu.
9	Systém musí umožnit vytváření dalších politik a akcí pomocí jednoduchého skriptovacího jazyka	ANO	Nabízené řešení umožňuje vytváření dalších politik a akcí pomocí jednoduchého skriptovacího jazyka.
10	Systém musí podporovat vytváření vlastních dotazů vyhodnocovaných v reálném čase – např. "Jaké je seriové číslo všech počítačových monitorů" s minimálními nároky na zatížení počítačů a sítě	ANO	Nabízené řešení podporuje vytváření vlastních dotazů vyhodnocovaných v reálném čase – například umí zodpovědět dotaz: "Jaké je seriové číslo všech počítačových monitorů" s minimálními nároky na zatížení počítačů a sítě.
11	Systém musí podporovat širokou škálu platforem pro pracovní stanice i servery – Windows, Macintosh, Linux, UNIX operační systémy	ANO	Nabízené řešení podporuje širokou škálu platforem pro pracovní stanice i servery – Windows, Macintosh, Linux, UNIX operační systémy.
12	Systém musí poskytovat snadno použitelné uživatelské rozhraní i možnost ovládání pomocí příkazové řádky a integrační API	ANO	Nabízené řešení poskytuje snadno použitelné uživatelské rozhraní i možnost ovládání pomocí příkazové řádky a integrační API.
13	Součástí systému musí být integrovaný přístup na vzdálenou plochu počítačů bez nutnosti použít produkt třetí strany (minimum Windows a Linux)	ANO	Nabízené řešení obsahuje integrovaný přístup na vzdálenou plochu počítačů bez nutnosti použít produkt třetí strany (včetně Windows a Linux).
14	Systém musí umožnit nastavené jakéhokoliv spravovaného počítače jako brány do jiného segmentu sítě pro minimalizaci provozu na WAN síti	ANO	Nabízené řešení umožňuje nastavení jakéhokoliv spravovaného počítače jako brány do jiného segmentu sítě pro minimalizaci provozu na WAN síti.
15	Konzole musí umožnit řízení práv a rolí pro řízení přístupů k jednotlivým počítačům nebo jejich skupinám a k jednotlivým funkcionalitám	ANO	Nabízené řešení obsahuje konzoli, která umožňuje řízení práv a rolí pro řízení přístupů k jednotlivým počítačům nebo jejich skupinám a k jednotlivým funkcionalitám.
16	Systém musí umožnit zjistit nespravované zařízení na síti (počítače, směrovače, tiskárny a podobně) a vzdálenou centrální distribuci agenta	ANO	Nabízené řešení umožňuje zjistit nespravované zařízení na síti (počítače, směrovače, tiskárny a podobně) a vzdálenou centrální distribuci

			agenta.
17	Systém musí automatizovat správu záplat operačních systémů Windows, UNIX, Linux a Macintosh	ANO	Nabízené řešení automatizuje správu záplat operačních systémů Windows, UNIX, Linux a Macintosh.
18	Systém musí automatizovat správu záplat pro aplikace dalších vendorů, včetně Adobe, Mozilla, Google, Oracle a dalších	ANO	Nabízené řešení automatizuje správu záplat pro aplikace dalších vendorů, včetně Adobe, Mozilla, Google, Oracle a dalších.
19	Dodavatel řešení musí poskytovat pro svůj systém připravené balíčky záplat jednotlivých vendorů v řádu jednotek dnů po jejich poskytnutí vendorem	ANO	Dodavatel i výrobce řešení budou poskytovat pro svůj systém připravené balíčky záplat jednotlivých vendorů v řádu jednotek dnů po jejich poskytnutí vendorem
20	Jednotlivé záplaty musí být možno seskupovat pro jednodušší nasazení	ANO	Nabízené řešení obsahuje jednotlivé záplaty, které je možno seskupovat pro jednodušší nasazení.
21	Systém musí umožnit správu záplat i offline virtuálních počítačů (aby nebyly ohroženy hned po zapnutí)	ANO	Nabízené řešení umožňuje správu záplat i offline virtuálních počítačů (aby nebyly ohroženy hned po zapnutí).
22	Systém musí umožnit i snadné vytváření vlastních specifických záplat	ANO	Nabízené řešení umožňuje snadné vytváření vlastních specifických záplat.
23	Systém musí reportovat v reálném čase zpět stav instalace záplaty, např. záplata chybí, běží instalace, instalace provedena, instalace neprovedena z důvodu chyby a podobně.	ANO	Nabízené řešení reportuje v reálném čase zpět stav instalace záplaty, např. záplata chybí, běží instalace, instalace provedena, instalace neprovedena z důvodu chyby a podobně.
24	Systém musí přehledně, v reálném čase zobrazovat kde byly instalace provedeny, kdy a kým či kde jednotlivé záplaty mohou být nainstalovány	ANO	Nabízené řešení přehledně a v reálném čase zobrazuje, kde byly instalace provedeny, kdy a kým či kde jednotlivé záplaty mohou být nainstalovány.
25	Systém musí automaticky vyhodnotit shodu jednotlivých počítačů s politikou (např. minimální úroveň záplat)	ANO	Nabízené řešení automaticky vyhodnocuje shodu jednotlivých počítačů s politikou (např. minimální úroveň záplat).

26	Systém musí poskytovat možnost nabídnout záplaty nebo instalační balíčky uživatelům se stanovením nejpozdějšího data pro její instalaci	ANO	Nabízené řešení poskytuje možnost nabídnout záplaty nebo instalační balíčky uživatelům se stanovením nejpozdějšího data pro její instalaci.
27	Systém musí umožnit odložení restartu počítače po instalaci záplaty s vyžadovaným restartem	ANO	Nabízené řešení umožňuje odložení restartu počítače po instalaci záplaty s vyžadovaným restartem.
28	Systém musí detekovat a napravovat situaci, kde dříve instalovaná záplata byla odstraněna nebo přepsána	ANO	Nabízené řešení detekuje a napravuje situaci, kde dříve instalovaná záplata byla odstraněna nebo přepsána.
29	Systém musí umožnit automatickou reinstalaci odinstalovaných záplat	ANO	Nabízené řešení umožňuje automatickou reinstalaci odinstalovaných záplat.
30	Systém musí umožnit vytvoření odinstalační úlohy pro záplaty	ANO	Nabízené řešení umožňuje vytvoření odinstalační úlohy pro záplaty.
31	Systém musí umožnit správu napájecích schémat počítačů z centrální konzole	ANO	Nabízené řešení umožňuje správu napájecích schémat počítačů z centrální konzole.
32	Systém musí umožnit nastavit pravidla hybernace, standby módu a uložení souborů před vypnutím	ANO	Nabízené řešení umožňuje nastavit pravidla hybernace, standby módu a uložení souborů před vypnutím.
33	Systém musí umožnit nastavení různých schémat podle detekovaných vlastností počítače	ANO	Nabízené řešení umožňuje nastavení různých schémat podle detekovaných vlastností počítače.
34	Systém musí umožnit wake-on-lan i na sítích, kde jsou směrovače bez podpory této technologie (nepřeposílají wake-on-lan packet)	ANO	Nabízené řešení umožňuje wake-on-lan i na sítích, kde jsou směrovače bez podpory této technologie (nepřeposílají wake-on-lan packet).
35	Systém musí umožnit naplánované probuzení počítačů, např. před začátkem pracovní doby nebo pro provedení pravidelné údržby	ANO	Nabízené řešení umožňuje naplánované probuzení počítačů, např. před začátkem pracovní doby nebo pro provedení pravidelné údržby.
36	Systém musí poskytnout možnost distribuci balíčků na různé platformy	ANO	Nabízené řešení poskytuje možnost distribuci balíčků na různé platformy.
37	Balíčky musí být instalovatelné na základě různých politik (např. podmínka minimální paměti nutné	ANO	Nabízené řešení obsahuje balíčky, které jsou instalovatelné na základě

	pro software a podobně)		různých politik (např. podmínka minimální paměti nutné pro software a podobně).
38	Systém musí umožnit uživatelům bez administrátorských práv na stanici instalaci softwarových balíčků z katalogu	ANO	Nabízené řešení umožňuje uživatelům bez administrátorských práv na stanici instalaci softwarových balíčků z katalogu.
39	Systém musí umožnit předběžné zaslání balíčku na koncové stanice před samotnou instalací	ANO	Nabízené řešení umožňuje předběžné zaslání balíčku na koncové stanice před samotnou instalací.
40	Systém musí podporovat možnost instalace balíčku podle přihlášeného uživatele na stanici	ANO	Nabízené řešení podporuje možnost instalace balíčku podle přihlášeného uživatele na stanici.
41	Systém musí poskytovat jednoduchý, ale silný skriptovací nástroj pro přesné zacílení distribuce a instalace balíčků (psaní podmínek)	ANO	Nabízené řešení poskytuje jednoduchý, ale silný skriptovací nástroj pro přesné zacílení distribuce a instalace balíčků (psaní podmínek).
42	Systém musí obsahovat plně integrovanou možnost instalace operačních systémů na nové počítače přes síť - "bare-metal provisioning" a rovněž možnost migrace operačních systémů nebo jejich obnovu na stávajících počítačích včetně možnosti migrace uživatelských dat	ANO	Nabízené řešení obsahuje plně integrovanou možnost instalace operačních systémů na nové počítače přes síť - "bare-metal provisioning" a rovněž možnost migrace operačních systémů nebo jejich obnovu na stávajících počítačích včetně možnosti migrace uživatelských dat.
43	Systém musí umožnit vytvoření obrazu operačního systému pro distribuci operačního systému nezávislého na cílovém hardware	ANO	Nabízené řešení umožňuje vytvoření obrazu operačního systému pro distribuci operačního systému nezávislého na cílovém hardware.

2. Požadavky na implementaci řešení

Implementace řešení bude dodána v následujících fázích:

A.) Zpracování detailního návrhu řešení SIEM

1. Analýza stávajících interních předpisů Zadavatele dotčených projektem SIEM
2. Specifikace hardware, který bude součástí dodávky řešení
3. Specifikace požadavků na provozní prostředí
4. Popis metodiky vyhodnocení testovacího provozu pro předání díla do rutinního provozu.
5. Návrh integrace SIEM s informačními systémy provozovanými nebo využívanými Zadavatelem, které budou umožňovat napojení na SIEM.
6. Analýza prostředí na potřeby Log management, tj. počty jednotlivých komponent pro dohledování, sběr technických parametrů (protokol, typ logu), stanovení typického objemu log dat za den.
7. Zpracování získaných dat o Log management procesu a stanovení základních tříd Data_retention
8. Stanovení základních kategorií log dat pro směrování do SIEM modulu – bezpečnostní log data, log data s vlivem na služby, log data s vlivem na aplikace, log data s vlivem na systémy.
9. Analýza aktiv a stanovení základních kategorií aktiv (Assets) – Analýza IP adresního plánu a sledovaného prostředí. Zjištěna aktiva budou rozložena do tříd client, server, network, storage s přidělením hodnoty aktiva ve stupních critical, important, normal, low.
10. Ohodnocení aktiv v kontextu jimi obsažených/zpracovávaných informací a dat vázaných na zákony ČR (Spisová služba, Ochrana osobních údajů) a legislativu Objednatele (Důvěrné informace, Monetizační informace).
11. Analýza datových toků a pravidel na perimetrech datových sítí (firewallů) – analýza architektury datových komunikací, kdo může s kým komunikovat, kdo je omezen komunikovat, analýza nastavení systémové politiky detekčních systémů IDS/IPS.
12. Analýza potřeb výstupních informací procesů Configuration management (potřeby na nastavení Dasboard a nastavení Reportů o kondici aktiv – zranitelnosti, počet změn sledovaného prostředí, aktuální verze SW), Incident Response (potřeby na nastavení Dasboard a nastavení Reportů o počtu incidentů, trendy, compliance reporting).
13. Detailní popis implementace, včetně časového harmonogramu,
14. Popis instalačních procedur pro instalaci SIEM
15. Návrh akceptačních kritérií pro předání díla do testovacího provozu včetně návrhu akceptačního protokolu pro předání díla do testovacího provozu; akceptační kritéria musí obsahovat výčet všech požadavků na funkčnost díla.
16. Detailní návrh bude podroben interní oponentuře Zadavatele. V případě připomínek Zadavatele je Dodavatel povinen tyto připomínky do detailního návrhu řešení zapracovat. Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky. Detailní návrh řešení se stane jeho předáním majetkem Zadavatele, který jej bude moci plně využít pro svoje potřeby ke všem způsobům užití, a to bez dalšího souhlasu zhotovitele nebo zpracovatele.

B.) Implementace

Implementace SIEM do prostředí Zadavatele začně na základě akceptovaného a předaného Detailního návrhu řešení.

S ohledem na velký počet kritických informačních systému budou v první řadě realizovány významné informační systémy, dle definovaných požadavků Zákona o kybernetické bezpečnosti. Následně po zapojení těchto informačních systémů do bezpečnostního monitoringu budou v rámci rutinního provozu vybrány další informační systémy z identifikovaných kritických z pohledu bezpečnosti, které budou potupně napojovány na bezpečnostní monitoring MHMP.

Významné informační systémy

Následující informační systémy, identifikovány jako Významné Informační Systémy z pohledu Zákona o kybernetické bezpečnosti. Rovněž se jedná o aplikace, které na základě své kritičnosti budou primárně zařazeny do systému bezpečnostního monitoringu prostředí MHMP.

Id	Název
1.	GINIS EKO - Jednotný ekonomický systém
2.	Spisová služba GINIS - SSL
3.	Portál Praha.eu - Internetové aplikace a prezentace
4.	Elektronická pošta (Exchange server)

Důležité IS

Níže uvedené informační systémy, mají nižší prioritu než významné informační systémy.

S ohledem na tuto skutečnost není v současnosti nutné je zařadit hned do systému bezpečnostního monitoringu. Tyto IS budou postupně zařazeny do systému bezpečnostního monitoringu či sběru a archivace bezpečnostních logů v rámci služby poskytování služeb základní podpory (SLA/helpdesk/konzultace/Bezpečnostní monitoring) pro kompletní SIEM dle čl. 2.1.2. Smlouvy o zajištění provozu a podpory.

Následující IS tak budou plánovány postupně až po úplném připojení všech významných informačních systémů do systému bezpečnostního monitoringu. Systémy budou postupně vybrány dle aktuálního hodnocení rizik těchto informačních systémů.

Id	Název
5.	CRŘ- řidičské oprávnění - systém MD
6.	CRV - registr vozidel - systém MD
7.	Dopravní přestupky
8.	Správní řízení

9.	Zveřejňování podkladů na jednání Zastupitelstva (OBIS)
10.	Zveřejňování dat o grantech a žadatelích na grantovém portálu
11.	Pošta pro MČ - ZRIS (Základní radniční informační systém)
12.	Městská policie – Informační Systém MP
13.	Hosting e-SPIS pro MMČ a zřízené organizace
14.	Hosting Proxio/Agendio pro MMČ
15.	Zajištění vzdáleného přístupu do modulu TED (OBIS)
16.	Správa a evidence majetku pro MČ a MMČ, MP
17.	Proxio/Agendio - moduly ENO, CENO, LENO
18.	Systém ISKŘ
19.	Service komunikačních a informačních technologií ZBS
20.	Správa a evidence majetku SEM
21.	Elektronická pošta
22.	Active Directory
23.	Personalistika FLUX
24.	Konektivita Magnet
25.	Konektivita Mepnet
26.	Datové systémy Flux
27.	Datové systémy GIS
28.	Datové systémy Gordic
29.	Datové systémy Marbes
30.	Datové systémy MP Orga
31.	Informační systém o území hl. m. Praha (ISU) - Digitální mapy (GIS)
32.	Základní registry přes CzechPoint - systém MV
33.	Základní registry Hledáček
34.	Příprava podkladů na jednání Rady a Zastupitelstva, zpracování smluv, evidence

	pohledávek a závazků (OBIS)
35.	Grantová agenda - systém GRANTY

Implementace SIEM do prostředí Zadavatele bude probíhat v této souslednosti:

1. **Instalace SIEM do prostředí**

- Vlastní instalace HW/SW SIEM.
- Nastavení síťové komunikace (přidělení IP adres, nastavení DNS, NTP), nastavení přístupů pro obsluhu.
- Nastavení konfigurace pro sběr log dat.
- Nastavení konfigurace pro sběr flow.
- Nastavení síťové komunikace s LDAP.
- Nastavení základní eskalace o provozních anomáliích.

2. **Nastavení Assesment and Risk management**

- Nastavení tříd aktiv
- Nastavení profilů aktiv
- Vložení aktiv do profilů, tříd a přidělení odpovídající hodnoty.
- Nastavení základních profilů skenování zranitelností pro třídy aktiv client, server.
- Možnosti a nastavení Reconciliace aktiv. Detekce konfiguračních změn, detekce přidaného/odebraného aktiva.
- Nastavení základní eskalace o provozních anomáliích sběru zranitelností.

3. **Nastavení Flow**

- Konfigurace pasivního sběru (TAP), sondy, kolektoru.
- Napojení dat z flow na SIEM.
- Nastavení základní eskalace o provozních anomáliích sběru flow.

4. **Nastavení Log management**

- Nastavení příjmu log dat.
- Ověření ovládání dálkové správy sběru log dat.
- Detailní nastavení konektorů pro sběr logů z definovaných komponent.
- Vývoj a doplnění konektorů pro nestandardní zařízení a formáty log dat.
- Nastavení základní Data_retention politiky.
- Nastavení základní eskalace o provozních anomáliích sběru log dat.

5. **Nastavení korelačních pravidel na SIEM**

- Nastavení základních továrních korelačních pravidel.
- Detailní nastavení korelačních pravidel.
- Doplnění individuálních korelačních pravidel pro specifické požadavky.
- Nastavení sledování performance a capacity monitoringu s eskalací o provozních

anomáliích SIEM.

6. Vytvoření Dasboard profilů a reportů

- Aktivace generování továrních reportů.
- Tvorba výstupních sestav dle požadavků Objednatele.
- Uzpůsobení Dashboard potřebám Objednatele.

7. Ladění False-positives Alarms

- Nastavení eskalace z korelačních pravidel dle potřeb procesu Incident Response (eskalační matice, způsob eskalace).
- Ladění detekce událostí na skutečném provozu formou sledování výpočtu Event score
- Magnitude, hodnoty aktiv v detekované události, významu zranitelností v detekované události, četnosti zachycených událostí – treshold pro alert.
- Detekce úspěšnosti konektorů ve zpracování log dat – detekce chyb zpracování log dat.

3. Školení pracovníků Zadavatele

Předmětem veřejné zakázky je rovněž provedení školení pro uživatele a administrátory Zadavatele k používání a správě SIEM:

Školení 3 administrátorů SIEM v celkovém rozsahu 24 hodin. Školení bude probíhat v sídle Zadavatele, a to nejpozději během testovacího provozu dle harmonogramu uvedeného v detailním návrhu řešení.

Za organizační zajištění školení zodpovídá dodavatel. Zadavatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti.

4. Ostatní požadavky

Součástí dodávky je udělení veškerých potřebných licencí pro užívání a správný chod celého SIEM, a to v rozsahu dle návrhu smlouvy o dílo a dále následovně.

Součástí dodávky jsou:

Licence SIEM pro zajištění provozu v produkčním prostředí, včetně tzv. Maintenance (předplatné aktualizace SW) na 36 měsíců

Další potřebný SW:

Součástí zakázky bude kromě licencí vlastního informačního systému SIEM také dodávka a udělení potřebného počtu všech případných dalších licencí veškerého dalšího software potřebného k provozování všech požadovaných součástí této zakázky, a to včetně jejich technické podpory. To se týká operačního systému, databází, aplikačních serverů, či jiných komponent potřebných pro provoz řešení.

Součástí nabídkové ceny je i cena licencí a dodání serverového operačního systému nutného pro provoz nabídnutého řešení, a to včetně jeho maintenance po dobu 36 měsíců od zahájení podpory. V případě potřeby CALů pro přístup k MS Windows serverům zahrne Dodavatel též cenu potřebných CAL licencí do nabídkové ceny.

V případě, že serverový operační systém, který je nutný pro provoz nabídnutého řešení, není

jedním z operačních systémů podporovaných v rámci IT infrastruktury Zadavatele (Microsoft Windows Server 2008 R2 a vyšší, FreeBSD, Debian, CentOS/RedHat), je součástí nabídkové ceny též cena administrátorského školení v rozsahu 40 hodin pro 5 pracovníků pověřených Zadavatelem pro správu tohoto serverového systému.

V případě nabídky řešení formou tzv. virtual appliance (předkonfigurovaný virtuální image od výrobce daného řešení) je přípustný provoz na platformě VMware.

Provozní prostředí

Infrastruktura Zadavatele je provozována na platformách Microsoft Windows Server, FreeBSD, Debian, CentOS/RedHat a jsou provozovány LDAP adresáře MS Active Directory a SUN/Oracle eDirectory a OpenLDAP a MS ForeFront. Je využíváno řešení virtualizace na platformě VMware vSphere 5 a vyšší. Aplikační servery jsou provozovány jak virtuálně, tak hardwarově.

Zadavatel povoluje možnost rutinního provozu nabízeného řešení na těchto platformách v prostředí Zadavatele.

Poskytování služeb technické podpory provozu a maintenance SIEM

Poskytovatel bude poskytovat Objednateli služby spočívající v zajištění podpory SIEM (dále jen „**Služby**") na základě **Smlouvy o zajištění provozu a podpory programového vybavení.**

Smlouva zhrnuje tyto služby:

1. **Služby údržby SIEM – maintenance**
    - Poskytování nových verzí SIEM a opravných patchů dle aktuální technologické úrovně,
    - Podpora certifikovaného bezpečnostního konzultanta,
    - Poskytování služeb monitoringu a dohledových služeb nad platformou SIEM, tj. zaručený provoz, v režimu 24/7/365, monitoringu nad dodaným HW/SW řešením).
    - a to vše včetně aktualizací dokumentace v rozsahu dle čl. 7.12 této Smlouvy.

2. **Služby základní podpory SIEM**
    - Poskytování služby HotLine/Helpdesk včetně servisní technické podpory SIEM dle parametrů SLA sjednaných touto Smlouvou.
    - Poskytování poradenských služeb prostřednictvím HotLine/Helpdesk při řešení běžných provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.
    - Poskytování služeb Správa provozu služby SIEM - bezpečnostního monitoringu (24/7/365), prostřednictvím vyhodnocovacího centra pro řešení incidentů, a to denně v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.

3. **Služby rozšířené podpory SIEM**
    - Školení dle požadavků Objednatele nad sjednaný rozsah.
    - 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.

Podrobné vymezení služeb technické podpory provozu a maintenance SIEM je obsaženo v Příloze č. 3 Smlouvy o technické podpoře.