Příloha č. 1a zadávací dokumentace č.j. MUCL/144935/2023

Technická specifikace předmětu plnění

I. Obecné požadavky objednatele

Předmětem smlouvy o dílo je dodávka a implementace komplexního bezpečnostního systému sítě IT objednatele specifikovaného touto přílohou. Objednatel požaduje vytvoření dostatečně silného a bezpečného prostředí informačních technologií pro zajištění bezproblémového chodu městského úřadu při výkonu státní správy a samosprávy.

Objednatel požaduje integrované řešení s jednou centrální správou pro všechny požadované systémy přes jedno webové rozhraní. Je vyžadován unikátní přístup pro každého administrátora a zároveň volitelně možnost sdílených přístupů (jeden přístup pro více administrátorů) a integrací všech zmíněných částí níže do jedné platformy XDR (Extended EDR).

V rámci dodaného systému požaduje objednatel poskytování outsoursované služby MDR (Managed Detection and Response) přímo od výrobce v režimu 24/7/365 po celou dobu platnosti licence.

II. Zabezpečení vstupu do sítě na perimetru

2.1 Základní parametry požadovaného řešení – Next Generation Firewall

Objednatel požaduje dodání řešení Next-generation Firewall typu hardware appliance. Administrace řešení musí být možná přes webové rozhraní s podporou textového rozhraní tzv. „cli“. Součástí dodávky musí být veškeré licence pro zajištění požadovaných funkcí.

Kompletní řešení se musí skládat ze dvou fyzických zařízení (hardware appliance) zajišťující funkcionalitu vysoké dostupnosti (active-passive) a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware). Dodané řešení musí podporovat hardware akceleraci skrze dedikovaný čip (nezávislý na standardním procesoru).

K dodanému řešení je požadována podpora od výrobce 24/7/365, záruka na dodaný hardware a licenci po dobu 5 let.

2.2 Požadované funkce dodávaného řešení

2.2.1 Základní požadavky na funkcionality dodávaného řešení
Stavové filtrování paketů
Překlady komunikace (příchozí i odchozí)
Podpora funkcionality typu SD-WAN (včetně funkce rozkládání zátěže mezi primární a záložní internetovou linkou a WAN failover na základě dostupnosti WAN konektivity).
Montáž do standardních 19" skříní (rack).
100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu telnet/ ssh konzole)
Propojení a využívání Active Directory
Podpora bezagentového přihlášení uživatelů nezávislé na portu komunikace
DHCP server a DNS forwarder pro konkrétní sítě
Možnost automatické zálohy systému a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy
Vynucení šifrování záloh
Logování a rozšířený reporting (vč. statistik uživatelských aktivit)

Podpora vrácení se na předchozí verzi software (po aktualizaci na novou verzi systému)
Vlastní API rozhraní pro propojení s dalšími interními nástroji
Licenčně neomezený počet uživatelů a internetových domén.
2.2.2 Požadavky na proaktivní ochranu perimetru
IDS/IPS filtr nastavitelný na konkrétní komunikaci (pravidla firewall)
Možnost vytvářet vlastní IPS pravidla
Blokování komunikace C&C a typu Botnet a možnost specifikace výjimek
Identifikování kompromitovaného systému na základě C&C komunikace
Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce).
Logování a reportování
2.2.3 Požadavky na vzdálené přístupy (VPN)
IPSEC – propojení vzdálených lokalit, včetně podpory IKEv2
SSL VPN i IPSEC – připojení vzdálených PC
SSL VPN - Odlišný certifikát / uživatel
Možnost vzdálené instalace VPN klienta
Zobrazení aktuálně připojených uživatelů v GUI
Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat
Neomezený počet SSL VPN a IPSEC klientů v ceně
Logování a reportování
2.2.4 Požadavky na ochranu přístupů na internet
Filtrování HTTP, HTTPS a FTP
SSL / TLS skenování neomezené jen na HTTPS protocol
Ochrana skenováním antimalware
URL filtrování (min. 75+ kategorií)
Blokování datových typů na základě přípony souboru a MIME hlavičky
Propojení s Active Directory
Možnost definovat výjimky (minimálně na zdrojové IP, cílové IP a webové stránky)
Podpora platnosti pravidel pouze ve specifikovaný čas
Pravidla musí být možno specifikovat na skupinu/uživatele z Active Directory
Podpora Sandboxingu
Logování a reportování
2.2.5 Požadavky na reverzní proxy ochranu interních webových serverů a aplikací
Ochrana skenováním antimalware motorem
Filtrování http a https komunikace
Automatické přesměrování http komunikace na https
Podpora nahrávání vlastních certifikátů pro jednotlivé virtuální servery
Možnost monitorovat nebo blokovat (odmítnout) komunikaci
Přeposílání originální hlavičky (pro zobrazení skutečných zdrojů komunikace na cílovém serveru)

Podpora zabezpečení koncových aplikací vytvářením přihlašovacích formulářů navázaných na Active Directory
Ochrana proti útokům na aplikace
Ochrana proti podvržení cookies (podepisování)
Blokování komunikace na základě reputační služby výrobce
Blokování útoků typu SQL injection
Možnost specifikace výjimek
Logování a reportování
2.2.6 Požadavek o možnost rozšíření o správu WiFi
Dodávané řešení musí být rozšiřitelné o správu wifi zařízení (vše od stejného výrobce) a nesmí být k tomu vyžadováno zakoupení další licence (pokud bude vyžadováno zakoupení, musí být součástí nabídky pro neomezený počet WiFi AP a neomezené funkcionality, které řešení v této kategorii poskytuje).

2.3 Minimální technické požadavky a propustnosti deklarované výrobcem

Požadavek na propustnost sítě	
Hardware akcelerace	například pomocí ASIC čipu
Active/passive cluster	2 fyzická zařízení
Propustnost	Hodnota
Firewall	>50Gbps
IPSEC VPN	>30 Gbps
IPS	>12 Gbps
NGFW	>12 Gbps
Latence	<5 µs
Konkurenční spojení	>12 miliónů
Nová spojení / sekunda	>250000

III. Zabezpečení koncových bodů – PC stanic a severů

3.1. Základní specifikace požadovaného řešení

Požadováno je zabezpečení operačních systémů na koncových (uživatelských) počítačích a serverech.

Jsou požadovány moduly od jednoho výrobce, které budou integrovány do jednoho celku s jednou centrální správou přes webové rozhraní. Centrální správa bude řešena v cloudu, přičemž umístění cloudového prostředí se připouští pouze v rámci EU. Součástí dodávaného řešení bude veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz pro:

- 350 uživatelů
- 30 serverů (operačních systémů)
- 350 stanic

K dodanému řešení je požadována podpora MDR od výrobce v režimu 24/7/365 po dobu 5 let.

3.2 Požadované funkce dodávaného řešení

3.2.1 Základní požadavky	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Podporované OS	Windows 8 a vyšší, Windows server 2016 a vyšší, Linux servery Na OS Linux se připouští omezenější funkcionality než na OS Windows.
Podpora klientů pro operační systémy ve virtuálním prostředí v rozsahu popisu.	VMware vSphere a Microsoft Hyper-V
Integrace s Active Directory	
Aktualizační cache a optimalizace komunikace	Komponenta zajišťující centrální stahování aktualizací a jejich redistribuci v rámci lokální sítě + komunikační proxy pro komunikaci s centrální správou
Instalace nových verzí klientů koncových klientů v rámci aktualizačního procesu (navíc k běžné aktualizaci bezpečnostních signatur).	Nesmí vyžadovat manuální aktualizaci programových komponent.
Klientskou část musí být možné skriptovat (například instalovat v režimu tiché instalace a instalovat novou verzi přímo z lokální cache)	-
Instalace (aktualizace) nových verzí centrální správy v ceně licencí po celou dobu platnosti licence	-
Logování bezpečnostních incidentů	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)
Nastavení politik na úrovni skupina/uživatel/server	-
API rozhraní pro propojení s nástroji třetích stran	-
Dvoufázové ověřování při přihlášení do administrátorské konzole	
Podpora českého jazyka	Minimálně pro klienta software na koncovém systému uživatele.
3.2.2 Požadavky na běžnou antimalwarovou kontrolu	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Rezidentní antimalware ochrana	Aktualizace min. 4 x denně
Heuristická analýza	-
Použití online signatur při výskytu podezřelých souborů	-
Skenování souborů před stažením z internetu	Před uložením na disk
Plánované skenování	-
Definice výjimek	Na plánovaný sken i anti-malware ochranu, a to minimálně na soubor, složku, proces, exploit,

	webovou stránku a C&C komunikaci.
3.2.3 Požadavky na proaktivní ochranu	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Blokování C&C komunikace a komunikace typu Botnet	-
HIPS (Host-Based IPS)	-
Kontrola zařízení (minimálně USB vyjímatelná zařízení, USB šifrovatelná vyjímatelná zařízení, optická média, bluetooth, multimediální zařízení, Wi-Fi)	Pro každé ID zařízení nebo modelovou řadu zařízení musí být možnost zvlášť zvolit akce (povolit, pouze monitorovat, blokovat).
Data Loss Prevention	Blokace přenosů dat na základě datového typu a obsahu souboru.
Aplikační kontrola	Včetně možnosti samostatného monitorování výskytu nepovolených aplikací a blokace aplikací z pravidelně aktualizovaného seznamu výrobce.
Ochrana přístupu na internet minimálně v rozsahu, URL filtrování (30+ kategorií, Data Loss, blokování přístupů na veřejné emailové portály).	-
3.2.4 Požadavky na ochranu nově generace	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Anti – Exploit	Požadována ochrana blokování útoků využívajících zranitelností v operačním systému nebo aplikacích.
Ochrana před známými typy průniků	(například APC, DLL Hijacking, Enforce Data Execution Prevention, Hollow Process, Reflective DLL Injection, Stack Pivot atd.)
Anti – Exploit alespoň pro základní aplikace (MS Office, Java, Internetové prohlížeče apod.)	-
Anti – ransomware	Požadováno blokování i neznámých malware kategorie „Ransomware“ a „Crypto-Ransomware“ vč. funkcionality roll-back (vrácení původních, již zašifrovaných souborů po zastavení Crypto-Ransomware, max. 5 zašifrovaných souborů, před jejich obnovou pro prevenci přetížení paměti. Funkcionalita zastavení síťového šifrování (přes počítačovou síť).
Přímá ochrana MBR	Například proti ransomware
Ochrana proti zvýšení oprávnění útočníka	-
Aplikační whitelisting pro servery	-
Monitoring modifikace kritických systémových souborů pro servery	-
Ochrana proti přepisování kódu v paměti	-
Ochrana proti odcizení přihlašovacích údajů	-

Machine Learning technologie	Včetně analýzy důvodu označení za škodlivý kód a potlačení False Positive detekce antimalware
Automatické vyčištění systému na aplikační úrovni	-
Automatická izolace postižených stanic od sítě na úrovni klient endpoint protection na koncovém systému uživatele.	-
3.2.5 Požadavek na XDR (Extended Endpoit Detection & Response)	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Alertování	Při zachyceném incidentu vygenerování alertu
Průzkum incidentu na základě záznamu v systému XDR	Zobrazení a označení zdroje malware (kudy se malware dostal do sítě).
Zjednodušený náhled na nákazu	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření
Grafické znázornění průběhu nákazy	Minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a souborové úrovni a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres, analýza souborů přes Machine Learning
Možnost globálního vyčištění a blokování nalezeného malware.	-
Vytvoření „hash“ pro soubor na úrovni lokálního klienta a vyhledání infikovaných počítačů na základě tohoto „hash“ malware	-
Automatické vyhodnocení incidentů	-
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby)	Minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.
Podpora Threat Huntingu	Práce s koncovými systémy v reálném čase zasílání dotazů, příkazů apod. na koncové systémy přes XDR rozhraní pomocí vlastních a předdefinovaných dotazů (jejich rozsah záleží na výrobci).

IV. Zabezpečení emailové komunikace

4.1 Základní parametry požadovaného řešení – Next Generation Email Protection

Požadováno je řešení ochrany a zabezpečení emailové komunikace využívající nástroj nové generace. Administrace řešení musí být možná přes webové rozhraní s podporou použití API. Centrální správa bude řešena v cloudu, přičemž umístění cloudového prostředí se připouští pouze v rámci EU. Součástí dodávaného řešení bude veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz pro:

- 350 uživatelů.

K dodanému řešení je požadována podpora MDR od výrobce v režimu 24/7/365 po dobu 5 let.

4.2 Požadované funkce dodávaného řešení

4.2.1 Základní požadavky	
Požadované vlastnosti a funkce	***Popis – upřesnění***
Podporované emailové servery	Kompatibilita musí být zajištěna s jakýmkoliv SMTP serverem (pro zachování možnosti změny stávajícího emailového řešení)
Integrace s Active Directory	Minimálně na úrovni výčtu emailových adres
Logování emailové komunikace	Minimálně v následujícím rozsahu: Datum, Čas, Příjemce, Odesílatel, Předmět, provedená akce
Plnohodnotná správa přes webové rozhraní	Bez nutnosti používá SSH přístupy apod
Vynucení dvoufaktorového ověření pro administrátory	
Možnost odděleného auditního přístupu	Tzn. uživatel bez možnosti změny politik
Centrální karanténa	S možností doručit uživatelům emaily označené jako spam z karantény
Uživatelská karanténa	Dostupná přes nějaký druh webového portálu i pro koncové uživatele minimálně s možností úplně zakázat nebo povolit.
Zasílání sumáře karantény uživatelům	Seznam emailů nebo odkaz na karanténu musí být možno zasílat minimálně 3x denně v předem zvolené časy během pracovních dní (od pondělí do pátku), případně volitelně i v sobotu a nastavení musí být globální i oddělitelné pro každou skupinu uživatelů zvlášť.
Skenování odchozího i příchozího provozu	
API rozhraní pro propojení s nástroji třetích stran	Musí umožňovat propojení s EDR (nebo XDR) řešením
4.2.2 Požadavky na bezpečnostní funkce	
Ochrana antimalware a antispam motorem	
Ochrana motorem využívající strojového učení (machine learning) a neurálních sítí	
Blokování emailů obsahující URL odkazy na malware	
Rozdělení spamů na minimálně 2 kategorie (dle pravděpodobnosti) s možností nastavení akcí pro každou kategorii zvlášť	
Pro emaily obsahující malware možnost nastavit úplné smazání emailu nebo uložení do karantény	
Reputační služba výrobce	
Podpora neomezeného množství domén a IP adres	
Možnost nastavení politik pro každou doménu zvlášť	
Funkce relay nastavitelná na konkrétní doménu (na jakou adresu mail serveru se emaily doručí)	
Logování a reportování	
4.2.3 Požadavky na rozšířené bezpečnostní funkce	
Blokování různých datových typů v emailech (například spustitelné soubory, skripty apod.)	
Předdefinovaný seznam blokovaných datových typů výrobcem (doporučení výrobce)	

Blokování emailů na základě velikost emailu (větší než)
Blokování emailů na základě velikosti příloh (větší než)
Blokování emailů na základě kombinace kritérií velikosti emailu a velikosti přílohy (větší a menší než) – například příloha menší než 10 MB a celá zpráva menší než 20 MB.
Filtrace emailů na základě jejich obsahu s použitím klíčových slov (s podporou regulárních výrazů), včetně možnosti importu
Možnost nastavení pravidel zvlášť pro příchozí a odchozí poštu
Podpora šifrování odchozí emailů na základě předem definovaných pravidel
Podpora alespoň dvou typů šifrování – celého emailu nebo jen příloh
Podpora šifrování alespoň S/MIME, případně jsou možné i jiné typy šifrování zajišťující podobnou funkcionalitu
Podpora vynucení TLS 1.3 komunikace konkrétním uživatelem
Podpora vynucení šifrování emailu uživatelem (například Add-in do poštovního klienta, přidání příkazu do předmětu nebo jinak)
Nastavitelné akce (min. smazání emailu, smazání příloh, přesunutí do karantény)
Funkce notifikování příjemce a administrátora
Možnost nastavení všech funkcí bezpečnostního omezení emailů na konkrétní odesílatele (pro konkrétní doménu i pro konkrétní emailové adresy).
4.2.4 Požadavky na ověřování emailů a další funkce
Ochrana proti spamům / phishing emailům
Ověřování uživatelů – DMARC, SPF, DKIM
Funkce ochrany podvržení identit
Možnost definice akcí při detekci podvržení identity – minimálně v rozsahu varování v těle emailu, uložení emailu do karantény, změna předmětu, smazání zprávy
Možnost definování akce pro neskenovatelné emaily (zašifrovaný obsah apod.) – minimálně uložit do karantény, označit změnou předmětu, smazat.
Greylisting nebo podobná bezpečnostní technologie umožňující „zdržovat“ komunikace na úrovni navazující SMTP komunikace
Skenování příloh emailů
Sandboxing – s vynucením používání datového centra v EU
Blokace na základě RBL
Blokování emailů na základě reputační služby výrobce
Blokování emailů na základě reputace URL adres v emailech
Možnost volitelné akce při otevření nebezpečného URL odkazu uživatelem z emailu – minimálně na úrovních zablokovat a varovat uživatele a možnost úpravy hlášení směrem k uživateli pro obě varianty
Skenování odkazů URL v emailech i v době otevření tohoto URL uživatelem
Možnost náhledu uživatelů na vlastní emailové fronty přes webový uživatelský portál (například v době výpadku emailového serveru)
Podpora globálních černých a bílých listin
Podpora uživatelských černých a bílých listin nastavitelných přes webový uživatelský portál

Kontrola emailové fronty ze stejného webového rozhraní
Kontrola a práce s emailovou karanténou ze stejného webového rozhraní bez nutnosti využívat externích služeb (další server, externí databáze apod.)
Náhled uživatele do své karantény pomocí „uživatelského portálu“ (jen pro emaily konkrétního uživatele) a možnost uvolnění spamů
Logování a prohledávání logů min. na úrovni: Odesílatel, Příjemce, Předmět emailu
Ochrana před únikem citlivých informací, filtrování příchozích a odchozích emailů pomocí předdefinovaných pravidel (citlivé informace, osobní identifikovatelné údaje, finanční informace atd.).
Logování a reportování

4.3 Minimální technické požadavky a propustnosti deklarované výrobcem

Požadavek	
Minimální propustnost emailů *)	1000 emailů / 24 hodin / uživatel
Minimální možnost navýšení řešení pouze změnou licence *)	5 x tolik uživatelů
Aktualizace centrální správy musí být prováděna výrobcem.	Bez nutnosti součinnosti
Vestavěná kontextová nápověda.	Nápověda přes webové rozhraní dostupná v jednotlivých menu zvlášť (tak aby se po kliknutí objevila nápověda pro danou sekci nastavení).
Role-Based Access Management	Podpora definice jednotlivých přístupů a jejich úrovní přístup do systému – minimálně v rozsahu auditního přístupu, podpory uživatelů a globálního administrátora.

*) Naplnění těchto limitů se nepředpokládá, nicméně pro zajištění udržitelnosti na ně dodané řešení musí být připraveno.

V. Zabezpečení mobilních zařízení

5.1 Základní specifikace požadovaného řešení

Požadováno je řešení ochrany a zabezpečení mobilních systémů na koncových zařízeních uživatelů a chytrých zařízeních, tzv. Unified Endpoint Managemant včetně Mobile Security. Centrální správa bude řešena v cloudu, přičemž umístění cloudového prostředí se připouští pouze v rámci EU. Součástí dodávaného řešení bude veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz pro:

- 100 zařízení,
- 100 uživatelů mobilních zařízení.

Součástí dodávky zabezpečení mobilních zařízení není HW. Na dodaný software je požadována podpora výrobce a záruka na dobu 5 let pro následující prostředí:

5.2 Požadované funkce dodávaného řešení

5.2.1 Základní požadavky	
Požadované vlastnosti a funkce	***Popis – upřesnění***
Podporované klientské systémy	Android a iOS, IoT zařízení
Integrace s Active Directory	
Stejný nástroj se musí využívat pro správu ochrany počítačů i chytrých zařízení.	
Instalace nových klientů přes průvodce	Uživatelé musí mít možnost přidávat svá zařízení přes „uživatelských portál“
Instalace nových politik součástí instalace	Musí mít možnost proběhnout v jedné instalační úloze.
Instalace nových programů součástí instalace klienta	Musí mít možnost proběhnout v jedné instalační úloze.
Instalace (aktualizace) nových verzí centrální správy v ceně licencí po celou dobu platnosti licence	
Podpora BYOD	Včetně možnosti oddělení politik pro zařízení organizace a vlastněných uživatelem
Skupinování a aplikace bezpečnostních politik minimálně na skupiny zařízení a jednotlivá zařízení	
Výpis zařízení uživatele a jejich stavu pro každé zařízení.	
Zobrazení výrobního (sériového) čísla a IMEI čísla chytrého zařízení v centrální správě	Především možnost pozdějšího dohledání v případě ztráty/odcizení zařízení.
Podpora Android Enterprise a Samsung Knox	
Logování bezpečnostních incidentů	Globální logování ze všech komponent software dostupné z centrální správy. Filtrace dle uživatele, počítače nebo skupin (uživatelů a počítačů)
5.2.2 Požadavky na zabezpečení systému	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Antimalware ochrana	Minimálně pro platformu Android
Machine learning (engine používající strojové učení)	Minimálně pro platformu Android
Webová filtrace (včetně URL filtrování)	-
Ochrana WIFI připojení	Minimálně kontrola bezpečnostni zvolené Wifi sítě
Možnost definice Wifi sítí	Zařízení bude poté mít předdefinovanou wifi síť včetně přístupového hesla
Možnost schvalování aplikací pro instalaci na koncovém zařízení	Možnost povolení stahování nových aplikací pouze přes Wifi
Skenování souborů stažených z internetu	Minimálně pro platformu Android
Plánované skenování	Minimálně pro platformu Android

Minimální délka a složitost hesla	Možnost nastavení politiky délky hesla a složitosti (použití speciální znaků, velká a malá písmena, číslice), podpora přihlášení pomocí gest a biometrického přihlášení (Face ID a otisk prstu)
Ochrana proti použití stejného hesla znovu	
Automatický zámek po uplynuté době	
Maximální stáří hesla	
Vynucení šifrování zařízení	
Možnost provádět geolokaci zařízení	Včetně auditní stopy (kdo a kdy zařízení vyhledával)
Funkce vzdáleného smazání dat v zařízení	
Vynucení minimální verze OS	
Možnost provedení resetování zařízení do továrního nastavení	
Možnost zakázání kamery	
5.2.3 Požadavky na správu zařízení	
Požadované vlastnosti a funkce	***Popis - upřesnění***
Podpora vzdálené instalace politik	
Podpora vzdálené instalace aplikací	Z vlastního úložiště i za využití obchodů výrobce (Google Play a App Store)
Specifikace vyžadovaných software (například, antimalware, VPN klient apod.)	
Možnost specifikace zakázaných software	Například přeinstalované aplikace od výrobce zařízení nebo nežádoucí aplikace.
Možnost exportu zařízení do xls	Export kvůli inventarizaci – minimálně v rozsahu: jméno zařízení, popis, druh hardware, verze OS, skupina, stav správy, nainstalované aplikace, sériové číslo.
Možnost rozšíření správy o Windows 10 a macOS.	Podpora těchto mobilních zařízení (notebooky).
Kontrola stavu zařízení a reportování	Reportování minimálně v rozsahu – odpovídá nebo neodpovídá požadavkům na zařízení

VI. MDR (Managed Detection and Response)

6.1 Bližší požadavky na zabezpečení

Požadováno je SOC (Security Operation Center) typu MDR po celou dobu platnosti licence přímo od výrobce nabízeného řešení.

MDR musí splňovat:

- 24/7/365 expertně vedené monitorování hrozeb včetně reakcí.
- Aktivní zadržování hrozeb ze strany výrobce v rámci MDR (výrobce útoky přeruší, čímž se zabrání šíření).

- Výrobce disponuje rozsáhlým týmem odborníků, kteří aktivně řeší problémy se zákazníkem v rámci MDR (odstranění nákaz apod.) a garantuje zapojení toho týmu v případě potřeby, kterou je aktivní nákaza v licencí pokrytém perimetru objednatele.
- Reakce na incidenty v plném rozsahu – kompletní odstranění hrozby i neaktivních částí (v celé síti objednatele).
- Proaktivní volání (oznámení a řešení) podporou během aktivních incidentů (ze strany výrobce).
- Automatické, pravidelné reportování (min. 1x za měsíc).
- Pravidelná kontrola aktuálního stavu řešení dle potřeby k zajištění všech parametrů produktu.
- Analýza příčiny nákazy jako prevence budoucího opakování (příp. návrh na příslušné opatření).
- Přidělený kontakt v případě aktivní nákazy