Obsah

[**a) NAC** **2**](#_Toc221110660)

[Bezpečný přístup do sítě 2](#_Toc221110661)

[Základní popis 2](#_Toc221110662)

[Technická specifikace 2](#_Toc221110663)

[**b) PIM/PAM 15**](#_Toc221110664)

[1. Základní popis 15](#_Toc221110665)

[2. Definice pojmů 16](#_Toc221110666)

[3. Požadavky na systémy a protokoly pro řízení hesel a bezpečné přístupy 16](#_Toc221110667)

[4. Technické požadavky na PIM/PAM technologii 16](#_Toc221110668)

[5. Analýza a rozsah nasazení 18](#_Toc221110669)

[6. Požadavky na licencování 19](#_Toc221110670)

[7. Podrobné technické požadavky na řešení 19](#_Toc221110671)

[8. Předpokládaná součinnost ze strany zadavatele 27](#_Toc221110672)

[**c) Síťové sondy 28**](#_Toc221110673)

[1. Základní požadavky na dodávku a implementaci - technická specifikace 28](#_Toc221110674)

[2. Požadavky na funkční vlastnosti a technické parametry dodávaných zařízení 29](#_Toc221110675)

[1) Funkční vlastnosti 29](#_Toc221110676)

[2) Technické a výkonnostní parametry dodávaných zařízení 34](#_Toc221110677)

[1 kus … Monitorovací sonda 2x10Gbps (hardware appliance) 34](#_Toc221110678)

[1 kus ... Zařízení pro zpracování a vyhodnocení dat (virtual appliance) 35](#_Toc221110679)

[3) Požadavky na vybrané příklady použití 37](#_Toc221110680)

[**d) SIEM 39**](#_Toc221110681)

[**e) SOC 43**](#_Toc221110682)

[**Požadované služby v rámci záruky poskytované na části plnění a) až e) 45**](#_Toc221110683)

## a) NAC

# Bezpečný přístup do sítě

## Základní popis

Systém musí umožňovat nasazení a správu Network Admission Control (NAC). Tento řeší bezpečné připojení koncových stanic a konkrétních uživatelů na základě procesu autentizace (rozpoznání identity zařízení a uživatele) a autorizace (zpřístupnění konkrétních datových zdrojů podle uživatelské role, stavu koncového zařízení) a dalších atributů v rámci kontextu uživatele.

Integrované funkce zajišťují komunikaci s AAA serverem (RADIUS) a nastavují komplexní, přitom unifikované, bezpečnostní politiky pro autentizaci a autorizaci koncových bodů.

Architektura musí zaručit, že všichni uživatelé (mobilní zaměstnanci, ale i dodavatelé nebo prodejci) budou vždy jednoznačně identifikováni a prostřednictví přidělených rolí jim bude zajištěn bezpečný přístup ke všem informacím v síti, na které mají nárok.

Po ověření identity uživatele je mu přiřazena jedna z předem definovaných rolí, prostřednictvím které se může následně pohybovat v síti se všemi odpovídajícími právy i omezeními. Využitím informace získané při ověření identity spolu s rolemi skupin uživatelů nebo serverů připojených k síti, minimalizujeme rizika neoprávněných přístupů a zjednodušujeme celý proces nasazení bezpečnostních pravidel v síti i jejich následnou správu.

Bezpečnostní management musí poskytnout zjednodušenou správu bezpečnostních politik a umožnit tak jejich konzistentní nastavení v rámci celé sítě. Předpokladem je řízení pravidel přístupu na LAN i WLAN přístupové vrstvě, včetně tzv. „Guest Access“. Přitom v procesu definice pravidel bude bráno v úvahu více parametrů, které má systém k dispozici (identita uživatele, pracovní skupina, místo, čas, typ zařízení, atd.). Budou definovány různé třídy přístupu podle různých vstupních parametrů, které budou aplikovány v definicích pravidel (policy).

Komunikaci koncové stanice musí být možné dynamicky přesunout do jiného pracovního segmentu (ale i např. karantény) nebo uplatnit přístupové filtry tzv. „za běhu“ pomocí řízení CoA (Change of Aathorization = proces aplikace pravidel pomocí rozšíření protokolu RADIUS, popsaném v RFC) na základě aktuálního vyhodnocení vstupních parametrů (typ koncového zařízení, jeho stav, apod.)

Systém by měl být rozšířitelný i o řízení bezpečného transportu datovou sítí (implementace šifrování na rozhraních přepínačů) a možnosti škálovatelné filtrace přístupů k datovým zdrojům na základě uživatelských bezpečnostních rolí.

Komponenty centrálního bezpečnostního managementu, s vazbou na externí autentizační databáze, např. AD, LDAP mají být využitelné i pro přiřazení bezpečnostních politik na dalších zařízení (např. firewall) na základě uživatelské identity nebo jeho skupinové bezpečnostní role.

Důraz je kladen na centrální správu, dohled a možnosti vyhodnocení událostí, generace reportů apod. na jednom místě.

## Technická specifikace

Dodaná zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následujících tabulkách.

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry.*

*Uvedený požadovaný způsob splnění funkcionality/vlastnosti je minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

NAC

| **Požadovaná funkcionalita/vlastnost** | **Minimální způsob splnění funkcionality/vlastnosti** | **Doplní účastník dle nabízeného zařízení** |
| --- | --- | --- |
| **Formát zařízení** |  |  |
| Je dostupné ve formě Virtuální Appliance | Ano |  |
| Požadovaný počet podporovaných koncových zařízení, současně aktivních | 3185 |  |
| **Škálování** |  |  |
| Umožňuje instalovat jako agregovanou platformu celého řešení | Ano |  |
| Umožňuje instalovat jako distribuovanou platformu centrálně řízeného celého řešení | Ano |  |
| **Obecná charakteristika ověřovacího řešení** |  |  |
| Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.) | Ano |  |
| Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup | Ano |  |
| V rámci ekosystému vytvořenému pomocí integrační platformy musí být možno použít adaptivní řízení síťových prvků organizace, které umožnuje rychle reagovat na útoky metodou přímého využití sítě jako vynucovacího prostředku (konkrétní scénáře odpojení uživatele). V praxi toto může znamenat odpojení problematického koncového zařízení přímo od rozhraní LAN přepínače nebo od WiFi přístupového prvku na základě signalizace od detekčního bezpečnostního systému umístěného uvnitř sítě. | Ano |  |
|  |  |  |
| Řešení musí mít možnost, při dokoupení licencí, být plně redundantní | Ano |  |
| Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity | Ano |  |
| Umožňuje snadné zálohování , rychlou a úplnou obnovu konfigurace | Ano |  |
| Poskytuje AAA funkce (viz níže) | Ano |  |
| Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control) | Ano |  |
| Zohlednění kontextu v definici pravidel přístupu (např. typ autentizace, zařízení (NAD), technologie, čas, lokalita, identita uživatele, apod.) | Ano |  |
| Možnost zabezpečené komunikace mezi uzly distribuovaného řešení pomocí IPsec | Ano |  |
| Zabezpečení komunikace RADIUS/TACACS+ mezi přístupovými prvky a AAA serverem pomocí IPsec | Ano |  |
| Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují) | Ano |  |
| Certifikace UC APL, Common Criteria, a FIPS 140-2 | Ano |  |
| Řešení je pozicováné v “Leaders” Gartner kvadrantu po dobu 5 posledních let | Ano |  |
| **AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)** |  |  |
| RADIUS pro autentizaci, autorizaci, zaznamenávání | Ano |  |
| Možnost rozšíření licence pro podporu TACACS+ | Ano |  |
| Možnost rozšíření licence pro podporu MFA pro TACACS+ | Ano |  |
| Proxy funkce pro externí RADIUS | Ano |  |
| Podpora 802.1X protokolů EAP (Extensible Authentication Protocol):   * EAP-TLS * EAP-PEAP (Protected EAP)   + PEAP-MSCHAPv2   + PEAP-GTC (Generic Token Card) * EAP-TTLS (Tunneled TLS) * EAP-FAST (Flexible Authentication via Secure Tunneling) * EAP-FASTv2 (EAP Chaining) | Ano |  |
| Podpora Web-Based a Non-802.1X autentizace:   * MAB (MAC Authentication Bypass) * Web Authentication (WebAuth)   + Local WebAuth   + Central WebAuth (CWA) * Self-Registered Guest Access | Ano |  |
| Podpora ověřování s certifikáty:   * TLS (Transport Layer Security) * SCEP (Simple Certificate Enrollment Protocol) | Ano |  |
| Podpora Passive Identity Authentication:   * Passive Identity Services (získání identity z AD, SIEM, apod.) | Ano |  |
| Možnost autentizace s integrovanými externími systémy:   * SAML, včetně SSO * OAuth 2.0/OpenID Connect * Kerberos * AD, LDAP | Ano |  |
| Podpora TEAP (Tunneled Extensible Authentication Protocol) dle IETF standardu (RFC 7170) pro duální autentizaci | Ano |  |
| Podpora interních autentizačních TEAP protokolů:   * EAP-TLS (certificate-based) * MSCHAPv2 (username/password-based) * EAP-GTC (token-based authentication) * EAP-TTLS (for additional flexibility) | Ano |  |
| Automatické zakázání non-FIPS autentizačních protokolů (např. PAP/ASCII, CHAP, and MS-CHAPv1) při aktivaci FIPS módu | Ano |  |
| **Podporované databáze uživatelů (s možností definovat pořadí průchodu** |  |  |
| Interní (pro uživatele i koncová zařízení) | Ano |  |
| Active Directory | Ano |  |
| Active Directory – více nezávislých domén | Ano |  |
| Možnost autentizace oproti více AD domén, i když nejsou v trust režimu | Ano |  |
| LDAP (RFC 2251) | Ano |  |
| RADIUS Token indentity source (RFC 2865) | Ano |  |
| RSA RADIUS token server | Ano |  |
| Autentizace pomocí údajů obsažených v uživatelském certifikátu | Ano |  |
| Možnost vyčítání informací o uživateli z Active Directory (Passive Fingerprint) | Ano |  |
| **Ověřování uživatelů a zařízení** |  |  |
| Ověření uživatelů heslem nebo certifikátem | Ano |  |
| Ověření MAC adresou připojovaného zařízení | Ano |  |
| Ověření stroje a uživatele (ve všech kombinacích) pomocí EAP Chaining s certifikáty nebo PAC soubory | Ano |  |
| Ověření stroje a uživatele (ve všech kombinacích) pomocí TEAP | Ano |  |
| **Rozpoznávání typu koncových zařízení a jejich stavu** |  |  |
| Možnost dokoupení licence pro automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou | Ano |  |
| Předdefinované profily pro běžná mobilní zařízení | Ano |  |
| Možnost zákaznického nastavení profilů zařízení nebo vytváření vlastních „signatur“ pro rozpoznávání nových nebo specifických typů zařízení | Ano |  |
| **Autorizace: pružný systém pro definici pravidel pro přístup k síti** |  |  |
| Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle   * uživatele (role, skupiny) * stavu a typu koncového zařízení (viz výše) * místa připojení * přístupového zařízení (konkrétní přepínač, WiFi koncentrátor, SSID, VPN koncentrátor) * historie připojení a autentizace | Ano |  |
| Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě | Ano |  |
| Možnost rozšíření o omezení přístupu k síti pomocí filtrů aplikovaných v síťové infrastruktuře i na výstupu ze sítě, s využitím informací získaných v procesu autentizace na vstupu | Ano |  |
| Možnost mapování bezpečnostní role uživatele, podle AD skupin, na jeho aktuální datové spojení (session) i bez podpory 802.1X na přístupovém zařízení nebo koncovém zařízení. | Ano |  |
| Podpora Change of Authorization (CoA, RFC 3576) | Ano |  |
| Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů | Ano |  |
| Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti | Ano |  |
| Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat | Ano |  |
| Možnost rozšíření o spolupráci uživatele na uvedení stanic do požadovaného stavu (informací, odkazem,spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru) | Ano |  |
| Možnost aktivovat na přistupujících stanicích zákaznické skripty v rámci autorizačních kroků | Ano |  |
| **Accounting** |  |  |
| Zaznamenávání aktivity uživatelů a zařízení připojených k síti | Ano |  |
| Dotazovací systém, korelace záznamů, centralizované výkazy | Ano |  |
| Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů) | Ano |  |
| Knihovna předpřipravných reportů přímo na appliance | Ano |  |
| **Funkce GUEST serveru** |  |  |
| Vytváření casově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi | Ano |  |
| Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů | Ano |  |
| Zohlednění bezpečnostní role administrátora (sponzora) přístupu pro hosty, odrážející se v právech konfigurace | Ano |  |
| Samoobslužný portál pro uživatele | Ano |  |
| Optimalizace autentizačního web portálu i pro mobilní platformy | Ano |  |
| Plná lokalizace portálu pro sponzory (administrace) i pro hosty (autentizace) | Ano |  |
| Rozhraní pro integraci s externími operátory pro zasílání SMS zpráv s autentizačními údaji | Ano |  |
| Veškeré potřebné funkce pro guest access (portály pro sponzory, captive portály pro přihlašování, atd.) obsaženy v základní licenci a instalovaném SW | Ano |  |
| Možnost vytváření více virtuálních portálů pro administraci dočasných (guest) účtů i vlastní autentizaci. Např. podle typu přístup LAN/WiFi, lokality, apod. | Ano |  |
| Možnost modifikovaných virtuáních portálů pro guest access pomocí integrovaného editoru vzhledu portálu | Ano |  |
| Ověření přes HTTP a HTTPS | Ano |  |
| **Podpora BYOD** |  |  |
| Onboarding (registrace, provisioning, nastavení klientských zařízení) | Ano |  |
| Onboarding/provisioning proces formou samoobsluhu | Ano |  |
| Portál pro registraci nových zařízení s možností samoobsluhy pro uživatele (přidání, odebírání, vynucení odpojení ze sítě, apod.) | Ano |  |
| Specifické politiky pro BYOD zařízení | Ano |  |
| Možnost nastavení limitu BYOD zařízení pro jednoho uživatele | Ano |  |
| Appliance poskytuje funkce pro distribuci nastavení přístupu (802.1X supplicant) se zohledněním typu platformy, uživatele, apod. | Ano |  |
| Automatické a pro uživatele transparentní zažádání o certifikát a jeho doručení na koncovou platformu | Ano |  |
| Podpora interní CA, pro vydávání certifikátů BYOD zařízením | Ano |  |
| Interní CA lze řetězit jako subordinate pod firemní CA | Ano |  |
| Automatické vyplnění CN uživatele v certifikátu | Ano |  |
| Uzamčenní certifikátu pro konkrétní koncovou platformu (zapsání ID stanice přímo do certifikátu) | Ano |  |
| Uřivatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení) | Ano |  |
| **Podpora MDM** |  |  |
| Integrace s MDM systémy | Ano |  |
| Podpora workflow pro registrace do MDM | Ano |  |
| Podpora externích MDM platforrem a zohlednění informací z MDM v pravidlech přístupu | Ano |  |
| Nástroje MDM přímo v rozhraní samoobslužného portálu uživatelských zařízení pro zamykání, mazání, apod. | Ano |  |
| API mezi appliance a MDM pro obousměrný přenos informací | Ano |  |
| **Device Management** |  |  |
| Podpora protokolu TACACS+ pro možnost řízení přístupu administrátorů na síťová zařízení | Ano |  |
| Okamžitý informace o prováděných příkazech na síťových zařízeních | Ano |  |
| Možnost aktivace služby TACACS+ bez nutnosti instalace dalšího systému nebo SW | Ano |  |
| Podpora distribuovaného řešení TACACS+ (více výkonných TACACS+ serverů s centrální správou) | Ano |  |
| Řízení konfiguračních nebo přehledových příkazů na prvcích infrastruktury podle role administrátora | Ano |  |
| Možnost definice sad příkazů a jejich přiřazení podle role administrátora | Ano |  |
| Při specifikaci příkazů lze použít wildcard a regex syntaxi | Ano |  |
| Možnost signalizace „privilege“ úrovně s oprávněními již definovanými ve spravovaném zařízení | Ano |  |
| Proxy TACACS+ | Ano |  |
| Možnost integrace vícefaktorové autentizace pro řízení přístupu k prvkům sítě | Ano |  |
| Konfigurační wizard pro aktivaci TACACS+ služeb a jejich konfiguraci | Ano |  |
| Generace přehledových reportů prováděných akcí na prvcích sítě | Ano |  |
| **Funkce pro správu ověřovacího systému** |  |  |
| Centralizovaná správa | Ano |  |
| Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému | Ano |  |
| Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení | Ano |  |
| Grafické rozhraní pro definici pravidel přístupu k síti | Ano |  |
| Grafické rozhraní pro monitorování, definici výkazů, řešení problémů | Ano |  |
| Wizardy v GUI plaxormy pro asistované a rychlé nastavení profilování, guest access, BYOD, řízení přístupu a propagace bezpečnostních rolí, apod. | Ano |  |
| Nástroje pro audit konfigurace přístupové infrastruktury s doporučením na best practice nastavení | Ano |  |
| Kontrola definice dynamických ACL v GUI appliance před aplikací na přístupové prvky | Ano |  |
| Diagnostika problemů (systémová, údaje o chybách přihlašování, TCP dump, packet capture) | Ano |  |
| Sledování session (sezení) přímo v rozhraní GUI s možností okamžitého odpojení nebo přesměrování do karantény | Ano |  |
| Zaznamenávání událostí na externí syslog server | Ano |  |
| Podpora SNMPv3 | Ano |  |
| NTP pro synchronizaci času | Ano |  |
| SMTP pro zasílání zpráv a výstrah přes e-mail | Ano |  |

36 kusů přepínačů

|  |  |  |
| --- | --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Minimální způsob splnění požadované funkcionality/vlastnosti** | **Doplní účastník dle nabízeného zařízení** |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| Typ přepínače | L2/L3 přepínač |  |
| Formát přepínače | Stohovatelný |  |
| Stohování požadováno | ANO |  |
| Minimální počet dedikovaných stohovacích portů | 2 |  |
| Minimální počet zařízení ve stohu | 8 |  |
| Minimální kapacita sběrnice stohu | 80 Gb/s |  |
| Stateful Switch Over v rámci stohu | ANO |  |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |  |
| Redundantní ventilátory | ANO |  |
| Minimální počet portů 10/100/1000 Base-TX s podporou 802.1 at/af | 24 |  |
| Uplink porty - minimálně | 4x1GE SFP |  |
| Min. velikost sdíleného systémového bufferu | 6MB |  |
| Minimální velikost MAC address tabulky | 16000 |  |
| Min. počet IPv4 routes | 1000 |  |
| Min. počet IPv6 routes | 1000 |  |
| Min. počet konfigurovatelných security ACL | 1000 |  |
| IEEE 802.3ad (Link Aggregation) | ANO |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |  |
| IEEE 802.1Q | ANO |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1x | ANO |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |  |
| RADIUS CoA | ANO |  |
| Podpora instance spanning-tree protokolu per VLAN | ANO |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |  |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |  |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |  |
| OSPFv2 | ANO |  |
| OSPFv3 | ANO |  |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO |  |
| IGMPv2, IGMPv3 | ANO |  |
| IGMP snooping | ANO |  |
| MLD snooping | ANO |  |
| Minimální počet HW QoS front | 8 |  |
| QoS classification – ACL, DSCP, CoS based | ANO |  |
| QoS marking - DSCP, CoS | ANO |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |  |
| QoS Policing | ANO |  |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |  |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |  |
| Možnost definovat povolené MAC adresy na portu | ANO |  |
| PACL, VACL | ANO |  |
| IEEE 802.1ae na uplink portech | ANO |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |  |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |  |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |  |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |  |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |  |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |  |
| IEEE 802.3az | ANO |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |  |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |  |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |  |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | ANO |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |  |
| SSHv2 | ANO |  |
| CLI rozhraní | ANO |  |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |  |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |  |
| Plná kompatibilita s dodávaným NAC řešením | ANO |  |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |  |
| SNMPv2/v3 | ANO |  |
| Podpora network boot (iPXE) | ANO |  |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |  |
| NTPv3 server | ANO |  |

1 kus přepínače

|  |  |  |
| --- | --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Minimální způsob splnění požadované funkcionality/vlastnosti** | **Doplní účastník dle nabízeného zařízení** |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
|  |  |  |
| Typ přepínače | L2/L3 přepínač |  |
| Formát přepínače | Stohovatelný |  |
| Stohování požadováno | ANO |  |
| Minimální počet dedikovaných stohovacích portů | 2 |  |
| Minimální počet zařízení ve stohu | 8 |  |
| Minimální kapacita sběrnice stohu | 80 Gb/s |  |
| Stateful Switch Over v rámci stohu | ANO |  |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |  |
| Redundantní ventilátory | ANO |  |
| Minimální počet portů 10/100/1000 Base-TX s podporou 802.1 at/af | 48 |  |
| Uplink porty - minimálně | 4x1GE SFP |  |
| Min. velikost sdíleného systémového bufferu | 6MB |  |
| Min. Velikost MAC address tabulky | 16000 |  |
| Min. počet IPv4 routes | 1000 |  |
| Min. počet IPv6 routes | 1000 |  |
| Min. počet konfigurovatelných security ACL | 1000 |  |
| IEEE 802.3ad (Link Aggregation) | ANO |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |  |
| IEEE 802.1Q | ANO |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1x | ANO |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |  |
| RADIUS CoA | ANO |  |
| Podpora instance spanning-tree protokolu per VLAN | ANO |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |  |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |  |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |  |
| OSPFv2 | ANO |  |
| OSPFv3 | ANO |  |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO |  |
| IGMPv2, IGMPv3 | ANO |  |
| IGMP snooping | ANO |  |
| MLD snooping | ANO |  |
| Minimální počet HW QoS front | 8 |  |
| QoS classification – ACL, DSCP, CoS based | ANO |  |
| QoS marking - DSCP, CoS | ANO |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |  |
| QoS Policing | ANO |  |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |  |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |  |
| Možnost definovat povolené MAC adresy na portu | ANO |  |
| PACL, VACL | ANO |  |
| IEEE 802.1ae na uplink portech | ANO |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |  |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |  |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |  |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |  |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |  |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |  |
| IEEE 802.3az | ANO |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |  |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |  |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |  |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | ANO |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |  |
| SSHv2 | ANO |  |
| CLI rozhraní | ANO |  |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |  |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |  |
| Plná kompatibilita s dodávaným NAC řešením | ANO |  |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |  |
| SNMPv2/v3 | ANO |  |
| Podpora network boot (iPXE) | ANO |  |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |  |
| NTPv3 server | ANO |  |

20 kusů modulů SFP, plně kompatibilních s dodávanými přepínači ve specifikaci 1000BASE-SX SFP transceiver module, MMF, přesně 850nm, DOM

## b) PIM/PAM

Dodávka a implementace systému PIM/PAM – technická specifikace

## Základní popis

Zadavatel poptává systém pro řízení a správu privilegovaných účtů (dále jen PIM/PAM), který zajistí jednotnou správu přístupu k privilegovaným účtům a monitorování operací prováděných pod těmito účty s vazbou na konkrétního administrátora, který v danou chvíli účet používá, včetně dvou faktorové autentizace a poskytnutí podrobného seznámení se správou dodaného systému pro IT pracovníky zadavatele.

Jednotlivé informační systémy, které Zadavatel provozuje jsou spravovány privilegovanými účty, které jsou využívány pro správu aplikací nebo systémových služeb a jako takové představují významné bezpečnostní riziko pro každou organizaci.

Z hlediska bezpečnosti umožňují téměř neomezený přístup a manipulaci s informačními aktivy organizace, v případě kompromitace privilegovaného účtu je organizace vystavena velkému riziku zneužití nebo vyzrazení informací nebo jejich zneužití.

Požadavek řídit privilegované účty je hlavním požadavkem zákona o kybernetické bezpečnosti č. 264/2025 Sb. a standardů kybernetické bezpečnost.

Cílem projektu je řešit:

* Vyhledání a inventarizace privilegovaných účtů
* Bezpečná správa hesel a SSH klíčů pro privilegované účty
* Komplexní správa privilegovaných účtů – uživatelů
* Bezpečný přístup na cílový systém pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu
* Centrální kontrolní bod pro izolaci, řízení a sledování všech aktivit správců
* Monitoring a nahrávání vzdálených relací a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání
* Kontrola čtyř očí (Dual Control) a oddělení rolí (Segregation of Duties)
* Auditní stopa a personalizace využití sdílených účtů
* Bezpečný mechanismus pro vyzvedávání hesel a SSH klíčů pro aplikace

Systém, který bude zajišťovat jednotnou správu a monitoring privilegovaných účtů Zadavatele. Systém bude dodán včetně analýzy stávajícího stavu, dodávky technologie (HW, SW, licence), instalace, konfigurace, uvedení do provozu, a následné zajištění technické podpory, zajištění záruky výrobce a zajištění dostupnosti softwarových aktualizací, a to na všechny části a komponenty dodaného Systému (HW, SW i licence) po dobu pěti let.

Řešení musí být instalováno ve formě HW/virtuální appliance a bude zajištěna vysoká dostupnost HA řešení, Bude provozována na stávající virtualizační infrastruktuře Zadavatele dle výchozího stavu (viz Příloha č. 11 zadávací dokumentace – Stávající stav).

Zadavatel požaduje, aby vlastní přihlašovací údaje a klíče k cílovým systémům (k operačním systémům, databázím, zařízením, aplikacím apod.) byly chráněné a šifrované v databázi systému.

Připojení do sítě LAN bude realizováno spojením minimálně dvou fyzických ethernetových síťových linek konfigurovaných tak, aby konektivita byla zachována při výpadku jedné linky.

## Definice pojmů

Pojem privilegovaný účet označuje účet v operačním nebo informačním systému, který má vysoké oprávnění. Jedná se o účty typu root v Linux/UNIX systémech, účty typu Administrátor ve Windows systémech, systémové účty používané aplikacemi nebo sdílené účty, které nejsou vázané na fyzickou osobu.

S těmito účty pracují privilegovaní uživatelé. Pojem privilegovaný uživatel označuje fyzickou osobu, která používá privilegované účty. Jedná se o pracovníky provozu, dodavatele, nebo vývojáře.

Cílový systém označuje systém, na který se privilegovaný uživatel připojuje prostřednictvím privilegovaných účtů.

## Požadavky na systémy a protokoly pro řízení hesel a bezpečné přístupy

Podpora musí být zajištěna minimálně pro následující technologie:

* Windows 7, 8, 8.1, 10, Windows Server 2008, 2012, 2016, 2019
* Linux Red Hat, Suse, Debian, Centos, Unix, AIX
* Active Directory
* Virtualizační platformy VMWare, HyperV, Citrix
* Databáze MS SQL, Oracle, MySQL,
* Zařízení Fortinet, Cisco, Juniper

Podpora přihlášení bez nutnosti manuálně vkládat heslo a nahrávání relací minimálně pro následující aplikace a protokoly:

* protokoly: RDP, SSH, Telnet
* DB klienti: SQL Management Studio
* Web GUI: Edge, Chrome

## Technické požadavky na PIM/PAM technologii

* Řešení bude poskytovat správcovský přístup na cílový systém prostřednictvím privilegovaných účtů, ke kterým má uživatel přístup dle bezpečnostní politiky. Účty a systémy, ke kterým nemá práva přístupu, nebudou pro uživatele viditelné.
* Řešení bude umožňovat víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém.
* Správcovský přístup na cílový systém bude zprostředkován pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace jako je např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, SAML a RADIUS).
* Řešení musí umožňovat silnou autentizaci přistupujících uživatelů pomocí multifaktorové autentizace - MFA. MFA musí být nedílnou součástí nabídky řešení, může se jednat jak o nativní nástroj PIM/PAM řešení, tak MFA nástroj třetí strany.
* Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V záznamech je možné zpětně vyhledávat využitím metadat, které budou mimo jiné minimálně obsahovat:
  + u RDP relací spuštěné aplikace a události
  + u SSH relací jednotlivé příkazy
* Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI dodávaného řešení.
* Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditorem), který v případě potřeby má možnost sledovanou relaci ukončit.
* Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data pořízení, uživatele a spuštěného příkazu.
* Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML atp.).
* Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v zabezpečeném úložišti.
* Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě tak, aby k nim měl přístup pouze oprávněný uživatel.
* Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.
* Řešení musí splňovat požadavky na bezpečnostní certifikaci odpovídající úrovni ochrany přístupů k privilegovaným účtům a citlivým systémům organizace.
* Řešení musí být dimenzované minimálně pro 650 cílových systémů a neomezený počet přihlašovaných uživatelů (interní správci a externí dodavatelé)
* Řešení umožňuje centrální webový přístup přes zabezpečený HTTPS protokol a podporuje prohlížeče Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash)
* Systém centrálního webového přístupu – VPN-less, přes HTTPS protokol je dodán jako aplikace
* Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS (není tedy například nutné otevírat z klientské stanice RDP/SSH/... protokoly mezi uživatelem a jump Serverem bude vždy otevřený pouze bezpečný WebSocket protokol (port 443).

## Analýza a rozsah nasazení

V rámci nasazení systému bude probíhat analýza, která popíše implementaci řešení včetně detailního návrhu harmonogramu realizace této části plnění. Harmonogram plnění musí být plně v souladu s podmínkami dle Smlouvy, která tvoří přílohu č. 1 zadávací dokumentace, zejm. s harmonogramem, který tvoří přílohu č. 2 Smlouvy.

Obsahem analýzy bude upřesnění instalace, parametrizace, definování workflow, popis realizace integrace s navazujícími systémy provozovanými v prostředí zadavatele.

Výsledkem bude popis způsobu a postup vlastní implementace v prostředí zadavatele v tomto rozsahu:

* Analýza stávajícího stavu privilegovaných účtů v infrastruktuře Zadavatele (servery, aktivní síťové prvky, management systémy, databáze)
* Vytvoření detailní harmonogramu realizace projektu
* Implementace technického řešení v rámci technické specifikace:
  + Dodávka a instalace komponent systému včetně HA zapojení
  + Integrace s Active Directory (LDAP) a Email serverem Zadavatele
  + Nastavení dvoufaktorové autentizace
  + Nastavení politik, workflow, pro PIM/PAM (Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení).
  + Nastavení nahrávání privilegovaných relací, základní popis práce s relacemi, reporty a další.
  + Návrh zálohování a obnovy (popisem nastavení pravidelného zálohování a obnovou řešení ze záloh DRP).
  + Integrace se systémy provozovaných Zadavatelem:
    - RDP protokol pro Windows platformu
    - SSH protokol pro OS Linux/Unix platformu
    - Vytvoření účtů pro kmenové zaměstnance Zadavatele a přiřazení oprávnění k příslušným serverům.
    - Vytvoření účtů pro externí pracovníky a přiřazení oprávnění k příslušným serverům.
    - Řízený přístup na webové aplikace Zadavatele, například správa Snap-in MS AD, správa webových konzolí hypervizorů, nebo management konzolí bezpečnostních systémů – FW, switche, AV systém.
* Testování a ověření funkčnosti řešení:
  + Funkční testy ověří, že implementované řešení poskytuje bezchybně všechny požadované funkcionality uvedené v této Technické specifikaci, včetně požadovaných integrací.
  + Zátěžové testy budou simulovat práci uživatelů při obvyklých činnostech. Tím dojde k prověření vlastností PIM/PAM řešení na produkčním serveru s generovanou zátěží.
  + Akceptační testování bude vykonáno na základě připravených testovacích scénářů.
* Provozní dokumentace
* Zaškolení obsluhy systému v rozsahu 2 MD

## Požadavky na licencování

Z pohledu licenční politiky jsou požadovány perpetuální licence s příslušnou maintenance v licenčním modelu.

Privilegovaným uživatelem je ten, který potřebuje účet a pověření s oprávněním ke správě/ administraci privilegovaným oprávněním, aby tak měl možnost vykonávat administraci v jednom nebo více systémech (například hesla databázového serveru, hesla bezpečnostních appliancí, popř. jiné pověření týkající se infrastruktury IT).

Níže uvedené informace popisují základní informace pro zvolení vhodného řešení a licenčního modelu

Požadavky na počty privilegovaných uživatelů a k nim počet potřebných vztažených licencí s dodaným PIM/PAM jsou uvedeny v následující tabulce:

| Počet privilegovaných uživatelů (interních/externích) | Počet spravovaných zařízení a aplikací |
| --- | --- |
| 10/50 | 650 |

* Licence není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů. Součástí licence je i řešení redundance a taktéž geo-redundance (active-active).
* Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému.

## Podrobné technické požadavky na řešení[[1]](#footnote-1)

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry.*

*Uvedený požadovaný způsob splnění funkcionality/vlastnosti je minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Správa privilegovaných přístupů - podrobné technické požadavky na systém** | | | |
| **Oblast** | **Požadavky na řešení** | **Minimální způsob splnění požadované funkcionality/vlastnosti** | **Doplní účastník dle nabízeného řešení** |
|  | **Architektura** |  |  |
| Architektura řešení | Řešení je dodáváno jako HW nebo virtuální appliance (obsahuje i OS) s podporou pro virtuální prostředí dle výchozího stavu Zadavatele | Ano |  |
| Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení s hardeningem zajištěným výrobcem řešení. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro High Avaliability (HA) a Disaster Recovery (DR). | Ano |  |
| Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému. | Ano |  |
| Vysoká dostupnost | Podpora instalace v režimu vysoké dostupnosti. | Ano |  |
| Princip fungování | Systém dokáže fungovat jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře. | Ano |  |
| Vyhledávání systémů | Řešení umožňuje vyhledávání systémů a privilegovaných účtů formou skenování RDP + SSH portů a importů z AD. | Ano |  |
| Onboarding systémů | Řešení disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů. | Ano |  |
| Zálohování systému | Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované. | Ano |  |
| Úložiště | Řešení umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS. | Ano |  |
| Proxy mód | Nástroj musí fungovat jako přístupová proxy. | Ano |  |
| Primární připojení | Podpora primárního spojeni, minimálně SSH a RDP protokolů mezi přistupujícím uživatelem a proxy. | Ano |  |
| Sekundární připojení | Podpora sekundárního připojení mezi proxy a monitorovaným systémem minimálně prostřednictvím protokolů SSH, RDP, VNC a TELNET. | Ano |  |
| Bezagentové řešení | Nástroj nesmí vyžadovat žádné instalace software agentů na monitorovaný systém. | Ano |  |
| Integrace s adresářovými službami | Nástroj musí podporovat integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory / RADIUS / KERBEROS / TACACS+ | Ano |  |
| Integrace s monitorovacími nástroji | Nástroj musí podporovat integraci se SIEM/SYSLOG. | Ano |  |
|  |  |  |  |
|  | **Funkční požadavky** |  |  |
| Řízení přístupů | Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné. | Ano |  |
| Striktní oddělení přístupových oprávnění | Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci. | Ano |  |
| Uživatelské role | Nástroj umožňuje tvorbu účtů s rozdílnými rolemi – minimálně správce, uživatel a auditor. | Ano |  |
| Víceúrovňové schvalování přístupů | Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem nebo vytvořením ticketu v helpdesk systému. | Ano |  |
| Bezpečnostní parametry | Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. | Ano |  |
| Jednotná centrální správa | Správa řešení je umožněna pomocí jednotné centrální správy. | Ano |  |
| Podpora MS Active Directory | Řešení musí podporovat plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v návaznosti na skupiny v AD. | Ano |  |
| Uživatelské rozhraní | Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML). | Ano |  |
| Silná autentizace | Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, LDAP, SAML, atp...). Řešení nabízí vlastní MFA nástroj, nebo bude součástí nabídky MFA třetí strany. | Ano |  |
| Šifrování a zabezpečení dat | Řešení musí splňovat šifrovací algoritmy minimálně na úrovni AES-256. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB a NIS2 | Ano |  |
|  | **Password Management** |  |  |
| Řízení hesel a SSH klíčů | Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i správcem PIM/PAM řešení. Hesla a SSH klíče se vyměňují bezagentsky. Řešení musí podporovat změnu přihlašovacích údajů minimálně pro typy systémů viz. bod "Podpora řízení hesel a bezpečné přístupy pro systémy", zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele. | Ano |  |
| Ukládání hesel | Řešení bezpečně ukládá citlivá data včetně šifrování hesel pomocí AES 256. | Ano |  |
| SSH klíče | Řešení bezpečně spravuje a distribuuje SSH klíče. | Ano |  |
| Rotace hesel a klíčů | Řešení umožňuje automaticky měnit hesla a SSH klíče pro specifické systémy či skupiny účtů. | Ano |  |
| Výjimky v rotaci hesel | Řešení umožňuje definovat výjimky pro zamezení automatických rotací hesel a SSH klíčů u určitých účtů. | Ano |  |
| Časové intervaly rotace hesel | Řešení umožňuje definovat časové intervaly pro provádění automatizovaných změn hesel a SSH klíčů. | Ano |  |
| Rotace hesel po každé relaci | Řešení umožňuje iniciovat změnu hesel a SSH klíčů po každém odhlášení. | Ano |  |
| Komplexita generovaných hesel | Řešení umožňuje definovat komplexitu generovaných hesel dle počtu znaků, využití malých / velkých písmen a speciálních znaků. | Ano |  |
| Rest API | Řešení musí umožňovat změnu hesel pomocí REST API. | Ano |  |
|  | **Řízení vzdálených relací** |  |  |
| Izolace relací | Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace, např. MS SQL Management Studio, WinSCP, atp. ), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, RADIUS nebo SAML). | Ano |  |
| Autentizace privilegovaných uživatelů | Řešení poskytuje různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně: 1.Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na PIM/PAM řešení. | Ano |  |
| 2.Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet). |
| 3.Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání. |
| Připojení do webových relací | Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě. PIM/PAM řešení zprostředkuje přihlášení do koncové webové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO. | Ano |  |
| Nahrávání relací | Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat - minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení. | Ano |  |
| Řešení umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin. | Ano |  |
| Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI dodávaného řešení. | Ano |  |
| Terminace relací | Řešení nabízí možnost automatické terminace definovaných aplikací nebo komunikace. Definice je možné plně editovat a uplatnit na cílové systémy a uživatele | Ano |  |
| Možnost sledování relací v reálném čase | Správce nástroje/auditor musí mít možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci uknočit. | Ano |  |
| Převzetí aktivní relace | Správce nástroje/auditor musí mít možnost převzít kontrolu nad klávesnicí a myší (obdoba funkcionality vzdálené plochy / „remote control“ známé z nástrojů typu TeamViewer) za účelem provedení servisního zásahu nebo opravy. | Ano |  |
| Pozvání uživatele | Řešení musí podporovat funkci „invite“ – možnost, aby interní administrátor mohl bezpečně přizvat do relace externího uživatele bez nutnosti, aby byl tento uživatel zahrnut do licenčního modelu. | Ano |  |
| Časové rámce relací | Řešení umožňuje vyžadování schválení relace v určitých časových rámcích- Např. pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení. | Ano |  |
| Blokace procesů | Řešení umožňuje blokování vybraných procesů na systémech Windows. | Ano |  |
| Blokace komunikace | Nástroj musí umožnit nastavení blokace všech, či vybraných TCP spojení zahájených z monitorovaného RDP serveru za účelem navázání neautorizovaných spojení. | Ano |  |
| Schvalování relací | Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu: | Ano |  |
| 1. Privilegovaný uživatel požádá o přístup |
| 2. Definovaní uživatelé obdrží žádost o schválení přístupu. |
| 3. Minimální definovaný počet uživatelů schválí žádost. |
| 4. Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému. |
| Zabezpečený webový přístup na relace | Řešení poskytuje možnost připojení na vzdálené relace pomocí prohlížeče a protokolu HTTPS (není tedy například nutné otevírat z klientské stanice RDP/SSH/... protokoly mezi uživatelem a jump Serverem bude vždy otevřený pouze bezpečný WebSocket protokol (port 443). | Ano |  |
| Kontrola relací | Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. | Ano |  |
| Přístup přes webové rozhraní | Systém umožňuje centrální webový přístup přes zabezpečený HTTPS protokol a podporuje prohlížeče Internet Explorer, Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash) | Ano |  |
| Přístup přes webové rozhraní | Systém centrálního webového přístupu přes HTTPS protokol, tzv. VPN less přístup, je dodán jako samostatná aplikace | Ano |  |
|  | **Audit a reporting** |  |  |
| Zobrazení aktivit uživatele | Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace. | Ano |  |
| Audit administrátorských akcí | Řešení musí umožňovat zobrazení veškerých aktivit administrátora řešení. | Ano |  |
| Přístup k reportům | Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele. | Ano |  |
| Export auditních dat | Systém musí umožňovat export auditních záznamů | Ano |  |
| Nezpochybnitelný auditní záznam | Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. | Ano |  |
| Zabezpečení auditních záznamů | Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel. | Ano |  |
| Audit záznamů relací | Při auditu či kontrole proběhlé relace nástroj musí mít možnost zobrazit metadata a videozáznam relace na jedné stránce. | Ano |  |
| Monitoring pomocí RestAPI | Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI - integrace s monitoring systémy zadavatele. | Ano |  |
|  | **Integrace a Podporované platformy** |  |  |
| Podpora systémů zadavatele | Řešení musí umožňovat správu pro různé druhy koncových systémů - minimálně v rozsahu viz. bod 4: "Požadavky na systémy a protokoly pro řízení hesel“ | Ano |  |
| Podpora řízení hesel | Řešení musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů - minimálně v rozsahu viz. bod 4: " Požadavky na systémy a protokoly pro řízení hesel“ | Ano |  |
| MFA - multi factor autentizace | Řešení musí buď nativně nebo integrací nástroje třetí strany, vynucovat multi factor autentizaci. Minimálně na úrovní LDAP/S, RADIUS, SAML. MFA je vyžadována jako nedílná komponenta požadovaného řešení. | Ano |  |
| SIEM integrace | Řešení musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog. | Ano |  |
|  | **Licenční model, podpora a certifikace** |  |  |
| Licencování | Licence musí být perpetuální s 5ti letou standardní zárukou. | Ano |  |
| Licence není omezena na počet přistupujících uživatelů nebo řízených privilegovaných účtů. | Ano |  |
| Licence je pro 650cílových zařízení nebo aplikací. | Ano |  |
| Podpora řešení | Dodávka musí obsahovat standardní záruku výrobce na období min. 5 let. | Ano |  |
|  | Technická podpora musí být minimálně v rozsahu 8x5. | Ano, min. 8 x 5 |  |
|  | Podpora musí zahrnovat možnost aktualizací a oprav dodaného software, včetně bezpečnostních záplat. | Ano |  |
| Certifikace | Řešení musí splňovat požadavky na bezpečnostní certifikaci odpovídající úrovni ochrany přístupů k privilegovaným účtům a citlivým systémům organizace, například certifikace dle **ANSSI CSPN (Certificat de Sécurité de Premier Niveau)** nebo obdobné nezávislé bezpečnostní certifikace. | Ano |  |

## Předpokládaná součinnost ze strany zadavatele

* Přístup do prostor zadavatele
* Součinnost správců IT technologií včetně přístupových údajů k dotčeným systémům (servisní účty apod.)
* Poskytnutí dokumentace stávajícího stavu provozu
* Vzdálený přístup pro specialistu – VPN
* Poskytnutí kontaktů a vytvoření komunikační matice
* Návrh termínů pro systémové odstávky bez zbytečného prodlení

.

## c) Síťové sondy

## Základní požadavky na dodávku a implementaci - technická specifikace

Předmětem plnění veřejné zakázky (VZ) je dodávka a kompletní implementace Nástrojů pro analýzu a monitoring síťového provozu SA, spočívající v nasazení řešení pro provozní, výkonnostní a bezpečnostní monitoring síťového provozu v hybridním prostředí s pokročilými analytickými funkcemi.

Plnění VZ bude obsahovat tyto základní komponenty a parametry:

* 1ks Zařízení pro zpracování a vyhodnocení dat s kapacitou nejméně 12TB ve formě virtuálního zařízení
* 1ks Monitorovací sonda s kapacitou 2x10Gbps (rozhraní SFP+) ve formě hardwarového zařízení
* 2ks kompatibilních 10Gbps SPF+ modulů (kabeláž realizovaná pomocí single-mode optických kabelů)
* Všechny dodávané komponenty budou dodány včetně veškerého software a licencí potřebných k jejich provozu
* Součástí dodávky bude kompletní nastavení, implementace a instalace dodávaných komponent a software do stávající infrastruktury zadavatele, včetně seznámení s obsluhou
* Součástí dodávaného řešení bude záruka a podpora výrobce na všechny dodávané komponenty, včetně veškerého dodávaného potřebného software, po celou dobu zakoupené standardní 5ti leté záruky.
* Podléhají-li některé z dodávaných komponent či software časově omezenému licencování, musí být dodáno jeho předplatné v délce trvání min. 60 měsíců

## Požadavky na funkční vlastnosti a technické parametry dodávaných zařízení

1. **Funkční vlastnosti**

Následující tabulka specifikuje požadované funkční vlastnosti poptávaného řešení. Funkční vlastnosti se vztahují na systém jako celek, tedy ***dané vlastnosti musí splňovat jak sondy, tak kolektor***.

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry (****zapsáním ANO, nebo NE****) a dále vyplní (dle konkrétních položek v tabulce), jakým konkrétním způsobem požadované parametry naplňuje (****Skutečná hodnota, popis splnění požadavku****), uvede odkaz na dokumentaci dodávaného zařízení, ze které bude zřejmé, jak dodané zařízení požadavky splňuje (****Dokumentace odkaz****).*

*Uvedené funkční parametry jsou minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

**Tabulka požadavků na Funkční vlastnosti**

|  |  |  |
| --- | --- | --- |
| **Požadované parametry** | **Splněno (ANO/NE)** | **Dokumentace (odkaz)** |
| Podpora standardů NetFlow v5, NetFlow v9, IPFIX pro export i příjem statistik o síťovém provozu v souladu s příslušnými RFC pro dané standardy. |  |  |
| Podpora pro spolehlivý a bezpečný přenos dat ve formátu IPFIX mezi sondami a kolektorem v souladu s RFC 7011. |  |  |
| Podpora pro nastavení času aktivní a neaktivní expirace toků (RFC 3954). |  |  |
| Monitorování v pasivním režimu (SPAN/TAP) a aktivním režimu (GRE/ERSPAN). |  |  |
| Deduplikace paketů na úrovni monitorovacích portů. |  |  |
| Monitorování MAC adres. |  |  |
| Monitorování VLAN tagů. |  |  |
| Monitorování výkonnostních parametrů sítě:   * round trip time, * server response time, * TCP retransmise |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu HTTP. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu SSL/TLS vč. TLS 1.3. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu DNS. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu DHCP. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu Samba. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu SMTP. |  |  |
| Identifikace a extrakce metadat z aplikačního protokolu QUIC. |  |  |
| Uživatelsky definované šablony pro export statistik o síťovém provozu ve formátu IPFIX, pomocí kterých je možné definovat exportované atributy. Uchazeč předloží přehled všech podporovaných atributů (tzv. IPFIX Enterprise Extensions). Zadavatel požaduje možnost exportovat v IPFIX výkonnostní parametry sítě i metadata z aplikačních protokolů. |  |  |
| Systém umožní vizualizaci statistik o provozu datové sítě v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu datových toků. |  |  |
| Systém zobrazuje výkonnostní metriky v grafech provozu společně s volumetrickými statistikami a to vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty volumetrických i výkonnostních metrik. |  |  |
| Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc bez nutnosti dotaz rozdělit dotaz na menší časové intervaly. Spuštění a vykonání dotazu není limitováno délkou časového intervalu nebo maximální dobou vykonávání dotazu. Dotazy, které se vykonávají dlouhou dobu, běží na pozadí a výsledky si uživatel může zobrazit, jakmile je dotaz dokončen a výsledky jsou dostupné. |  |  |
| Systém umožňuje filtrovat s využitím libovolných atributů flow statistik včetně aplikačních metadat nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). |  |  |
| Systém umožňuje agregovat síťové statistiky podle libovolných atributů a sumarizovat podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.). |  |  |
| Systém nabízí konfigurační šablony pro typické scénáře použití, například monitorování SaaS aplikací, analýza aplikačních protokolů apod. Tyto konfigurační šablony jsou vestavěné, poskytované výrobcem a pravidelně aktualizované. Jejich aplikace provede nastavení systému pro dané scénář použití. |  |  |
| Systém automaticky rozpozná každý zdroj flow dat, který mu tato data zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow dat automaticky zobrazuje graf průběhu provozu a umožňuje následně automaticky identifikovat ztrátu nebo významný pokles dat z daného zdroje. |  |  |
| Systém podporuje obohacování statistik o síťovém provozu o uživatelské identity z externích zdrojů. Jako transportní protokol slouží syslog, který do systému doručuje informace o identitě uživatele pro danou IP adresu. Systém následně obohacuje každý jednotlivý datový tok o identitu uživatele pro zdrojovou i cílovou adresu, pokud je tato informace dostupná. Současně je možné zpracovávat uživatelské identity z více zdrojů, v systému je možné uživatelsky definovat parsovací pravidla pro syslog zprávy pro rozšiřování podporovaných zdrojů uživatelských identit. |  |  |
| Systém nabízí funkcionalitu detekce útoků, bezpečnostních incidentů a anomálií na základě behaviorální analýzy provozu a umožňuje také detekci neznámých/nových útoků. Detekčních schopnosti pokrývají jednotlivé taktiky dle MITRE ATT&CK framework (uvedeny anglicky): Reconnaissance, Initial Access, Execution, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. Před detekcí anomálií na základě behaviorální analýzy je možné aktivovat deduplikaci datových toků pro zpřesnění detekce v případě, že síťový provoz prochází větším počtem měřících bodů. |  |  |
| K jednotlivým externím IP adresám jsou dostupné odvozené informace minimálně v rozsahu geolokace a identifikace SaaS aplikace nebo platformy, jejíž je aplikace součástí. Systém automaticky rozpoznává minimálně 1000 nejběžnějších SasS aplikací a platforem. |  |  |
| Systém pomáhá prioritizovat práci bezpečnostního analytika a poskytuje mu souhrnné informace o nejvýznamnějších událostech, nových incidentech (nebyly zaznmenány v předchozím období), rizikových stanicích a trendech. Předpokládá se využití prostředků umělé inteligence a asistované analýzy, nikoliv prostou prioritizaci událostí na základě severity. Systém automaticky provádí scoring jednotlivých zařízení v síti z hlediska jejich chování a sestavuje přehled zařízení seřazených podle dosaženého score. |  |  |
| Výrobce poskytuje automatické, pravidelné aktualizace databáze známých indikátorů kompromitace (tzv. threat intelligence) a databáze signatur. Aktualizace probíhají minimálně jednou denně. Uživatel může nad rámec indikátorů kompromitace poskytovaných výrobcem doplnit vlastní indikátory kompromitace bez nutnosti použití specializovaných datových formátů, tj. prostřednictvím CSV nebo TXT souborů. Indikátory kompromitace je možné získávat automaticky ze systému MISP bez nutnost skriptování (nativní vlastnost produktu). |  |  |
| Události je možné automaticky exportovat do systémů typu log management nebo SIEM prostřednictvím protokolu syslog ve standardizovaném formátu CEF. |  |  |
| Systém podporuje pokročilé dashboardy s libovolným počtem pohledů na data. Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). Existují předdefinované dashboardy od výrobce pro typické scénáře použití, seznam předdefinovaných dashboardů je možné uživatelsky rozšiřovat. |  |  |
| Systém nabízí předdefinovanou sadu reportů s možností plné konfigurace uživatelem. Reporty jsou obsahově ekvivalentní s dashboardy a umožňují zobrazit veškeré informace, které je možné zobrazit na dashboardu. Reporty jsou dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. |  |  |
| Systém nabízí REST API, které pokrývá přístup k datům i konfiguraci. REST API je plnohodnotně dokumentované a oficiálně podporované výrobcem. |  |  |
| Systém nabízí management aktivních relací (uživatelů připojených k systému) prostřednictvím grafického uživatelského rozhraní, REST API a konzole SSH. Administrátor systémů může jednotlivé relace ukončit. V rámci nastavení bezpečnostní politiky je možné konfigurovat session timeout pro grafické uživatelské rozhraní a REST API nezávisle na sobě. |  |  |
| Systém nabízí integraci LDAP/AD pro autentizaci a autorizaci uživatelů.V rámci konfigurace je možné prostřednictvím uživatelského rozhraní manuálně mapovat skupiny v rámci LDAP/AD na role v systému. |  |  |

1. **Technické a výkonnostní parametry dodávaných zařízení**

*Uvedené technické parametry jsou pro každou dodávanou komponentu (každý kus) minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

*U dodávaných komponent vyplní účastník v tabulkách* ***navíc konkrétní nabízený typ komponenty*** *(včetně označení případného software nutného pro provoz komponenty)* ***a výrobce komponenty****.*

1 kus … Monitorovací sonda 2x10Gbps (hardware appliance)

Zadavatel požaduje monitorovací sondu ve formě ***hardware appliance***, specializované zařízení v provedení tzv. rack-mount serveru vybavené síťovými rozhraními pro příjem kopie síťového provozu z tzv. mirror portů nebo TAPů, musí umožňovat generování metadat o síťovém provozu a jejich odesílání na zařízení pro zpracování a vyhodnocení dat. Součástí dodávky jsou také SFP+ moduly pro připojení sondy do infrastruktury zadavatele.

**Tabulka požadavků na Monitorovací sondu 2x10Gbps (hardware appliance)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Konkrétní typové označení a název nabízené komponenty | |  | | |
| Výrobce nabízené komponenty | |  | | |
| **Požadované parametry** | **Požadovaná minimální hodnota** | **Splněno (ANO/NE)** | **Skutečná hodnota** | **Dokumentace (odkaz)** |
| Monitorovací port s propustností 10Gbps a rozhraním SFP+ | 2 |  |  |  |
| Výkon v milionech paketů za vteřinu na 1 monitorovací port | 14 |  |  |  |
| Výkon v milionech paketů za vteřinu na celé zařízení | 28 |  |  |  |
| Export dat ve formátu IPFIX na více cílů současně | ANO |  |  |  |
| Velikost zařízení/provedení | 1U |  |  |  |
| Napájení | 1x230V |  |  |  |
| Počet dodaných SFP+ modulů (SM – Single Mode) | 2 |  |  |  |

1 kus ... Zařízení pro zpracování a vyhodnocení dat (virtual appliance)

Zadavatel požaduje zařízení pro zpracování a vyhodnocení dat ve formě ***virtual appliance,*** specializovaný software vybavený dostatečnou diskovou kapacitou pro dlouhodobé uložení metadat o síťovém provozu ve formátu NetFlow/IPFIX a kompatibilních. Zařízení musí zajišťovat normalizaci, uložení, zpracování, vizualizaci a konsolidovaný reporting agregovaných informací o monitorovaném síťovém provozu z libovolného počtu sond, routerů a dalších síťových prvků, která metadata o síťovém provozu poskytují.

**Tabulka požadavků na zařízení pro zpracování a vyhodnocení dat**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Konkrétní typové označení a název nabízené komponenty | |  | | |
| Výrobce nabízené komponenty | |  | | |
| **Požadované parametry** | **Požadovaná minimální hodnota** | **Splněno (ANO/NE)** | **Skutečná hodnota** | **Dokumentace (odkaz)** |
| Podpora virtualizace | Virtualizace zajišťující kompatibilitu s výchozím stavem (viz Příloha č. 11 ZD – Stávající stav) |  |  |  |
| Disková kapacita v TB | 12 |  |  |  |
| Minimální výkon (zatížení) v flows/s až do | 200 000 |  |  |  |
| Detekce anomálií a incidentů v minimálním množství flows/s | 5000 |  |  |  |
| Minimální doba retence bezpečnostních událostí (měsíců) | 18 |  |  |  |
| Oddělené zpracování dat ve vice datových kanálech pro detekci anomálií včetně konfigurace detekčních algoritmů, vlastních pravidel a base lines. Minimální počet datových kanálů | 5 |  |  |  |
| Min. počet cílů exportu událostí protokolem syslog s možností exportovat různé události na různé cíle | 10 |  |  |  |

1. **Požadavky na vybrané příklady použití**

Následující příklady použití navazují na výše požadované funkční a technické vlastnosti jednotlivých komponent a podrobně specifikují, jakým způsobem plánuje zadavatel poptávaný systém využít jako celek.

Příklady použití jsou popsány podrobně tak, aby bylo možné vyhodnotit soulad nabízeného řešení se záměrem zadavatele. Uchazeč posoudí každý jednotlivý případ použití systému jako celku a do tabulky uvede “ANO” nebo “NE” tak, aby bylo zřejmé, že jeho nabízené řešení splňuje požadavky na jednotlivé příklady použití.

Hodnota “ANO” pro daný příklad použití znamená, že daný případ použití je splněn úplně a bezvýhradně ve všech uvedených bodech. Uchazeč dále doloží soulad pro každý případ použití odkazem do uživatelské dokumentace.

**Zálohování a obnova logů o aktivitě na síti (NetFlow)**

Za účelem archivace logů o síťové komunikaci je požadována následující funkcionalita nabízeného řešení:

* K řešení je možné připojit standardizované datové úložiště (např. Samba, NFS, S3) na které je možné archivovat logy o síťové komunikaci.
* Data, která jsou předmětem zálohování je možné definovat pomocí libovolné kombinace atributů záznamů o síťovém provozu. Takových definic je možné vytvořit větší počet, bez explicitního omezení.
* Zálohování dat probíhá pravidelně, minimálně jednou za 24 hodin.
* Zálohovaná data je možné v případě potřeby obnovit tak, aby tato data bylo možné analyzovat standardními prostředky řešení identicky jako data, která jsou standardně v systému dostupná.
* Při obnově dat je možné zvolit, která data a za jaký časový interval (minimálně s denní granularitou), budou obnovena.

Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití produktu třetí strany, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

**Podpora pro tzv. FlowLogs**

Nabízené řešení musí být připravené na monitoring datového provozu v prostředí AWS nebo Azure s využitím technologie tzv. FlowLogs. Požadována je nativní podpora pro VPC FlowLogs v případě AWS a NSG FlowLogs v případě Azure. Požadované vlastnosti:

* Řešení podporuje nativní API AWS a Azure pro získávání příslušných FlowLogs z prostředí public cloud, která jsou periodicky (minimálně jednou za 5 minut) získávána z prostředí public cloud.
* Získávaná data ve formátu FlowLogs jsou normalizována a zpracována stejným způsobem jako statistiky o síťovém provozu ve formátu NetFlow/IPFIX s jednotným způsobem vizualizace, reportingu a manuální analýzy.
* Automaticky identifikuje zdroje dat z prostředí AWS a Azure a tyto zdroje pojmenuje podle příslušného pojmenování v prostředí AWS, resp. Azure bez nutnosti manuální konfigurace.
* Neexistují žádná omezení na místo nasazení (on-premise, public cloud) nebo omezení na kombinace zdrojů dat, řešení podporuje současně sběr dat z AWS, Azure, vlastních senzorů i flow dat z aktivních prvků.
* Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Výše specifikovaná funkcionalita je standardní součástí produktu a nevyžaduje nasazení dalšího software, virtuální nebo fyzické appliance např. pro konverzi dat.

**Pokročilé zpracování flow dat**

Nabízené řešení umožní přijímat data ve formátu NetFlow/IPFIX nejen z vlastních senzorů, ale i ze systémů třetích stran. Tato data je následně možné předávat do systémů třetích stran včetně duplikace, filtrování a konverze formátu. Požadované vlastnosti:

* Přijímaná data ve formátu NetFlow/IPFIX je možné duplikovat na libovolný počet cílů.
* Přijímaná data ve formátu NetFlow/IPFIX je možné pro konkrétní cíl libovolně konvertovat mezi formáty, konkrétně NetFlow verze 5, NetFlow verze 9, IPFIX.
* Přijímaná data ve formátu NetFlow/IPFIX je možné pro konkrétní cíl filtrovat, minimálně na základě zdrojových a cílových IP adres nebo sítí, VLAN tagů a L4 protokolů.
* Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Výše specifikovaná funkcionalita je standardní součástí produktu a nevyžaduje nasazení dalšího software, virtuální nebo fyzické appliance.

**Modelování topologie**

Nabízené řešení umožní vytvářet libovolné logické nebo fyzické topologie a na tyto topologie mapovat síťový provoz, resp. libovolně filtrovaný síťový provoz. Účelem je modelovat a vizualizovat prostředí datové sítě, význačné systémy a zobrazovat jejich síťový provoz a vytížení. Požadované vlastnosti:

* Uživatel může vytvořit prostřednictvím integrovaného grafického editoru libovolný počet topologií, které se skládají z uzlů reprezentujících routery, switche, servery nebo služby a tyto uzly jsou propojené spoji, které reprezentují datový provoz mezi definovanými uzly.
* Na spoje je možné mapovat libovolný datový provoz nebo jakoukoliv jeho podmnožinu určenou filtrem. Filtrovat provoz je možné na základě jakéhokoliv parametru statistik o síťovém provozu.
* Pro každý spoj je možné stanovit libovolnou propustnost (kapacitu) a to v režimu symetrické datové linky nebo asymetrické datové linky. Pro každý spoj je možné stanovit způsob výpočtu utilizace průměrem nebo 95-percentilem.
* Pro každou topologii je možné stanovit barevnou škálu utilizace a citlivosti, tj. od jaké utilizace systém signalizuje zvýšené zatížení.

Topologii je možné vizualizovat v podobě grafu nebo tabulky, kde jsou jednotlivé spoje seřazené podle zatížení. Obě formy vizualizace je možné kombinovat na dashboardu a v reportech.

## d) SIEM

Předmětem zakázky je návrh, dodání a implementace uceleného řešení pro kontinuální sběr, ukládání, zpracování a zobrazování bezpečnostních informací, událostí, logů a dalších strojových dat z heterogenních ICT zdrojů nejrůznějších výrobců v síti Zadavatele.

Toto řešení musí být možné provozovat vlastními stávajícími zaměstnanci Zadavatele.

Nabízené zařízení musí být schopno z definovaných zdrojů sbírat logy, převádět je do normalizované podoby, kategorizovat je, zobrazovat a důvěryhodně ukládat jejich originální i normalizovanou formu.

Musí rovněž obsahovat pokročilé analytické nástroje pro limity, korelace, generování alertů a vytváření reportů.

Zároveň musí zaručovat nemožnost ztráty, smazání či jakékoliv modifikace dat.

Přístupová práva k systému musí být nastavitelná s různými úrovněmi oprávnění pro různé operátory.

Práce s uloženými daty musí být intuitivní a probíhat přes jednotné centrální uživatelské rozhraní.

V systému musejí být výrobcem připravené nejčastěji požadované pohledy na data, reporty, současně ale musí mít operátor systému možnost tvorby, úpravy a ukládání vlastních přehledových sestav a informačních panelů.

Nabízené řešení musí dále umožňovat filtraci vstupních dat, vytváření vlastních pravidel pro jejich normalizaci (parserů), snadné vyhledávání dle požadavků operátora, korelací událostí, nastavení reportů a alertů.

Alerty musí být možné zasílat min. emailem dle nastavených pravidel.

Systém nebude vázán na kapacitu vlastního úložiště, pokud ano musí systém obsahovat licenci na uchování dat minimálně po dobu minimálně 25 měsíců, při očekávaném množství logů až 130GB/den.

Zálohování a následná obnova dat i konfigurace nesmí nijak ovlivnit provoz systému a narušit integritu dat.

Nabízený nástroj musí Zadavateli napomoci k dosažení shody s bezpečnostními směrnicemi a legislativními požadavky zejména tím, že sbírá logy z kritické ICT infrastruktury, aby bylo možno v případě kybernetického incidentu z uložených dat získat důležité forenzní informace.

Výrobce musí k nabízenému systému distribuovat pravidelné aktualizace.

Počet zdrojových zařízení nesmí být nijak omezen.

**Tabulka požadavků na Funkční vlastnosti**

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry (****zapsáním ANO, nebo NE****) a dále vyplní (dle konkrétních položek v tabulce), jakým konkrétním způsobem požadované parametry naplňuje vč. značkové specifikace a dále uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru.*

*Uvedené požadované parametry jsou minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Požadované povinné parametry** | **Splněno (ANO/NE)** | **Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | | **Účastník uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| Integrovaná appliance (HW se specializovaným firmware/software) nebo virtuální server se specializovaným software včetně operačního systému a podpůrných systémů (databáze apod.) |  | |  |  |
| Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware |  | |  |  |
| Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware |  | |  |  |
| Možnost bezagentový sběr logů s výjimkou systémů |  | |  |  |
| Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení. |  | |  |  |
| Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze. |  | |  |  |
| Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému. |  | |  |  |
| Příjem a zpracování logy, událostí a další strojově generovaných data minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). |  | |  |  |
| Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. |  | |  |  |
| Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy |  | |  |  |
| Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem.  Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání |  | |  |  |
| Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém |  | |  |  |
| Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení. |  | |  |  |
| Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování) |  | |  |  |
| Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran |  | |  |  |
| Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). |  | |  |  |
| Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb |  | |  |  |
| Konektory (specifické parsery) pro stávající technologie - min. a) min. na Active Directory, Windows (vč. DNS, DHCP), Exchange, Linux, a nabízené SW i HW řešení. |  | |  |  |
| Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech.  Odesílání alertů min SMTP, Syslog, TCP. |  | |  |  |
| Průměrný trvalý příjem min. 5000 událostí/s.  Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale.  Řešení musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události. |  | |  |  |
| Standardní záruka na 60 měsíců. |  | |  |  |
| Sběr událostí, jejich analýza a korelace v reálném čase, notifikace potenciálních bezpečnostních incidentů, podpora vyšetřování bezpečnostních událostí a incidentů. Viz. <https://cs.wikipedia.org/wiki/Security_Information_and_Event_Management> |  | |  |  |
| Software může být integrován s nabízeným systémem centrálního logování nebo samostatně zajišťovat sběr a správu logů a síťových toků s minimálně shodnými parametry, jako jsou požadovány pro systém centrálního logování |  | |  |  |
| Datová analýza v reálném čase s využitím vlastních detekčních mechanismů i integrovaných systémů. |  | |  |  |
| Integrovaný systém korelací událostí, propojování bezpečnostních událostí z různých zdrojů pro detekci komplexních útoků/událostí.  Obvyklá korelační pravidla budou součástí nabízeného systému a jeho aktualizací. |  | |  |  |
| Podpora automatických reakcí – minimálně deaktivace uživatelského účtu, blokování IP adresy na firewallu. Možnost vytváření vlastních akcí a pravidel pro jejich spouštění. |  | |  |  |
| Integrovaný systém upozorňování na podezřelé události přímo v rozhraní nástroje a e-mailem.  Možnost nastavení pravidel (např. úroveň závažnosti, zdroj) pro zasílání upozornění různým a příjemcům |  | |  |  |
| Podpora integrace se systémy třetích stran pro zlepšení detekčních schopností a využití standardizovaných frameworků, znalostních bází a nástrojů/rozhraní, např.  MITRE ATT&CK (povinná požadovaná integrace), VIRUSTOTAL apod. |  | |  |  |
| Podpora autentizace vůči Active Directory/LDAP, podpora RBAC (Role-based access control) |  | |  |  |

## e) SOC

Předmětem plnění této části veřejné zakázky je také dodávka, instalace, provedení implementace prostředků managementu bezpečnostních informací a událostí (dále jen „systém SIEM“), napojení na stávající prostředí a integrace se stávajícími bezpečnostními nástroji dle požadavků Zadavatele, včetně zaškolení zaměstnanců Zadavatele, poskytnutí nezbytné součinnosti.

Součástí následné standardní 5ti leté záruky bude externě provozovaná funkce bezpečnostního dohledu nad ICT infrastrukturou Zadavatele SOC v režimu 7 dní v týdnu 24 hodin denně (dále jen „24x7“).

Bezpečnostní dohledové centrum SOC vybraného Dodavatele bude centralizovat kontrolní činnosti, správu událostí a incidentů a koordinovat analýzy anomálií a aktivně spolupracovat na řízení krizových úkonů při zvládání následků incidentů s interním týmem Zadavatele.

Služba bezpečnostního dohledu bude využívat dostupné bezpečnostní nástroje Zadavatele, včetně nově dodávaných nástrojů, zahrnutých v této veřejné zakázce.

**Tabulka požadavků na Funkční vlastnosti**

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry (****zapsáním ANO, nebo NE****) a dále vyplní (dle konkrétních položek v tabulce), jakým konkrétním způsobem požadované parametry naplňuje vč. značkové specifikace a dále uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru.*

*Uvedené požadované parametry jsou minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Požadované povinné parametry** | **Splněno**  **(ANO/NE)** | **Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Účastník uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| Bezpečnostní dohledové centrum podporuje práci s nástroji Zadavatele v režimu 24x365, |  |  |  |
| Vykonávání kybernetického bezpečnostního dohledu v režimu 24x7x365, kdy operátor musí být v tomto režimu na svém pracovišti (forma pohotovosti není přípustná a Zadavatel toto může kdykoliv libovolně kontrolovat), zahájení řešení bezpečnostního incidentu, možnost kontaktu vybraného Dodavatele Zadavatelem s žádostí o řešení problému spojeného s poskytovanou službou, s žádostí o konzultaci. |  |  |  |
|  |  |  |  |
| Bezpečnostní dohledové centrum umístěné na území ČR a zpracovávající data výhradně dle právních norem ČR |  |  |  |
| Ukládání dat pro analytické činnosti výhradně na území ČR |  |  |  |
| Služba je dostupná v českém jazyce, komunikace v českém jazyce |  |  |  |
| Specialisté SOC vybraného Dodavatele budou přistupovat k zařízením RegioJet pouze po zabezpečených linkách z území EU |  |  |  |
| Personální zajištění služby pracovníky s odbornou způsobilostí bude vyhovovat požadavkům na zajištění kybernetické bezpečnosti v souladu s požadavky zákona 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, a to v celém průběhu služby a všech jejích procesů a rutin. |  |  |  |
| Bezpečnostní dohledové centrum umožní úplné oddělení výkonu bezpečnostních rolí od rolí provozních |  |  |  |
| Bezpečnostní dohledové centrum musí být certifikované dle ČSN EN ISO 27001 |  |  |  |
| Bezpečnostní dohledové centrum musí mít certifikaci Trusted introducer pro CSIRT týmy (https://www.trusted-introducer.org) minimálně úroveň Accredited |  |  |  |
| Informování odpovědných osob RegioJet o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail/SMS/telefon). |  |  |  |
| Detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně.  Prezentace reportu osobně nebo vzdáleně videokonferenční formou.  Prezentace měsíčních reportů v rozsahu max. 0,5MD |  |  |  |
| Služba zajistí provádění on-demand spouštění některých pravidel a z výstupu bude vytvářet reporty. |  |  |  |
| Vybraný Dodavatel v rámci služby zpracuje a poskytne Zadavateli každý měsíc report, ve kterém je popsáno:   * průběh realizace plnění služby za uplynulé období; * provedené služby za uplynulé období;   návrh doporučených opatření pro další období pro zvýšení bezpečnosti, dostupnosti a v prevenci eliminace incidentů. |  |  |  |
| Bude zajištěno porovnání neobvyklých počtů určitých událostí oproti jinému období z minulosti v podobě Base line |  |  |  |
| Služba zajistí shromažďování a možnost náhledu a následného porovnáni historických dat a jejich propojení v kontextu sledované události nebo incidentu |  |  |  |

## Požadované služby v rámci záruky poskytované na části plnění a) až e)

Součástí nabízeného řešení musí být následující služby poskytované dodavatelem v rámci standardní záruky:

* 7x24 podpora dodavatele na dodané komponenty a funkčnost dodaného řešení zahrnující následující dílčí služby:
  + „Single point of contact“ pro řešení veškerých incidentů, požadavků souvisejících s provozem celého nabízeného řešení.

Kategorie vad a SLA (pro části plnění a) až d))

|  |  |  |
| --- | --- | --- |
| Kategorie vad | Doba provozu | Reakční doba |
| Závažnost 1 – Kritická závada[[2]](#footnote-2) | 7x24 hodin | 1 hodiny od nahlášení závady |
| Závažnost 2 – Vážná závada[[3]](#footnote-3) | 7x24 hodin | 2 hodiny od nahlášení závady. |
| Závažnost 3 – Drobná vada[[4]](#footnote-4) | 7x24 hodin | 12 hodin od nahlášení závady |

Kategorie vad a SLA (pro část plnění e))

|  |  |  |
| --- | --- | --- |
| Kategorie vad | Doba provozu | Doba, v níž je třeba nahlásit závadu |
| Závažnost 1 – Kritická závada[[5]](#footnote-5) | 7x24 hodin | 1 hodiny od zjištění závady |
| Závažnost 2 – Vážná závada[[6]](#footnote-6) | 7x24 hodin | 2 hodiny od zjištění závady |
| Závažnost 3 – Drobná vada[[7]](#footnote-7) | 7x24 hodin | 12 hodin od zjištění závady |

* + Analýzu nahlášeného problému, jeho replikaci v laboratoři dodavatele a eskalaci na výrobce dané komponenty v případě, že dodavatel není schopen incident vyřešit ve vlastní režii.
  + Poskytování služeb prostřednictvím vzdáleného přístupu.
  + Proaktivní monitoring (24 x 7) dodaných komponent řešení se založením incidentu ze strany pracoviště technické podpory dodavatele v případě identifikace nestandardní situace nebo chybového stavu a doplněnou informací jména řešitele + kontaktu na něj v založeném incidentu.
  + Poskytování zpětné vazby ze strany dodavatele o průběhu řešení všech incidentů i prostřednictvím webového portálu.
  + Komunikace v českém jazyce.
* Firmware/Patch Management
  + Provádění upgrade jednotlivých komponent řešení 2x ročně v pravidelných intervalech. V případě vydání kritické aktualizace bude zákazník proaktivně informován a bude dohodnuto, zda bude aktualizace aplikována mimo pravidelný cyklus.

Služby poskytované jako součást standardní záruky budou poskytovány po dobu 60 měsíců.

1. Pojmy systém a řešení jsou v tabulce užívány jako synonyma. [↑](#footnote-ref-1)
2. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace a procesy organizace. Závada způsobuje úplné nebo téměř úplné odstavení klíčových procesů nebo podporovaných systémů. Neexistuje žádné dostupné řešení ani náhrada. Příklady kritických závad: selhání informačních systémů nebo jejich částí, odstavení klíčových databází, odstavení celého systému zálohování dat, selhání obnovení kriticky potřebných dat, významné snížení výkonu celého systému, významný kybernetický bezpečnostní incident [↑](#footnote-ref-2)
3. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace, ale bezprostředně neohrožující klíčové procesy organizace. Informační systémy a aplikace jsou částečně funkční nebo existuje dočasné řešení. Příklady závažných závad: nefunkční či jen částečné funkční funkce, zpomalení aplikace, chyba zálohování a obnovy bez bezprostředního rizika ztráty dat, ztráta vysoké dostupnosti řešení [↑](#footnote-ref-3)
4. Vada, jež nenaplňuje definici kategorie 1 a 2. Vada s minimálním dopadem na procesy organizace nebo vada bez dopadu na provoz (kosmetická vada). Celková funkčnost informačních systémů a aplikací není nijak ohrožena. Příklady drobných vad: nesprávně zobrazený prvek v rozhraní, chyba v reportu, varovná zpráva označující možný budoucí problém, drobná chyba konfigurace s minimálním dopadem na celkovou funkčnost [↑](#footnote-ref-4)
5. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace a procesy organizace. Závada způsobuje úplné nebo téměř úplné odstavení klíčových procesů nebo podporovaných systémů. Neexistuje žádné dostupné řešení ani náhrada. Příklady kritických závad: selhání informačních systémů nebo jejich částí, odstavení klíčových databází, odstavení celého systému zálohování dat, selhání obnovení kriticky potřebných dat, významné snížení výkonu celého systému, významný kybernetický bezpečnostní incident [↑](#footnote-ref-5)
6. Závada s významným dopadem na IT infrastrukturu, informační systémy a aplikace, ale bezprostředně neohrožující klíčové procesy organizace. Informační systémy a aplikace jsou částečně funkční nebo existuje dočasné řešení. Příklady závažných závad: nefunkční či jen částečné funkční funkce, zpomalení aplikace, chyba zálohování a obnovy bez bezprostředního rizika ztráty dat, ztráta vysoké dostupnosti řešení [↑](#footnote-ref-6)
7. Vada, jež nenaplňuje definici kategorie 1 a 2. Vada s minimálním dopadem na procesy organizace nebo vada bez dopadu na provoz (kosmetická vada). Celková funkčnost informačních systémů a aplikací není nijak ohrožena. Příklady drobných vad: nesprávně zobrazený prvek v rozhraní, chyba v reportu, varovná zpráva označující možný budoucí problém, drobná chyba konfigurace s minimálním dopadem na celkovou funkčnost [↑](#footnote-ref-7)