Dodávka a implementace XDR nástroje  
  
**Účel dokumentu:** Tento dokument specifikuje minimální technické a další požadavky na dodávku, implementaci a podporu systému Extended Detection and Response (XDR) pro zajištění kybernetické bezpečnosti Českého rozhlasu (v tomto dokumentu dále také jako „ČRo“ či „zadavatel“ či „objednatel“).

1. **Úvodní informace**
   1. **Cíl zakázky**

Předmětem veřejné zakázky je pořízení, implementace a zajištění následné podpory XDR nástroje, který zajistí automatizovanou detekci, analýzu a odpovídající reakci na bezpečnostní incidenty v síťovém prostředí a na koncových zařízeních zadavatele. Dodávaný systém musí umožňovat integraci dat z různých zdrojů (koncové body, síť, cloudové služby atd.) a poskytovat komplexní přehled o bezpečnostních hrozbách a incidentech v prostředí objednatele.

* 1. **Popis stávajícího řešení.**

V současnosti je pro zajištění kybernetické bezpečnosti v ČRo k detekci a reakci na kybernetické hrozby na koncových bodech nasazeno řešení Cortex XDR Pro od výrobce Palo Alto Networks. Toto řešení je nasazeno přibližně na cca 2100ks koncových pracovních stanicích v prevenčním režimu, přičemž se jedná převážně o stanice s operačním systémem Microsoft Windows a MacOS. Cortex XDR Pro je provozován bez dalších rozšiřujících modulů. Ke správě stávajícího řešení a k řešení incidentů je proškolen interní tým zaměstnanců zadavatele.

V rámci stávajícího nasazení jsou využívány zejména funkce pro:

* Detekci hrozeb na základě chování uživatele a zařízení,
* Forenzní analýzu incidentů,
* Automatickou reakci na vybrané události,
* Správu politik pro endpoint ochranu a detekci.

Stávající řešení je integrováno s interním systémem identity (Active Directory, dále pouze jako „AD“) a je připraven pro rozšířenou integraci se síťovými prvky a systémem SIEM. V prostředí jsou rovněž provozovány firewally Palo Alto Networks, jejichž logy nejsou zatím do XDR připojeny. Jsou nastavené bezpečnostní politiky pro zabezpečení prostředí ČRo. Jsou aplikované výjimky pro zachování funkcionalit definovaných SW, tyto výjimky jsou specifikované několika parametry. Distribuce agentů je v současné chvíli řešena přes nástroj System Center Configuration Manager od výrobce Microsoft v kombinaci s doménovými politikami a skupinami na AD.

* 1. **Rozsah plnění**
* Dodávka softwaru XDR splňující požadavky zadavatele včetně zalicencování požadovaných funkcionalit až pro 2300 koncových stanic.
* Implementace systému do stávající IT infrastruktury zadavatele (k tomu viz požadavky na implementaci níže).
* Proškolení dvou (2) administrátorů Objednatele ke správě a používání nově dodaného řešení, a to minimálně v níže uvedeném rozsahu:
  + Základní ovládání dodávaného řešení.
  + Distribuce klientů na koncové stanice s OS Windows, Linux, macOS.
  + Tvorba výjimek (například whitelist aplikace na základě definované sady kritérií apod.).
  + Propojení na řešení třetích stran (integrace logů z Next Generation Firewallů Palo Alto Networks, zasílání logů do systému SIEM IBM QRADAR).
  + Ukázka práce v novém řešení při analýze a řešení incidentů (například detekce malware apod.).
* Poskytnutí služby odborných konzultací k dodávanému řešení, a to v rozsahu celkem 9 MD využitelných zadavatelem po dobu trvání smlouvy.
* Zajištění poskytnutí podpory od výrobce dodávaného řešení po dobu 3 let (36 měsíců) od data zpřístupnění supportního portálu výrobce pro hlášení problémů objednatele s dostupností takového portálu v režimu 24/7/365.
* Dodání dokumentace nasazeného řešení v minimálním rozsahu popsaného níže v tomto dokumentu.

1. **Technické a další požadavky**

**Detailní popis technických požadavků zadavatele na poptávaný nástroj je uveden v  Příloha č. 6 ZD - Technická specifikace\_požadavky.**

* 1. **Požadavky na implementaci**

Implementace dodávaného řešení bude splňovat následující podmínky, které musí být ze strany poskytovatele splněny do jednoho (1) měsíce od data účinnosti smlouvy:

* Implementace ochrany dodaným řešením pro alespoň 1500 koncových pracovních stanic s operačním systémem Windows a MacOS v prevenčním režimu. Řešení v uvedeném počtu koncových stanic musí být nasazeno do 1 měsíce od data účinnosti smlouvy.
* Implementaci řešení na zbývající počet stanic objednatele předpokládá objednatel zajistit vlastními kapacitami, a to prostřednictvím proškolených administrátorů. V rámci školení tak bude zahrnuto předání odborných znalostí, mimo jiné, k instalaci systému na koncové stanice. Ze strany poskytovatele a jeho řešení musí být tedy zajištěna možnost následné instalace na další stanice. V případě potřeby předpokládá objednatel využití konzultačních služeb v rámci technické podpory (k tomu viz níže).
* Pokud je to relevantní, Objednatel vyžaduje migraci veškerých prvků stávajícího řešení, zejména:
  + Převod stávajících detekčních politik a pravidel.
  + Zachování nebo náhrada současných funkcionalit (např. behaviorální analýza, forenzní záznamy, reakční mechanismy).
  + Integrace s autentizačními systémy.
  + Převod dat a znalostní báze incidentů, pokud to typ řešení umožňuje.
* Zajištění integrace logů z provozovaných firewallů Palo Alto Networks v prostředí objednatele do nového XDR systému a jejich efektivního zpracování a využití v rámci detekčních a analytických mechanismů dodaného řešení.
* Zajištění implementace nových funkcionalit, které vyplývají z požadavků v příloze s definovanými parametry (Příloha č. 6 ZD Technická specifikace\_požadavky).
* Zajištění nepřerušeného provozu ochrany koncových zařízení během migrace, včetně řízeného přechodu a ověření funkčnosti prevenčního režimu dodaného řešení.
* Proškolení administrátorů a bezpečnostního týmu k novému řešení a způsobu jeho provozu.

Náklady spojené s implementací musí Dodavatel vyčíslit a uvést v tabulce pro výpočet nabídkové ceny, která je uvedena v příloze. Dodavatel musí výslovně uvést, zda dodávané řešení umožňuje využít stávající klienty, politiky či jiné komponenty již implementované v rámci současného nasazení systému Cortex XDR Pro.

* 1. **Harmonogram implementačních prací**

Dodavatel je povinen přiložit k nabídce předpokládaný plán implementace, včetně:

* Časového harmonogramu.
* Odhadu pracnosti na straně dodavatele a odhadované nutné součinnosti na straně objednatele.
* Přehledu nutných zdrojů (lidských, technických).
* Identifikace možných rizik a návrh jejich mitigace.
  1. **Technická podpora a údržba**

Specifikace podpory a údržby systému:

* Objednateli bude poskytnut přístup do supportního portálu výrobce, kde mu bude umožněno zakládat požadavky na řešení problémů s používáním či funkčností dodávaného řešení. Tento support portál je dostupný 24/7/365, další podmínky používání portálu včetně specifikace reakčních dob a sankcí při jejich nedodržení se řídí všeobecnými obchodními podmínkami výrobce dodávaného řešení.
* Nahlášené problémy budou řešeny ve lhůtách stanovených podmínkami výrobce řešení.
* Účelem podpory a údržby je zajistit funkčnost systému bez vad po smlouvou stanovenou dobu.
* Dodavatel se zavazuje k poskytnutí služby odborných konzultací k dodávanému řešení, a to v rozsahu 3 MD (člověkoden) ročně, celkem tedy 9 MD využitelných zadavatelem po dobu trvání smlouvy. 1 MD služeb představuje osm (8) hodin práce konzultačního technika.
  1. **Aktualizace**

Objednateli budou zpřístupněny pravidelné softwarové aktualizace provedených výrobcem dodaného řešení včetně databáze hrozeb po celou dobu trvání smlouvy.

* 1. **Dokumentace**

Dodavatel zpracuje jako součást implementace (instalace) systému XDR dokumentaci minimálně v rozsahu uvedeném níže v této kapitole. Dokumentace bude napsána v českém jazyce. Dokumentace bude dodána i v editovatelném formátu dokumentu, aby mohl objednatel případně do dokumentace zavádět nové skutečnosti či změny v průběhu používání dodaného řešení. Výsledná podoba dokumentace bude vzájemně odsouhlasen oběma stranami.

* Popis architektury systému
  + Topologie nasazení (on-prem, cloud, hybrid).
  + Popis komponent (agenti, serverové části, moduly, konektory, integrace se systémy třetích stran).
  + Síťové vazby (co kam komunikuje – porty, protokoly).
  + Diagram zapojení (vizualizace pro rychlou orientaci).
* Popis integrace s ostatními systémy
  + Popis napojení na SIEM.
  + Popis napojení na FW.
  + Popis napojení na další nutné komponenty (např. AD).
* Správa a provoz
  + Popis přístupových uživatelských rolí v systému a jejich oprávnění (na co má kdo oprávnění v rámci systému).
  + Postup přihlašování do správy systému (MFA / AD / SSO).
  + Popis správy agentů (nasazení, aktualizace, odinstalace, monitoring stavu agentů).
* Nastavení bezpečnostních politik
  + Popis nasazených bezpečnostních politik pro zajištění zabezpečení prostředí ČRo.
* Notifikace a logování
  + Popis nastavení alertů a notifikací na vzniklé incidenty.
  + Popis nastavení auditních logů událostí (kde se co eviduje, kdo co udělal), popis retenční doby logů a typu logovaných událostí.