Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Technická specifikace

Příloha č. 1 zadávací dokumentace pro zadávací řízení „Implementace systému Extended Detection and Response (XDR)“

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 Seznam zkratek 2
2 Úvod 6
2.1 Záměr SŽ v oblasti systému Extended Detection and Response 6
2.2 Předmět plnění veřejné zakázky 9
2.3 Parametry poptávaného řešení 12
2.3.1 Network Detection and Response 12
2.3.2 Endpoint Detection and Response 13
2.3.3 Lokality určené k provozu komponent XDR 13
2.3.4 Požadavky na technické funkcionality řešení 14
2.3.5 Požadavky na specifikaci virtualizačních prostředků SŽ 25
2.3.6 Dodávka hardwarových a softwarových prostředků 26
2.4 Oblasti, které nejsou předmětem plnění veřejné zakázky 27
3 Současný stav a popis prostředí 28
4 Požadavky na plnění 29
4.1 Jednorázové projektové činnosti 29
4.1.1 Před-implementační analýza 29
4.1.2 Instalace a konfigurace řešení 30
4.1.3 Optimalizace bezpečnostní / detekční politiky řešení 30
4.1.4 Napojení na platformu Log management / SIEM 31
4.1.5 Školení 31
4.2 Průběžné služby dodavatele řešení 32
4.2.1 Technická podpora servisního týmu SŽ 32
4.2.2 Údržba řešení 32
4.3 Konzultace a rozvojové aktivity 34
5 Fáze plnění a akceptační milníky 34

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
API	Rozhraní pro programování aplikací (Application Programming Interface)
APT	Pokročilé a trvalé kybernetické hrozby.
ARP	Protokol používaný pro identifikaci a rozlišení zařízení v síti.
CPU	Procesorová jednotka informačního systému.
CSV	Jednoduchý souborový formát určený pro výměnu tabulkových dat
ČD	České dráhy.
DC	Datové centrum.
DLL	Dynamicky volaná knihovna aplikace, nebo jiného druhu spustitelného kódu.
DNS	Systém správy doménových jmen, slouží k převodu jmenných záznamů na adresy informačních systémů a evidenci dalších podpůrných informací
Dodavatel	Subjekt, který se v rámci zadávacího řízení uchází o realizaci veřejné zakázky
EDR	Endpoint Detection and Response je nástroj pro detekci kybernetických hrozeb v prostředí koncových zařízení, podporu jejich vyšetřování a reakce.
EPP	Platformy pro ochranu koncových bodů (EPP) umožňují nasazení agentů nebo senzorů pro zabezpečení spravovaných koncových bodů, včetně stolních počítačů, notebooků, serverů a mobilních zařízení.
FPS	Počet síťových spojení (flows) uskutečněná za časovou jednotku jedné sekundy.
Gbps	Parametr specifikující objem datových bitů (v miliardách) přenesených v síti za danou časovou jednotku (sekunda).
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance
HTTP	HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro komunikaci s WWW servery
HW	Hardware označuje veškeré fyzicky existující technické vybavení informačních a komunikačních systémů.
ICAP	Protokol ICAP (Internet Content Adaptation Protocol) je určen k přenesení zpracování internetového obsahu na vyhrazené servery.
IMAP	Komunikační protokol pro přenos elektronické pošty.
IOC	Indikátor kompromitace (Indicator of Compromise, IOC) je ve forenzním světě důkaz, který v kybernetickém prostředí naznačuje, že došlo k narušení kybernetické bezpečnosti

IP	IP je zkratka pro "internetový protokol", což je soubor pravidel, jimiž se řídí formát dat odesílaných prostřednictvím internetu nebo místní sítě.
IS/ICT	Informační systémy a informační a kumunikační technologie.
JSON	JavaScript Object Notation je způsob zápisu dat nezávislý na počítačové platformě, určený pro přenos dat, která mohou být organizována v polích nebo agregována v objektech
LDAP	Definovaný protokol pro ukládání a přístup k datům na adresářovém serveru.
Mbps	Parametr specifikující objem datových bitů (v milionech) přenesených v síti za danou časovou jednotku (sekunda).
MD	Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day)
MS AD	Adresářová služba vyvýjená společnostní Microsoft.
NDR	Network Detection and Response je nástroj pro detekci kybernetických hrozeb v prostředí sítě, podporu jejich vyšetřování a reakce
NTP	Protokol pro syschronizaci systémového času.
On-premise	On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá
OpenIOC	Standardizovaný formát pro popis stop a artefaktů, s nimiž se setkáváme v průběhu vyšetřování kybernetických bezpečnostních událostí.
OS	Operační Systém
OT	Operational technology (OT) je hardware a software, který zjišťuje nebo způsobuje změny prostřednictvím přímého monitorování a/nebo řízení průmyslových zařízení, prostředků, procesů a událostí.
PCAP	Packet Capture neboli PCAP je aplikační programovací rozhraní, které zachycuje živá data síťových paketů z vrstev 2-7 modelu OSI.
PID	Identifikační číslo procesu.
POP3	Komunikační protokol pro přenos elektronické pošty.
PROXY	Prostředník mezi klientem a cílovým počítačem, překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient.
RAM	Operační paměť informačního systému.
RAT	Remote Access Tool – druh škodlivého kódu, který umožňuje vzdálené ovládání napadeného systému
s2s VPN	Site to site VPN
SLA	Dohoda o úrovni poskytovaných služeb (Service Level Agreement)
SMTP	Komunikační protokol pro přenos elektronické pošty.
SOC	Kybernetické bezpečnostní dohledové centrum.
SPAN	SPAN (Switched Port Analyzer) je vyhrazený port na přepínači, který přebírá zrcadlenou kopii síťového provozu z přepínače a odesílá ji na místo určení
SSL	Secure Sockets Layer, počítačový protokol, který zajišťuje bezpečnost dat odesílaných přes internet pomocí šifrování.
STIX	Jazyk a serializační formát používaný k výměně zpravodajských informací o kybernetických hrozbách.
SW	Software

SŽ	Správa železnic, státní organizace
TAXII	Formát, v němž jsou předávány zpravodajské údaje o hrozbách.
TCP	Jedná se o stavový a spolehlivý síťový komunikační protokol.
UDP	Jedná se o síťový komunikační protokol užívaná především k zasílání nestavovách datových rámců.
URL	Uniform Resource Locator (URL), označovaný jako webová adresa, je odkaz na webový zdroj, který určuje jeho umístění v počítačové síti a mechanismus jeho vyhledávání
USB	Univerzální sériové rozhraní informačního systému
vCPU	Virtuální procesorová jednotka informačního systému.
WAN	Wide Area Network je v informatice počítačová síť, která pokrývá rozlehlé geografické území
WEB	Rozhraní aplikace, nebo jiného informačního systému, které je přístupné prostřednictvím internetového prohlížeče nebo jeho alternativ.
WebUI	Grafické uživatelské rozhraní přístupné prostřednictvím internetového prohlížeče.
XDR	Extended Detection and Response je nástroj pro detekci kybernetických hrozeb, podporu jejich vyšetřování a reakce; systém funguje na základě shromažďování a korelace dat z různých bodů, jako jsou sítě, servery a pracovní stanice
XML	Extensible Markup Language je obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C
YARA	Programovací jazyk, fungují tak, že definuje řadu proměnných, které obsahují vzory nalezené ve vzorku škodlivého kódu.

Seznam zkratek pro specifické aplikace SŽ:

Zkratka	Popis
ASVC	Automatické stavění vlakových cest
DŘT	Dispečerská řídicí technika
DDTS	Dálková diagnostika technologických systémů
CDP	Centrální dispečerské pracoviště
CDS	Centrální dispečerský systém
DŽDC	Dispečer železniční dopravní cesty
DŽIN	Dispečer železniční infrastruktury
ED	Elektro dispečer
GVD	Grafikon vlakové dopravy
SSZT	Správa sdělovací a zabezpečovací techniky
ST	Správa tratí
SŽE	Správa železniční energetiky

TechDS	Technologický a dohledový systém
TDS	Technologická datová síť
TDCDP	Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP
VS	Vlakové soupravy

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace k veřejné zakázce s názvem „Implementace systému Extended Detection and Response (XDR)" (dále jen „veřejná zakázka"), pro organizaci Správa železnic, státní organizace (dále jen „SŽ"). Dokument popisuje technické a jiné požadavky SŽ kladené na veřejnou zakázku.

2.1 Záměr SŽ v oblasti systému Extended Detection and Response

SŽ očekává zavedení platformy, která umožní detekovat kybernetické bezpečnostní hrozby a podpoří vznikající proces Security Operations Center, který je budován v rámci interního týmu organizace SŽ. Požadovaná bezpečnostní platforma musí umožnit identifikaci nebezpečných projevů v síťovém provozu, jehož analýzu bude řešení provádět na základě pasivního odposlechu a bez jeho jakéhokoli ovlivnění a na koncových zařízeních prostřednictvím softwarového agenta. Řešení musí poskytovat funkcionality umožňující automatizaci mnoha kroků a procesů v rámci vyšetřování a reakcí na incident s cílem snížit zatížení specialistů, kteří by jinak museli pracovat s mnoha bezpečnostními technologiemi zvlášť a tím by byla snížena jejich efektivita.

Řešení XDR by mělo identifikovat čtyři hlavní typy kybernetických bezpečnostních rizik:

1. Neznámý malware:
    - Externí útočníci, kteří využívají moderní, dosud neznámý, škodlivý kód k napadení a ovládnutí zařízení v síti SŽ.
2. Cílené útoky:
    - Externí útočníci, kteří využívají sociální inženýrství, exploity, útoky hrubou silou nebo jiné techniky ke kompromitaci aplikací nebo koncových bodů, krádeži legitimních uživatelských pověření, vytvoření Command & Control, pohybu útočníka infrastrukturou (laterální pohyb) a krádeži, manipulaci nebo zničení dat.
3. Útoky zasvěcených osob:
    - Zaměstnanci nebo smluvní partneři se dopouštějí různých způsobů chování, včetně neoprávněného přístupu k souborům a datům, jejich krádeže, manipulace s nimi, užívání neschválených nástrojů a dalších nebezpečných postupů.
4. Rizikové chování:
    - Také dobře míněné, ale lehkomyslné chování zaměstnanců může vystavit organizaci SŽ útoku. Takové rizikové chování zahrnuje např. sdílení uživatelských účtů, zpřístupnění citlivých dat

neoprávněným uživatelům, umožnění vzdáleného přístupu ke koncovým bodům organizace SŽ a další.

Uvažované řešení by mělo zajistit reakci na stoupající nebezpečné napadení organizace SŽ kybernetickým útokem realizovaným externím či interním útočníkem, a to minimálně tím, že bude splňovat níže specifikované funkcionality nebo vlastnosti:

- Zajišťovat neustále sběr informací o chování zařízení v chráněných částech sítě pomocí komponent řešení NDR, popisovat toto chování v podobě metadat a ukládat tato metadata pro účely provádění dodatečné analýzy.
- Zajišťovat neustále sběr informací o chování zařízení, zabezpečených softwarovým agentem EDR, popisovat toto chování v podobě metadat a ukládat tato metadata pro účely provádění dodatečné analýzy.
- Metadata musí být možné zaznamenávat tzv. neselektivně, tedy o veškerém dění a nikoli jen o detekovaném podezřelém chování
    - toto má napomoci při aktivním hledání hrozeb (tzv. huntingu), jejichž charakteristika není výrobcem definována jako nebezpečné chování;
    - slouží pro tvorbu specifických detekčních use-case, odhalování aktivit interního útočníka a krádeže informací;
    - umožní zpětné prozkoumání vektorů průniku a zaznamenaných indikátorů kompromitace (tzv. IOC).
- Provádět detekci bezpečnostních kybernetických událostí v reálném čase v chráněných částech sítě a na zabezpečených koncových zařízeních
    - malware a nebezpečný kód;
    - specifický obsah (obsahová analýza);
    - nebezpečná, podezřelá nebo specifická aktivita;
    - reputační riziko komunikujících stran.
- Detekci bezpečnostních kybernetických událostí provádět pomocí vyhledávání signatur, heuristickou analýzou, vyhledáváním typického chování (behaviorální analýza) a detekcí pomocí detonace na sandboxu tzv. virtuálním provedením
    - součástí dodávaného řešení musí být kontinuální služba aktualizace signatur/definice chování malware/aktualizace pravidel sandboxu;
    - řešení musí umožnit definici vlastních detekčních pravidel.
- Provádět automatickou retrospektivní analýzu a detekci bezpečnostních kybernetických událostí v zaznamenaných metadatech o chování chráněných částí sítě

- výrobcem získané signatury jsou automaticky prověřovány v zaznamenaných a uložených metadatech;
- takto jsou odhalovány hrozby na které v okamžiku jejich realizace neexistovala signatura pro jejich odhalení.

Systém musí poskytovat jednotné uživatelské webové rozhraní pro práci specialistů s dodávaným řešením. Rozhraní musí umožnit rychlé zkoumání události dostupností kontextu v podobě záznamů o relevantním síťovém provozu, chování na koncovém zařízení a dalších souvisejících událostech/alertech – jak typově (stejný typ události/alertu na jiném aktivu), tak z hlediska stejných IP adres a dalších dostupných indikátorů.

2.2 Předmět plnění veřejné zakázky

Předmětem veřejné zakázky je dodávka, implementace a podpora řešení pro automatizovanou detekci a reakci na bezpečnostní incidenty v síťovém prostředí a na koncových zařízeních organizace SŽ, známé jako Extended Detection and Response (XDR). XDR nástroje poskytují sdruženou funkcionalitou vycházející z Network Detection and Response (NDR) a Endpoint Detection and Response (EDR), přičemž oba tyto nástroje jsou vzájemně úzce integrovány a poskytují své funkcionality v rámci jednotného uživatelského rozhraní a dalších vzájemných integrací, které podporují činnosti týmu Security Operations Center.

SŽ očekává nabídku na technické řešení, které bude do prostředí SŽ naimplementováno a po implementaci provozováno **po dobu 5 let**, přičemž po celou dobu bude řešení pokryto potřebnou licencí, technickou podporou výrobce a budou aktivovány všechny předplatné výrobce nezbytné k zajištění chodu řešení a splnění požadovaných funkcionalit. Spolu s dodávkou řešení, očekává SŽ také poskytování služby technické podpory od Dodavatele, a to na celou specifikovanou dobu provozu technického řešení.

Dodávané řešení musí splňovat následující požadavky na funkcionality – NDR:

- Záznam informací o síťové komunikaci v podobě, která umožní pozdější analýzu.
- Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorována jsou tedy všechna probíhající spojení na všech síťových portech.
- Pro účely podpory aktivního vyhledávání kybernetických hrozeb (tzv. hunting) je po řešení požadována podpora obsahové analýzy:
    - tedy bude možné definovat vlastní pravidla pro analýzu a detekci obsahu přenášeného v obsahu síťové komunikace, jako je např. v těle zpráv elektronické pošty, v přenášených souborech, v obsahu uloženém v kompozitních souborech (archívy, komprimované soubory, vnořené dokumenty);
    - pro výše uvedené druhy obsahu bude řešení generovat a ukládat popisná metadata;
    - bude možné pracovat s metadaty popisujícími obsahové části síťového provozu a pokládat do nich strukturované dotazy.
- Systém je schopný detekovat také malware skrytý hluboko v přenášeném obsahu, jako je např. v těle zpráv elektronické pošty, v přenášených souborech, v obsahu uloženém v kompozitních souborech (archívy, komprimované soubory, vnořené dokumenty).
- Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem sítě.
- Pravidla pro analýzu provozu umožní definovat podmínky odkazující se na přenášený obsah a parametry aplikační vrstvy – například:

  - odhalit přenášené soubory, kde koncovky soborů nesouhlasí s obsahem;
  - nebo čísla typických portů nesouhlasících s typem rozpoznaného komunikačního protokolu.
- Podpora monitorování provozu na rozhraních Ethernet s rychlostmi dle specifikací parametrů SPAN rozhraní v kapitole „2.3. Parametry poptávaného řešení" Technické specifikace.
- Umožňuje definovat pravidla hledající souběh událostí nebo posloupnost událostí v síťovém provozu a generovat upozornění (alerty), a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o provozu zpětně.

Dodávané řešení musí splňovat následující požadavky na funkcionality – EDR:

- Záznam informací o chování koncových zařízení v podobě, která umožní pozdější analýzu
  - probíhá pro veškeré chování koncového zařízení a bez ohledu na to, zda je detekováno kybernetické nebezpečí;
  - záznam informací o chování koncových zařízení probíhá díky softwarovému agentu, který je instalovaný na SŽ určených pracovních stanicích a serverech.
- Pravidla pro analýzu provozu umožní definovat podmínky odkazující se na:
  - spuštění a ukončení procesů,
  - souborové manipulace,
  - manipulace s registry,
  - síťových spojení včetně URL pro http spojení,
  - DNS překladů,
  - Manipulace s USB médii a přenosy souborů na ně,
  - Windows události (Windows Events).
- Umožňuje definovat pravidla hledající události v chování koncových zařízení, generovat upozornění (alerty), a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o chování zpětně.
- Umožňuje používat připravené nebo definovat a spouštět vlastní reakční činnosti na koncových zařízeních (automaticky, poloautomaticky, manuálně), které umožní alespoň:
  - obohacovat informace relevantní k detekovaným událostem:
    - získat otisk paměti běžícího procesu / celého systému,
    - získat ze zařízení podezřelý soubor,

        - získat aktuální směrovací nebo ARP tabulku,
    - reagovat v případě zaznamenaného bezpečnostního ohrožení:
        - odhlásit uživatele,
        - ukončit proces,
        - izolovat koncové zařízení, přičemž nesmí být zamezeno další vyšetřování a ovládání zařízení z rozhraní nástroje EDR.
- Oprávnění spouštět připravené činnosti (tasky) je možné řídit pro konkrétní analytiky nebo skupinu analytiků.

Dodávané řešení musí splňovat následující požadavky na funkcionality – XDR:

- Systém poskytuje jednotné webové uživatelské rozhraní pro analýzu zaznamenaného provozu a chování koncových zařízení, vyhodnocování detekovaných událostí a parametrizace řešení.
- Nedílnou součástí řešení musí být možnost řízení přístupových oprávnění k jednotlivým modulům systému a zpracovávaným/zaznamenaným metadatům. V rámci řízení přístupových oprávnění požaduje SŽ minimálně:
    - Umožnit přístup k detekovaným událostem XDR operátorům pracoviště Security Operations Center, přičemž jim nebudou zpřístupněna uložená metadata, která nejsou související s detekovanou událostí.
    - Umožnit, vybrané skupině analytiků přístup ke všem uloženým popisným informacím (metadatům), aby bylo možné provádět aktivní vyhledávání nebezpečných jevů (tzv. hunting).
- K dispozici jsou historické informace o síťovém provozu a chování koncových zařízení s určenou dobou retence pro následnou analýzu, přičemž tato data musí být chráněna před narušením jejich integrity.
- Detekce malware je prováděna pomocí vyhledávání signatur, heuristickou analýzou, vyhledáváním anomálního chování (behaviorální analýza) a detekcí na sandboxu virtuálním provedením.
- Součástí dodávky je kontinuální služba aktualizace signatur/definice chování malware/aktualizace pravidel sandboxu.

Nabízené řešení musí v oblasti otevřenosti platformy splňovat následující požadavky:

- Dokumentované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami, HTTP & XML nebo JSON API rozhraní. Přístupné informace musejí zahrnovat:
    - Aktiva zaznamenaná ve sledovaném prostředí,
    - Vygenerované události,
    - Uložená metadata.

- Předpřipravené integrační vazby na aplikace typu Log Management a SIEM pro následující kategorie událostí:
    - Kybernetické bezpečnostní události detekované ve sledovaném prostředí.
    - Auditní log řešení NDR a EDR,
    - Systémový log řešení NDR a EDR.
- Být připravené na aktivní dohled systémem provozního monitoringu Zabbix.

Všechny komponenty řešení požaduje SŽ provozovat v režimu on-premise (tedy ve své vlastní infrastruktuře). Tento požadavek vychází z potřeby nepřetržité možnosti sbírat metadata, ukládat je a vyhodnocovat bezpečnostní události i v situaci, kdy je vlivem provozní nedostatečnosti nebo působením kybernetické hrozby nedostupná internetová konektivita.

Přípustná integrace s online / CLOUD službami je pouze pro aktualizační služby a získávání informací o hrozbách. V případě nedostupnosti internetové konektivity umožní řešení manuální dodání aktualizací pro XDR řešení.

Není přípustné předávat data z prostředí SŽ ke zpracování k výrobci nabízeného řešení, pokud tuto aktivitu manuálně a pouze pro konkrétní vyšetřování neiniciuje pracovník SŽ.

2.3 Parametry poptávaného řešení

SŽ požaduje implementaci řešení Extended Detection and Response (XDR):

- Do síťového prostředí s požadavkem na analýzu síťového provozu o výkonnostní kapacitě specifikované v kapitole Technické specifikace s názvem „Lokality určené k provozu komponent XDR", ve sloupci „Provoz (Mbps)", tedy maximálně **10Gbps**.
- Na minimálně **10000 koncových zařízení** typu pracovní stanice a servery.
- S celkovou požadovanou retencí historických metadat o chování sítě a koncových zařízení po dobu minimálně **30 dní**.
- Schopností uložit metadata relevantní k detekovaným bezpečnostním událostem po dobu alespoň **12 měsíců**.
- Zajištěním vysoké dostupnosti na úrovni centrální management konzole pro účely zpracování alertů generovaných chráněným prostředím. Vysoká dostupnost musí být řešena způsobem automatického přenesení funkcionality tzv. Active / Standby nebo Active / Active na úrovni dodávané technologie.

2.3.1 Network Detection and Response

Zavedení nástroje Network Detection and Response se očekává do vybraných míst síťového prostředí SŽ, konkrétně do míst v síťové infrastruktuře, která jsou

chráněna firewallem externího perimetru SŽ, avšak budou určena jako vstupně/výstupní body infrastruktury nebo jinak exponovaná síťová prostředí.

Takovými místy v síťovém prostředí typicky jsou:

- Spojnice vnitřních sítí a externího perimetrového firewallu.
- Místa zakončující propojení datových center a sítí uživatelské WAN.
- Místa připojení významných administrativních objektů do sítě uživatelské WAN.
- Síťová propojení k třetím stranám (dodavatelé, servisní partneři, společnosti skupiny ČD).
- Místa propojující prostředí IT a technologické prostředí OT (Operational Technology), která jsou situována do oblastních ředitelství a centrálních dispečerských pracovišť SŽ.

2.3.2 Endpoint Detection and Response

Předmětem zabezpečení koncových zařízení nástrojem EDR jsou především zařízení SŽ, která jsou provozována v jejích vnitřních sítích, ale která umožňují mobilitu a mohou se tak pohybovat také v prostředí internetu.

Nástroj EDR, který bude instalován na vybraná koncová zařízení, nesmí být v kolizi s nástroji Endpoint Protection Platform (EPP), které SŽ provozuje – tedy aktuálně užívaným nástrojem výrobce F-Secure.

2.3.3 Lokality určené k provozu komponent XDR

SŽ požaduje řešení zabezpečení síťového provozu systémem Network Detection and Response, které pokryje až **20 lokalit** v rámci České republiky, které jsou uvedené v následující tabulce. Stejné lokality bude možné využívat pro potřeby instalace podpůrných komponent řešení Endpoint Detection and Response.

Sloučené řešení Extended Detection and Response bude disponovat centrálním rozhraním pro správu a analytické činnosti realizované pracovištěm Security Operations Center (SOC) SŽ. Centrální pracoviště bude situováno v lokalitě Praha.

Typ lokality	*Adresa lokality*	*Počet zařízení (IP adres)*	*Provoz (Mbps)**	*Provoz (Fps)**	*Rozhraní SPAN*	*Přípojka do WAN (Gbps)*
Datové centrum	Praha	700	3600	3750	1G/UTP i SFP	2x10
Datové centrum	Brno	200	400	417	1G/SFP	2x 1
Datové centrum	Plzeň	600	800	833	1G/UTP	2x 1 2x 10
Datové centrum Dispečerské pracoviště	Přerov	400	400	417	1G/UTP	1
Oblastní ředitelství	Ostrava	500	100	104	1G/SFP	2x 1
Oblastní ředitelství	Brno	200	100	104	viz. DC Brno *	2x 1
Oblastní ředitelství	Jihlava	200	100	104	1G/UTP	1

Oblastní ředitelství	Praha	200	100	104	1G/UTP	1
Oblastní ředitelství	Praha	900	100	104	1G/UTP	1
Oblastní ředitelství	Hradec Králové	700	500	521	1G/UTP	1
Oblastní ředitelství	Pardubice	500	300	313	N/A	2
Oblastní ředitelství	Plzeň	50	200	208	viz. DC Plzeň *	2 x 1
Oblastní ředitelství	České Budějovice	400	100	104	1G/UTP	2x1
Oblastní ředitelství	Ústí nad Labem	600	200	208	1G/UTP	2x1
Dispečerské pracoviště	Praha	300	100	104	1G/SFP	2x1
Organizační jednotka	Brno	500	200	208	viz. DC Brno *	2x 1
Organizační jednotka	Olomouc	900	800	833	1G/UTP	10
Technologická sdělovací místnost	Praha	400	600	625	1G/UTP	2x1
Technologická sdělovací místnost	Praha	100	400	417	1G/SFP	1
Externí subjekt	Olomouc	50	700	729	1G/UTP	1

**Lokality, které mají u parametru „Rozhraní SPAN" uvedeno „viz. DC", budou monitorovány v rámci zařízení umístěného do náležícího datového centra. Proto je nezbytné, aby NDR sonda umístěná v daném DC počítala také s kapacitou síťového provozu takto označených dalších lokalit.*

**Uvedené provozní hodnoty odpovídají momentálním hodnotám zaznamenaným měřením v referenčním pracovním dni, jsou navýšené o 25 % a zaokrouhleny na horní hodnoty. FPS jsou odvozeny od vzorku komunikací zachycených v centrální lokalitě SŽ a korelovány s právě zaznamenaným objemem provozu v Mbps. Z odpovídajícího referenčního poměru Mbps/Fps byly dopočítány všechny ostatní lokality.*

2.3.4 Požadavky na technické funkcionality řešení

Všechny parametry požadované v tomto dokumentu jsou pro dodavatele závazné a SŽ vyžaduje jejich naplnění.

Požadavky na vybrané funkcionality poptávaného řešení, které SŽ vyžaduje splnit technickými prostředky, a u nichž dodavatel musí popsat způsob, kterým jím nabízené řešení naplní daný požadavek, jsou specifikovány v tabulce, která tvoří přílohu č. 19 zadávací dokumentace. Nedílnou přílohou Zadávací dokumentace je dotazník „TS_XDR_dotazník.xlsx", ve kterém dodavatel potvrdí připravenost nabízeného řešení splnit vybrané požadavky a vyplní způsob, kterým je každý požadavek naplněn.

SŽ upozorňuje, že nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedeného v této kapitole Technické specifikace povede k vyloučení dodavatele ze zadávacího řízení. V případě, že bude nesplnění takového požadavku odhaleno až v průběhu provádění plnění, bude to považováno za hrubé porušení povinností dle přílohy č. 6 zadávací dokumentace – Závazného vzoru smlouvy a bude důvodem pro odstoupení od této smlouvy.

2.3.4.1 Požadavky na Network Detection and Response

Id	Oblast NDR	Požadovaná funkcionalita řešení NDR
1	Detekce	Možnost importu detekčních pravidel s podporou formátů YARA a zdrojů specifikace TAXII/STYX.
2	Detekce	Analýza síťového provozu v rámci systému se provádí pro veškerý síťový provoz bez ohledu na použité komunikační protokoly, a proto jsou sledována a analyzována všechna probíhající spojení na všech síťových portech.
3	Detekce	Možnost importu úplného záznamu síťové komunikace ve formátu PCAP pro kontrolu, popis a hloubkovou analýzu.
4	Detekce	Import popisu hrozeb od třetích stran a vlastních, které mohou být dodány ve formátech STIX, TAXII, CSV (podpora ThreatConnect).
5	Detekce	Detekce malwaru přenášeného přes jakýkoli nešifrovaný protokol.
6	Detekce	Podpora spolupráce s řešeními SSL Visibility pro kontrolu provozu přenášeného přes šifrované připojení.
7	Detekce	Detekce zpětných volání malwaru Command & Control.
8	Detekce	Detekce projevů nástrojů pro vzdálený přístup (RAT).
9	Detekce	Detekce pokusů o zneužití zranitelností na dálku prostřednictvím sítě.
10	Detekce	Definice výjimek pro vyloučení určité komunikace z inspekce daným pravidlem.
11	Detekce	Detekce malwaru zabaleného i hluboko v obsahu (v archivech a dalších složených dokumentech).
12	Detekce	Identifikace spojení využívajících neočekávané nebo neznámé protokoly (např. nesoulad portů a protokolů).
13	Detekce	Obsahová analýza pro detekci exfiltrace informací s možností nasazení v prostředí se značkami (klasifikátory) i bez nich (např. pomocí regulárních výrazů obsahových pravidel, vzorových šablon atp.).
14	Detekce	Funkce obsahové analýzy detekuje informace přenášené i hluboko v obsahu, bez ohledu na hloubku vložení a bez ohledu na formát souboru.
15	Detekce	Možnost definovat vlastní pravidla detekce nad libovolným typem přenášeného obsahu, charakteristikami chování nebo posloupností událostí v síti.

16	Detekce	Systém bude schopen aplikovat aktualizované signatury na historický síťový provoz uložený v popisných metadatech po dobu požadované retence, aby našel nyní známý malware, který nebyl v minulosti detekován.
17	Detekce	Detekce malwaru se provádí pomocí (všech níže specifikovaných způsobů): - signatur a pravidel, - heuristické analýzy, - vyhledávání typického chování (behaviorální analýza), - detekce v sandboxu pomocí virtuálního spuštění (detonace), - detekce anomálií.
18	Detekce	Detonace/virtuální spuštění podezřelého obsahu, který mohl být zachycen v jakémkoli místě dohledované sítě, v místním sandboxu s podrobným výstupem výsledku detonace v jednotné konzoli bezpečnostního analytika.
19	Detekce	Detekce anomálií pomocí modelů strojového učení a případné generování alarmů pro významné anomálie.
20	Detekce	Pravidla analýzy provozu umožňují definovat podmínky vztahující se k přenášenému obsahu a parametrům aplikační vrstvy, například detekovat přenášené soubory, u nichž koncovky soborů neodpovídají obsahu nebo typická čísla portů neodpovídající typu detekovaného komunikačního protokolu.
21	Detekce	Možnost definovat pravidla pro vyhledávání shody událostí nebo posloupnosti událostí v síťovém provozu a generovat výstrahy průběžnou analýzou okamžitých událostí a analýzou již uložených historických záznamů o provozu zpětně.
22	Detekce	Systém musí klasifikovat události podle MITRE ATT&CK frameworku uvedením odpovídající techniky a/nebo taktiky útočníka. Vlastní pravidla lze definovat tak, aby také používala kategorie MITRE ATT&CK frameworku.
23	Detekce	Retrospektivní analýza všech zaznamenaných údajů o chování sítě, která odhalí sled událostí vedoucích k projevům kybernetického incidentu.
24	Detekce	Možnost definovat pravidla (komunikační matice) pro vyhodnocení oprávněnosti odchozí komunikace vůči definovaným kritickým informačním systémům pomocí kombinací parametrů: - IP adresa/seznam IP adres/rozsah adres,

		- Skutečný typ detekovaného protokolu (nezávisle na definovaném čísle portu TCP/UDP), - Čísla portů (TCP/UDP).
25	Detekce	Schopnost systému identifikovat specifické komunikační protokoly vyskytující se v provozu organizace SŽ. Schopnost zahrnout takto identifikovaný protokol do definice detekčních pravidel.
26	Detekce	Podpora detekce síťového provozu ve spolupráci s PROXY systémy, které podporují protokol ICAP (Internet Content Adaptation Protocol).
27	Vyšetřování	Vestavěná funkce pro vyšetřování, shromažďování stop a generování zprávy o incidentu.
28	Vyšetřování	Průběžné zaznamenávání informací o síťové komunikaci ve formě, která umožňuje pozdější analýzu (metadata).
29	Vyšetřování	Export úplného záznamu, předem popsaných síťových komunikací, ve formátu PCAP pro další zkoumání.
30	Vyšetřování	Pro následnou analýzu jsou k dispozici historické informace o provozu se stanovenou dobou uchování.
31	Vyšetřování	Systém podporuje efektivitu vyšetřování tím, že dokáže automatizovaně spojovat jednotlivé bezpečnostní události, které mají společnou příčinu, do jedné události (incidentu).
32	Vyšetřování	Možnost průběžně zaznamenávat a zpětně analyzovat informace o všech síťových aktivitách (všechny níže uvedené): - IP adresy a jejich zeměpisná poloha, - identity uživatelů (např. e-mailové adresy pro rozhraní SMTP/POP3/IMAP a web-mail nebo uživatelská jména pro jiné protokoly), - čísla portů, - skutečný typ zjištěného protokolu, - parametry rozpoznaných komunikačních protokolů (například hlavičky SMTP, HTTP, …), - typ přenášených souborů (minimálně excel, word, powerpoint, pdf, exe, msi, obrazové formáty, archivní a kompresní formáty, včetně vnořených), - HASH přenášených souborů, - velikost přenášených souborů, - název a přípona přenesených souborů,

		- informace o tom, že soubor je zašifrovaný, a obecně informace o entropii obsahu souborů, - čas a délku spojení, - objem přenesených dat.
33	Vyšetřování	Extrakce obsahu souborů zachycených při jejich pohybu po síti pro forenzní účely pomocí systémové konzoly.
34	Vyšetřování	Zaznamenané informace o provozu umožňují vyhledávat spojení podle libovolného atributu popisujícího spojení nebo pomocí logického výrazu s relačními operátory odkazujícími na atributy spojení.
35	Vyšetřování	Vestavěná podpora pro řízení životního cyklu tiketů pro distribuci úkolů mezi uživatele systému/vyšetřovatele.
36	Vyšetřování	Geolokace komunikujících stran.
37	Vyšetřování	Možnost vlastní definice geolokačních tabulek IP adres (pro geolokaci privátní IP segmentů).
38	Vyšetřování	V oblasti detekce a vyšetřování Advanced persistent threats (APT) musí systém splňovat požadavek na viditelnost stop daného útoku a dostupnost forenzních dat ze všech zachytitelných fází útoku APT (podle fází cyber-kill-chain).
39	Vyšetřování	Systém přiřazuje informace o uživatelském účtu k zaznamenanému síťovému spojení.
40	Reakce	Schopnost automatizace pracovních postupů při nápravě kybernetických incidentů: - plně automatická reakce definovaná bezpečnostní politikou pro síťový provoz, - podporované metody: DROP při in-line zapojení, nebo TCP. Reset pro out-of-band připojení.
41	Reakce	Schopnost ukončit spojení na základě detekce.
42	Reakce	Schopnost umísit škodlivý email do karantény.

43	Reakce	Systém musí být schopen spouštět vyšetřovací nebo nápravné úlohy na koncových bodech prostřednictvím integrace s řešením EDR.
44	Rozhraní	Zdokumentované aplikační rozhraní pro integraci s dalšími bezpečnostními komponentami. Upřednostňujte rozhraní API http a XML nebo JSON.
45	Rozhraní	Předpřipravené integrační vazby na aplikace typu SIEM.
46	Rozhraní	Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní.
47	Rozhraní	Dashboard a možnosti jeho úprav pro grafické zobrazení informací a podpory rozhodovacího procesu (alert triage).
48	Rozhraní	Možnost detailního řízení přístupových práv pro více úrovní pracovníků SOC (analytici, operátoři, IT podpora, forenzní analytici, vyšetřovatelé).
49	Rozhraní	Možnost napojení na ActiveDirectory/LDAP pro autentizaci uživatelů systému.
50	Rozhraní	Jednotné uživatelské rozhraní pro veškerou analytiku, vyšetřování a reakci.
51	Rozhraní	Systém musí podporovat integraci s: - Komponenty pro detekci APT útoků na koncových zařízeních (EDR), způsobem plné integrace v řešení Extended Detection and Response (XDR).
52	Ostatní	Systém je platforma pro forenzní analytiku, detekci, vyšetřování a řízení reakcí na zaznamenané kybernetické události.
53	Ostatní	Systém musí být po hardware stránce dimenzován tak, že dodaný hardware bude umožňovat zpracování síťového provozu až do velikosti 10 Gbps.
54	Ostatní	Celková požadovaná retence všech historických dat o chování sítě v délce 30 dnů.
55	Ostatní	Metadata relevantní k detekovaným bezpečnostním událostem musí řešení uložit po dobu 12 měsíců.
56	Ostatní	Systém musí podporovat práci v hierarchickém režimu (včetně selektivní správy práv k informacím) pro případné budoucí zapojení podřízených organizací do bezpečnostního dohledu. Požadavek zahrnuje jednotné rozhraní pro vyšetřování, konfiguraci bezpečnostní politiky a správu řešení u všech podřízených organizací, vlastní rozhraní pro správu v každé

		podřízené organizaci a datová úložiště v každé podřízené organizaci.
57	Ostatní	Generování reportů dle předpřipravených šablon.
58	Ostatní	Tvorba a generování zákaznicky definovaných reportů.
59	Ostatní	Možnost nastavení automatického generování a odesílání reportů na emailové adresy.
60	Ostatní	Systém monitoruje svůj vnitřní chod a drží historické informace o událostech týkající se vlastního chodu a problémů.
61	Ostatní	Podpora instalace jednotlivých komponent řešení do virtuálního prostředí (VMware).
62	Ostatní	Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem sítě.
63	Ostatní	Podpora monitorování provozu na rozhraních Ethernet s rychlostmi 100Mbps, 1Gbps, 10Gbps a 25Gbps.
64	Ostatní	Obsahuje službu průběžné aktualizace signatur/definic chování a aktualizace pravidel sandboxu z komerčního zdroje.
65	Ostatní	Všechny komponenty řešení je možné provozovat v prostředí SŽ.

2.3.4.2 Požadavky na Endpoint Detection and Response

Id	Oblast EDR	Požadovaná funkcionalita systému
1	Detekce	Systém bezpečnostního monitorování koncových zařízení (stanic a serverů) s funkcionalitou EDR.
2	Detekce	Pokročilá detekce hrozeb: - detekce škodlivého kódu jeho rozpoznáním podle vzorů pro obsah, - detekce škodlivého kódu pomocí pravidel popisující chování, - detekce projevů činnosti útočníka na koncovém bodě, - analýza běžících procesů na stanici a jejich ohodnocení z hlediska činností, které provádějí nebo by mohly provádět.

3	Detekce	Systém bude kontinuálně zaznamenávat činnosti na koncových bodech v podobě metadat v těchto oblastech: - spuštění a ukončení procesů, - souborové manipulace, - manipulace s registry, - síťových spojení včetně URL pro http spojení, - DNS překladů, - manipulace s USB médii a přenosy souborů na ně, - Windows události (Windows Events).
4	Detekce	Systém bude možné napojit na vlastní nebo otevřené zdroje informací o hrozbách ve formátech JSON, CSV a STIX.
5	Detekce	Systém bude umožňovat import popisu IOC ve formátu OpenIOC a YARA.
6	Detekce	Systém musí klasifikovat události podle MITRE ATT&CK frameworku uvedením odpovídající techniky a/nebo taktiky útočníka.
7	Detekce	Vlastní pravidla lze definovat tak, aby také používala kategorie MITRE ATT&CK frameworku.
8	Detekce	Systém musí rozpoznat zranitelnosti nainstalovaného software na koncových bodech.
9	Vyšetřování	Systém umožní zhodnocení hrozby integrací na službu Virus Total nebo obdobnou službu.
10	Vyšetřování	Události budou zaznamenávány do centrálního úložiště v reálném čase a budou zpětně dostupné s časovou retencí požadovanou v technické specifikaci SŽ.
11	Vyšetřování	Systém musí být schopen nalézt soubor na disku koncového bodu dle: - obsahu, - hashe, - názvu, - velikosti, - koncovky, - času vytvoření/modifikace, - kombinace výše uvedeného.
12	Vyšetřování	Systém bude umožňovat vyhledávání souboru i pro smazané soubory.

13	Vyšetřování	Systém bude umožňovat vyhledávání souboru na souborovém systému, logickém i fyzickém disku v jejich využité (obsazené/alokované) i nevyužité části.
14	Vyšetřování	Systém bude pro běžící procesy schopen zaznamenat: - otevřené sokety, - souborové manipulace, - informace o DLL, které byly dynamicky přilinkovány včetně informace, zda byly injektovány, - obsazený virtuální adresní prostor, - identitu, pod kterou byl proces spuštěn.
15	Vyšetřování	Systém musí být schopen na vyžádání – nebo jako součást automatické reakce – získat informace o okamžitém stavu koncového bodu minimálně v oblastech: - Přihlášení uživatelé, - Vystavená síťová spojení, - Běžící procesy, - Seznam zavedených lokálních správců, - Seznam nainstalovaného software, - Seznam nainstalovaných důvěryhodných certifikátů, - Čas od spuštění počítače, - Stav antiviru, - Stav firewallu, - Seznam do paměti nahraných ovladačů, - Seznam klíčů a hodnot autorun v registrech, - Výpis obsahu DNS a APR vyrovnávacích pamětí, - HW inventář, - Obsah směrovací tabulky, - Seznam aktivních síťových rozhraní.
16	Vyšetřování	Systém bude umožňovat vyhledávání v metadatech dle libovolného parametru události (například jméno procesu, jméno rodiče, PID, hash, jméno souboru, jméno klíče v registrech, IP adresa serveru, URL spojení).

17	Vyšetřování	V případě potřeby musí být systém schopný spustit rozšířené úlohy zjišťující stav koncového bodu v oblasti: - získání historie navštívených stránek webového prohlížeče, - získání záznamu síťového provozu koncového bodu, - získání obrazu logického disku nebo fyzického disku, - získání obrazu paměti.
18	Vyšetřování	Systém musí být schopný zobrazit činnosti určitého procesu ve vztahu k: - souborovým manipulacím, - manipulacím s registry, - síťovým spojením, - spuštěným podprocesům, - to vše graficky na časové ose.
19	Vyšetřování	Systém musí umožnit přístup ke koncovému bodu pomocí sezení v reálném čase (konzolový přístup) pro účely vyšetřování a reakce.
20	Reakce	Systém umožní provedení akce na koncovém bodě nebo bodech odesláním úlohy k provedení a také interakcí s koncovým bodem v reálném čase.
21	Reakce	Automatizace reakce na incidenty automatickým nebo polo-automatickým spouštěním akcí (nachystaných výrobcem i uživatelem definovaných) na koncových bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.
22	Reakce	Ochrana koncového bodu zabráněním spuštění procesu dle hash nebo výrazu YARA.
23	Reakce	Systémová správa podporovaná na koncovém bodu prostřednictvím nástroje EDR: - správa uživatelů (přidání, odebrání, povolení, zablokování, - instalace a odinstalace aplikací, - změna nastavení operačního systému (například zapnutí firewallu a antivirového systému).
24	Reakce	Forenzní analýza: - vzdáleně – získáním obrazu paměti určitého procesu, - vzdáleně – získáním obrazu celé paměti, - vzdáleně – získáním obrazu disku.

25	Reakce	Systém musí umožnit na stanici: - Smazat soubor, - Ukončit proces, - Síťová izolace koncového bodu (při zachování komunikace systému s EDR řešením), - Modifikace/mazání obsahu registrů, - Instalace a odinstalace aplikací a záplat, - Odhlášení uživatele, - Zapnutí a vypnutí firewallu, - Restartování, vypnutí a hibernace koncového bodu.
26	Reakce	Systém musí být schopen automatického spuštění vybrané akce jako automatické odpovědi na určitý alert.
27	Reakce	Schopnost agenta systému provádět více akcí současně.
28	Reakce	Systém musí umožnit zobrazení běžících procesů na koncovém bodě v reálném čase a základní manipulaci s nimi – například jejich ukončení a získání obrazu paměti procesu.
29	Reakce	Systém musí umožnit zobrazení vzdáleného souborového systému koncového bodu a základní manipulace se soubory – například získání souboru, smazání souboru.
30	Reakce	Automatizace vybraných reakcí na incidenty (dle definovaných a schválených scriptů).
31	Reakce	Automatickým spouštěním akcí (nachystaných i uživatelem definovaných) na koncových bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.
32	Rozhraní	Dokumentované standardizované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní.
33	Rozhraní	Předpřipravené integrační vazby na aplikace typu SIEM.
34	Rozhraní	Systém musí podporovat integraci s: - Komponenty pro detekci APT útoků na síťovém provozu (NDR), způsobem plné integrace v řešení Extended Detection and Response (XDR).
35	Rozhraní	Jednotné uživatelské rozhraní pro analytiku, vyšetřování a reakci společnou pro prostředí sítě i koncových bodů.
36	Rozhraní	Alerty generované systémem musí být zobrazovány v centrální konzoli řešení XDR.

37	Rozhraní	Systém disponuje jednotným rozhraním pro správu, detekci, vyšetřování a reakci, které je součástí poptávaného řešení Extended Detection and Response.
38	Ostatní	Systém bude napojen na zdroj aktualizovaných informací o hrozbách (threat-intelligence) a bude z toho zdroje provádět pravidelně aktualizace.
39	Ostatní	Systém musí podporovat koncové body s operačními systémy: - Windows 7 a výše, - Windows Server 2008 R2 a výše, - Linux CentOS 6 a výše, - RedHat Enterprise Linux 6 a výše, - macOS 10.11 a výše.
40	Ostatní	Na koncových stanicích musí agentská část využívat zanedbatelnou část zdrojů – agent by neměl překročit po většinu času jednotky (max. 4%) využití CPU.
41	Ostatní	Agent systému musí být odolný proti odinstalování a pokusům jej zastavit nebo poškodit.
42	Ostatní	Odinstalace agentů musí vyžadovat zvláštní autentizaci (heslo pro odinstalaci).
43	Ostatní	Systém musí být schopný zaznamenávat metadata o chování koncových bodů, alerty a výsledky úloh i pro koncové body, které jsou dočasně mimo síť, jejich uchováním na koncovém bodě až do jejich odeslání do systému alespoň po dobu 5 dní.

2.3.5 Požadavky na specifikaci virtualizačních prostředků SŽ

V souvislosti se schválenou strategií IS/ICT SŽ, konkrétně cílem zajištění dlouhodobého koncepčního a efektivního rozvoje IS/ICT, požaduje SŽ využití možností jeho hardwarové a virtualizační platformy pro jednotlivé komponenty poptávaného řešení.

Pro veškeré prostředky, které je možné provozovat v platformě SŽ, vyplní dodavatel specifikaci technických požadavků na platformu SŽ, a to do připraveného listu „Specifikace HW požadavků" v XDR dotazníku, který je nedílnou součástí zadávací dokumentace (Příloha č. 19).

SŽ limituje celkové požadavky na výpočetní výkon a kapacitu, který je připravena pro účely projektu nabídnout na:

Parametr výkonu a kapacity	Maximální dostupná hodnota

Počet vCPU	1240
Kapacita RAM	3600 GB
Kapacita disků	99000 GB

2.3.6 Dodávka hardwarových a softwarových prostředků

Výjimkou, kdy není nutné využití platformy SŽ, jsou samozřejmě komponenty řešení, které virtualizaci neumožňují. V takovém případě uvede dodavatel veškeré náklady na hardware, který je součástí dodávaného řešení a nebude provozován v platformě SŽ, do své cenové kalkulace.

Pokud bude součástí nabízeného řešení také dodávka technických a programových prostředků, bude dodavatel povinen respektovat následující omezení:

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**") Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: *„Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

- *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
- *ZTE Corporation, Šen-čen, Čínská lidová republika".*

Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost Metodiku k varování ze dne 17. prosince 2018 (dále jen „**metodika**"), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou provedla SŽ analýzu rizik související s předmětnou veřejnou zakázkou na služby, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to SŽ identifikovala rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

SŽ tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

2.4 Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností SŽ uvádí, že následující oblast **není** předmětem plnění této veřejné zakázky:

- Výběr, dodávka a implementace síťových aktivních prvků nezbytných pro zajištění monitoringu síťového provozu v lokalitách, kde není aktuálně k dispozici dostatečný zdroj zrcadleného síťového provozu.
- Výběr, dodávka a implementace dodatečných nástrojů pro inspekci šifrovaného síťového provozu.
- Výběr, dodávka a implementace nástroje pro distribuci instalačního balíčku řešení EDR na koncová zařízení SŽ.

3 Současný stav a popis prostředí

Současný stav ICT prostředí SŽ je popsán v přiložených dokumentech:

- Analýza prostředí – architektura (Příloha č. 2 zadávací dokumentace)
- Analýza prostředí – sítě (Příloha č. 3 zadávací dokumentace)
- Platforma 2.0 - souhrn podporovaných infrastrukturních služeb, technologií a architektonických principů, která definuje základní rámec pro návrh řešení ICT (Příloha č. 4 zadávací dokumentace)

4 Požadavky na plnění

SŽ očekává dodávku komplexního řešení, která bude sestávat z jednorázových projektových činností, dodávky nástroje se souvisejícími technickými komponenty a průběžných služeb dodavatele řešení.

4.1 Jednorázové projektové činnosti

Jednorázové projektové činnosti jsou nedílnou součástí dodávaného řešení, jsou zahrnuty mezi akceptační milníky a je k nim vázána etapizace dodávky a fakturace.

4.1.1 Před-implementační analýza

1	**Před-implementační analýza**
Popis	Před-implementační analýza popisuje způsob a podmínky nasazení technologie Extended Detection and Response do prostředí SŽ. Dokument musí popisovat charakteristiku dodávaného technického řešení, popis jednotlivých jeho komponent, navrhovaný způsob zapojení do prostředí SŽ a samozřejmě způsob integrace na technologie využívané pracovištěm Security Operations Center. Dokument musí mít charakter detailní technické specifikace pro všechny uvažované implementační postupy, na jejichž předběžném schválení závisí umožnění provádět technické zásahy do prostředí SŽ.

Výstupy	Výstupem tohoto kroku bude dokument obsahující alespoň:
	• Popis dodávaného technického řešení a jeho komponent
	• Návrh architektury dodávaného řešení v prostředí SŽ
	• Detailní popis implementačních kroků
	• Detailní technická specifikace
	  ○ Umístění technologií
	  ○ Napájení
	  ○ Síťové segmenty pro správu technologie
	  ○ IP adresace
	  ○ HW požadavky na virtualizační platformu SŽ
	  ○ Požadavky na síťové prostupy
	  ○ Požadavky na přístup do internetu
	  ○ Požadavky na vzdálený přístup pro správu technologie
	  ○ Požadavky na systémový monitoring
	• Postup napojení řešení na technologie pracoviště SOC
	  ○ Log management / SIEM
	• Požadované součinnosti na SŽ

	• Návrh akceptačních testů • Katalog projektových rizik a návrh způsobu jejich ošetření • Specifikace kroků, součinností dodavatele a jejich rozsah v MD, při ukončení projektu (exit plán), které budou součástí poskytované služby • Detailní harmonogram implementace řešení

4.1.2 Instalace a konfigurace řešení

2	**Instalace a konfigurace řešení**
Popis	V této části projektu dojde k dodání, instalaci a konfiguraci všech komponent technického řešení Extended Detection and Response, které naplní požadavky předmětu veřejné zakázky a naplní specifika projektu uvedená v dokumentu před-implementační analýza.
Výstupy	Výstupem tohoto kroku bude funkční technické řešení Extended Detection and Response, které bude: • Obsahovat všechny potřebné licence, předplatné a technické podpory výrobce. • Dodáno s nezbytným hardwarem pro komponenty, které není vhodné provozovat ve virtuálním prostředí SŽ. • Nasazeno na všech požadovaných lokalitách. • V souladu se schválenou architekturou. • Zcela funkční pro výkon funkce Extended Detection and Response, tak jak SŽ požaduje v této Technické specifikaci. • Napojeno na systémový monitoring SŽ (výše specifikovaný Zabbix). • Schopno vyhovět definovaným akceptačním testům v rozsahu požadovaném SŽ.

4.1.3 Optimalizace bezpečnostní / detekční politiky řešení

3	**Optimalizace bezpečnostní / detekční politiky řešení**
Popis	V této části projektu bude dodavatelem provedeno vyhodnocení účinnosti nasazeného řešení Extended Detection and Response, upravena bezpečnostní / detekční politika a zdokumentovány všechny provedené konfigurační úpravy, které vedou k vyšší efektivitě detekce pro analytický tým SOC SŽ.
Výstupy	Výstupem tohoto kroku bude funkční technické řešení Extended Detection and Response, které bude mít upravenu bezpečnostní / detekční politiku tak, že bude minimalizován objem falešných detekcí, které by musel analytický tým SOC zpracovávat. SŽ požaduje provedení alespoň následujících činností: • Zohlednění reálných dostupných IP adresací SŽ v detekčních politikách. • Upřesnění konkrétních druhů validních aktiv SŽ zaznamenaných v komunikacích, které jsou důležité pro fungování detekčních pravidel (DNS, SMTP, WEB, NTP, PROXY, MS AD).

	• Aplikace výjimek, které doporučí SŽ. Všechny upravené konfigurace budou zdokumentovány a předány jako výstup této části projektu.

4.1.4 Napojení na platformu Log management / SIEM

4	**Napojení na platformu Log management / SIEM**
Popis	V této části projektu bude dodavatelem provedeno napojení technického řešení Extended Detection and Response na systém pro ukládání a zpracování logů (Log management) a systém SIEM, pro detekci bezpečnostní událostí spojených s platformou XDR, nebo událostmi, které řešení XDR vygeneruje.

Výstupy	Výstupem tohoto kroku bude návrh a dokumentace vhodných bezpečnostních scénářů pro platformu SIEM (use-cases), tedy návrh situací a kombinace stavů, které je nad prostředím XDR vhodné sledovat. Jedná se zejména o tyto situace:
	• Nestandardní pokusy o přístup k prostředí XDR.
	  ○ do systémového prostředí
	  ○ do aplikačních rozhraní WebUI
	  ○ do aplikačních rozhraní API
	• Pokus o manipulaci s daty uloženými v prostředí XDR.
	• Změna systémového času, která může znamenat narušení schopnosti detekovat kybernetické bezpečnostní události.
	Výstupem tohoto kroku bude také funkční technické řešení Extended Detection and Response, které bude:
	• Napojeno na technologii Log management.
	  ○ auditní logy technologie XDR
	  ○ systémové logy technologie XDR a souvisejících operačních systémů
	  ○ bezpečnostní logy technologie XDR a souvisejících operačních systémů
	  ○ všechny logy budou zdokumentované pro účely jejich zpracování v technologii Log management SŽ
	• Napojeno na technologii Security Information and Event Management / SIEM).

4.1.5 Školení

5	**Školení**
Popis	V této části projektu bude dodavatelem provedeno zaškolení technického servisního týmu SŽ a týmu Security Operations Center SŽ. Cílem je přenesení znalostí o správě dodaných nástrojů a předání rutinní správy na tým SŽ. Druhé specifické školení by se mělo hlouběji zaměřit na školení práce s XDR řešením, jehož odběratelem bude pracoviště SOC SŽ.

Výstupy	Výstupem tohoto kroku bude realizované školení se zaměřením na využívání a správu technického řešení Extended Detection and Response: • Prezenční školení servisního týmu SŽ složeného z minimálně 8 osob, které bude mít časovou dotaci alespoň 3 MD. Toto školení bude zaměřeno zejména na: o komponenty systému o konfigurační parametry komponent o ladění výkonnostních a kapacitních parametrů řešení o troubleshooting o update a upgrade. • Prezenční školení týmu SOC SŽ v prostorách výrobce zakončené certifikací účastníků. SŽ nominuje 4 pracovníky a bude požadovat naplnění časové dotace alespoň 3 MD. Toto školení bude zaměřeno zejména na: o užívání nástroje XDR o tvorba a úprava detekčních pravidel o vyšetřování a analýza událostí o aktivní vyhledávání kybernetických hrozeb.

4.2 Průběžné služby dodavatele řešení

4.2.1 Technická podpora servisního týmu SŽ

	Technická podpora servisního týmu SŽ
Popis	Technická podpora bude řízena dle parametrů uvedených ve zvláštních obchodních podmínkách SŽ, konkrétně ustanovením kapitoly „12. SERVISNÍ MODELY“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“. SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve zvláštních obchodních podmínkách SŽ, konkrétně ustanovením kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“.
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ a definovaných v servisní smlouvě s dodavatelem.

4.2.2 Údržba řešení

	Údržba řešení
Popis	Dodavatel zajistí pravidelnou údržbu všech komponent dodaného řešení, a to včetně bezpečnostní údržby. Cílem je, aby byl zajištěn provoz řešení v aktuálních verzích produktu, které budou považovány za stabilní a bezpečné. Dodavatel zajistí aplikaci výrobcem vydávaných opravných balíčků, nových funkcionalit a bezpečnostních záplat.

	• Aktivní sledování a využívání nových postupů v oblasti zabezpečení systémů a komunikací • Průběžné aplikování bezpečnostních oprav od výrobců • Sběr podkladů pro aktualizaci dokumentace / evidence aktiv SŽ • Pravidelná profylaxe.
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ a definovaných v servisní smlouvě s dodavatelem.

4.3 Konzultace a rozvojové aktivity

	Konzultace a rozvojové aktivity
Popis	Dodavatel poskytne SŽ služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 50 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ. Jedná se o rozvojové aktivity, které budou souviset především ve změnami v prostředí SŽ, které mohou mít dopad na provoz řešení NDR.
Výstupy	Výstupem tohoto bude poskytnutí služby konzultace na vyžádání podle potřeb SŽ.

5 Fáze plnění a akceptační milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být SŽ separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. SŽ akceptuje výstupy dané Fáze, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentací této veřejné zakázky. V opačném případě je dodavatel povinen napravit nedostatky dodávky.

Fáze	**Popis**	**Kapitola obsahující požadavky**
Fáze 1	Jednorázové projektové činnosti: - Před-implementační analýza - Instalace a konfigurace řešení	4.1.1 4.1.2
Fáze 2	Jednorázové projektové činnosti: - Optimalizace bezpečnostní / detekční politiky řešení - Napojení na platformu Log management / SIEM	4.1.3 4.1.4
Fáze 3	Jednorázové projektové činnosti: - Školení	4.1.5
Fáze 4	Průběžné služby dodavatele řešení: - Technická podpora servisního týmu SŽ - Údržba řešení	4.2.1 4.2.2
Fáze 5	Konzultace a rozvojové aktivity	4.3