Příloha č. 2 Výzvy k podání nabídky

**Bližší specifikace**

Pro zjištění stavu infrastruktury (resp. její části) je třeba prostřednictvím dlouhodobého auditu síťového provozu identifikovat aktiva v rozsahu infrastruktury Správy železnic, státní organizace, resp. jejich hlavní části, ověřit stav infrastruktury organizace a doporučit opatření pro zvýšení bezpečnosti, a to především v těchto oblastech:

* Zjištění a detekce použitých protokolů, služeb a zařízení na úrovni NonIP (OT/ICS/SCADA, ethernet, apod.) a IP (protokoly na IP vrstvě, především OT/ICS/SCADA a protokoly na IPv4 a IPv6) používaných ve vnitřním prostředí (technologické a IT sítě).
* Zjištění a ověření komunikačních matic a komunikačních vektorů používaných ve vnitřním prostředí (technologické a IT sítě).
* Detekce cílených a neznámých hrozeb pomocí pokročilé analýzy chování síťové komunikace.
* Detekce výskytu známého malware, virů, zranitelností a dalších známých útoků a hrozeb ve vnitřním prostředí (technologické a IT sítě) včetně využití znalostních bázi komerčních zdrojů Threat Intelligence a jejich korelace.
* Ověření souladu s vybranými firemními politikami vč. GDPR a obecnými bezpečnostními zásadami.
* Detekce anomálií a nedostatků ve výkonnosti sítě a aplikací.
* Detailní viditelnost do síťového provozu – ověření přenášených aplikačních dat na kritických systémech především na úrovni OT/ICS/SCADA L2 a L3 ISO/OSI modelu a zobrazení komunikačních map pro jednotlivé zařízení, protokoly, služby a síťové segmenty.

Službou bude po dobu 30 dní monitorován zrcadlený provoz v určených částech sítí (samostatných geografických lokalitách) a následně bude vypracována technická zpráva (dokumentace), popisující identifikovaná aktiva v rozsahu:

* Přehled identifikovaných aktiv na úrovni zařízení, systémy, sítě, komunikační jednotky, segment.
* Přehled detekovaných typů provozu v OT/ICS/SCADA a IT sítích na úrovni L2 – L7 ISO/OSI modelu komunikace včetně jejích četnosti a objemu.
* Komunikační mapy u identifikovaných aktiv na úrovni IP to IP (device to device u OT/ICS/SCADA), IP to Subnet, Subnet to Subnet.
* Klasifikace identifikovaných typů provozu dle určení pravděpodobnostních charakteristik odvozených z užitých typů protokolů, event. aplikačních dat a indikování potenciální kritičnosti daných typů provozu.
* Návrh klasifikace identifikovaných aktiv a provozů pro účely Analýzy rizik.

a nejzávažnější detekované bezpečnostní a provozní incidenty v Auditních reportech pro jednotlivé lokality:

* Detekce neznámých útoků a hrozeb
* Detekce známých útoků a hrozeb
* Ověření s bezpečnostními zásadami a politikami, nebo obecnými „best practices“.
* Výkonnost sítě a aplikací
* Vizualizace mapy síťové komunikace u kritických systémů a identifikovaných nedostatků.

Auditní reporty budou zpracovány bezpečnostním analytikem dodavatele, který s maximální odborností analyzuje jednotlivé detailní informace popisující každou detekovanou událost ve formátu:

* Zjištění - co bylo detekováno,
* Hrozby a možné dopady - jaké mohou být dopady pro infrastrukturu nebo systémy organizace,
* Doporučení - jak lze působení dané hrozby minimalizovat a jak mu do budoucna předcházet. Informace budou relevantní pro dané zařízení, segment sítě, nebo organizační jednotku.

Požadované dílčí výstupy vypracované zprávy technické dokumentace pro analýzu rizik:

* Identifikace konkrétní instance aktiv a jejich rozsahu ve zpřístupněných sítích.
* Identifikace rozsahu, četnosti, objemů a typů provozu konkrétních instancí aktiv ve zpřístupněných sítích.
* Identifikace reálné úrovně zabezpečení sítě a provozní spolehlivosti.
* Návrh a doporučení klasifikace identifikovaných aktiv a jejich typových provozů pro účely Analýzy rizik dle zákona č. 181/2014, Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
* Popis stavu sítí s jednotkami relevantních událostí bez falešně pozitivních detekcí. Report bude obsahovat URL odkazy na události pro zpětné prohlédnutí v analytické technologii (dostupné alespoň 6 měsíců v prostředí zadavatele), včetně seznamu zařízení, event. uživatelů, podsítí, kterých se identifikovaný nedostatek týká.
* Popis identifikovaných bezpečnostních, provozních nebo výkonnostních incidentů vč. detailního popisu incidentu, hrozby a doporučení pro nápravu.

Manažerský přehled

Průběžné analytické výstupy s bezpečnostním dopadem budou okamžitě reportovány zadavateli včetně URL odkazu pro jeho vizualizaci v monitorovací technologii.

Data zpracovávaná a ukládaná monitorovací technologií musí být uživateli dostupná 6 měsíců po ukončení analýzy v původním formátu analytických nástrojů, včetně aplikací pro jejich prohlížení a exporty. Zhotovitel poskytne nasbíraná data a aplikace pro jejich prohlížení včetně všech běhových prerekvizit ve formátu vhodném pro virtualizační platformu VMWare.

Vyhodnocení bude probíhat paralelně s užitím vlastních HW appliance dodavatele v 6 až 10 lokalitách, dle dispozic zadavatele, přičemž v případě výstupu analýzy indikujícího možný bezpečnostní dopad může být paralelní vyhodnocení zadáno požadavkem zadavatele celkem až pro 20 lokalit současně. Analytické jednotky musí být v jednotlivých lokalitách schopny odbavit vstupy současným zapojením 1GE a 10GE síťových rozhraní.

**V případě potřeby je Zadavatel ochoten poskytnout součinnost v následujícím rozsahu:**

* Určení kontaktní osoby pro zajištění obousměrné komunikace a sdílení požadavků.
* Předání informací (písemné/ústní) o topologii a architektuře sítě.
* Předání informací (písemné/ústní) o seznamu používaných provozních aplikací a jejich určení.
* Určení přípojných bodů pro monitoring a zajištění konfigurace zdroje dat na příslušných síťových prvcích včetně zajištění místa v RACKu a zdroje energie.
* Zajištění síťové konektivity pro management porty dohledových prvků/sensorů.
* Zajištění přístupů přes VPN k nasazeným dohledovým prvkům/sensorů.
* Zajištění datových zdrojů pro dlouhodobé uložení naměřených dat.
* V rámci konzultací:

Ověření identifikovaných aktiv a vysvětlení procesů vztahujících se k daným informačním aktivům