|  |  |
| --- | --- |
|  | **Příloha č. 1 – Technické požadavky Zadavatele** |
| Název veřejné zakázky | **NÁKUP ŘEŠENÍ SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE A JEHO IMPLEMENTACE A PODPORA IV** |
| Ev. číslo veřejné zakázky | VZ2025012 |
| *(dále to celé jen „Veřejná zakázka“)* | |

Tato příloha zadávací dokumentace představuje seznam technických požadavků Zadavatele stanovených jako požadované minimum na Řešení SOAR. Dodavatel vyplní minimálně položky, které jsou označeny k vyplnění „[DOPLNÍ DODAVATEL]“.

**Řešení musí být provozováno on-prem na virtualizovaných prostředcích Zadavatele. Rozsah požadovaných virtualizačních prostředků uvede uchazeč v tomto dokumentu v části Požadované virtualizované prostředky. V případě požadavku na HW prostředky musí být tyto prostředky nedílnou součástí ceny.**

**Požadavky**

| **ID** | **Popis požadavku Zadavatele** | **Splnění požadavku**  *„ANO“ nebo „NE“* | **Podrobný popis splnění** |
| --- | --- | --- | --- |
| **Řešení SOAR musí obsahovat tyto funkce správy případů** | | | |
| FCE1-1 | Funkce správy případů musí spojovat deduplikovaná data o hrozbách a příjem dat z informačních zdrojů (Feeds), možnosti obohacení z platforem pro Threat intelligence (TIP). | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-2 | Korelace souvisejících případů na základě sdílených IOC. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-3 | Řešení SOAR musí umožňovat analytikům definovat šablony, které jsou základem případů; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-4 | SOAR musí umožňovat do šablon zahrnout manuální i automatizované úlohy. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-5 | Úkoly případu musí být možno dynamicky přiřadit konkrétním uživatelům a odborníkům na danou problematiku. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-6 | SOAR musí zahrnovat realizaci a podporu principu neodmítnutelnosti včetně časové osy událostí nebo časové osy případu. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-7 | Analytici musí mít možnost zaznamenávat poznámky k případu nebo vyšetřování. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-8 | Obohacení případů musí být možno uložit pomocí atributů | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-9 | Musí být realizována prioritizace Případů na základě objektivního bodového hodnocení IOC vázaného na dané upozornění nebo případ. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE1-10 | Případy musí být možno přímo přiřadit k položkám Threat intelligence: rodiny malwaru, skupiny aktérů hrozeb, incidenty, atd. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí disponovat dokumentovaným API pro automatizaci činností napříč bezpečnostními funkcemi** | | | |
| API-1 | SOAR musí obsahovat návrháře playbooků a interaktivní režim pro tyto návrháře; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| API-2 | SOAR musí obsahovat předpřipravené integrační aplikace s IBM QRadarem  a MS Sentinelem. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| API-3 | SOAR musí umožňovat vytvářet vlastní integrace prostřednictvím klienta HTTPS Playbook a spouštěčů Web Hook. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| API-4 | SOAR musí podporovat vývoj vlastních aplikací v jazyce Python | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| API-5 | Spouštěče SOAR Playbook musí být možno založit na nově získaných informacích, které odpovídají předem definovaným kritériím. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **Ukazatele, které jsou přiřazeny k případům, musí být možno ukládat do úložiště zpravodajských informací;**  **tato možnost musí být plně integrována do řešení SOAR, ale lze ji také integrovat nebo přesunout do MISP** | | | |
| UK-1 | Datový model musí být v souladu s Diamond model pro analýzu narušení; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| UK-2 | Musí být podporovány i další modely analýzy narušení, chování. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| UK-3 | Datový model SOAR jmusí být rozšiřitelný pomocí vlastních typů indikátorů, značek a atributů; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí dokázat přijímat, deduplikovat, normalizovat a obohacovat data Open Source a Premium Feed Intelligence v rámci integrované platformy Threat intelligence (TIP)** | | | |
| FCE2-1 | SOAR musí podporovat API Ingest; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE2-2 | * Musí mít schopnost přijímat kanály Intelligence X | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE2-3 | SOAR musí podporovat STIX/TAXII ingest; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE2-4 | SOAR musí podporovat příjem na základě e-mailu. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE2-5 | SOAR musí podporovat přijímání událostí MISP | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE2-6 | Musí podporovat rozšíření prohlížeče pro příjem dat z blogů a webových stránek. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí poskytovat open source a proprietární kanály jako hotový produkt** | | | |
| APS-1 | Mezi kanály s otevřeným zdrojovým kódem musí být vyhrazený kanál pro renomované oborové blogy kybernetické bezpečnosti, jako jsou Microsoft Security, Bleeping Computer, Cisco Talos a další | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| APS-2 | Vlastní informace poskytované nástrojem SOAR. Musí rovněž poskytovat informace specifické pro odvětví státní správy. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí mít přizpůsobitelné možnosti ovládacího panelu** | | | |
| DEV-1 | Obsah panelu je dynamicky řízen vlastním dotazovacím jazykem SOAR; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| DEV-2 | Možnost sledování metrik, jako je střední doba detekce (MTTD) a střední doba odezvy (MTTR). | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| DEV-3 | Obsah panelu musí obsahovat předdefinované widgety. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí:** | | | |
| OSS-1 | SOAR musí šířit indikátory do cílových technologických kontrol včetně produktů SIEM a EDR. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-2 | SOAR musí přijímat výstrahy a incidenty z platforem SIEM. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-3 | SOAR musí přijímat pozorovatelná data z kontrol technologií; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-4 | SOAR si musí zachovat schopnost přijímat nové indikátory z jakéhokoli zdroje nebo datového bodu a provádět ad-hoc dotazy napříč řešeními SIEM (AQL pro QRadar a KQL pro Sentinel) | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-5 | SOAR musí podporovat obousměrnou integraci do MISP | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-6 | SOAR musí poskytovat integrované obohacení grafického uživatelského rozhraní a umožňuje týmům prošetřovat IOC a incidenty.  Mezi partnery pro obohacení patří: VirusTotal a další | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| OSS-7 | SOAR musí poskytovat možnost obohacení o vlastní kontextové nástroje, jako jsou například DomainTools, Shodan, HaveIBeenPawned a další | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí podpořit kontextualizaci zranitelnosti a stanovení priorit** | | | |
| SEC-1 | SOAR musí podporovat agregaci a ukládání objektů zranitelnosti v rámci nativního datového modelu; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| SEC-2 | SOAR musí agregovat data CVE z důvěryhodných úložišť, jako jsou Vulnerability Tooling, National Vulnerability Database (NVD) nebo Cybersecurity and Infrastructure Security Agency (CISA); | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| SEC-3 | SOAR musí umět obohacovat objekty zranitelnosti v SOAR na základě zdrojů obohacení, jako je například Twitter; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| SEC-4 | SOAR musí disponovat připravenými integracemi se všemi hlavními nástroji pro správu zranitelností, jako jsou Rapid7, Tenable Nessus, Qualys, Defender TVM. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| SEC-5 | SOAR musí dokázat identifikovat a přiřadit známé zprávy Intel související s vytvořenou zranitelností. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí poskytovat komponentu rozšíření prohlížeče, která dokáže skenovat webové stránky a hledat na nich objekty Intel** | | | |
| BRO-1 | Rozšíření prohlížeče využívá zpracování přirozeného jazyka k identifikaci techniky MITRE z volného textu na webové stránce; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| BRO-2 | Pokud rozšíření prohlížeče identifikuje protivníka, jsou analytikovi předloženy známé aliasy (podle MITRE ATT&CK); | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR využívá vlastní analytiku k** | | | |
| ANL-1 | Identifikaci anonymizovaných globálních trendů indikátorů u zákazníků prodejců (počty falešně pozitivních výsledků, počty pozorování); | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| ANL -2 | Poskytnutí kontextové informace o povaze IOC; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| ANL -3 | Objektivnímu poskytování hodnocení hodnoty zpravodajských kanálů; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí poskytovat funkci Investigation and enrichment Graph,**  **která analytikům umožňuje zkoumat vztahy mezi vlastníky Intelligence** | | | |
| FCE3-1 | Případy jsou přímo korelovány se zpravodajskými položkami v platformě. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE3-2 | Protivníkovy aliasy lze v rámci analýzy grafu spojit do jednoho uzlu; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| FCE3-3 | Vyšetřování grafů lze ukládat a zpřístupňovat dalším zúčastněným stranám klienta. | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **SOAR musí poskytovat možnost generování zpráv** | | | |
| ZPR-1 | Reportovací engine musí podporovat dynamické generování grafů a tabulek; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| ZPR-2 | Reportovací engine musí podporovat možnost vkládání obrázků; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| ZPR-3 | Reportovací engine musí podporovat možnost zahrnout Intel Graph Investigations; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| ZPR-4 | Reportovací engine musí podporovat možnost KLIENTA přidávat volný text; | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |
| **Požadované virtualizované prostředky** | | | |
| --- | Požadované virtualizované prostředky k řádnému plnění předmětu VZ | [DOPLNÍ DODAVATEL] | [DOPLNÍ DODAVATEL] |