**Rámcový protokol pre implementáciu**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  | **Rámcový protokol pre implementáciu - nastavenie MISP a TIP - Súpis činností, ktorými dôjde k naplneniu dodania SaaS** | | | | |  |
|  | **Parciálna časť inštalácie služby** | **Podkategórie postupnosti realizovaných implementácií** | **Súpis činností pre naplnenie nasadenia kategórie inštalácie** | **Dátum a Podpis zodpovednej osoby za stranu Objednávateľa - CSIRT - ORKIB:** | **Dátum a Podpis zodpovednej osoby za stranu Dodávateľa:** |  |
|  | **Hlavné časti** | **Podkategórie** |  |  |  |  |
|  | **MISP** | MISP | * Inštalácie softvéru MISP do prostredia objednávateľa * Nastavenie zobrazenia / hlásenia pozorovaní * Doplnenie o požiadavky organizácie na zvýšenie pokrytia a detekcie |  |  |  |
|  | * Organizácia/ normalizácia inputov a feedov do MISP |  |
|  | MISP to MISP (môžu byť vykonané v časti Dodatočné) | * Nastavenie dizajnu ako sprocesovať prepojenie z neverejného do verejného |  |
|  | MISP a SIEM (môžu byť vykonané v časti Dodatočné) | * Napojenie s ohľadom na zvýšenie pokrytia a detekcie * Kontrola integrácie do SIEM * Integrácia ako nadstavba v podobe tagovania - kontent pre SIEM |  |
|  | **Integrácia TIP** | Integrácia | Pripojenie platformy spravodajstva o hrozbách |  |  |  |
|  | Integrácia | Spustenie dátového konektoru |  |
|  | Integrácia | Napojenie rozhrania API pre nahrávanie informácií o hrozbách |  |
|  | Integrácia | Integrácia a napojenie na feedy STIX/TAXII 2.1 |  |
|  | **TI Platforma** | TI Platforma | Nastavenie správy používateľov pomocou RBAC s SSO |  |  |  |
|  | TI Platforma | Nastavenie RFI na témy |  |
|  | TI Platforma | Nastavenie zdrojov hrozieb |  |
|  | TI Platforma | Nastavenie mesačných spravodajských správ a mesačných geopolitických správ / v spolupráci s Výrobcom a podľa požiadaviek VJ CSIRT |  |
|  | **Threat Intelligence** | Threat Intelligence | Nastavenie a dohľad nad možnosťou priradenia upozornenia rôznym analytikom TI |  |  |  |
|  | Threat Intelligence | Testovanie knižníc hrozieb – testovanie / nastavenie správ a analýz, ako sú (CVE, TTP, súhrny) |  |
|  | Threat Intelligence | Testovanie položiek / knižníc hrozieb – korelácia medzi položkami (TA, malvér, kampane) |  |
|  | Threat Intelligence | Testovanie, či je možné exportovať knižnicu položiek / hrozieb v rôznych formátoch (JSON, PDF atď.) |  |
|  | **Ochrana značky / Zneužitie značky** | Ochrana značky | Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |  |  |
|  | Zneužitie značky | Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |
|  | **Tretia strana** | TIP\_Tretia strana | Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |  |  |
|  | TIP\_Tretia strana | Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |
|  | **Zraniteľnosti** | TIP\_Zraniteľnosti | "Potreba obohatiť zraniteľnosti" - Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |  |  |
|  | TIP\_Zraniteľnosti | "Potreba obohatiť zraniteľnosti" - Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |
|  | TIP\_Zraniteľnosti | "Potreba obohatiť zraniteľnosti" - Nastavenie tejto predmetnej časti TIP sa uskutoční na základe checklistu od VJ CSIRT (V závislosti a pomere na kvalitu aj množstvo) |  |
|  | **Správa upozornení** | TIP\_Správa Upozornení | Kontrola (1/2) požiadaviek, ktoré sú definované pre kategóriu Správa upozornení v prílohe č.3 Špecifikácia požiadaviek pre TIP |  |  |  |
|  | TIP\_Správa Upozornení | Kontrola (2/2) požiadaviek, ktoré sú definované pre kategóriu Správa upozornení v prílohe č.3 Špecifikácia požiadaviek pre TIP |  |
|  | **Filtrovanie údajov** | TIP\_Filtrovanie Údajov | Nastavenie/revízia vyhľadávania funkcií na základe prednastavenia vlastných značiek (tags)/ tém na základe preddefinovaných požiadaviek od VJ CSIRT |  |  |  |
|  | TIP\_Filtrovanie Údajov | Nastavenie / testovanie funkcií filtrovania na základe (zdrojovej krajiny, cieľovej krajiny, obchodného sektora, prvého videnia, techniky MITRE, bežných TTP, zraniteľností, kategórie obsahu) |  |
|  | **Indikátory kompromitácie** | TIP\_IOCs | Nastavenie / testovanie schopnosti zalistovať alebo filtrovať IOC |  |  |  |
|  | TIP\_IOCs | Nastavenie Whitelistu / na základe preddefinovaných požiadaviek od CSIRT |  |
|  | **Konzoly Vyobrazenia** | TIP\_Dashboardy | Vytvorenie a nastavenie vlastných informačných panelov / dashboardov |  |  |  |
|  | TIP\_Dashboardy | Prehľad/ preskúšanie informačných panelov platformy na základe: výstrah, IOC, hrozieb, zraniteľností |  |  |  |
|  | **Dokumentácia** | TIP\_Dokumentácia | Kontrola a odovzdanie dokumentácie v EN alebo SK jazyku |  |  |  |
|  | TIP\_Dokumentácia | Kontrola komplexnej dokumentácie API / potvrdenie od CSIRT, že je možné procesne postupovať na základe predmetnej dokumentácie |  |
|  | **Dodatočné** | MISP do MISP | Synchronizácia používateľa, testovanie a ukážka, riadenie toku dát, nastavenie MISP na MISP – prepojenie z neverejného do verejného – tok IOC |  |  |  |
|  | Feeds do MISP | Možnosti, presahy, nastavenie bezplatných informačných kanálov, open source, atď. |  |