**Prehľadová tabuľka kategórií požiadaviek a funkcionalít TIP** – slovenská verzia

|  |  |  |
| --- | --- | --- |
| **Kategórie:** | **Opis požiadaviek uvedený ako minimálne požiadavky/ funkcionality:** |  |
| **Integrácie** | **Požiadavky na Integráciu:**   * Bezpečnostný stack – SIEM * Bezpečnostný stack – MISP * Integrácia a export IOC cez STIX/TAXII 2.1 * Funkcia výberu, ktoré IOC budú integrované |  |
| **TIP platforma** | **Požiadavky kategórie platformy TI:**   * Poskytne správu používateľov pomocou RBAC * MFA * Komunikácia výhradne cez HTTPS * Povoliť vytváranie upozornení prostredníctvom e-mailu alebo volaní rozhrania API * Protokol auditu, audit logu |  |
| **Threat Intel** | **Požiadavky na kategóriu knižnice hrozieb - Threat Intel:**   * Knižnica musí mať funkcie vyhľadávania a filtrovania * Poskytuje knižnicu správ o útočníkoch * Poskytuje knižnicu správ o malvéri * Poskytuje knižnicu správ o významných incidentoch * Možnosti filtrovania informácií (MITRE Matrix) * Umožňuje požiadať o RFI na rôzne témy * Monitoruje hrozby na dark webe * Mesačné spravodajské správy (globálne a lokálne, so zameraním na Slovensko a EÚ) * Mesačné geopolitické správy (globálne a lokálne so zameraním na Slovensko a EÚ) * Vlastný zdroj hrozieb |  |
| **Ochrana značky / Zneužitie značky** | **Požiadavky na kategóriu Ochrany značky a Zneužívania značky:**   * Monitoruje otvorené a uzavreté zdroje na internete * Monitoruje zmienky o našej organizácii, projektoch, značkách * Monitoruje citlivé údaje na internete (možné úniky údajov) * Monitoruje registráciu typosquat domén (a certifikátov) * Vykonáva odstránenie alebo pomoc s odstránením webových stránok (zastavenie šírenia webových stránok/domén) * Monitoruje možné hrozby pre dôležitých ľudí * Schopnosť odhaliť uniknuté prístupové kľúče * Schopnosť odhaliť uniknuté poverenia * Rozpoznať phishingové webové stránky * Monitorujte uniknuté alebo citlivé údaje na github, pastebin atď. * Monitoruje internetovú prítomnosť VIP/riadiacich pracovníkov |  |
| **Tretia strana** | **Požiadavky na kategóriu Tretej strany:**   * Posúdiť riziko dodávateľa/dodávateľa tretej strany * Funkcia upozornenia na možnú kompromitáciu dodávateľa tretej strany |  |
| **Zraniteľnosť** | **Požiadavky na kategóriu zraniteľností:**   * Schopnosť obohatiť systém o ďalšie informácie o zraniteľných miestach * Prioritizovanie slabých miest * Zdôraznenie kritických slabých miest v konkrétnych produktoch |  |
| **Správa Upozornení** | **Požiadavky na kategóriu Správa upozornení:**   * Upozornenie je dostatočne popisné na to, aby sa dalo preskúmať prideleným analytikom * Upozornenie poskytuje dostatok odporúčaných akcií na nápravu * Odporúčané akcie možno vykonať prostredníctvom platformy TI * Upozornenie je označené pomocou MITRE TTP * Alert má príslušné IOC analyzované zo zdroja * Možnosť priradiť upozornenie rôznym analytikom TI * Možnosť označiť/otagovať výstrahu vlastnými značkami/tagmi * Vytváranie poznámok a ukladanie príloh * Možnosť filtrovania výstrah a ich exportu na základe definovania * Vykonávanie hromadných akcií s upozorneniami, ako sú (whitelisting, označovanie, zmena stavu atď.) * Ukladanie filtra upozornení pre budúce použitia * Dotaz na údaje výstrahy * Vytváranie novej logiky detekcie * Upravovanie vstavanej logiky detekcie * Možnosť pridania nového privilegovania v logike detekcie * Vytváranie automatizačných pracovných postupov pre výstrahy - upozornenia * Nájdenie/preskúmanie potenciálnych hrozieb súvisiacich s organizáciou * Spustenie predvolených reportov na údaje výstrah * Spustenie vlastných reportov o údajoch výstrah Časové naplánovanie reportov na údaje výstrah |  |
| **Súhrnná knižnica hrozieb** | **Požiadavky na kategóriu Knižnice hrozieb:**   * Rôzne druhy správ a analýz, ako sú (CVE, TTP, súhrny) * Popis techník MITRE a prepojenie na súvisiace položky * Informačný kanál správ o hrozbách * Súhrn správ o hrozbách * Prehľad existujúcich položiek * Súvzťažnosť medzi položkami (TA, malvér, kampane) * Zobrazenie súvisiacej položky IOC * IOC položky je možné presunúť nadol na stránku IOC * Položku je možné exportovať v rôznych formátoch (JSON, PDF atď.) * Položku IOC je možné pridať do blocklist feedu * Položka zobrazuje súvisiace chyby zabezpečenia * Položka zobrazuje súvisiace techniky MITRE * Položka môže byť označená záložkou * Položka môže byť označená vlastnou značkou alebo menovkou * Položka obsahuje odkazy na externé zdroje |  |
| **Filtrovanie údajov** | **Požiadavky na kategóriu Filtrovania:**   * Možnosť filtrovania na základe (krajiny zdroja, cieľovej krajiny, sektora podnikania, prvého videnia, technika MITRE, bežnej TTP, chyby zabezpečenia, kategórie obsahu) * Vyhľadávanie s použitím textového reťazca alebo zástupného znaku * Pokročilé vyhľadávanie pomocou dotazu * Vyhľadávanie podľa prednastavenia vlastných tagov/tém |  |
| **Informačné kanály** | **Požiadavky na kategóriu Informačných kanálov:**   * Použitie vlastných informačných kanálov * Umožnenie pridanie servera STIX/TAXII * Umožnenie pridanie servera MISP * Možnosť podľa informačného kanála povoliť alebo zakázať hrozby * Posúdenie spoľahlivosti informačného kanála hrozieb (IOC, ak je k dispozícii jeden informačný kanál) |  |
| **Indikátory kompromitácie** | **Požiadavky na kategóriu Indikátorov kompromitácie:**   * Zoznam a filtrovanie IOC * Vyhľadávanie IOC je možné vykonať pomocou zástupných znakov * Platforma podporuje # (hashtagy) typov IOC * Tagy/vlastné tagy možno použiť na vyhľadávanie IOC * Poskytnutie privilégií - whitelisting pre IOC * Export IOC vo formáte CSV * Export IOC vo formáte STIX * Export IOC vo formáte MISP * Analýza VirusTotal okrem IOCs, samostatné predplatné virustotal nie je potrebné * Analýza IOC z (pdf, html, word) dokumentov je podporovaná a môže byť zahrnutá do zoznamu hrozieb * Podporovaná analýza IOC z e-mailov a možnosť zahrnúť ich do informačného kanála hrozieb |  |
| **Rozhranie API** (dostupné v štandardnom programovacom jazyku - python, javascript, golang) | **Požiadavky na kategóriu API:**   * Podpora API pre IOC * Podpora API pre vyhľadávanie/filtrovanie * Podpora rozhrania API pre upozornenia * Podpora API pre spracované informácie * Jednoduchá správa API tokenov * Komplexná dokumentácia pre API |  |
| **Konzoly Vyobrazenia** | **Požiadavky na Informačné panely:**   * Podpora vytvárania vlastných informačných panelov * Panel informovania o situácii - t.j. informačný panel a vyobrazenie kategórií * Základné informačné panely, výstrahy, IOC, hrozby, zraniteľné miesta |  |
| **Dokumentácia** | **Požiadavky na Dokumentáciu:**   * Dokumentácia je dostupná buď v anglickom alebo slovenskom jazyku * Dokumentácia je k dispozícii pre každú funkciu platformy * Dokumentácia sa aktualizuje spolu s novou verziou/funkciou platformy |  |
| **Dodatočné** | **Požiadavky na kategóriu Ostatné:**   * 24/7 podpora platformy |  |