Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

CSIRT.SK

Všeobecné informácie o službe

MISP AFRODITA

od **VJ CSIRT**

MISP AFRODITA

TLP:CLEAR

Verzia 2.1

Obsah

Všeobecné informácie

VJ CSIRT poskytuje vybraným orgánom verejnej moci (skr. OVM) služby tzv. „Cyber Threat Intelligence“ (skr. CTI), čo predstavuje formu kybernetického spravodajstva o aktuálnych udalostiach a hrozbách, ktoré figurujú v kybernetickom priestore. Identifikované skutočnosti v rámci služieb CTI sú daným OVM doručené v čo najkratšom čase, avšak s ohľadom na povahu identifikovanej hrozby a jej prípadného napojenia na prebiehajúce incidenty.

Výstupom služieb CTI sú v tomto prípade **indikátory kompromitácie** (skr. IoC), ktoré sú nahraté do nástroja **MISP** (Malware Information Sharing Platform). Cez tento nástroj sú predmetné IoC odoslané do externých inštancií nástroja MISP, ktoré sú nasadené v infraštruktúre daného OVM. Odoslané IoC slúžia ako informačné a preventívne dáta, ktoré majú pomôcť OVM overiť prítomnosť IoC vo vlastnej infraštruktúre.

Na uvedené účely bola preto v sieti GOVNET vytvorená inštancia nástroja MISP s názvom ***„Afrodita“,*** na ktorú sa vybrané OVM môžu pripojiť stať sa tak odberateľom služieb CTI.

Aktuálne poskytuje VJ CSIRT všetky identifikované IoC formou **PUSH**, teda „tlačením“ IoC z inštancie MISP „*Afrodita*“ do externej inštancie nástroja MISP pre daný OVM. Takto je zabezpečený prenos IoC v čo najkratšom čase, resp. hneď po nahratí IoC do inštancie MISP „*Afrodita*“. Viac informácií o prenose IoC formou PUSH je možné nájsť v oficiálnej dokumentácii nástroja MISP.

Navyše je prenos IoC podmienený protokolom **TLP** (Traffic Light Protocol) – aktuálne sú preposielané na OVM všetky IoC, ktoré sú označené ako **TLP:CLEAR** alebo **TLP:GREEN**. V špeciálnych prípadoch môže ísť o IoC s označením **TLP:AMBER**, alebo **TLP:AMBER+STRICT**.

***Poznámka**: Služby CTI poskytované VJ CSIRT sú zamerané primárne na identifikáciu a zdieľanie IoC, nie na ich odstránenie z infraštruktúry konkrétneho OVM. VJ CSIRT v tomto smere poskytuje iba odborné poradenstvo, nie technickú podporu spojenú s fyzickým odstránením prípadných IoC.*

Výhody služby Afrodita od VJ CSIRT

Konštituenti, používajúci túto službu, získavajú využívaním služby Afrodita prístup k pravidelným informáciám o indikátoroch kompromitácie z aktuálneho diania v kybernetickom priestore na pravidelnej báze. Môžu tak **overovať prítomnosť IoC** vo svojej infraštruktúre, alebo nasadiť preventívne opatrenia, aby predišli pokusom o vykonanie predmetného útoku. Navyše si konštituenti môžu dané IoC **korelovať** s inými udalosťami v inštancii MISP Afrodita, čím je možné rozšíriť kontext samotných IoC, ale aj celej udalosti. V neposlednom rade je táto služba spojená s možnosťou **ukladať**[1] si dané IoC v nástroji MISP, ktorý slúži práve na prácu s IoC a ich zdieľanie.

MISP Afrodita je pravidelne doplňovaný o nové udalosti a IoC z aktuálneho diania v kybernetickom priestore od Cyber Threat Intelligence oddelenia vo VJ CSIRT, čo zaručuje zlepšenie prehľadu a lepšiu prípravu na potenciálne hrozby u konštituentov. Inštancia MISP Afrodita poskytuje taktiež možnosti **obohacovania IoC voči Threat Intelligence platforme od Recorded Future** (ďalej len „TIP RF“).

Ako je uvedené v kapitole 2, systém zohľadňuje úrovne dôvery pomocou **TLP** a umožňuje cielené zdieľanie dát na základe definovaných pravidiel. Zapojením sa do MISP-u sa zabezpečuje súlad s vybranými právnymi predpismi, vrátane požiadaviek Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 - **NIS2** a **Zákona o kybernetickej bezpečnosti a s ním súvisiacich predpisov**.

[1] *MISP Afrodita slúži ako úložisko relevantných IoC, najmä z incidentov, alebo vlastných nálezov, nie ako úložisko všetkých IoC (vrátane false-positive), ktoré konštituent obdrží.*

Nahrávané dáta do inštancie MISP Afrodita

MISP Afrodita je plnený primárne dvoma spôsobmi zo strany VJ CSIRT:

1. IoC **z pravidelného monitoringu** kybernetického priestoru. VJ CSIRT na dennej báze preveruje aktuálne udalosti v kybernetickom priestore na Slovensku, ale aj v zahraničí. V prípade relevantných nálezov z rôznych kampaní, zraniteľností, alebo iných incidentov, sú IoC z danej udalosti pridané do internej inštancie nástroja MISP vo VJ CSIRT, prejdú procesom obohacovania o dodatočné asociované dáta a sú diseminované až po inštanciu MISP Afrodita, odkiaľ sú dostupné pre konštituentov.
2. IoC **z incidentov**. VJ CSIRT vo výnimočných prípadoch zdieľa do inštancie MISP Afrodita IoC aj z uzatvorených incidentov, ak ide o IoC, ktoré spadajú pod označenie **TLP:CLEAR**, prípadne **TLP:GREEN**. Často však ide o výber IoC, nie o kompletný zoznam z incidentu, keďže niektoré IoC samostatne spadajú pod označenie **TLP:AMBER** alebo vyššie, prípadne podliehajú GDPR.

Prístup do inštancie MISP Afrodita

Prístup do inštancie MISP Afrodita je striktne podmienený prístupom do siete Govnet. Ak týmto prístupom aktuálne nedisponujete, je potrebné kontaktovať NASES a požiadať ich o povolenie prístupu na inštanciu MISP Afrodita cez oficiálne komunikačné kanály.

Možnosti prístupu do MISP Afrodita:

- priamy prístup,
- synchronizácia vlastnej inštancie nástroja MISP.

Priamy prístup

Získanie priameho prístupu do inštancie MISP Afrodita je podmienené úvodnou registráciou do služby Afrodita. Registráciu, spolu s celým jej postupom, nájdete na stránke csirt.sk/afrodita, kde treba vykonať uvedené kroky. Jedným z krokov je doručenie služobných e-mailových adries[2] do schránky CTI tímu. Po ich doručení je danej organizácii vytvorený prístup do inštancie MISP Afrodita pre uvedené e-maily.

Prístupové údaje sú zaslané organizácii formou ZIP súboru zabezpečeného heslom, pričom tento ZIP súbor a jeho heslo sú organizácii doručené dvoma samostatnými komunikačnými kanálmi s cieľom minimalizovať riziko úniku hesla, alebo ZIP súboru s prístupmi. Ak je organizácia zapojená do služby Achilles, využijú sa pre odoslanie týchto informácií kontaktné údaje z VISKB.

Pred odoslaním prístupov na organizáciu sú v inštancii MISP Afrodita vytvorené jednotlivé kontá a sú im nastavené dočasné heslá, ktoré si používatelia pri prvom prihlásení musia zmeniť. Ak je prihlásenie úspešné a došlo k zmene dočasného hesla na nové, daný používateľ môže začať pracovať v inštancii MISP Afrodita. V prípade problémov s prihlásením je potrebné kontaktovať CTI tím.

[2]Musí sa jednať o služobné e-mailové adresy, keďže prístup do inštancie MISP Afrodita pre danú organizáciu je viazaný na oficiálnu e-mailovú doménu predmetnej organizácie.

Je potrebné pripomenúť, že na úspešný prístup k inštancii MISP Afrodita týmto spôsobom je potrebné mať pripojenie do siete Govnet. Bez splnenia tejto podmienky nie je možné získať prístup.

Synchronizácia vlastnej inštancie nástroja MISP

V prípade, že organizácia disponuje vlastnou inštanciou nástroja MISP (alebo vlastným bezpečnostným dohľadovým centrom, SOC), môže ju synchronizovať s inštanciou MISP Afrodita. Na tento proces bol vytvorený samostatný manuál, ktorý je k dispozícii pri registrácii sa do služby Afrodita. V tomto manuáli sú obsiahnuté všetky náležitosti a kroky na synchronizáciu vlastnej inštancie nástroja MISP s inštanciou MISP Afrodita. Aj v tomto prípade je však požadovaný prístup do siete Govnet.

Súčasťou manuálu však nie je návod na nasadenie samotného nástroja MISP. V takom prípade vás vieme znova odkázať na oficiálnu dokumentáciu nástroja MISP od jeho vývojárov z CIRCL.LU, kde sú opísané aj spôsoby jeho nasadenia.

Čo služba Afrodita NEponúka

Počas ponúkania služby Afrodita sme sa stretli s viacerými nesprávne interpretovanými informáciami o tom, čo všetko MISP Afrodita ponúka. Výstupy a aktivity tejto služby sú opísané v predošlých kapitolách, v tejto však uvádzame aj to, čo Afrodita aktuálne neponúka.

1. **Priame pripojenie na TIP RF**. Obohacovanie a využívanie podobných služieb TIP RF je možné iba cez inštanciu MISP Afrodita. Priamy prístup na TIP RF nie je vytváraný pre žiadnu organizáciu.
2. **Súvislý a neregulovaný tok dát z TIP RF priamo k odberateľovi služby.** Z pohľadu relevancie a prehľadnosti je tok dát z TIP RF do inštancie MISP Afrodita regulovaný, aby sa tam dostali iba relevantné IoC, ktoré nepovažujeme za false-positive. Navyše sa tak prechádza zahlcovaniu inštancie MISP Afrodita a odoberateľ získava vyselektované informácie, ktoré sú relevantné pre danú organizáciu.
3. **Zdieľanie dát mimo siete Govnet**. Prístup do Govnetu je nevyhnutnou podmienkou pre odoberanie služby Afrodita, keďže inštancia MISP Afrodita je dostupná iba cez Govnet a prístup získavajú iba organizácie verejnej správy, čo korešponduje s konštituenciou VJ CSIRT.
4. **Sťahovanie IoC z inštancie MISP Afrodita formou PULL.** Model poskytovania služby Afrodita je nastavený výhrade na formu PUSH, teda na odosielanie IoC z Afrodity smerom von. Forma teda PULL nie je v súčasnosti podporovaná.
5. **Publikácia IoC z inštancie MISP Afrodita cez webové kanály (angl. web feeds).** Z dôvodu publikácie inštancie MISP Afrodita iba v rámci siete Govnet, nie je možné vytvárať webové feedy, ktoré by si organizácie mohli sťahovať.

Využitie ostatných funkcií nástroja MISP

Inštancia MISP Afrodita je, okrem iného, stále inštanciou nástroja MISP. Základné funkcionality tohto nástroja ostali zachované, preto je možné ich v rámci pridelenej role ďalej využívať. Ako príklad uvádzame používanie REST API, ktoré MISP poskytuje, na automatizáciu niektorých procesov (napr. stiahnutie všetkých dostupných IoC z celej inštancie MISP Afrodita).

V prípade, že odoberateľ potrebuje využiť službu nástroja MISP, ktorá mu nie je v daný moment dostupná, môže kontaktovať VJ CSIRT a daná situácia bude riešená samostatne.

Oficiálna dokumentácia nástroja MISP

Pre lepšie pochopenie a oboznámenie sa s nástrojom MISP, prípadne na pomoc pri riešení problémov, odporúčame prečítať si oficiálnu dokumentáciu, ktorá pochádza priamo od tvorcu a aktívneho vývojára tohto nástroja – organizácie **CIRCL.LU**. Nájdete ju na odkaze **https://www.circl.lu/doc/misp/.**

Kontaktné údaje

V prípade otázok na službu Afrodita a jej poskytovania môžete kontaktovať Vládnu jednotku CSIRT, konkrétne CTI tím, na e-mailovej adrese **cti@csirt.sk**