



Všeobecné informácie o službe MISP „Afrodita“ od VJ CSIRT



Výhody služby MISP „Afrodita“

Konštituenti používajúci túto službu získajú prístup k pravidelným informáciám o indikátoroch kompromitácie z aktuálneho diania v kybernetickom priestore na pravidelnej báze. Môžu tak **overovať prítomnosť indikátorov kompromitácie (skr. 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, 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.

Systém zohľadňuje úrovne dôvery pomocou **TLP – Traffic Light Protocol** a umožňuje ciele 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.

Nástroj MISP ako Threat Intelligence služba od VJ CSIRT

Vládna jednotka CSIRT poskytuje svojej konštituencii prístup k inštancii nástroja MISP s názvom „Afrodita“, ktorý slúži ako úložisko a korelačný systém pre rôzne indikátory kompromitácie, ktoré do MISP-u nahráva VJ CSIRT, alebo autorizovaný konštituent. V rámci tohto nástroja je možné korelovať a prehľadávať nahraté IoC, čím vzniká centralizovaný spôsob na identifikáciu a zber IoC pre bezpečnostné potreby konštituentov.

Možnosti plnenia inštancie MISP „Afrodita“

Samotní konštituenti majú možnosť nahrávať IoC do tohto MISP-u, pričom je po ich nahratí potrebná validácia od analytika VJ CSIRT. Po úspešnej validácii sú IoC nahraté od konštituentov publikované v inštancii MISP „Afrodita“ a VJ CSIRT si vyhradzuje právo publikovať tieto IoC aj vo svojej internej inštancii nástroja MISP pre účely rozširovania svojho detekčného dátového setu. Prípadná neúspešná validácia, alebo označenie IoC za false-positive, má za následok odstránenie buď predmetných IoC, alebo celej udalosti z inštancie MISP „Afrodita“ a upovedomenie konštituenta, že došlo k takejto úprave, spolu s náležitým odôvodnením.

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 metadáta a sú prešírené až po inštanciu MISP „Afrodita“.
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:WHITE**, 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.

Požiadavky na poskytovanie služby MISP „Afrodita“

MISP „Afrodita“ je poskytovaná dvoma spôsobmi, ktoré si vyžadujú splnenie samostatných požiadaviek. Pripomíname, že sa tieto spôsoby navzájom nevylučujú, takže konštituent vie požiadať o jeden, alebo aj o oba spôsoby poskytovania služby MISP „Afrodita“ naraz.

Spôsoby poskytovania sú nasledujúce:

1. Priamy prístup do inštancie MISP „Afrodita“

- **Informácie** - Konštituent získa priamy prístup do inštancie MISP „Afrodita“ tak, že mu pracovníci VJ CSIRT vytvoria prihlasovacie údaje, pomocou ktorých sa do tejto inštancie nástroja MISP prihlási a môže tak využívať poskytovanú službu. Počet kont pre konštituenta nie je obmedzený, avšak odporúčame žiadať o vytvorenie prístupov primárne pre osoby, pre ktoré to je relevantné (napr. riešitelia incidentov, bezpečnostní analytici, atď.). Práca s nástrojom MISP si vyžaduje dávku technickej zdatnosti a aspoň základnú znalosť narábať s dátami ako sú indikátory kompromitácie, čo je potrebné vziať do úvahy pri výbere osôb, pre ktoré konštituent požiada o vytvorenie prístupu do inštancie MISP „Afrodita“.
- **Spôsob registrácie** – Na adresu cti@csirt.sk odošle konštituent e-mail, v ktorom požiada o vytvorenie prístupov pre explicitne uvedený zoznam e-mailových adries². Po obdržaní požiadavky sa v inštancii MISP „Afrodita“ vytvoria dané prístupy a späťne sa odošlú konštituentovi vo forme zaheslovaného ZIP adresára na kontaktnú osobu (ak je iná ako odosielateľ žiadosti, treba uviesť kontakt). Heslo od ZIP adresára bude konštituentovi doručené sekundárnym kanálom³ (napr. cez SMS). Po prvom prihlásení pomocou vygenerovaných prístupov sa pre každé konto vyžaduje zmena hesla.

² VJ CSIRT v tomto prípade akceptuje iba služobné e-mailové adresy, nie súkromné.

³ Ak konštituent nemá konto vo VISKB, je potrebné poslať v e-mailovej žiadosti aj spôsob, akým má byť odoslané heslo od ZIP adresára. Musí ísť o komunikačný kanál iný ako e-mail.

- **Podmienky registrácie** – Konštituent musí mať prístup do siete GOVNET, konkrétne na webovú lokalitu <https://afrodita.soc.gov.sk> (port 443).

2. Prepojenie inštancie MISP „Afrodita“ a internej inštancie konštituenta

- **Informácie** – Konštituent si vo svojej infraštruktúre nasadí vlastnú inštanciu nástroja MISP, ktorú má plne vo svojej správe. Následne sa táto inštancia prepojí s inštanciou MISP „Afrodita“, odkiaľ budú odosielané IoC (a iné dáta) tzv. formou **PUSH**, takže budú IoC odosielané smerom z MISP „Afrodita“ do internej inštancie nástroja MISP u konštituenta.
- **Spôsob registrácie** – Na adresu cti@csirt.sk odošle konštituent e-mail, v ktorom požiada o prepojenie inštancií nástroja MISP. VJ CSIRT má pre tento postup vytvorený samostatný dokument, ktorý odošle konštituentovi ako odpoveď, kde je detailne popísaný postup a požiadavky, ktoré sú od konštituenta požadované na realizáciu prepojenia.
- **Podmienky registrácie** – Konštituent musí mať prístup do siete GOVNET, konkrétne na webovú lokalitu <https://afrodita.soc.gov.sk> (port 443), a to hlavne z internej inštancie nástroja MISP. Ďalej musí spĺňať dodatočné požiadavky, ktoré sú uvedené v manuáli na prepojenie inštancií nástroja MISP (odoslané od VJ CSIRT).

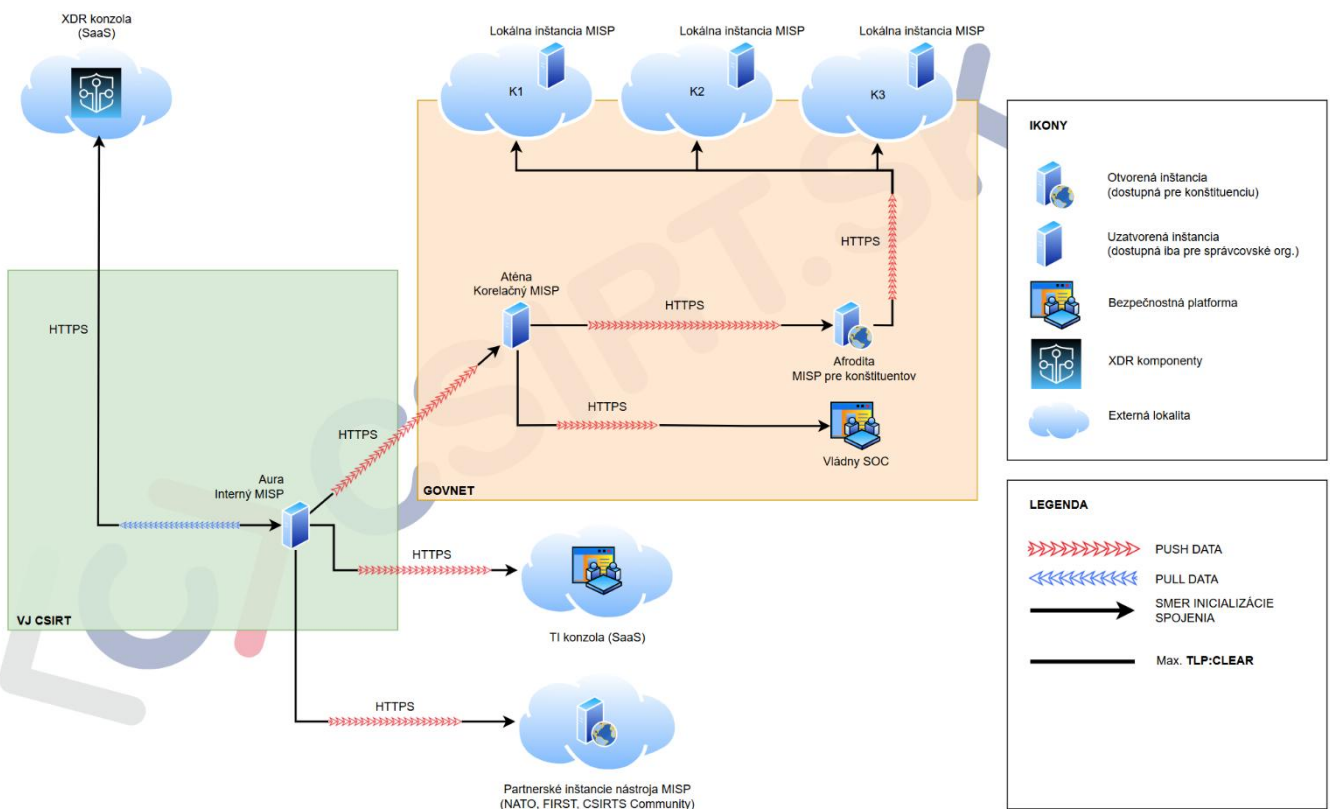
Po splnení uvedených požiadaviek a úspešnej registrácii konštituenta na odber služby MISP „Afrodita“ je táto služba náležito otestovaná. VJ CSIRT je počas testovania v priamej komunikácii s konštituentom, kde sa z obidvoch strán potvrdí korektné nastavenie služby (napr. úspešný prenos IoC, úspešné prihlásenie, alebo úspešné prepojenie inštancií nástroja MISP). Všetky prípadné komplikácie týkajúce sa poskytovania tejto služby sú riešené priebežne počas testovania.

Kontaktné údaje

V prípade otázok na službu MISP „Afrodita“ a jej poskytovania môžete kontaktovať Vládnu jednotku CSIRT na e-mailovej adrese cti@csirt.sk.

System nástrojov MISP pre konštituenciu

VJ CSIRT prevádzkuje systém inšancií nástroja MISP, ktoré sú navzájom prepojené na zabezpečenie lepšieho dosahu v rámci siete GOVNET (a mimo nej) pre odosielanie IoC na rôzne prepojené a partnerské inšancie nástroja MISP. Obrázok 1 ukazuje infraštruktúru tohto systému, spolu s prepojením na inšancie konštituentov (označených ako „K[N]“, napr. „K1“) a prepojením na partnerské inšancie nástroja MISP (napr. NATO MISP, alebo FIRST MISP). Týmto spôsobom dochádza aj k obohacovaniu IoC v jednotlivých inštanciách pomocou ich zdieľania a komunikácie medzi inštanciami. Koncový používateľ, ktorý je pripojený na inštanciu MISP „Afrodita“, tak získava aktuálne a plnohodnotné informácie a IoC, ktoré boli priebežne obohatené pri prechode týmto systémom.



Obrázok 1 - Infraštruktúra systému inšancií nástroja MISP