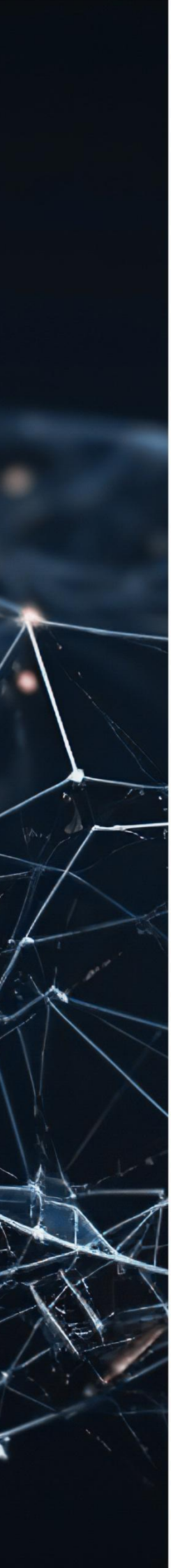


Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Systém včasného varovania

Výhody služby
Systém včasného varovania

MIRRI SR vytvoril a prevádzkuje Systému včasného varovania (angl. Early Warning System, EWS) za účelom budovania proaktívnych služieb v oblasti kybernetickej bezpečnosti pre organy verejnej moci na Slovensku. Cieľom tohto riešenia je poskytnúť zapojeným organizáciám vybrané nástroje a služby kybernetickej bezpečnosti vykonávané buď v režime 24/7 alebo 8/5 podľa príslušnej služby. Tento systém je primárne určený na zvyšovanie preventívnych opatrení a zvýšenie rýchlosti detekcie a reakcie na bezpečnostné hrozby cielené na organizácie.

Bezpečnostný monitoring je služba kybernetickej bezpečnosti, ktorá poskytuje rozšírenú detekciu a reakciu. Táto služba je navrhnutý tak, aby umožňovala lepšie chrániť IT prostredie tým, že poskytuje prehľad o hrozbách, integráciu medzi rôznymi bezpečnostnými vrstvami a možnosti rýchlej reakcie na incidenty.

Implementácia systému EWS prináša služby, ktoré je možné využiť na zlepšenie úrovne kybernetickej bezpečnosti, správu koncových bodov v rámci jednotlivých Orgánoch verejnej moci (ďalej len „OVM“). Medzi zlepšenia patria:

1. centralizovaný zber logov z bezpečnostných udalostí a ich koreláciu (SIEM),
2. zlepšenie detekcie a reakcie na kybernetické hrozby (angl. Incident Management, IM),
3. ochranu a monitoring koncových zariadení a serverov (angl. eXtended Detection and Response, XDR)
4. detekciu známych zraniteľností na koncových zariadeniach a serveroch (angl. Vulnerability Management, VM).
5. analýzu sieťovej premávky (angl. Network Detection and Reponse, NDR),
6. platformu pre zdieľanie informácií o hrozbách (angl. Threat Intelligence, TI) v podobe služby MISP Afrodita

Opis poskytovaných služieb

Systém Riešenie pozostáva z jednotnej konzoly, v ktorej majú prístup jednotlivé OVM iba k svojím dátam a výstrahám. Analytici SOC majú prístup ku všetkým dátam, aktívam, alertom a zraniteľnostiam. **Analytici SOC majú možnosť vo všetkých moduloch dodaného riešenia prispôsobiť/nastaviť politiky, pravidlá a procesy dodaného riešenia pomocou jednej centrálnej manažment konzoly alebo API rozhrania, a to pre každé OVM jednotlivo a zároveň pre všetky spoločne.** Dáta jednotlivých OVM sú oddelené na úrovni takzvaných produktových inštancií (Product Instance) a pomocou roly vytvorenej pre dané OVM.

Bezpečnostný monitoring môže pozostávať z nasledujúcich technológií a k tomu prislúchajúcich služieb:

1. SIEM – centralizovaný zber a korelácia udalostí

a. Zber udalostí (syslog) z koncových zariadení, serverov, sieťových zariadení a iných relevantných systémov (nenahrádza Log management systém, ktorým by malo disponovať každé OVM).

b. Korelácia udalostí podľa definovaných *use-cases* (pracovné scenáre), v rámci Dohody o bezpečnostnom monitoringu.

c. Detekcia anomálií, pokusov o útok, neštandardných správaní či opakujúcich sa vzorov.

d. V prípade vyhodnotenia incidentu je udalosť odoslaná na analýzu do SOC.

2. XDR + Vulnerability Management na koncových zariadeniach a serveroch

a. Nasadenie XDR agentov na pracovných staniciach a serveroch – sledovanie správania systému, procesov, aktivít súborov, sieťových spojení.

b. Detekcia škodlivého správania, exploitov, ransomvéru, pokusov o pohyb v sieti, neautorizovaných zmien.

c. Automatizované reakcie: blokovanie, izolácia zariadenia, upozornenie na SOC.

d. Zároveň modul VM: identifikácia softvérových zraniteľností, konfigurácií, správanie podľa skóre rizikovosti, návrhy nápravy.

e. Centrálna správa bezpečnostných politík. OVM má prístup do konzoly s oprávnením „read only“.

3. NDR – analýza sieťovej premávky

a. Monitorovanie sieťovej prevádzky (hlavičky/pakety) – analýza metadát, tokov, neštandardných spojení, anomalít v komunikácii.

b. Detekcia podozrivej komunikácie, abnormálnych tokov, možných pokusov o prienik či C2 komunikačných kanálov.

c. Bez dostupnosti obsahu (bez dešifrovania), čisto na základe metadát a sieťových vzorcov.

d. Prepojenie s XDR / SIEM – centralizovaný prehľad.

4. Threat Intelligence – zdieľanie informácií o hrozbách prostredníctvom MISP Afrodita

a. Ponúkame prístup k centrálne spravovanej databáze indikátorov kompromitácie (Indicators of Compromise – IoC), spravovanej pod gesciou VJ CSIRT (analogicky ako u MISP Afrodita).

b. Naše znalosti o hrozbách sú pravidelne aktualizované – správy z monitoringu kyberpriestoru, globálnych kampaní, známych útokov a exploitov.

c. Možnosť pre klienta nahrávať vlastné IoC (zistené pri incidente, audit, forenzika) – po validácii sú IoC publikované v systéme.

d. Umožní koreláciu nových IoC s existujúcimi a ich porovnanie s historickými alebo globálnymi údajmi.

e. Výsledkom je včasná prevencia, možnosť vyhľadávania zraniteľností a ohrození vo vlastnej infraštruktúre, nasadzovanie proaktívnych opatrení.

Špecifikácia poskytovaných služieb

Názov	Režim služby	Nástroj	Výstup / Prístup
Monitoring procesov na koncových zariadeniach a reakcia na detegované udalosti	24/7	XDR	Prístup na čítanie do konzoly XDR
Zber, vyhodnocovanie a korelácia logov	24/7	SIEM	Mesačný prehľad incidentov
Automatizácia vyšetrovacích a reakčných procesov	24/7	SOAR	Mesačný prehľad incidentov
Monitoring sieťovej komunikácie	24/7	NDR	Prístup na čítanie do konzoly NDR
Bezpečnostný monitoring L1 a L2	24/7	N/A	Správa o incidente
Analýza L3 (analýza škodlivého kódu a forenzná analýza)	8/5	XDR, Sandbox	Správa o analýze škodlivého kódu alebo forenzná správa
Threat Intelligence a Threat Hunting	8/5	Služba Afrodita	Prístup do MISP Afrodita
Externé skeny zraniteľností	8/5	Služba Achilles	Mesačné skeny zo služby Achilles
Interné skeny zraniteľností	8/5	XDR (Modul VA)	Detegované zraniteľnosti v konzole XDR
Penetračné testovanie	8/5	Služba Ares	Záverečná správa o vykonanom testovaní
Simulácie phishingových útokov	8/5	N/A	Vyhodnotenie phishingového testu
Prenos vedomostí	8/5	Služba Kyberaréna	Certifikát o absolvovaní školenia
Koordinácia pri riešení kybernetických bezpečnostných incidentov	8/5	VJ CSIRT	Vytvorenie odporúčaní na zlepšenie

Podmienky spolupráce a aktivácie služby

Pre aktiváciu služby je potrebné vykonať nasledovné:

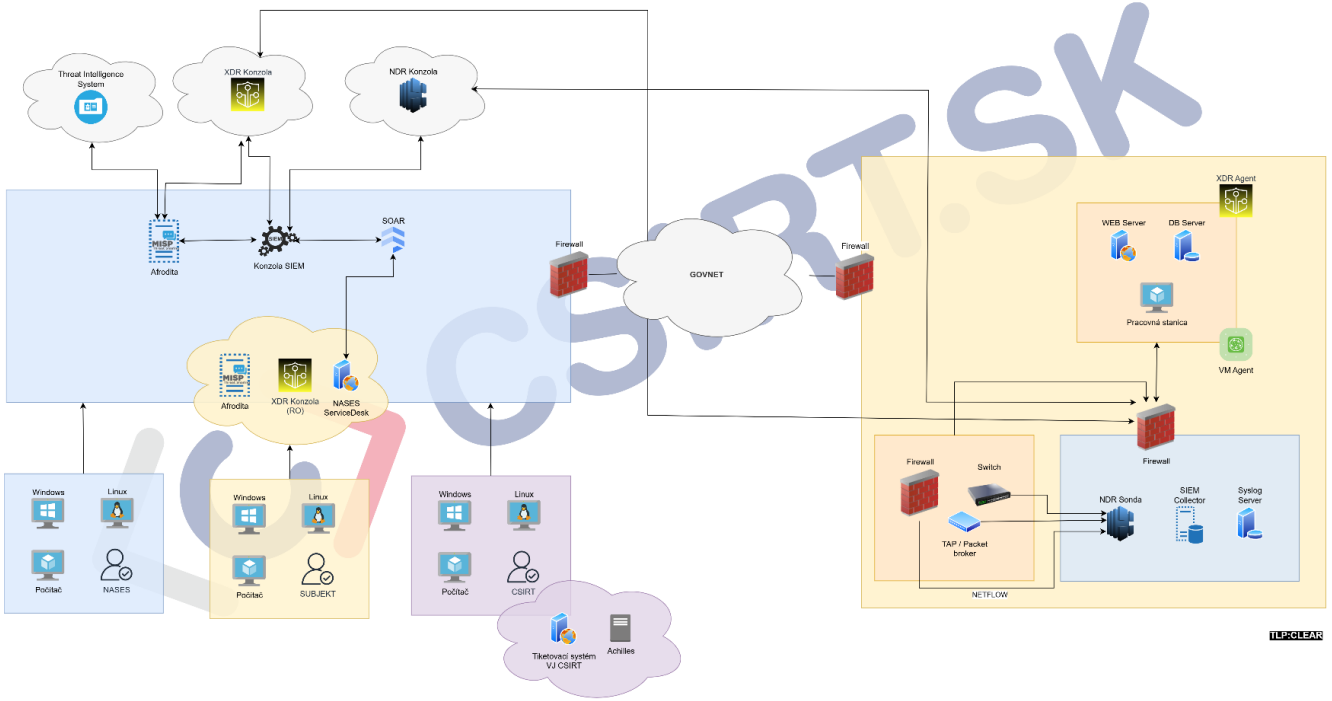
1. podpis Dohody o službách kybernetickej bezpečnosti s definovanými *prípadmi použitia* pre SIEM a reakcie spolu s rozsahom monitorovaných aktív;
2. nasadenie XDR agentov s funkcionalitou VM agenta na pracovných staniciach a serveroch;
3. odoslanie vybraných logov (syslog) do nášho SIEM, tento krok je podmienený inštaláciou hardvéru u žiadateľa a pripojením do siete Govnet;
4. konfigurácia sieťového toku pre NDR (potrebný SPAN port alebo zariadenie TAP/NPB na odosielanie premávky);
5. pripojenie do služby Threat Intelligence prostredníctvom MISP Afrodita – nastavenie prístupu do platformy (pripojenie do siete Govnet), prípadne dohodnutie kanálov pre nahrávanie indikátorov kompromitácie a komunikáciu.

Kontaktné údaje

V prípade otázok na Systém včasného varovania a jeho poskytovanie môžete kontaktovať VJ CSIRT na e-mailovej adrese **onboard@csirt.sk.**

Architektúra služby

Systém včasného varovania spočíva v nasadení agentov na koncové body, ktoré vykonávajú tzv. ochranu proti škodlivému kódu, rozšírenú detekciu škodlivých aktivít alebo detekciu zraniteľností. Telemetrické dáta sú zasielané do cloudovej konzoly, ktorá poskytuje ucelený pohľad na stav bezpečnosti v celom monitorovanom prostredí. Biznis architektúra riešenia navrhuje pokrytie koncových bodov orgánov verejnej moci (OVM), zber dát z týchto OVM v centrálnej konzole, odkiaľ ich konzumuje SIEM platforma a nad týmito dátami vykonáva dohľad bezpečnostné dohľadové centrum (SOC).



Obr. 1: Logická architektúra vybraných aspektov služby EWS