MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Katalóg služieb Vládnej jednotky CSIRT[1]

Vládna jednotka CSIRT

Verzia 1.3 | info@csirt.sk | 04. 03. 2026

[1] Služby VJ CSIRT sú definované na základe osvedčených medzinárodných štandardov (FIRST CSIRT Services Framework), keďže VJ CSIRT je držiteľom prestížnej certifikácie SIM3

TLP: CLEAR

ID služby	Názov	Opis	Režim poskytovanej služby	Nevyhnutné podmienky poskytovania služby	Výstup zo služby
Reaktívne služby					
1	Koordinácia pri riešení incidentov a podpora krízového manažmentu	Komunikácia, distribúcia upozornení, koordinácia aktivít, distribúcia informácií k jednotlivých zložkám, hlásenie stavu riešenia	8/5	Žiadosť o súčinnosť pri riešení KBI	Správa z riešenia kybernetického bezpečnostného incidentu (KBI) s odporúčaniami a konzultácie počas riešenia
2	Poskytovanie služby L1, L2 a L3 po žiadosti o súčinnosť pri riešení KBI	Príjem, triáž, analýza a reakcia na detegované hlásenia	8/5	Žiadosť o súčinnosť pri riešení KBI	Správa z riešenia KBI s odporúčaniami a konzultácie počas riešenia
3	Digitálna forenzná analýza	Zaistenie digitálnych stôp s evidenciou tzv. Chain of Custody. Analýza týchto stôp a vypracovanie forenznej správy	8/5	Žiadosť o súčinnosť pri riešení KBI	Správa z riešenia KBI obsahujúca výstupy forenznej analýzy
4	Analýza škodlivého kódu	Identifikácia typu, funkcionalít a správania malvéru	8/5	Žiadosť o súčinnosť pri riešení KBI a analýzy škodlivého kódu	Správa z riešenia KBI obsahujúca výstupy analýzy škodlivého kódu
Proaktívne služby					
5	Externé skenovanie známych zraniteľností (Achilles)	Skenovanie vonkajších IP adries s cieľom posúdenia zraniteľností. Skenovanie realizované systémom Achilles, ktorý prevádzkuje VJ CSIRT.	8/5	Registrácia Achilles	Správa o výskyte známych zraniteľností zo systému Achilles pre aktíva zapísané vo VISKB a informácie

					o úniku prihlasovacích údajov z Have I Been Pwnd
6	Interné skenovanie známych zraniteľností	Skenovanie zraniteľností na koncových zariadeniach pomocou agenta XDR a infraštruktúrnych serverov pomocou interného skenovania zraniteľností	8/5	Registrácia do systému EWS	Správa o výskyte známych zraniteľností pre vybrané interne aktíva aktíva
7	Penetračné testovanie (Ares)	Externý penetračný test infraštruktúry s analýzou údajov z otvorených zdrojov (OSINT)	8/5	Registrácia Ares	Záverečná správa obsahujúca nálezy objavené počas penetračného testovania
		Penetračný test webovej aplikácie	8/5	Registrácia Ares	
		Bezpečnostný audit konfigurácie podľa súladu s tzv. CIS benchmarks	8/5	Registrácia Ares	
8	Objavovanie nových zraniteľností (Ares)	Objavenie nových zraniteľností v softvérových produktoch a knižniciach	8/5	Objavené zraniteľnosti	Detailný popis zraniteľnosti aj s príkladom jej zneužitia
9	Zdieľanie informácií o hrozbách (Afrodita)	Cielená threat intelligence podľa OVM, monitorovanie uniknutých dát, prehľady aktuálnych hrozieb, distribúcia indikátorov kompromitácie (IoCs)	8/5	Registrácia Afrodita alebo Registrácia do systému EWS	Prístup do platformy MISP (Afrodita), informácie o aktuálnych hrozbách
10	Prenos vedomostí (Kyberaréna, Portál CTF, Kyberbezpečnostná hra)	Realizácia tréningov a vzdelávania (napr. Table-Top cvičenia, simulácia útokov na infraštruktúru v podobe cvičenia). Poradenstvo v oblasti technológií,	8/5	Registrácia Kyberaréna alebo Registrácia portál CTF alebo Kyberbezpečnostná hra alebo Metodiky a	Poskytovanie odborných konzultácií a školení pre odborných IT ale aj laických zamestnancov verejnej správy. Poskytovanie prednášok pre študentov

		politík, návrhu zlepšenia internej infraštruktúry a prípravy IRA		návody alebo Naše publikácie	a zamestnancov stredných škôl
11	Publikačná činnosť	Zverejňovanie informácií o známych zraniteľnostiach, kampaniach a činnosti aktérov hrozieb	8/5	Varovania alebo Tlačové správy alebo kanál RSS	Mesačná správa CSIRT.SK a prehľad bezpečnostných udalostí vo svete a u nás, Mesačný prehľad kritických a závažných softvérových zraniteľností a kanál RSS
12	Analýza údajov z otvorených zdrojov (OSINT)	Analýza údajov z otvorených zdrojov (OSINT) pre potreby OČTK	8/5	OSINT	Správa o nálezoch získaných z analýzy údajov z otvorených dát
13	Pokročilá analýza a diagnostika hardvérových zariadení	Extrakcia a analýza čipov z dosiek plošných spojov, dynamická analýza zberníc, získavanie firmvéru, detekcia podozrivého bezdrôtového vysielania či útoky bočnými kanálmi na testovanie odolnosti zariadení	8/5	Laboratórium hardvérovej a dátovej analýzy	Záverečná správa obsahujúca nálezy objavené počas analýzy alebo diagnostiky
14	Vývoj nástrojov pre automatizáciu procesov v oblasti kybernetickej bezpečnosti	Vývoj a údržba nástrojov na automatizáciu procesov, bez ktorej by bolo potrebné násobné množstva personálnych kapacít	8/5	Zvýšenie spôsobilostí Vládnej jednotky CSIRT alebo GitHub	Vývoj systémov Achilles, Domino, Abuzikmi, Proteos

Služby v spolupráci s vládnym SOC, ktorý prevádzkuje NASES					
15	Podporné činnosti pri procesoch spojených s bezpečnostným monitoringom v rámci Vládneho SOC	Činnosti spojené s odosielaním telemetrie zo zariadení určenej pre vyhodnocovanie bezpečnostných udalostí a systém včasného varovania.	8/5	Registrácia do systému EWS	Pripojenie organizácie a ďalších zdrojov do služieb bezpečnostného monitoringu
16	Monitoring procesov na koncových zariadeniach a reakcia na detegované udalosti	Nasadenie nástroja s rozšírenými možnosťami detekcie a reakcie na koncových zariadeniach (XDR)	24/7	V spolupráci s Vládnym SOC (NASES), potrebná Registrácia do systému EWS	Hlásenia kybernetických bezpečnostných incidentov a pravidelný mesačný prehľad z bezpečnostného monitoringu
17	Zber a vyhodnocovanie logov	Zber, spracovanie a vyhodnocovanie sieťových a systémových logov (SIEM)	24/7	V spolupráci s Vládnym SOC (NASES), potrebná Registrácia do systému EWS	Hlásenia kybernetických bezpečnostných incidentov a pravidelný mesačný prehľad z bezpečnostného monitoringu
18	Monitoring sieťovej komunikácie a detekcia známych hrozieb	Nasadenie nástroja na monitorovanie dátových tokov (Netflow)	24/7	V spolupráci s Vládnym SOC (NASES), potrebná Registrácia do systému EWS	Hlásenia kybernetických bezpečnostných incidentov a pravidelný mesačný prehľad z bezpečnostného monitoringu
19	Bezpečnostný monitoring L1 a L2	Dohľad nad hláseniami generovanými nasadenými nástrojmi na monitoring. Reakcia na generované hlásenia, ich základná triáž, vyšetrenie a eskalácia	24/7	V spolupráci s Vládnym SOC (NASES), potrebná	Hlásenia kybernetických bezpečnostných incidentov a pravidelný mesačný

		hlásení OVM spolu so zisteniami a odporúčaniami ďalších krokov		Registrácia do systému EWS	prehľad z bezpečnostného monitoringu