MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

SEKCIA KYBERNETICKEJ BEZPEČNOSTI
ODBOR RIADENIA KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI
VLÁDNA JEDNOTKA CSIRT

Achilles, Ares a Afrodita

Tri piliere proaktívnej kybernetickej bezpečnosti

Alexander Valach, Vedúci analytického oddelenia

ACHILLES

PLÁN OBNOVY

Financované Európskou úniou
NextGenerationEU

TLP:CLEAR

CSIRT.SK

26. 11. 2025

CSIRT.SK

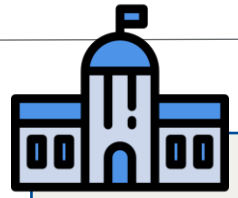
- **Aktuálne dve pobočky**
  - Bratislava
  - Košice
- **Medzinárodná spolupráca**
  - FIRST (USA)
  - TF CSIRT / Trusted Introducer (**certifikovaný tím – SIM3**)
  - ENISA – CSIRTs Network (EÚ) (**tím na úrovni ENISA Expert**)
- **Národná spolupráca**
  - národný SK-CERT a iné CSIRT tímy
  - akademický sektor (UPJŠ KE, STU BA)
  - bezpečnostné zložky

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

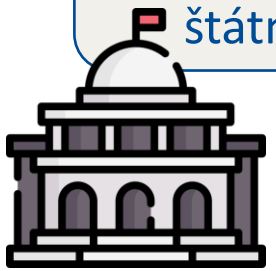
CSIRT.SK

CSIRT.SK

Konštituencia



Ministerstvá a ústredné orgány štátnej správy



Štátne orgány (GP SR, NKÚ SR, ÚOOU SR, ...)

Obce a VÚC

Komory

Iné právnické osoby

Činnosť CSIRT.SK

Oddelenie reaktívnych činností

- Správa IT infraštruktúry
  - Správa vlastných systémov
  - Poradenstvo, aj pre OVM
- Riešenie incidentov
  - Incident handling
  - Základná analýza
  - Konzultácie, odporúčania
- Prevencia incidentov
  - OSINT, monitoring hrozieb

Analytické oddelenie

- Hodnotenie zraniteľností
- Penetračné testovanie
- Monitoring OVM
- Pomoc pri IH
- Threat intelligence

Oddelenie vzdelávania a preventívnych činností

- Publikovanie varovaní, odporúčaní a návodov
- OSINT, monitoring hrozieb
- Školenia v rámci konštituencie
- Vývoj nástrojov pre vlastné potreby
- Kyberaréna

Oddelenie AKH

- Forenzná analýza
- Malvér analýza
- Chip-off lab
- Analýzy incidentov na úrovni L3
- Správa vlastných IT systémov
- Publikovanie odporúčaní a návodov
- Prevencia incidentov
- Monitoring OVM

Medzinárodná spolupráca a reprezentácia

Spolupráca s partnermi

Participácia na projektoch a novelizácii zákonov

Administratívne činnosti

Verejné obstarávania

Tri piliere proaktívnej kybernetickej bezpečnosti

CSIRT.SK

1. Služba (nielen) plošného vyhľadávania zraniteľností (**Achilles**)
2. Služba zdieľanie informácií o hrozbách (**Afrodita**)
3. Služba hodnotenia zraniteľností a penetračného testovania (**Ares**)
4. Kybernetickú bezpečnosť totiž takisto tvorí triáda (**technológie + procesy + ľudia**)
5. Pozor na **falošný pocit bezpečnosti**

MISP AFRODITA

ARES by CSIRT.SK ATTACK TO PROTECT

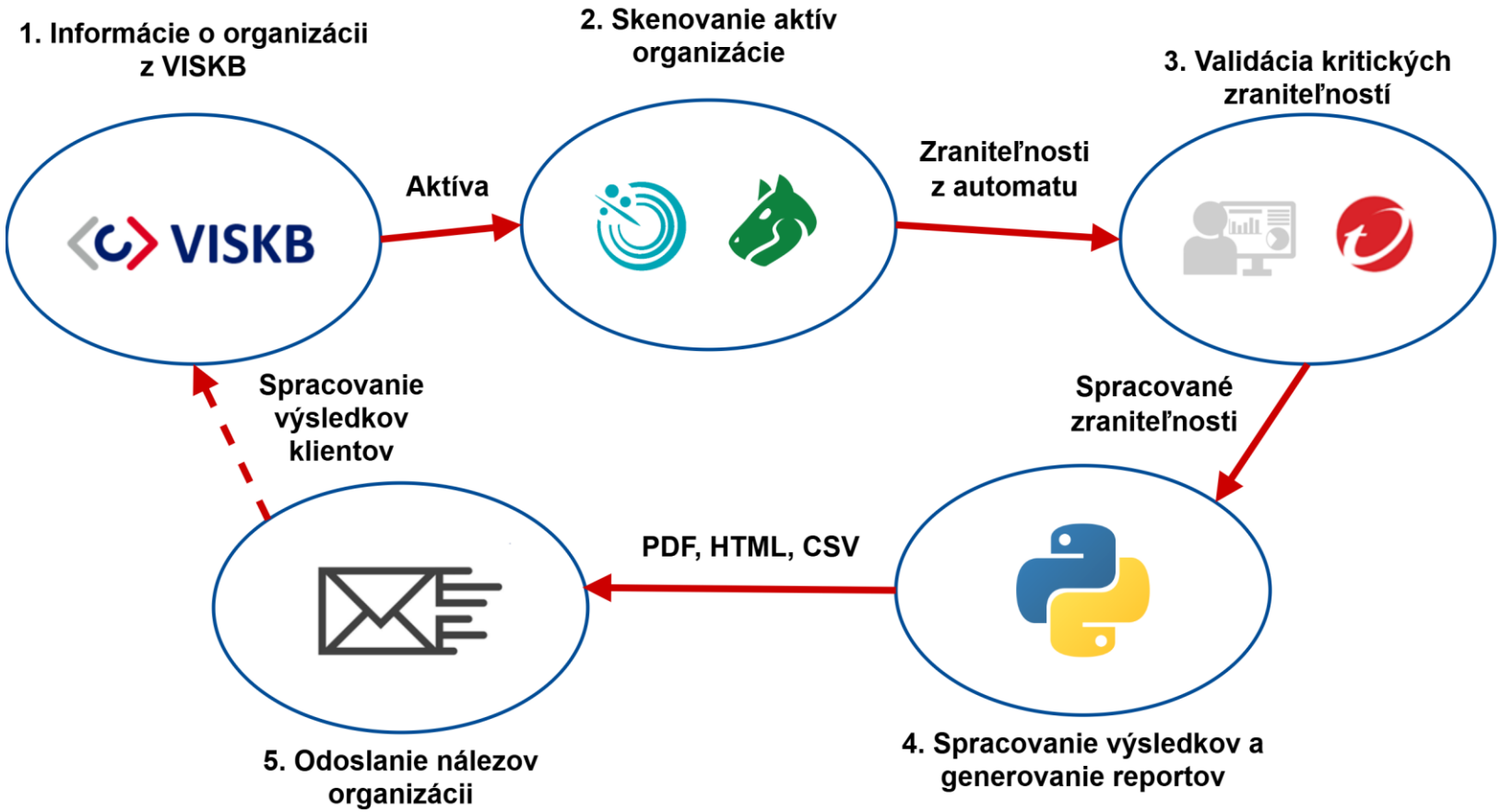
ACHILLES

Služba Achilles

CSIRT.SK

Architektúra služby Achilles

CSIRT.SK

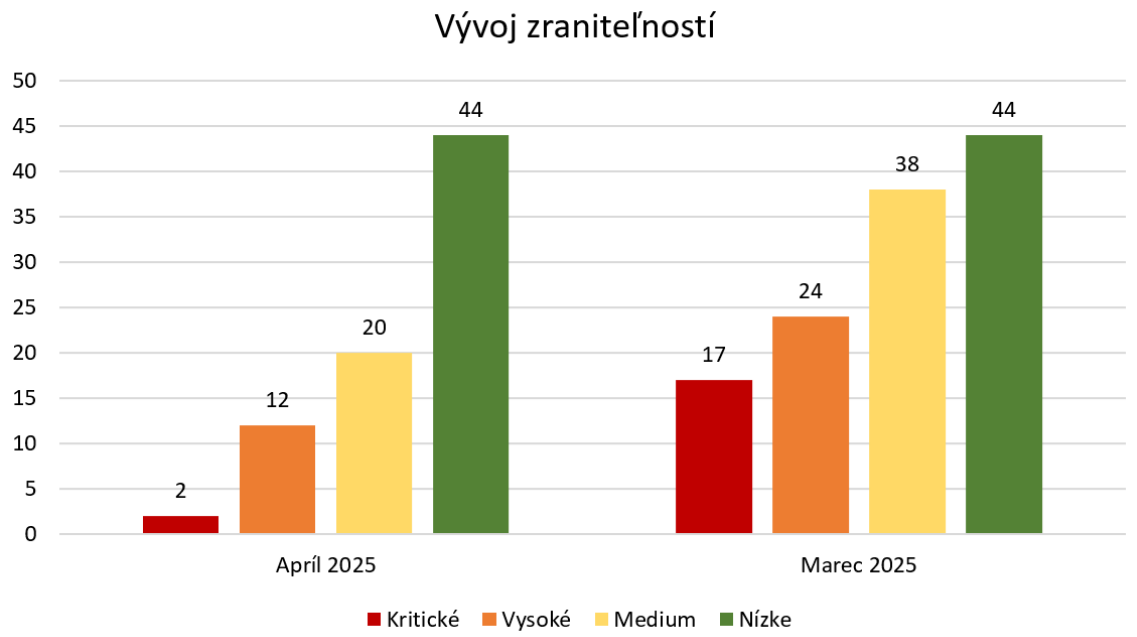


Výhody služby Achilles

1. **Mesačné správy** s identifikovanými zraniteľnosťami
2. Informácie o **aktívne zneužívaných** zraniteľnostiach a kampaniach
3. **Odporúčania** pre **zníženie rizika** zneužitia zraniteľnosti

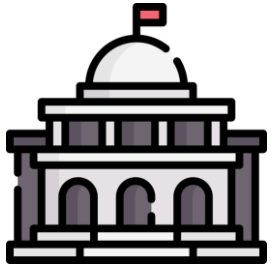
[redacted]

Vulnerability name:	Unsupported Web Server Detection
DNS:	[redacted].sk
Port:	*443*
Description:	*According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.* *Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.*
Solution:	*Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.*
CVSS v3.0:	*10*
Reference:	*IAVA: 0001-A-0617*



Dosiahnuté výsledky

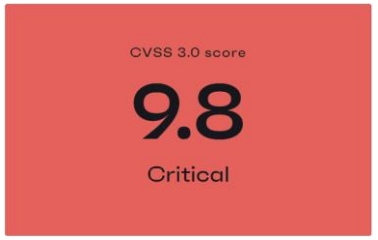
CSIRT.SK



Viac ako **330 skenovaných organizácií**

Viac ako **32 000 IP adries**

Odoslaných viac ako **2 900 reportov identifikovaných zraniteľností**



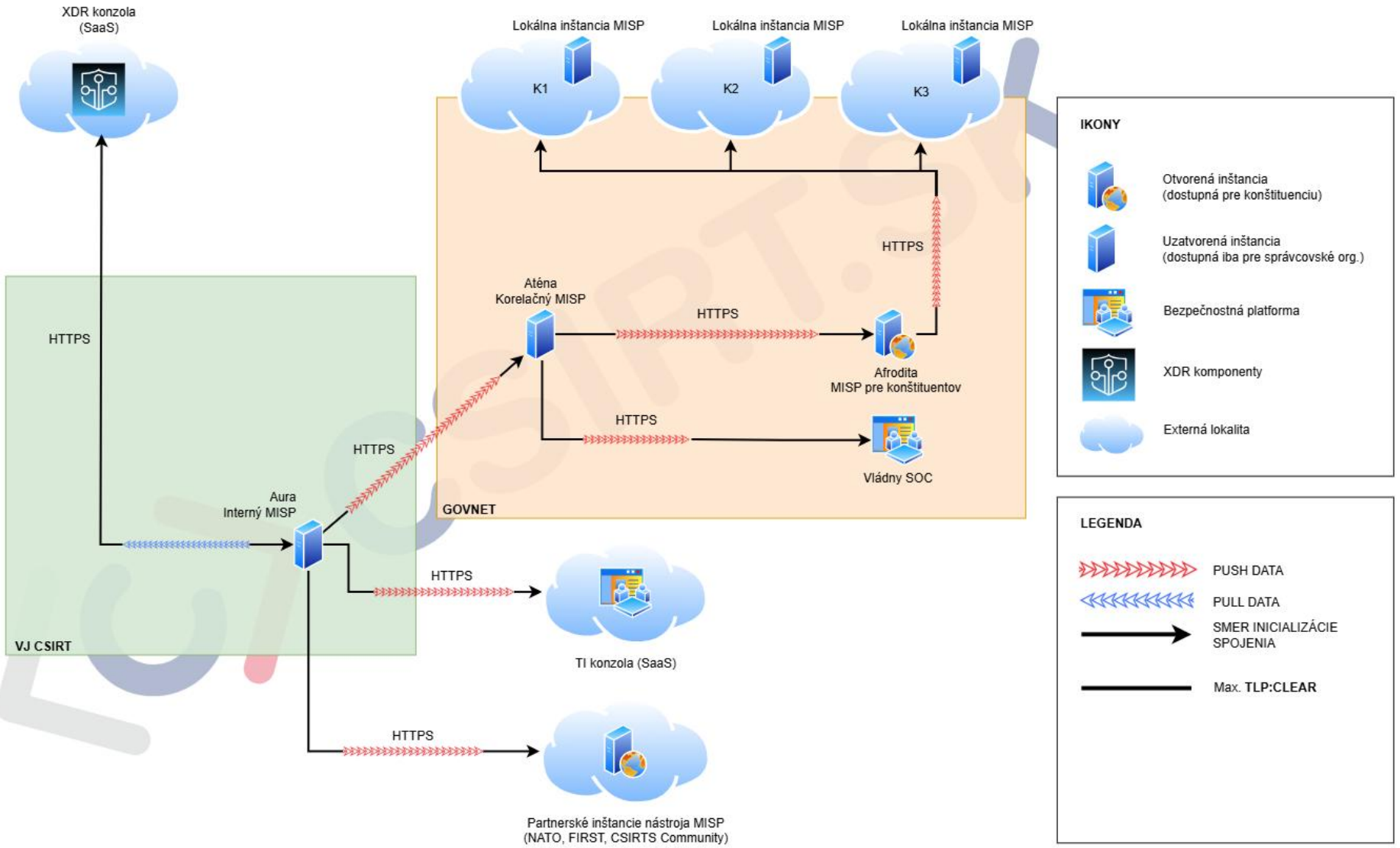
Počet **kritických zraniteľnosti** subjektov **klesá**, lebo sú o nich včas informovaní

1. Budovanie povedomia o potrebe **komunikovať** s VJ CSIRT
2. Zlepšenie viditeľnosti (princíp „**Know Your Customer**“)
3. Zlepšenie komunkácie s konštituenciou (**Opravené!**)

Služba Afrodita

CSIRT.SK

Architektúra služby Afrodita



Výhody služby Afrodita

1. Služba priamo podporuje **prevenciu**, detekciu a **rýchle reakcie** na hrozby (napr. včasné varovanie pred plánovanou kampaňou DDoS)
2. Zabezpečuje **obohacovanie dát a zdieľanie** informácií o hrozbách
3. Výstupom služby je aj mesačný tzv. **Threat Intelligence Report**

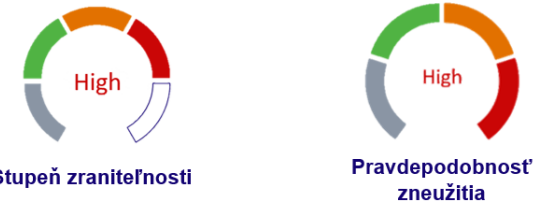
Služba Ares

CSIRT.SK

1. Služba **penetračného testovania** a bezpečnostného auditu **konfigurácie**
2. Invazívne **testovanie zraniteľností (**predchádza mu **Dohoda)**
3. Podrobný opis nálezu aj tzv. **Proof of Concept** a **odporúčania** na nápravu

1.1. XML external entity (XXE) injection

Hodnotenie zraniteľnosti



Zistený stav

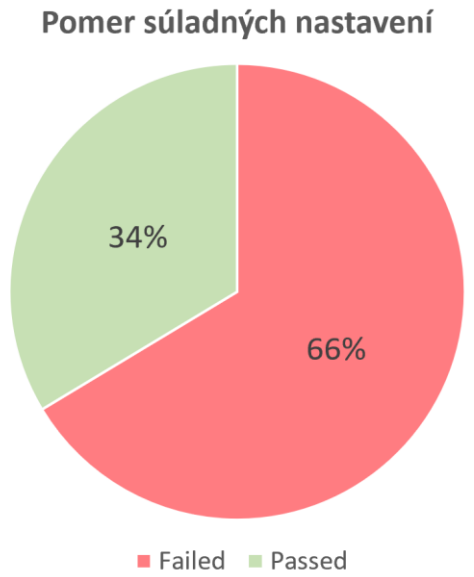
Úpravou XML údajov spracovávaných aplikáciou je možné pristúpiť k súborom v súborovom systéme servera. SampleReader nemá predvolene zakázané XXE.

ARES
by CSIRT.SK
ATTACK TO PROTECT

Bezpečnostný audit konfigurácie

CSIRT.SK

1. Overovania súladu konfigurácie s tzv. **CIS benchmarks**
2. Neinvazívne **testovanie odporúčaných nastavení**
3. Opis nálezov aj s **odporúčaniami na nápravu**
4. Najčastejšie **doménový radič** (Windows AD) alebo **firewall**



CIS Windows Server 2022 3.0.0 Benchmark Audit

ID	Category	Name	Severit	R	F	Test Result	Severit
1.1.4	Account Policies	Minimum password length	Medium	13	14	Failed	Medium
1.1.5	Account Policies	Password must meet complexity requirements	Passed	1	1	Passed	Medium

Zhrnutie

CSIRT.SK

1. Dávajte si pozor na **falošný pocit bezpečnosti**
2. Triáda (technológie + **procesy + ľudia**)
3. Využite naše služby, ktoré poskytujeme **bezodplatne**
4. Začnite už dnes registráciou do služby **Achilles**

ΛCHILLΣS

Achilles

Afrodita

Ares