



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Správa zraniteľností a kybernetických hrozieb

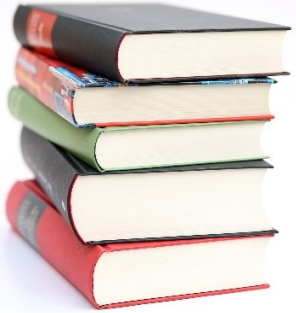
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

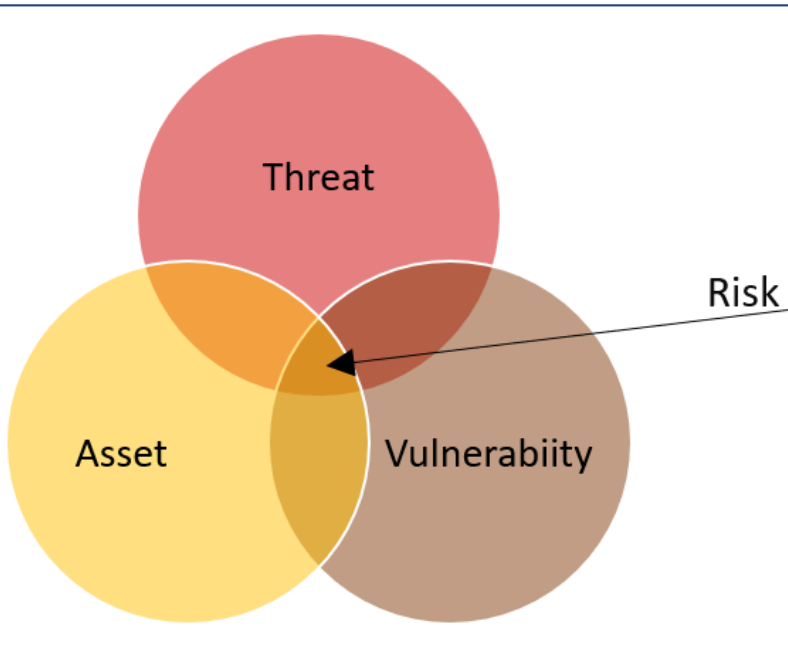
KC KYB UNIZA, <https://kc.uniza.sk/>

Jana.Uramova@fri.uniza.sk



Ciele

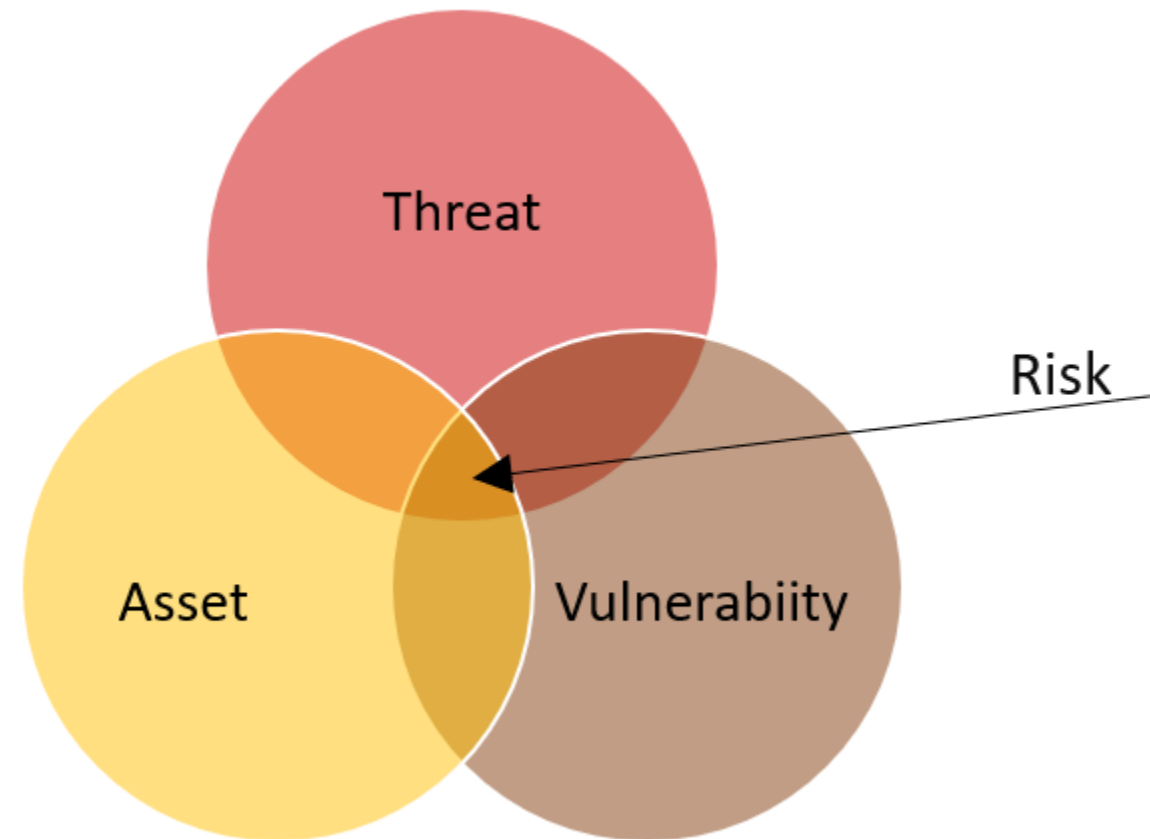
- Pochopiť, kde správa zraniteľností (Vulnerability Management, VM) zapadá do širšieho rámca riadenia rizík (NIST CSF, ISO 27001/27002, CIS).
- Oboznámiť sa s právnymi/prevádzkovými požiadavkami v SR (zákon + vyhláška) relevantnými pre VM a povinnosti prevádzkovateľov ZS a KZS.
- Poznať hlavné triedy nástrojov a procesov pre identifikáciu, hodnotenie a mitigáciu zraniteľností (skenery/nástroje, patch management, konfigurácia, pen-test).
- Získať praktický plán (checklist), ktorý možno preniesť do interného procesu.



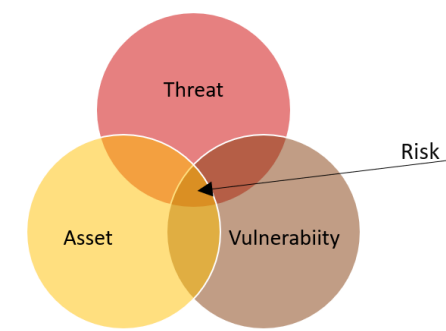
Úvod a nadviazanie na predošlé témy

Aktíva, zraniteľnosti, hrozby

- Manažér KB chce byť pripravený na akýkoľvek typ útoku
 - zabezpečiť aktíva siete organizácie.
- Na tento účel je potrebné identifikovať:
 - **Aktíva (assets)** - Všetko, čo má pre organizáciu hodnotu a musí byť chránené, vrátane serverov, infraštruktúrnych zariadení, koncových zariadení a najväčšieho aktíva – údajov a iného duševného vlastníctva
 - **Zraniteľnosti (vulnerabilities)** - Slabé miesto v systéme alebo jeho dizajne, ktoré by mohol útočník zneužiť.
 - **Hrozby (threats)** - Akékoľvek potenciálne nebezpečenstvo pre aktívum.



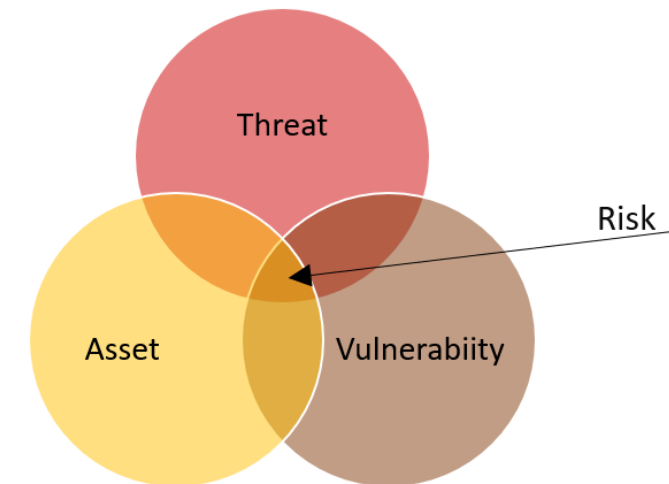
Hrozba, zraniteľnosť a riziko



Pojem	Vysvetlenie
Threat	Potenciálne nebezpečenstvo pre aktívum (údaje alebo samotnú sieť).
Vulnerability	Slabé miesto v systéme alebo jeho dizajne, ktoré môže byť zneužitá hrozbou.
Attack Surface	Celkový súčet zraniteľností v danom systéme, ktoré sú prístupné útočníkovi. Opisuje rôzne miesta, kde by sa útočník mohol dostať do systému a kde by mohol získať údaje zo systému.
Exploit	Mechanizmus, ktorý sa používa na využitie zraniteľnosti s cieľom kompromitovať aktívum. Zneužitia môžu byť REMOTE alebo LOCAL. Vzdialené zneužitie je také, ktoré funguje cez sieť bez predchádzajúceho prístupu k cieľovému systému. Pri lokálnom zneužití má aktér hrozby určitý typ používateľského alebo administratívneho prístupu ku koncovému systému. Nemusí to nevyhnutne znamenať, že útočník má fyzický prístup ku koncovému systému.
Risk	Pravdepodobnosť, že konkrétna hrozba zneužije určitú zraniteľnosť aktíva a spôsobí nežiadúci následok.

Identifikácia aktív

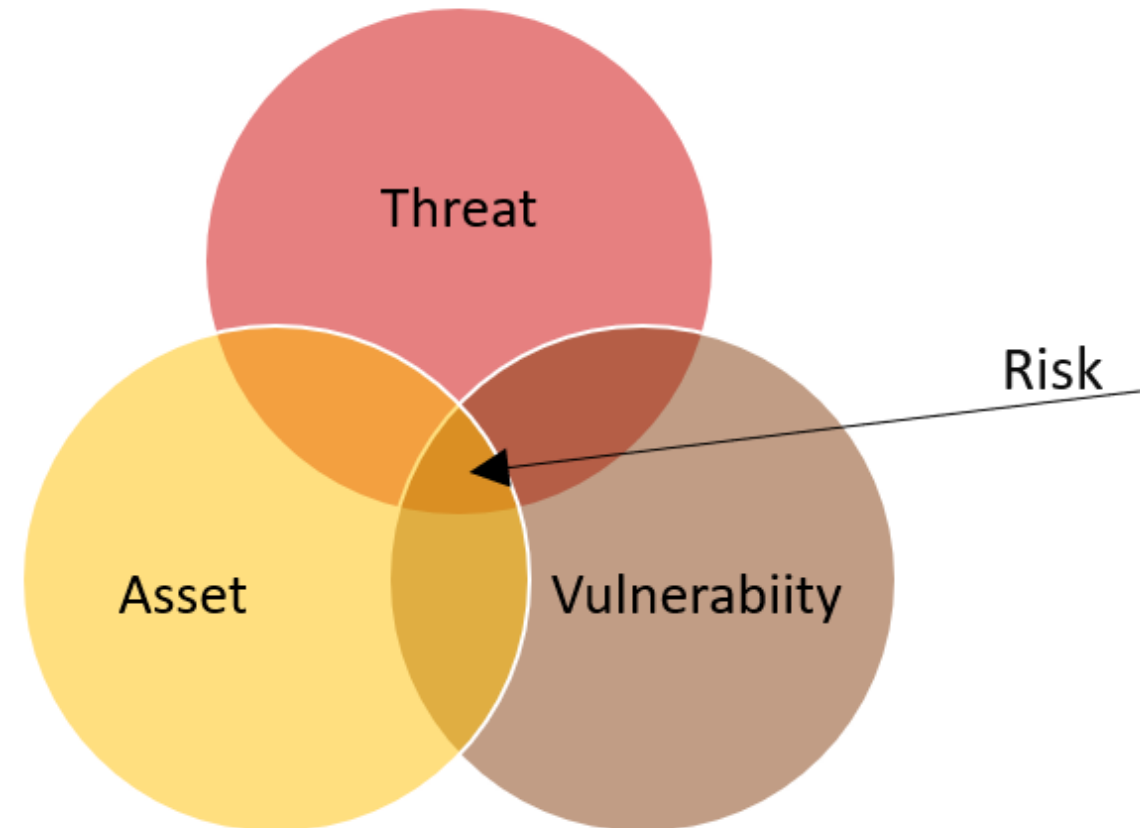
- Aktíva = súbor všetkých **zariadení** a **informácií**, ktoré organizácia vlastní alebo spravuje
- Správa aktív pozostáva z:
 - **inventarizácie** všetkých aktív
 - **posúdenia** z hľadiska úrovne ochrany potrebnej na prekazenie potenciálnych útokov
 - **vypracovania a zavedenia politík a postupov** na ich ochranu.
- Táto úloha môže byť náročná, keďže mnohé organizácie musia chrániť:
 - **interných** používateľov a zdroje,
 - **mobilných** pracovníkov
 - **cloudové** a virtuálne služby.
- Okrem toho musia organizácie určiť:
 - **kde** sú uložené kritické informačné aktíva
 - **ako** sa k nim získava prístup
- Informačné aktíva sa **líšia**, rovnako ako hrozby voči nim.
 - každé z týchto aktív môže prilákať **rôznych útočníkov**,
 - ktorí majú **rôzne úrovne zručností a motivácie**.



Prečo je manažovanie zraniteľností dôležité

Identifikácia zraniteľností a hrozieb

- Identifikácia hrozieb poskytuje organizácii **zoznam možných hrozieb** pre **konkrétne** prostredie.
- Pri identifikácii hrozieb je dôležité položiť si niekoľko otázok:
 - **Aké sú možné** zraniteľnosti systému?
 - **Kto** môže chcieť tieto zraniteľnosti **zneužiť** na prístup ku konkrétnym informačným aktívam?
 - Aké sú **dôsledky (impact)**, ak sa zraniteľnosti systému zneužijú a naruší sa CIA pre aktíva?





Konceptuálny rámec pre riadenie zraniteľností

Riadenie zraniteľností (Vulnerability Management, VM)

- VM je proces:

identifikácia → hodnotenie → priorizácia → mitigácia → overenie

- a súčasť riadenia technických rizík v rámci:
 - NIST SP 800-40 — Creating a Patch and Vulnerability Management Program
 - NIST SP 800-30 — Guide for Conducting Risk Assessments
 - NIST Cybersecurity Framework (CSF) — core functions and mapping (Identify/Protect/Detect/Respond)
 - ISO/IEC 27002:2022 — Annex A / Control 8.8 Management of technical vulnerabilities
 - CIS Controls — Continuous Vulnerability Management (Control 7)
 - Zákon o KB č. 69/2018 Z.z. (novel. 366/2024 Z. z.)
+ Príloha č. 1 k vyhláške 227/2025 Z. z.:
Rozsah bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona



Zákon o KB č. 69/2018 Z.z., novelizácia 366/2024 Z. z.

Zákon o KB 69/2018, novelizácia 366/2024

Čl. I

§ 1 Predmet zákona

Tento zákon upravuje



a) podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä

1. postavenie a povinnosti prevádzkovateľa základnej služby,
2. bezpečnostné opatrenia,
3. **hlásenie** kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a **zraniteľnosti**,
4. riešenie kybernetického bezpečnostného incidentu,
5. opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,

Pojem zraniteľnosť

§ 3 Vymedzenie základných pojmov

(1) Na účely tohto zákona sa rozumie

....

- q) **zraniteľnosťou** akýkoľvek **nežiaduci stav** alebo **chyba** technického prostriedku alebo programového prostriedku, alebo **nedostatok procesu** vrátane **nesprávnej bezpečnostnej konfigurácie**, ktorá môže byť zneužitá kybernetickou hrozbou,



Povinnosti NBU v kontexte zraniteľnosti



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

§ 5 Úrad

(1)

Úrad v oblasti kybernetickej bezpečnosti

- s) **prijíma vnútroštátne hlásenia** o kybernetických bezpečnostných incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a o **zraniteľnostiach**,

- t) **prijíma hlásenia** o kybernetických bezpečnostných incidentoch, kybernetických hrozbách a **zraniteľnostiach zo zahraničia** a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,

Úloha CSIRT pre verejné SaIS v kyber. priestore SR v kontexte zraniteľností

§ 6 Národná jednotka CSIRT

(5) Úrad prostredníctvom národnej jednotky CSIRT na účely **zverejňovania zraniteľností** alebo zamedzenia ich zneužitia plní úlohu koordinátora vo veciach komunikácie o zistených alebo nahlásených zraniteľnostiach medzi PZS, výrobcom alebo dodávateľom produktu IKT alebo služby IKT a inými dotknutými osobami.

- a) identifikuje a kontaktuje dotknuté osoby,
- b) **komunikuje o zraniteľnosti** s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT,
- c) **oznamuje PZS zraniteľnosť**, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužitelnosti; opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté,
- d) poskytuje **pomoc** osobám **oznamujúcim zraniteľnosti**,
- e) riadi zverejňovanie zraniteľností



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

(6) Úrad zabezpečí, aby bolo možné oznamovať zraniteľnosti **aj prostredníctvom JIS KB** vrátane **anonymných** oznámení a na žiadosť oznamovateľa zabezpečí zachovanie jeho anonymity vo vzťahu k oznámeným skutočnostiam.

(7) Ak ide o **zraniteľnosť** týkajúcu sa služby, ku ktorej vykonáva služby jednotka CSIRT v inom členskom štáte Európskej únie, postúpi úrad oznámenie o zraniteľnosti tejto jednotke CSIRT a informuje o tom oznamovateľa.

(8) Úrad prostredníctvom CSIRT vykonáva **neinvazívne zisťovanie a hodnotenie zraniteľností verejne prístupnej siete a informačného systému v kybernetickom priestore Slovenskej republiky,**



Národná stratégia v kontexte zraniteľnosti

§ 7 Národná stratégia kybernetickej bezpečnosti a národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy

(2) Národná stratégia kybernetickej bezpečnosti obsahuje najmä

...

e) identifikáciu opatrení na zabezpečenie pripravenosti a **schopnosti reakcie na** kybernetické hrozby, **zraniteľnosti** a kybernetické bezpečnostné incidenty a zotavenia z nich vrátane spolupráce medzi verejným sektorom a súkromným sektorom,

...

(3) V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie

...

c) **riadenia zraniteľností** vrátane podpory a sprostredkovania koordinovaného **zverejňovania zraniteľností**,

Úloha CSIRT v kontexte zraniteľnosti



§ 15 Úlohy jednotky CSIRT

...

(2) Preventívne služby sa zameriavajú na **prevenciu** kybernetických bezpečnostných **incidentov**

...

- d) **monitorovaním a evidenciou zraniteľnosti**, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov,
- i) **vykonávaním neinvazívneho zisťovania a hodnotenia zraniteľnosti** verejne prístupnej siete a informačného systému v rozsahu pôsobnosti jednotky CSIRT podľa odseku 1, ktoré nemá negatívny vplyv na tieto siete a informačné systémy, ako ani na služby, ktoré poskytujú a činnosti, ktoré zabezpečujú,
- j) vykonávaním **hodnotenia zraniteľnosti**, ktoré boli zistené podľa písmena h), po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

Povinnosti PZS v kontexte zraniteľností

§ 19 Povinnosti prevádzkovateľa základnej služby

(6) Prevádzkovateľ základnej služby je ďalej povinný

- h) vytvoriť a zaviesť **účinný mechanizmus včasného informovania** štatutárneho orgánu a zodpovedných vedúcich zamestnancov o kybernetických hrozbách, **zraniteľnostiach**, kybernetických bezpečnostných incidentoch, udalostiach odvrátených v poslednej chvíli, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrovania rizík s cieľom dodržiavania tohto zákona,



Povinnosti PZS v kontexte zraniteľnosti



§ 24 Hlásenia

(5) Prevádzkovateľ základnej služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti **hlási aj**

a) významnú kybernetickú hrozbu, o ktorej sa dozvie,

b) udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident,

c) **zraniteľnosť** ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika.

1 z 18 bezpečnostných opatrení

§ 20 Bezpečnostné opatrenia

(1) ... prijímajú sa s cieľom

a) **identifikovať** zraniteľnosti, kybernetické hrozby a riziká,

...

d) **reagovať** na identifikované zraniteľnosti a kybernetické bezpečnostné incidenty a minimalizovať ich vplyv na siete a informačné systémy a

...

(2) Bezpečnostné opatrenia sa prijímajú aspoň pre

...

b) **správu zraniteľností a kybernetických hrozieb,**

...



Príloha č. 1 k vyhláške 227/2025 Z. z.: „Rozsah bezpečnostných opatrení pre oblasti KB podľa § 20 ods. 2 zákona“

Položka	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb podľa § 20 ods. 2 písm. b) zákona prijíma PZS tak, že:	IKT – PZS	IKT – PKZS	OT – PZS	OT – PKZS
12	je zabezpečená informovanosť o identifikovaných kybernetických hrozbách s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie (IKT) a operačné technológie (OT)	ÁNO	ÁNO	ÁNO	ÁNO
13	sú získavané informácie o zraniteľnostiach používaných informačných systémov vrátane hodnotenia, do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu	ÁNO	ÁNO	ÁNO	ÁNO
14	je najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností	ÁNO	-	ÁNO	ÁNO
15	je najmenej raz za 6 mesiacov vykonávané pravidelné posudzovanie zraniteľností	-	ÁNO	-	-
16	sú určené priority aktualizácií na základe posúdenia rizík a analýzy vplyvov	ÁNO	ÁNO	ÁNO	ÁNO
17	na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností	-	ÁNO	-	ÁNO



Databáza zraniteľností

Oblasti záujmu (KB je jedna z nich)

MITRE corporation

- * 1958, nezisková spoločnosť z USA, ktorá slúži ako **objektívny poradca** v oblasti systémového inžinierstva pre vládne agentúry, vojenské aj civilné
 - Považuje sa za dôveryhodnú pri poskytovaní výsledkov a odporúčaní založených na údajoch bez konfliktu záujmov
- zjednotenie **vlády, priemyslu a akademickej obce** na spoluprácu pri riešení veľkých spoločenských výziev, od reakcie na pandémie cez bezpečnosť na diaľniciach, sociálnu spravodlivosť až po KB
- prevádzkované federálne financované výskumné a vývojové centrá (FFRDCs)
 - v súčasnosti MITRE prevádzkuje šesť zo 42 existujúcich FFRDC



Aerospace



AI & Machine Learning



Aviation & Transportation



Cybersecurity



Defense & Intelligence



Government Innovation



Health



Homeland Security



Telecom

Common Vulnerabilities and Exposures (CVE) Database

- Americká vláda sponzorovala **MITRE Corporation**, aby vytvorila a spravovala katalóg známych bezpečnostných hrozieb s názvom Common Vulnerabilities and Exposures (**CVE**).
- Zámer programu CVE pre verejne známe bezpečnostné zraniteľnosti je:

identifikovať a definovať

definuje jedinečné CVE identifikátory

katalogizovať a uchovať

k dispozícii je 296 000 záznamov CVE, ktoré je možné vyhľadať a stiahnuť

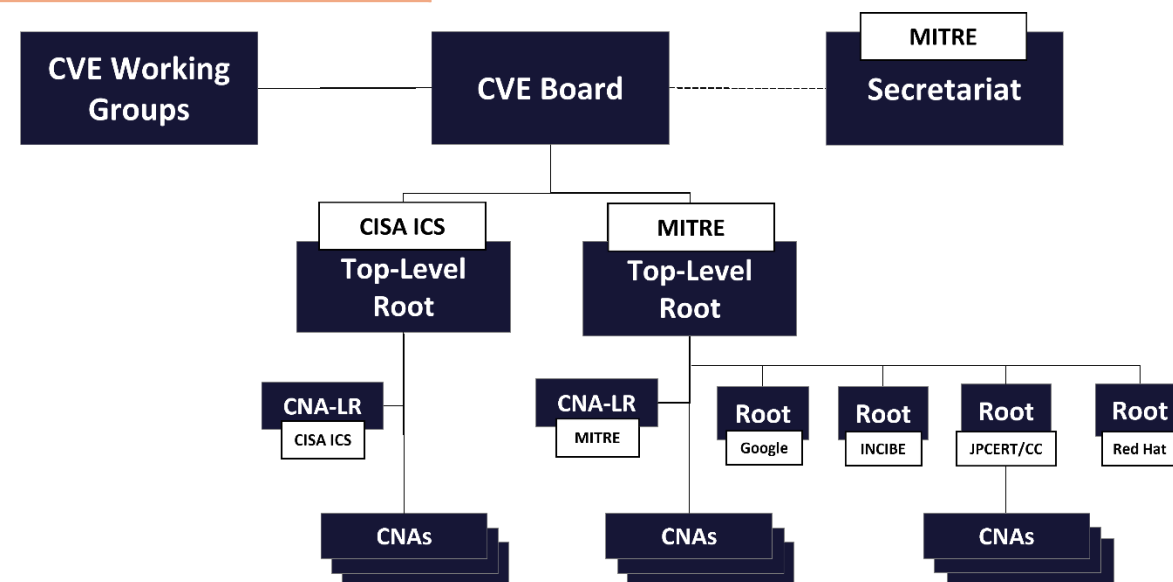
Root – **manažérske** funkcie

CNA (CVE Numbering Authority) – **operačné** funkcie

Každý [CVE záznam](#) obsahuje:

- CVE ID [číslo](#) so štyrmi alebo viacerými číslicami v časti poradového čísla daného ID (napr. „CVE-1999-0067“, „CVE-2014-12345“, „CVE-2016-7654321“).
- Stručný [popis](#) chyby zabezpečenia
- Akékoľvek relevantné [referencie](#) (t. j. správy o zraniteľnosti a upozornenia).
- Stav: Rezervované/Zverejnené/Odmietnuté

<https://www.cve.org/>



Rejected CVE

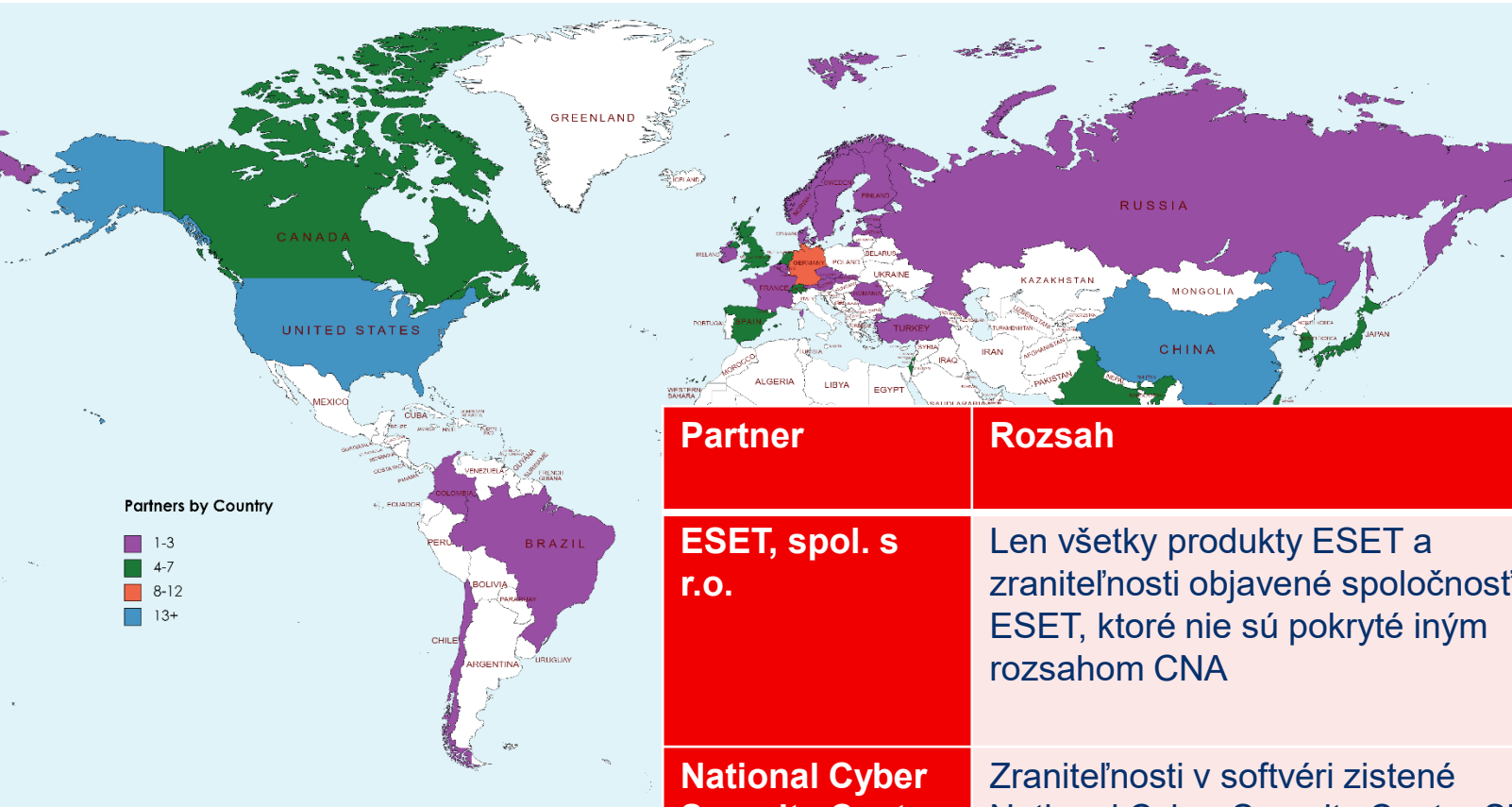
Podľa pravidiel MITRE a CNA sa záznam označí ako **REJECTED** v týchto prípadoch:

- **Chyba pri pridelovaní**
 - CVE identifikátor bol pridelený **omylom**, hoci zraniteľnosť v skutočnosti neexistovala.
 - Typické pri „false positive“ alebo nesprávne interpretovanom správaní softvéru.
- **Duplicitné zadanie**
 - Rovnaká zraniteľnosť bola nahlásená **viackrát** a dostala viac CVE ID.
 - V takom prípade sa necháva jedno „platné“ CVE, ostatné sa označia ako **REJECTED** s odkazom na správny záznam.
- **Nespĺňa kritériá CVE**
 - Hlásený problém sa nakoniec vyhodnotí ako „nepredstavuje bezpečnostnú zraniteľnosť“ podľa pravidiel CVE Programu.
 - Napríklad ide o funkčnú chybu, **neškodný bug** alebo správanie mimo scope CVE.
- **Administratívne dôvody**
 - Niektoré CVE ID sa **alokujú dopredu** (pre vendorov alebo pre konkrétny časový rámec). Ak sa nakoniec nepoužijú, vrátia sa späť a označia sa ako **REJECTED**.

"This candidate was rejected. Reason: It was a duplicate of CVE-XXXX-YYYY."

Viac ako 476 partnerov z **35** krajín participuje

Sú CNA partneri aj zo SR?



<https://www.cve.org/ProgramOrganization/CNAs>

<https://www.cve.org/PartnerInformation/ListofPartners>

Partner	Rozsah	Rola programu	Typ organizácie	Krajina*
ESET, spol. s r.o.	Len všetky produkty ESET a zraniteľnosti objavené spoločnosťou ESET, ktoré nie sú pokryté iným rozsahom CNA	CNA	Dodávatelia a projekty, výskumníci zraniteľností	Slovak Republic
National Cyber Security Centre SK-CERT	Zraniteľnosti v softvéri zistené National Cyber Security Centre SK-CERT a zraniteľnosti nahlásené National Cyber Security Centre SK-CERT na koordinované zverejnenie, ktoré nie sú v pôsobnosti iného CNA	CNA	Národné a priemyselné CERTs	Slovak Republic

Príklad: CVE s CVSS skóre

- zraniteľnosť protokolu DES a 3DES:

CVE-2016-2183 Detail

Current Description

The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **7.5 HIGH**

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

QUICK INFO

CVE Dictionary Entry:

[CVE-2016-2183](#)

NVD Published Date:

08/31/2016

NVD Last Modified:

08/16/2022

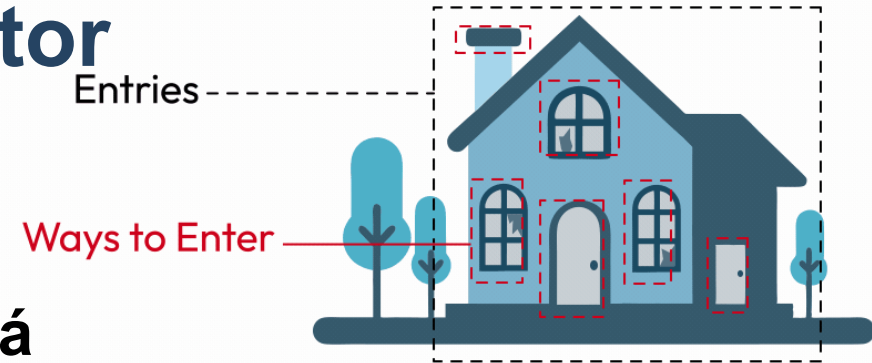
Source:

Red Hat, Inc.

Vector = Attack vector = Access Vector

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



- spôsobu, akým môže byť zraniteľnosť zneužitá
- odkiaľ alebo akým spôsobom útočník môže spustiť útok, aby zraniteľnosť využil
- hlavné typy **attack vectorov** v CVE/ NVD databázach (podľa CVSS – Common Vulnerability Scoring System)
 - **Network (N)** – zraniteľnosť môže byť zneužitá cez sieť (napr. internet, LAN).
 - **Adjacent (A)** – útočník musí byť „blízko“ v sieti (napr. v rovnakej Wi-Fi sieti).
 - **Local (L)** – útočník musí mať lokálny prístup k systému (napr. používateľský účet alebo terminál).
 - **Physical (P)** – útočník musí fyzicky manipulovať so zariadením (napr. USB port, zariadenie).

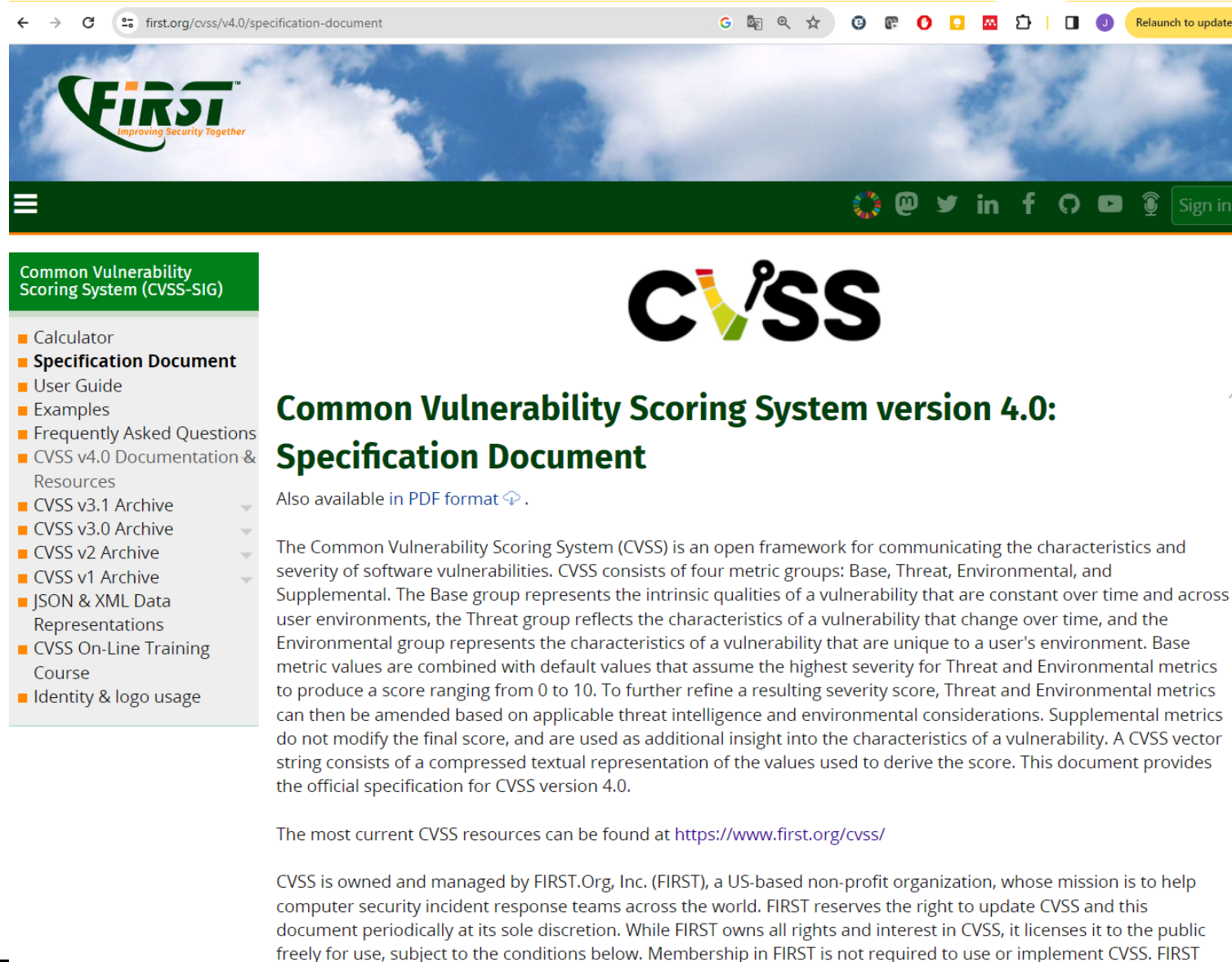


Hodnotenie zraniteľností

Common Vulnerability Scoring System (CVSS)

Prehľad o CVSS

- nástroj na hodnotenie zraniteľností (**vulnerability assessment tool**)
- uvádza spoločné **atribúty** a **závažnosť** zraniteľností
 - v počítačových hardvérových a softvérových systémoch
- poskytuje **štandardizované** skóre zraniteľnosti
- poskytuje **otvorený rámec** s metrikami, pre všetkých používateľov
- pomáha **prioritizovať** zraniteľnosti
- **FIRST** - The Forum of Incident Response and Security Teams:
 - bolo určené ako správca CVSS
 - aby podporilo jeho prijatie na celom svete



Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document**
- User Guide
- Examples
- Frequently Asked Questions
- CVSS v4.0 Documentation & Resources
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System version 4.0: Specification Document

Also available in PDF format [↗](#).

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at <https://www.first.org/cvss/>

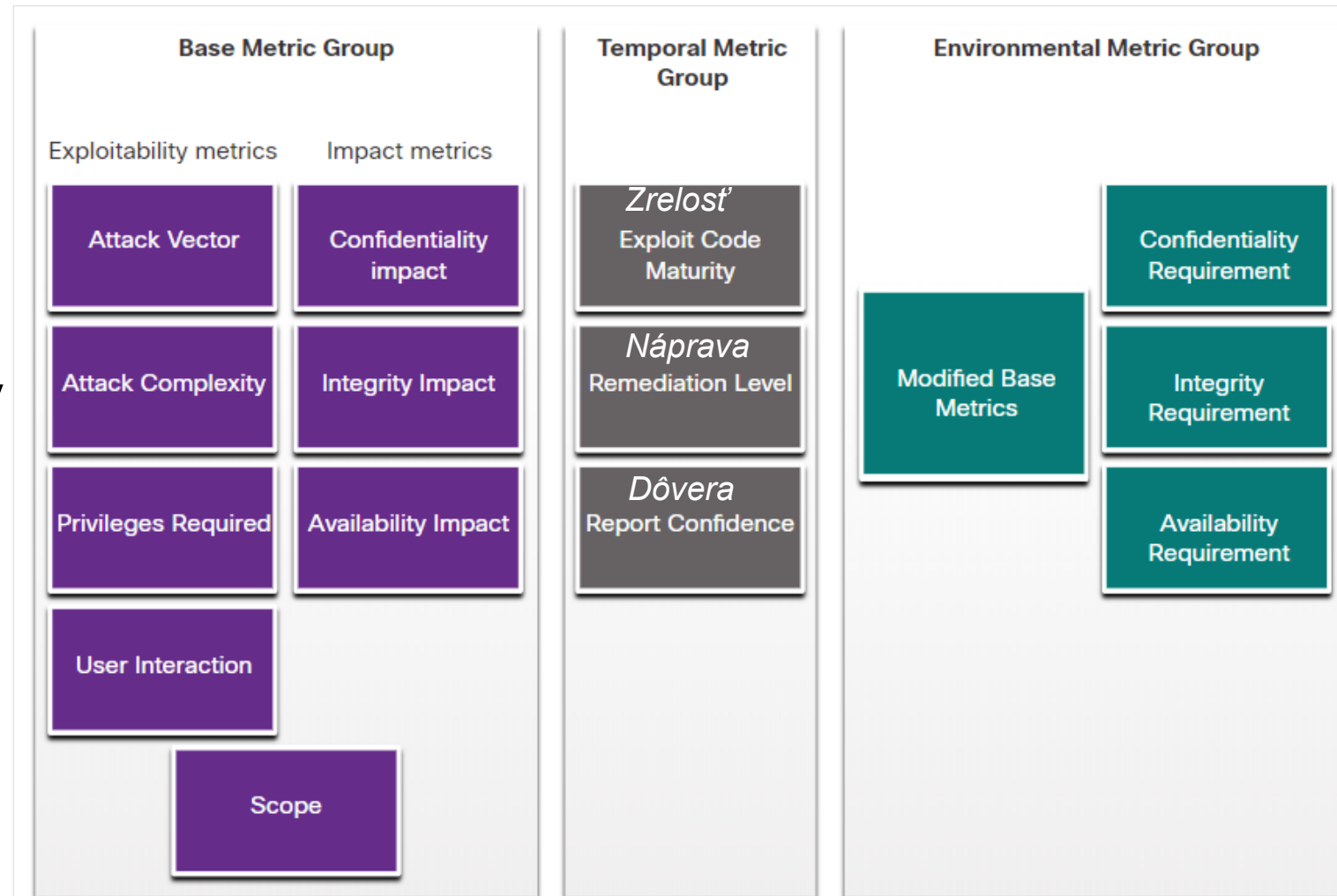
CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all rights and interest in CVSS, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST

<https://www.first.org/cvss/v4.0/specification-document>

Common Vulnerability Scoring System (CVSS)

CVSS Metric Groups

- CVSS používa tri skupiny metrík na posúdenie zraniteľností:
 - Base Metric Group:** Predstavuje charakteristiky zraniteľnosti, ktoré sú konštantné v priebehu času aj v rôznych kontextoch
 - Temporal Metric Group:** Meria charakteristiky zraniteľnosti, ktorá sa môže časom meniť, ale nie v používateľských prostrediach
 - Environmental Metric Group:** Meria aspekty zraniteľnosti, ktoré sú špecifické v prostredí konkrétnej organizácie



Proces CVSS

- Proces CVSS využíva nástroj s názvom **CVSS v4.0 Calculator**
- **Calculator** je ako **dotazník**, v ktorom sa robia voľby popisujúce zraniteľnosť v každej skupine metrík
- Neskôr sa **vygeneruje skóre** a zobrazí sa číselné hodnotenie závažnosti

Ukážka pre výpočet podľa CVSS v4.0 Calculator

3.8
(Low)

Base Score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

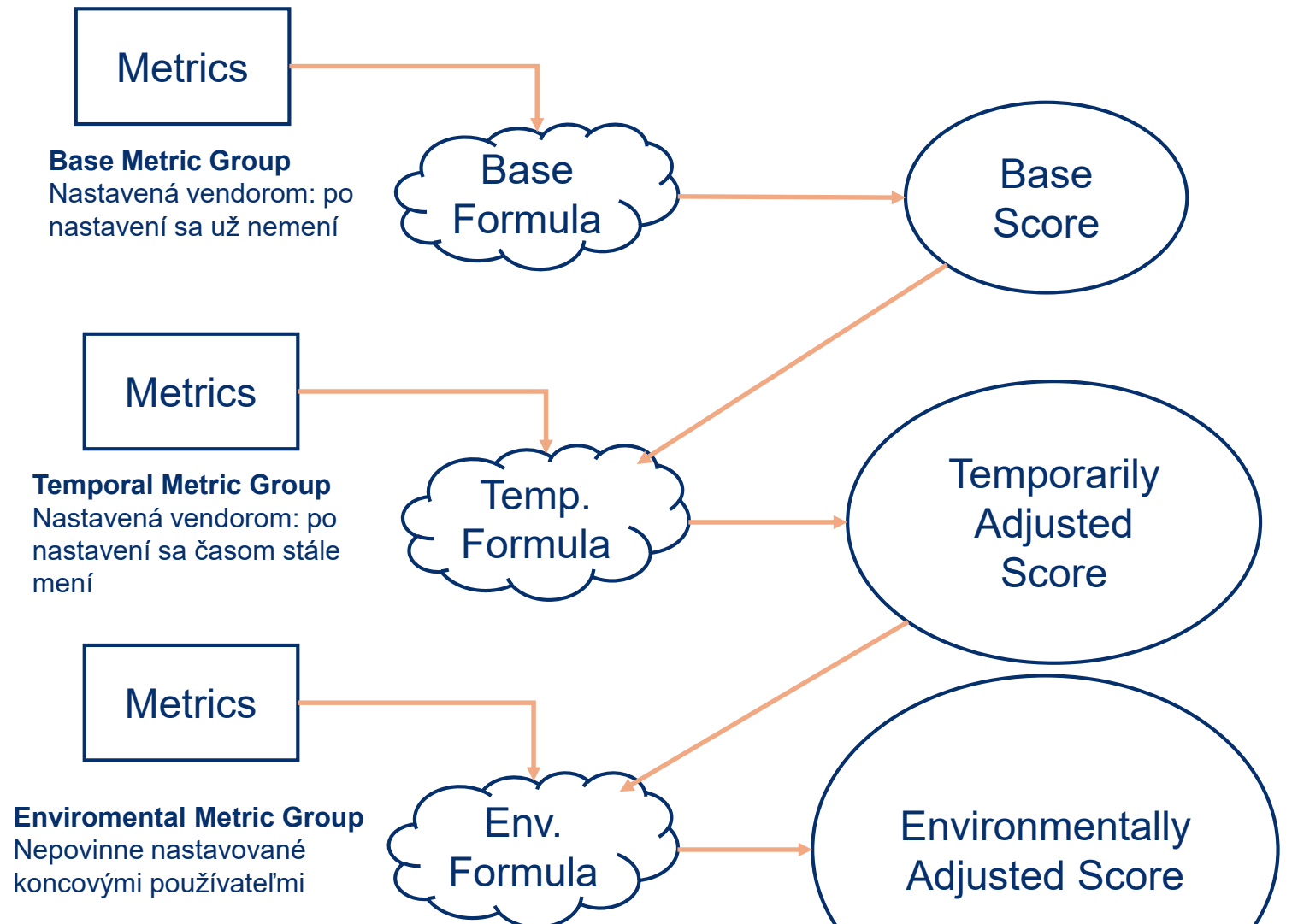
Availability (A)

None (N) Low (L) High (H)

Vector String - CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:A/A:N

Proces CVSS (Pokr.)

- Po vyhodnotení skupiny **Base Metric Group**:
 - Sa vyhodnotia hodnoty skupín **Temporal** a **Environmental Metric Group**
 - A tie modifikujú výsledky Base Metric Group
 - aby poskytli celkové skóre.



Common Vulnerability Scoring System (CVSS)

CVSS Reports



- Čím **vyššie** je hodnotenie závažnosti =>
 - tým väčší je potenciálny **dopad** zneužitia
 - tým väčšia je **naliehavosť** riešenia tejto zraniteľnosti.
- Akákoľvek zraniteľnosť presahujúca 3.9 by sa **mala riešiť**.
- Rozsahy pre CVSS skóre a zodpovedajúci kvalitatívny význam je uvedený v tabuľke >>

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

!!! CVSS > 3.9 !!!

Common Vulnerability Scoring System (CVSS)

Skenery/nástroje majú svoje určovanie „severity“



- Príklad: GVM Severity
 - Mapovanie CVSS (z NVT feedu) na 3 kategórie

Rating	CVSS Score
Log	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical (len v novších verziách)	9.0 – 10.0
False Positive / Error	označenie výsledku ako chybový alebo nerelevantný

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

!!! CVSS > 3.9 !!!

Ďalšie informačné zdroje o zraniteľnostiach

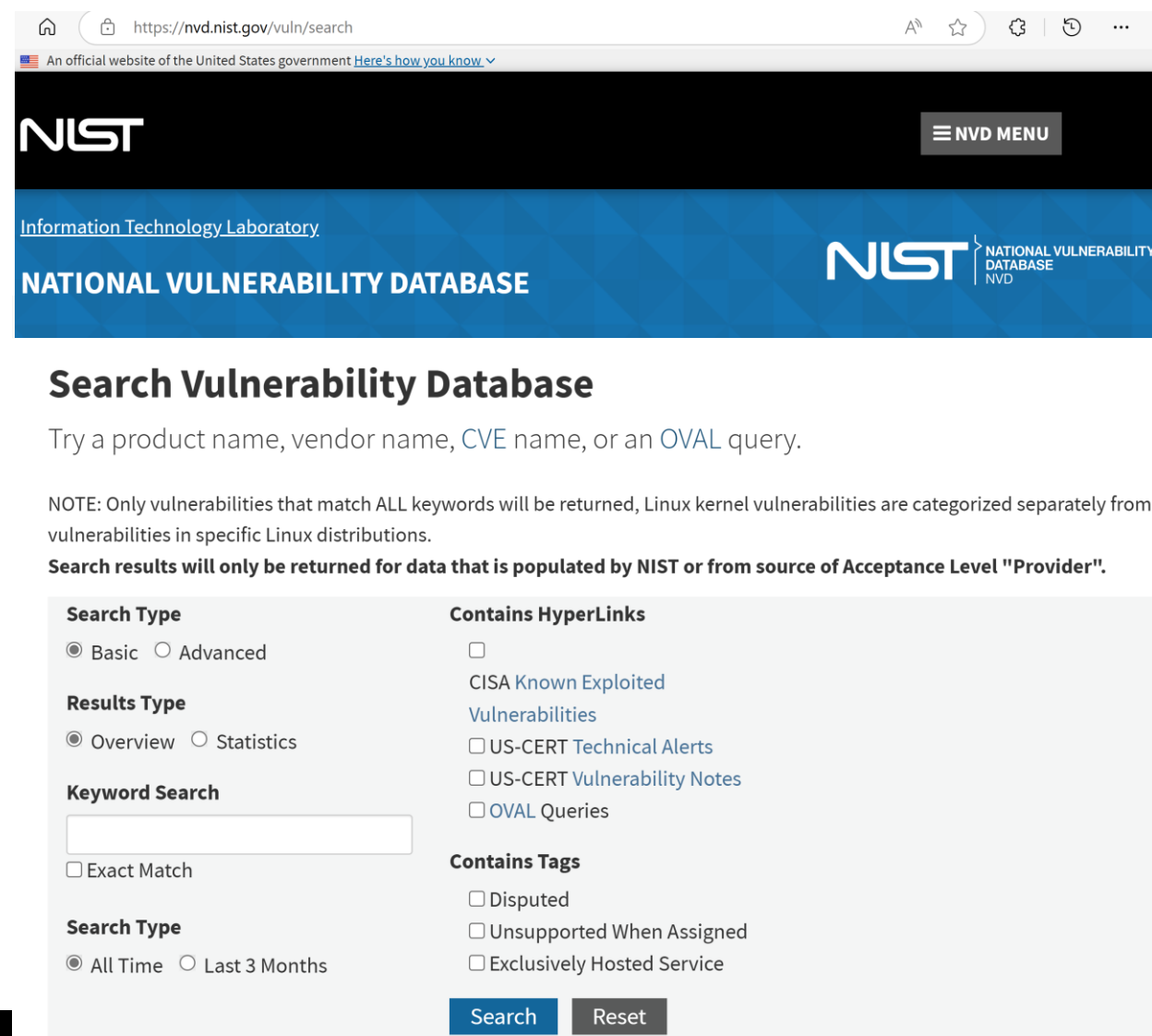
National Vulnerability Database (NVD)

Skóre CVSS **nie je uvedené** v zozname CVEs na <https://www.cve.org/>

- Je uvedené v inej databáze, tzv. NVD:

National Vulnerability Database (NVD):

- využíva identifikátory CVE a poskytuje dodatočné informácie o zraniteľnostiach
 - skóre zraniteľností CVSS
 - technické detaily
 - dotknuté subjekty
 - zdroje na ďalšie vyšetovanie.
- Databázu vytvorila a spravuje **NIST**
 - National Institute of Standards and Technology (NIST) vlády USA



The screenshot displays the NVD search interface. At the top, there's a navigation bar with the NIST logo and a menu icon. Below it, the text 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE' are visible. The main heading is 'Search Vulnerability Database'. A search prompt asks to try a product name, vendor name, CVE name, or an OVAL query. A note specifies that only vulnerabilities matching all keywords will be returned, and Linux kernel vulnerabilities are categorized separately. Search filters include 'Search Type' (Basic/Advanced), 'Results Type' (Overview/Statistics), 'Keyword Search' (with a text input and 'Exact Match' checkbox), 'Search Type' (All Time/Last 3 Months), 'Contains HyperLinks' (CISA Known Exploited Vulnerabilities, US-CERT Technical Alerts, US-CERT Vulnerability Notes, OVAL Queries), and 'Contains Tags' (Disputed, Unsupported When Assigned, Exclusively Hosted Service). 'Search' and 'Reset' buttons are at the bottom.

<https://nvd.nist.gov/vuln/search>

Zhrnutie databáz, ich účelu a kto ich spravuje

CVE, CVSS, NVD

Skratka databázy	Úloha	Kto spravuje	Hlavný účel
CVE (Common Vulnerabilities and Exposures)	Jedinečný identifikátor pre každú známu zraniteľnosť. Např. CVE-2025-12345	MITRE	Poskytnúť jednotný identifikátor pre zraniteľnosť, aby sa o nej dalo konzistentne komunikovať
CVSS (Common Vulnerability Scoring System)	Štandard na hodnotenie závažnosti zraniteľnosti pomocou číselného skóre (0–10)	FIRST	Poskytnúť metriku, ktorá vyjadruje, ako nebezpečná je zraniteľnosť a aká je pravdepodobnosť jej zneužitia
NVD (National Vulnerability Database)	Verejná databáza, ktorá spája CVE ID s CVSS skóre, popisom, opravami a ďalšími údajmi	NIST (USA)	Centralizovaný zdroj informácií o zraniteľnostiach, umožňuje vyhľadávanie podľa produktu, skóre, vektora útoku a iné

Automatizácia, alebo.. aby to nebolo len „na papieri“

SCAP - Security Content Automation Protocol

- SCAP je súbor štandardov a špecifikácií navrhnutých tak, aby umožnili:
 - automatizovanú správu zraniteľností
 - audit konfigurácií
 - meranie stavu zabezpečenia
 - hodnotenie zhody s bezpečnostnými politikami
- Zraniteľnosť sa zhromažďuje a uchováva pomocou **SCAP**
 - vyhodnocuje informácie a priraduje jedinečné ID pre zraniteľnosť
- Verzia: 1.3
- Stav: konečný
- Špecifikácia: [NIST Special Publication \(SP\) 800-126 rev 3](#)

Nástroje SCAP:

- The SCAP Content Validation Tool
 - navrhnutý na overenie správnosti toku údajov protokolu SCAP pre konkrétny prípad použitia podľa toho, čo je definované v SP 800-126
 - Možno stiahnuť: [SCAP Content Validation Tool](#) (49 MB), SHA256 na webe..

Security Content Automation Protocol

SCAP

▪ Jazyky SCAP:

- XCCDF: The Extensible Configuration Checklist Description Format
- OVAL®: Open Vulnerability and Assessment Language
 - Hlavná súčasť štandardu SCAP
- OCIL: Open Checklist Interactive Language
- Asset Identification
- ARF: Asset Reporting Format

▪ Identifikačné schémy

- CCE™: Common Configuration Enumeration
- CPE™: Common Platform Enumeration
- Software Identification (SWID) Tags
- CVE®: Common Vulnerabilities and Exposures

▪ Metriky

- CVSS: Common Vulnerability Scoring System
- CCSS: Common Configuration Scoring System

▪ Integrita

- TMSAD: Trust Model for Security Automation Data

<https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/scap-1-3>

- OVAL sa používa na popis bezpečnostných zraniteľností alebo požadovanej konfigurácie systémov
- OVAL definície
 - definujú bezpečný stav niektorých objektov v počítači:
 - konfiguračné súbory
 - povolenia súborov
 - procesy, ...
 - sa vyhodnocujú pomocou tlmočníka nazývaného scanner
- CPE
 - slúži na identifikáciu IT platforiem a systémov pomocou jednoznačne definovaných názvov
 - zahŕňa aj metódu na kontrolu mien oproti systému a formát popisu na viazanie textu a testov na meno
- CWE
 - zoznam slabých stránok softvéru
 - poskytuje tiež informácie o prevencii, implementácii a zmiernení slabých stránok

Čoho všetkého sa týka...

Testovanie zraniteľností siete

- zahŕňa tieto 3 aktivity:

Aktivita	Popis	Nástroje a tímy
Risk analysis	Jednotlivci vykonávajú komplexnú analýzu dopadov útokov na kritické aktíva a fungovanie spoločnosti	<i>SimpleRisk, Eramba, Monarc, ...</i> Manažér rizík, špecialista na analýzu rizík, interní alebo externí konzultanti, rámce riadenia rizík.
Vulnerability Assessment	Skenovanie hostiteľa, skenovanie portov, skenovanie iných zraniteľností a služieb, manažovanie záplat/opráv (patch management)	<i>GVM (OpenVas), Rapid7, Nessus, Qualys, Nmap, Ovasp-Zap, Microsoft Baseline Analyzer, ...</i> Bezpečnostní analytici, analytici zraniteľností, systémoví administrátori.
Penetration Testing	Použitie hackerských techník a nástrojov na preniknutie cez sieťovú obranu a identifikáciu hĺbky potenciálneho prieniku	<i>Metasploit Framework, CORE Impact, Burp Suite, Aircrack-ng, ...</i> Etickí hackeri, penetrační tester, red team, bezpečnostní konzultanti.



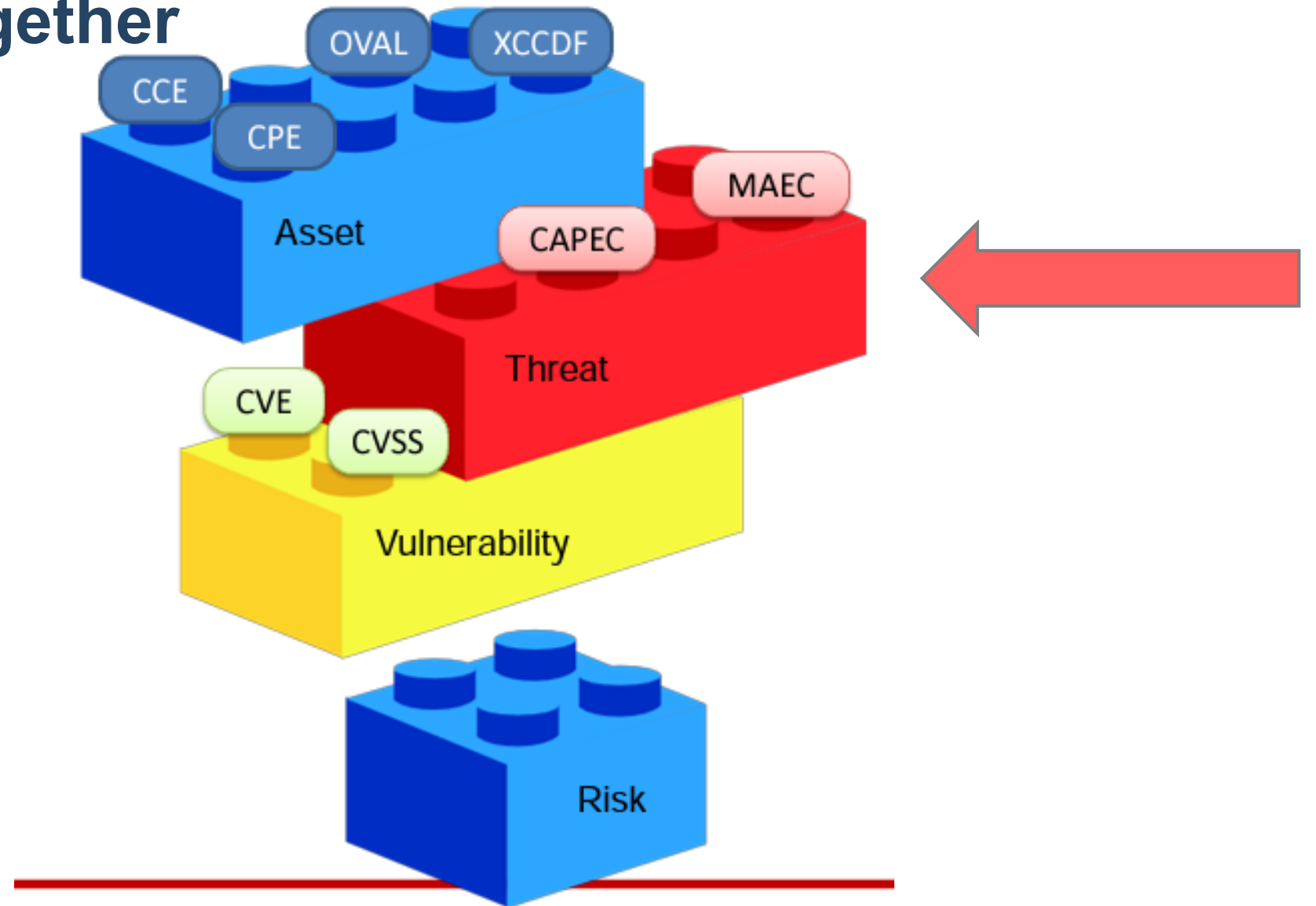
Hrozby – popis a modelovanie

Pre zdieľanie informácií o hrozbách (útoky, malvér, ...)

Ako popísať vzory útočných vektorov?

Aké štandardy a nástroje sú dostupné pre popis hrozieb?

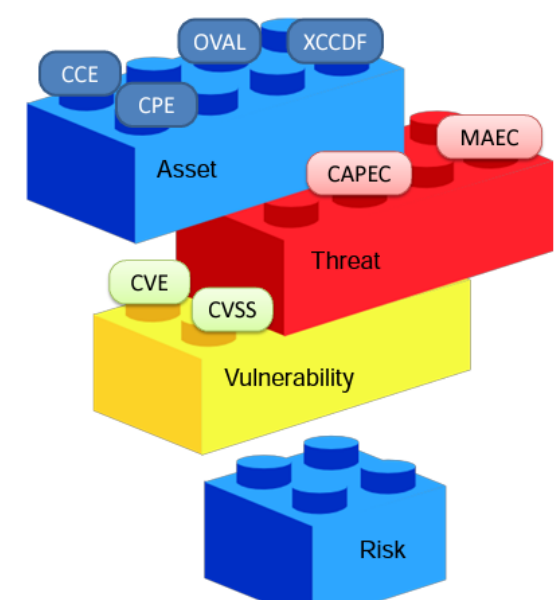
Putting it all together



Common Attack Pattern Enumeration and Classification

CAPEC

- Zdieľaný štandard indexovania pre bežné vzory útokov používané pri zneužitíach alebo malvéri
 - Databáza *útokových vzorov* – opisuje **spôsoby, ako môže útočník zaútočiť**, napr. „SQL Injection“, „Privilege Escalation“ alebo „Phishing“
 - Popis na vyjadrenie útočných vektorov
- Penetration Testing Management Platforms
 - využívajú CAPEC na mapovanie do Attack Chains, ktoré môžu byť tiež prepojené s rámcom MITRE ATT&CK
 - Aby poskytli úplný obraz
- Celkový počet vzorov útokov: 559 (zoznam ver. 3.9)
- Slúži pre threat modeling, vzdelávanie, penetračné testovanie alebo integráciu do TI platforiem.



Príklady známych vzorov útokov:

- HTTP Response Splitting ([CAPEC-34](#))
- Session Fixation ([CAPEC-61](#))
- Cross Site Request Forgery ([CAPEC-62](#))
- SQL Injection ([CAPEC-66](#))
- Cross-Site Scripting ([CAPEC-63](#))
- Buffer Overflow ([CAPEC-100](#))
- Clickjacking ([CAPEC-103](#))
- Relative Path Traversal ([CAPEC-139](#))
- XML Attribute Blowup ([CAPEC-229](#))

<https://capec.mitre.org/community/usage.html>

Integrácie CAPEC



Hlavné typy nástrojov, ktoré CAPEC využívajú:

1. Threat Modeling Tools

- **Microsoft Threat Modeling Tool** – integruje CAPEC attack patterns na podporu analýzy a identifikácie hrozieb.
- **OWASP Threat Dragon** – pri modelovaní útokov môže využiť CAPEC vzory pre kategorizáciu útokov.
- **IriusRisk** – komerčný nástroj pre threat modeling, podporuje CAPEC pre identifikáciu a klasifikáciu hrozieb.

2. Penetračné testovanie / Red Team Tools

- Niektoré komerčné penetračné testovacie platformy alebo simulátory útokov (napr. **Core Impact**, **Immunity Canvas**) odkazujú na CAPEC attack patterns pri generovaní testovacích scenárov.

3. Security Education & Research Tools

- CAPEC je často integrovaný do vzdelávacích platforiem a laboratórií, napr. MITRE ATT&CK + CAPEC pre výučbu identifikácie a prevencie útokov.
- Rôzne akademické nástroje využívajú CAPEC ako referenčný zdroj útokových vzorov pri štúdiu kybernetickej bezpečnosti.

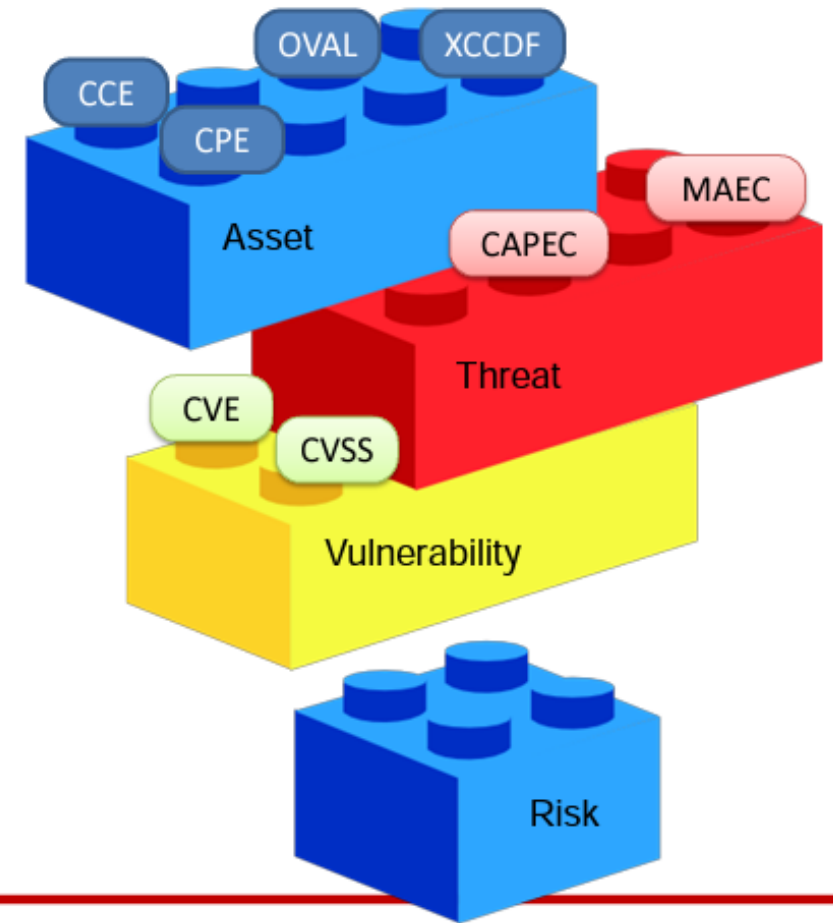
4. Vulnerability Management / Threat Intelligence Platforms

- Niektoré TI platformy a SIEM nástroje môžu importovať CAPEC attack patterns na mapovanie incidentov alebo klasifikáciu útokov podľa známych vzorov.

Štandard MAEC™



- komunitou vyvinutý štruktúrovaný jazyk
 - na kódovanie a zdieľanie verných informácií o **malvéri** na základe atribútov:
 - správania
 - artefaktov
 - vzťahov medzi vzorkami malvéru, ...
- **Výhody:**
 - Eliminácia nejednoznačnosti a **nepresnosti** v popisoch malvéru
 - Znížená duplicita úsilia o analýzu škodlivého softvéru
 - Vylepšené všeobecné **povedomie** o malvéri
 - Znížená celková doba **odozvy** na hrozby škodlivého softvéru
- Intergráciu MAEC majú rôzni dodávateľia sandboxov, EDR/CTI riešení a analytických nástrojov
- Reportovací modul Cuckoo Sandbox 2.x vytvára výstup MAEC 5.0



<https://maecproject.github.io/about-maec/>

Globálne dostupná znalostná báza o taktikách a technikách protivníka

MITRE ATT&CK (v17 – Október 2025)



- je celosvetovo dostupná vedomostná báza protivníkových taktík a techník založená na skutočnom pozorovaní
 - používa sa ako základ pre vývoj špecifických modelov hrozieb a metodológií
 - v súkromnom sektore
 - vo vládnom sektore
 - v komunite produktov a služieb kybernetickej bezpečnosti
- Aktuálna verzia **MITRE ATT&CK** je **v17.1** — platná od **22. apríla 2025**
 - ATT&CK sa priebežne aktualizuje (major-releases spravidla dvakrát ročne)

Globálne dostupná znalostná báza o taktikách a technikách protivníka

MITRE ATT&CK (v17 – Október 2025)

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (2)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Access Tokens	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Discovery	Remote Services (3)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (5)	Decobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Email Bombing
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Create or Modify System Process (5)	Deploy Container	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (2)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Debugger Evasion	Taint Shared Content	Data from Information Repositories (3)	Fallback Channels	Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Native API	Event Triggered Execution (17)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Victim-Owned Websites	WiFi Networks	Valid Accounts (4)	Scheduled Task/Job (5)	Exclusive Control	Event Triggered Execution (17)	Execution Guardrails (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
			Serverless Execution	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			Shared Modules	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	OS Credential Dumping (8)	Group Policy Discovery		Email Collection (2)	Non-Standard Port		Resource Hijacking (4)
			Software Deployment Tools	Implant Internal Image	Hide Artifacts (14)	File and Directory Permissions Modification (2)	Steal Application Access Token	Log Enumeration		Input Capture (4)	Protocol Tunneling		Service Stop
			System Services (3)	Modify Authentication Process (2)	Hijack Execution Flow (12)	Hide Artifacts (14)	Steal or Forge Authentication Certificates	Network Service Discovery		Screen Capture			System Shutdown/Reboot
			User Execution (4)	Scheduled Task/Job (5)	Process Injection (12)	Impair Defenses (11)	Steal or Forge Kerberos Tickets (5)	Network Share Discovery		Video Capture			
			Windows Management Instrumentation	Modify Registry	Scheduled Task/Job (5)	Impersonation	Steal Web Session Cookie	Network Sniffing					
				Office Application Startup (5)	Valid Accounts (4)	Indicator Removal (10)	Unsecured Credentials (3)	Password Policy Discovery					
				Power Settings		Indirect Command Execution		Peripheral Device Discovery					
				Pre-OS Boot (5)		Masquerading (11)		Permission Groups Discovery (3)					
				Scheduled Task/Job (5)		Modify Authentication Process (2)		Process Discovery					
				Server Software Component (5)		Modify Cloud Compute Infrastructure (3)		Query Registry					
				Software Extensions (2)		Modify Cloud Resource Hierarchy		Remote System Discovery					
				Traffic Signaling (2)		Modify Registry		Software Discovery (1)					
				Valid Accounts (4)		Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Location Discovery (1)					
						Obfuscated Files or Information (17)		System Network Configuration Discovery (2)					
						Plist File Modification		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (12)		System Service Discovery					
						Reflective Code Loading		System Time Discovery					
						Rogue Domain Controller		Virtual Machine Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Subvert Trust Controls (5)							
						System Binary Proxy Execution (14)							
						System Script Proxy Execution (2)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (3)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Virtualization/Sandbox Evasion (3)							
						XSL Script Processing							

•14 taktík
•211 techník
•468 sub-technik

•166 skupín (threat actor entities)
•755 softvérových nástrojov (pre realizáciu útokov)
•47 kampaní (série útokov alebo operácií, ktoré sú spojené s určitou skupinou alebo hrozbou)
•44 mitigácií (pre techniky)
•37 dátových zdrojov (Napr. logy, sieťový traffic, udalosti z antivírusu, ..)

Pomáhajú SIEM/EDR nástrojom vyhodnocovať, či sa nejaká technika deje v systéme.



CAPEC and ATT&CK by MITRE

CAPEC

- Zameriava sa na **bezpečnosť aplikácií**
- Vypočítava zneužitia proti zraniteľným systémom
 - popisuje spoločné **atribúty a techniky**
 - SQL Injection, XSS, Session Fixation, Clickjacking
- Zahŕňa social engineering / supply chain
- Súvisí s Common Weakness Enumeration (CWE)

ATT&CK

- Zameriava sa na **obranu siete**
- Založené na spravodajstve o hrozbách (threat intelligence) a výskume red tímu
- Poskytuje kontextové pochopenie škodlivého správania
 - opisuje operačné fázy v životnom cykle protivníka, pred a po zneužití (napr. Persistence, Lateral Movement, Exfiltration)
 - podrobne popisuje špecifické taktiky, techniky a postupy (**TTP**), ktoré používajú útočníci pri pokročilých a perzistentných hrozbách (**APT**)
 - na realizáciu svojich zámerov pri zacielení, kompromitovaní a fungovaní v sieti svojej obete
- Podporuje testovanie a analýzu možností obrany

CAPEC and ATT&CK by MITRE

Ako spolu súvisia...

- Mnohé vzory útokov vymenované CAPEC sú využívané protivníkmi prostredníctvom špecifických techník popísaných ATT&CK.
 - Toto umožňuje kontextové pochopenie vzorov útokov v rámci operačného životného cyklu protivníka
- Vzory útokov CAPEC a súvisiace techniky ATT&CK sa medzi sebou (v prípadoch keď je to možné a vhodné) na seba odkazujú (cross referencing)

Použite CAPEC na:

- Modelovanie hrozieb aplikácií
- Školenie a vzdelávanie vývojárov
- Penetračné testovanie

Použite ATT&CK na:

- Porovnanie obranných schopností počítačovej siete
- Obranu proti Advanced Persistent Threat (pokročilej pretrvávajúcej hrozbe)
- Hľadanie nových hrozieb (Hunting..)
- Zlepšenie spravodajstva o hrozbách
- Cvičenia emulácie protivníka

**Cyber Threat
Intelligence
(CTI)**



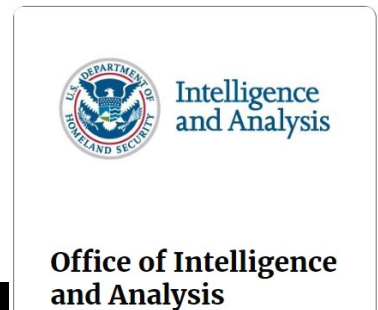
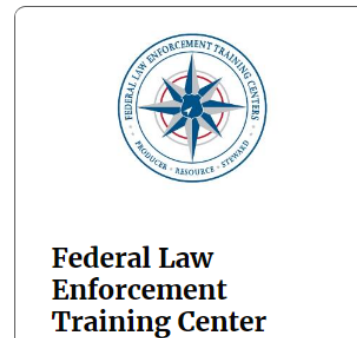
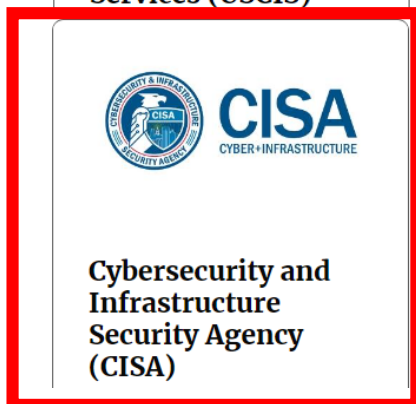
Zdieľanie informácií o hrozbách (CTI)

Ministerstvo pre vnútornú bezpečnosť USA

U.S. – Department of Homeland Security (DHS)

<https://www.dhs.gov/operational-and-support-components>

- je určené ako Sektorová agentúra pre riadenie rizík pre sektor kritických služieb, ktorý poskytuje služby v oblasti prevencie, pripravenosti, reakcie a obnovy počas každodenných operácií aj reakcie na incident
- operačné a podporné zložky, ktoré v súčasnosti tvoria DHS:



Threat Intelligence Services

Automated Indicator Sharing



Homeland
Security



CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY



- The Automated Indicator Sharing (AIS) je bezplatná služba, ktorú ponúka U.S DHS – by CISA
- AIS umožňuje **výmenu** indikátorov **kybernetických hrozieb** v reálnom čase medzi
 - U.S. Federal Government
 - a privátnym sektorom
- AIS vytvára **ekosystém**, keď je rozpoznaná hrozba
- Neskôr sa okamžite **zdieľa** s komunitou, aby im pomohla chrániť ich siete pred danou hrozbou
- Čo sa zdieľa:
 - CTIs - cyber threat indicators
 - DM - defensive measures

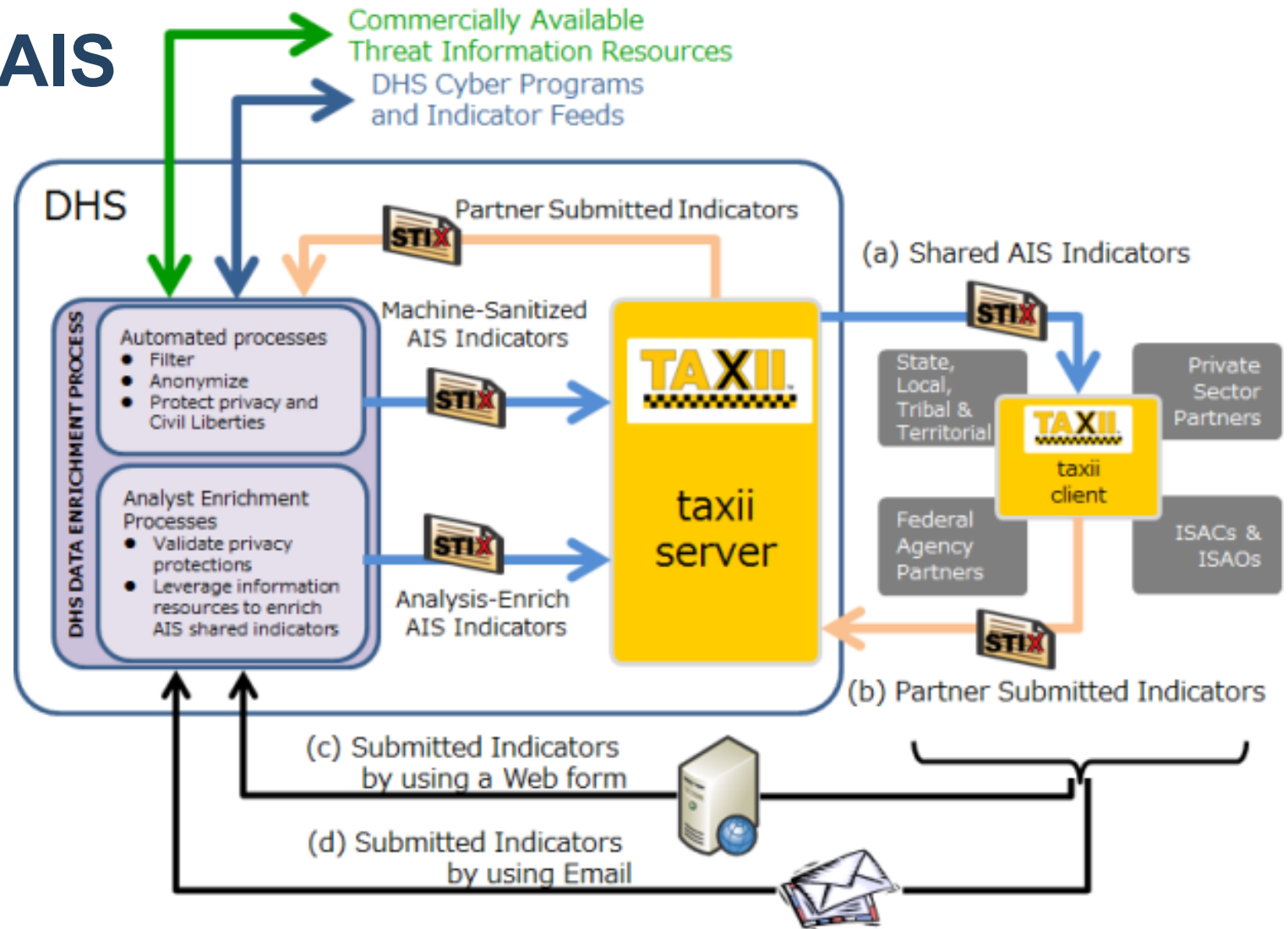
- Ako sa zdieľa:
 - Pomocou protokolov:
 - Na popis – STIX
 - Na prenos - TAXII

<https://www.cisa.gov/ais>

Automated Indicator Sharing

Open Standards for AIS

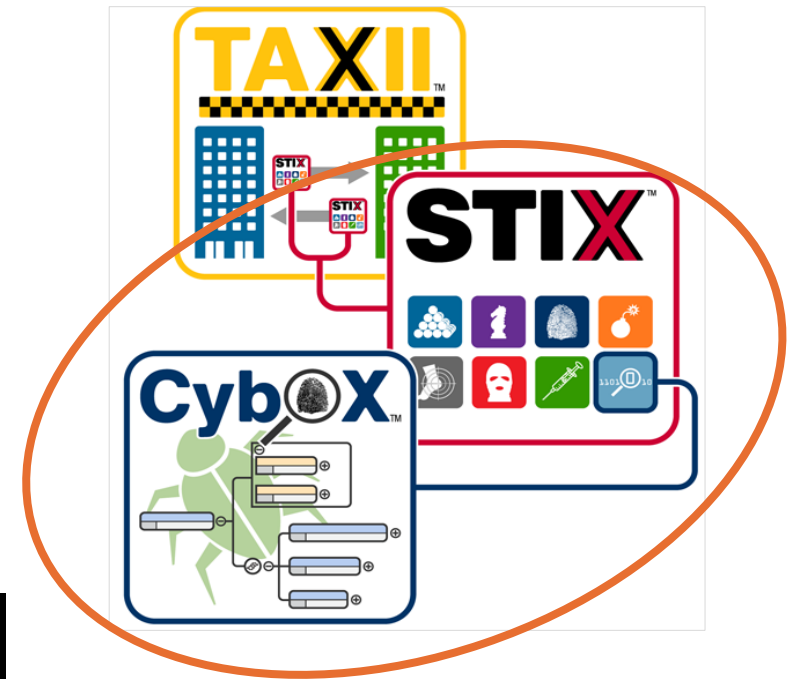
- AIS používa otvorené štandardy:
 - STIX™
Structured Threat Information Expression for CTIs and DMs information
 - dátový model na popis
 - TAXII™
Trusted Automated Exchange of CTIs for machine-to-machine communications
 - protokol aplikačnej vrstvy, ktorý umožňuje komunikáciu CTIs cez HTTPS
 - má podporu pre STIX
- CISA rešpektuje súkromie v organizácií
 - AIS pri odosielaní podaní, ich automaticky anonymizuje
 - identita predkladateľa sa nezverejňuje bez jeho predchádzajúceho výslovného súhlasu



<https://www.hitachi.com/hirt/publications/hirt-pub17007/index.html>

Štruktúra STIX 2.0

- A. STIX Domain Objects (SDO) → popisujú hrozby, útočníkov, kampane, zraniteľnosti...
- B. STIX Relationship Objects → prepájajú objekty (vzťahy)
- C. STIX Cyber-Observable Obj. → popisujú konkrétne technické artefakty (hash, IP, súbor,...)



A) STIX Domain Objects (SDOs)

Objekty, ktoré **opisujú svet hrozieb, aktérov a udalostí**:

Objekt	Popis
Attack Pattern	Vzor útoku – popisuje techniky, ktoré útočník používa (napr. z MITRE ATT&CK).
Campaign	Súbor súvisiacich útokov zameraných na rovnaké ciele alebo s rovnakým cieľom.
Course of Action	Opatrenie alebo odporúčanie, ako zmierniť alebo zabrániť útoku.
Grouping	Zoskupenie viacerých objektov STIX, ktoré patria k sebe (napr. incident + indikátory).
Identity	Popisuje organizáciu, osobu alebo skupinu (napr. firma, výskumný tím, vláda).
Incident	(Novinka v STIX 2.1) Reálna bezpečnostná udalosť, ktorá sa stala.
Indicator	Indikátor kompromitácie (IOC) – napr. hash, IP, URL spojená s hrozbou.
Infrastructure	Popisuje infraštruktúru útočníka – servery, C2 siete, domény, botnety.
Intrusion Set	Kolekcia kampaní, útokov a techník patriacich jednej skupine útočníkov.
Location	Geografické miesto (napr. krajina, mesto, región, IP geolokácia).

A) STIX Domain Objects (SDOs), pokračovanie

Objekty, ktoré **opisujú svet hrozieb, aktérov a udalostí**:

Objekt	Popis
Malware	Softvér vytvorený s cieľom poškodiť alebo zneužiť systémy.
Malware Analysis	Výsledok alebo popis analýzy malvéru (sandbox, statická analýza atď.).
Note	Ľubovoľné poznámky, komentáre alebo hodnotenia analytika.
Observed Data	Popis reálne pozorovaných údajov (napr. log z IDS, hash z detekcie).
Opinion	Vyjadrenie názoru analytika (napr. „myslím, že tento malware súvisí s APT29“).
Report	Súhrn viacerých objektov do správy (napr. mesačný CTI report).
Threat Actor	Osoba alebo skupina, ktorá realizuje útoky.
Tool	Legitímny alebo škodlivý softvér používaný v útoku (napr. Mimikatz, nmap).
Vulnerability	Slabina v softvéri alebo systéme, ktorú útočník môže využiť.

B) STIX Relationship Objects (SROs)

- Objekty, ktoré prepájajú iné STIX objekty:

Objekt

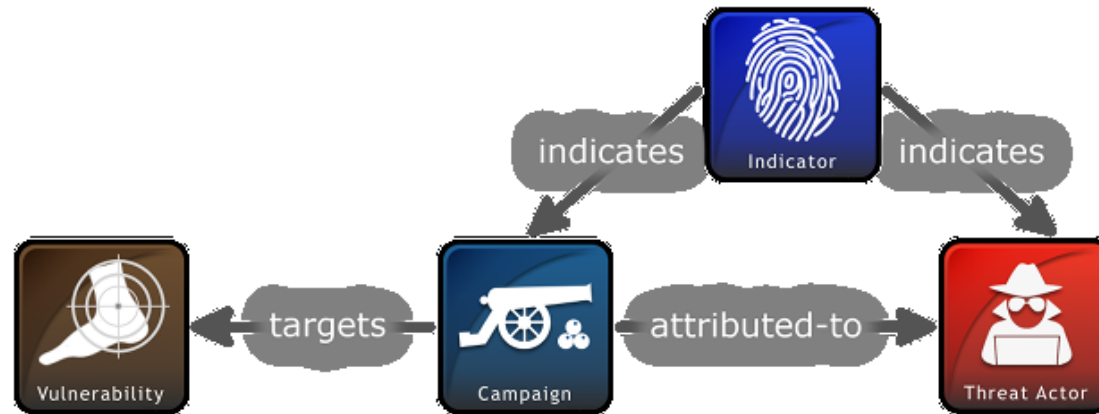
Popis

Relationship

Všeobecné prepojenie medzi dvoma objektmi (napr. „malware uses infrastructure“).

Sighting

Informácia, že konkrétny objekt (napr. IOC) bol pozorovaný v reálnom svete.



C) STIX Cyber-Observable Objects (SCOs)

- Objekty, ktoré opisujú **konkrétne technické artefakty** – sú to „CybOX“ objekty integrované priamo do STIX 2.x:
- Opisuje „čo sa stalo“ alebo „čo vidíme“
- **Účel:**
 - Umožniť, aby rôzne nástroje (IDS, SIEM, EDR, ...) hovorili rovnakým jazykom pri popise udalostí
 - aby sa observable dalo automaticky spracovať a porovnávať medzi systémami

Objekt	Popis
Artifact	Dátový artefakt – súbor, obrázok, dokument, base64 obsah.
Autonomous System	Informácie o AS (Autonomous System Number).
Directory	Adresár v súborovom systéme.
Domain Name	Doménové meno.
Email Address	E-mailová adresa.
Email Message	Celý e-mail – hlavičky, telo, prílohy.
File	Súbor (názov, hash, veľkosť, atď.).
IPv4 Address	IPv4 adresa.
IPv6 Address	IPv6 adresa.

C) STIX Cyber-Observable Objects (SCOs)

Objekty, ktoré opisujú **konkrétne technické artefakty** – sú to „CybOX“ objekty integrované priamo do STIX 2.x:

Objekt

MAC Address

Mutex

Network Traffic

Process

Software

URL

User Account

Windows Registry Key

X.509 Certificate

Popis

MAC adresa.

Synchronizačný objekt v systéme (typický pri malware).

Popis sieťovej komunikácie (TCP, UDP, porty, spojenie).

Proces bežiaci v OS (názov, PID, parent process, atď.).

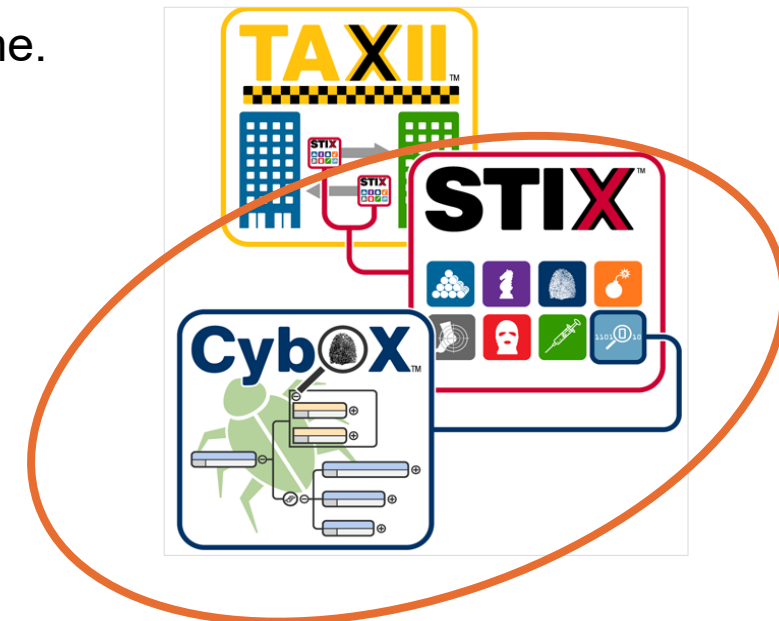
Softvér alebo aplikácia nainštalovaná v systéme.

Uniform Resource Locator.

Používateľské konto.

Kľúč alebo hodnota v registroch Windows.

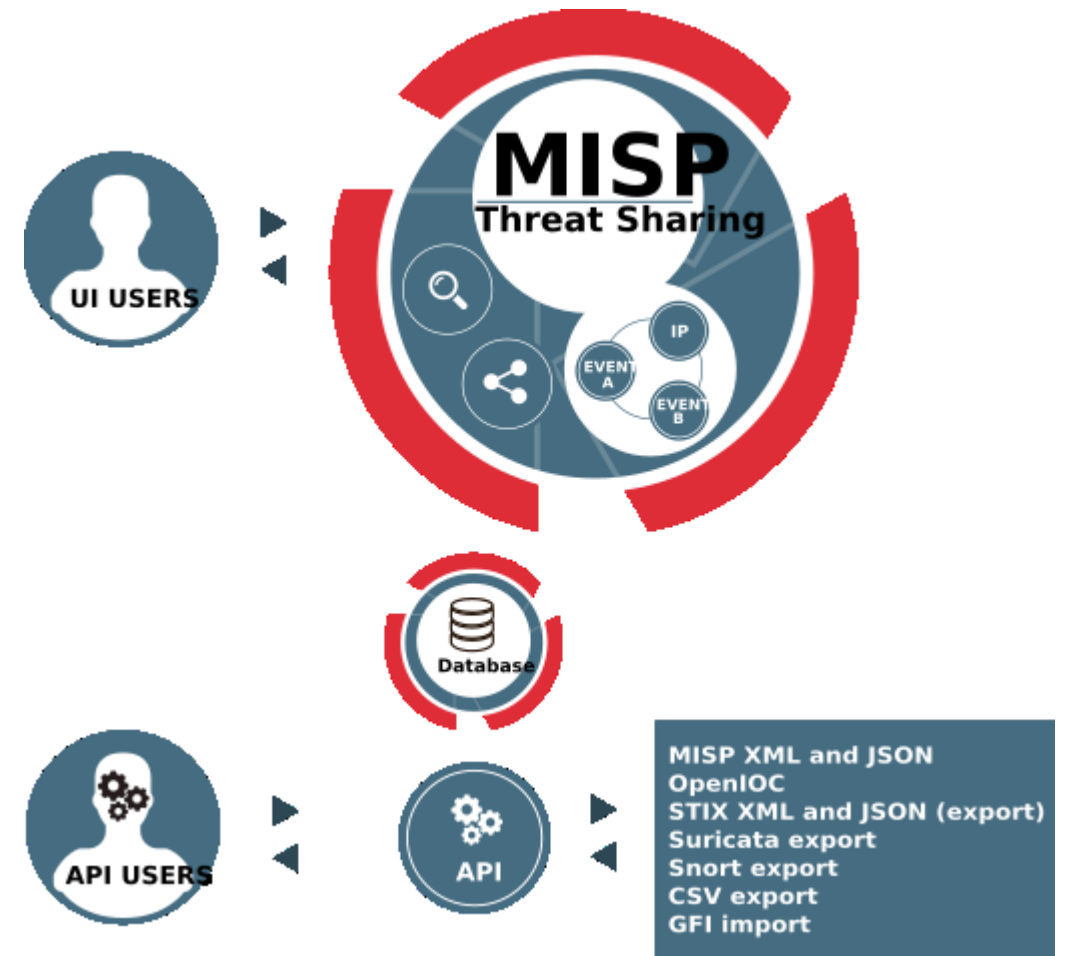
Certifikát X.509.



Threat Intelligence Communication Standards

MISP - Malware Information Sharing Platform

- open source platforma na zdieľanie IOC pre novoobjavené hrozby
- MISP je podporovaná EÚ
 - CIRCL vedie vývoj MISP
 - Computer Incident Response Center Luxembourg
- je široko používaný
 - vládnymi inštitúciami
 - národnými CERTs
 - súkromnými spoločnosťami,
 - finančným sektorom
 - a ďalšími organizáciami po celom svete.
- MISP umožňuje automatizované zdieľanie IOCs medzi ľuďmi a strojmi pomocou STIX a iných export formátov
 - Zdieľanie a import dát:
 - Generovaním **Snort/Suricata/Bro/Zeek IDS pravidiel**
 - pomocou **STIX, OpenIOC, text alebo csv** exportov



<https://www.misp-project.org/features/>

MISP - Malware Information Sharing Platform

OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulsunoy@circl.lu
Tags	ttp:white circl:osint-feed Type:OSINT estimative-language:likelihood-probability-"very-likely"
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Events

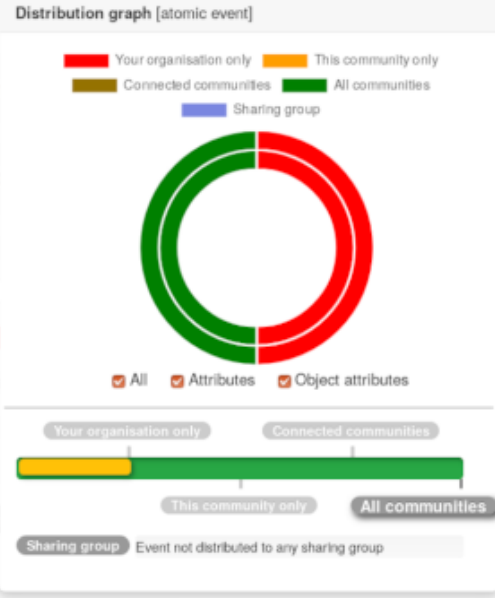
- 2016-05-27 (3883)
 - 2016-05-23 (3844)
 - 2016-05-06 (3826)
- Org: CIRCL
 Date: 2016-05-23
 Info: OSINT - Operation Ke3chang
 Resurfaces With New TidePool Malware



Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability-"almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability-"very-unlikely"	

Malicious activities

Event ID	10878
Uuid	5a6c700c-0eb8-468
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy
Tags	
Date	2018-05-04
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	Malicious activities
Published	No
#Attributes	2
Last change	2018/05/04 02:38:12
Extends	
Extended by	
Sightings	0 (0)
Activity	



Threat Level:

Analysis:

Event Info: Ransomware found on a production server

Extends event: 5ad8687b-De10-4a8b-a157-46a5950d210f

Matched event

Id: 10728

Analysis: Completed

Threat level: Low

Tags:

- circl:osint-feed tlp:white
- malware_classification:malware-category="Ransomware"
- osint:source-type="blog-post"
- misp-galaxy:ransomware="CSGO Ransomware"
- misp-galaxy:ransomware="MC Ransomware"

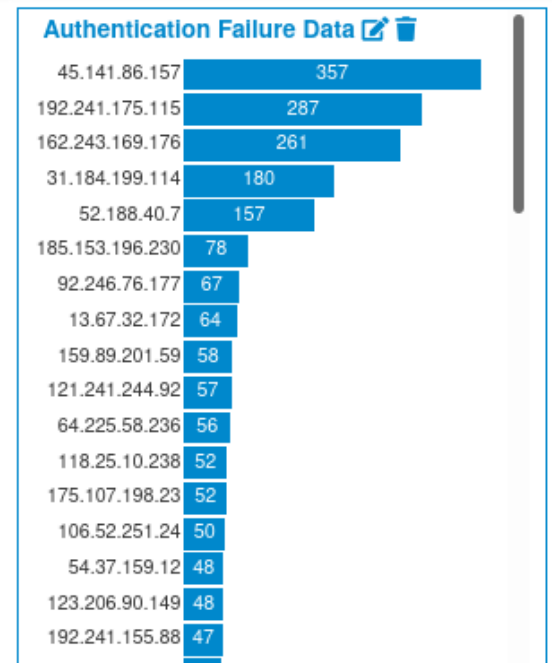
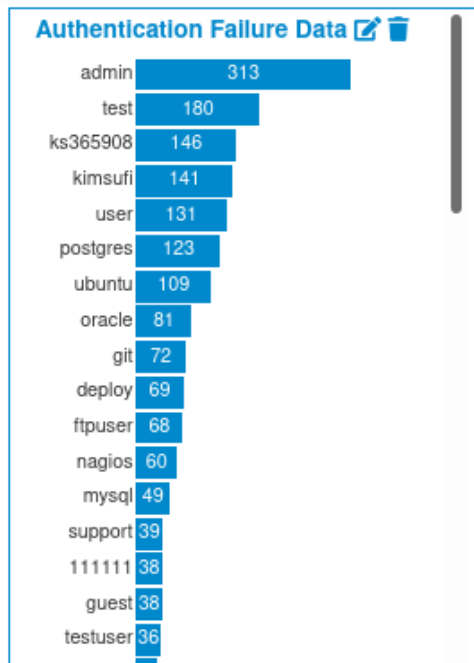
Info: OSINT - Minecraft & CS:GO Ransomware Stir For Media Attention

estimative-language:confidence-in-analytic-judgment="high"

High

Well corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No or

- View Dashboard
- Add Widget
- Import Config JSON
- Export Config JSON
- Save Dashboard Config
- List Dashboard Templates



Achievements of my organization

Achievements Unlocked!

- Congratulations, you have shared your first event!
- You have been using tags, good job!
- Taxonomies have been used in your events.
- Galaxies have no secrets for you in this Threat Sharing universe.

Next on your list:

Threat Intelligence Platforms

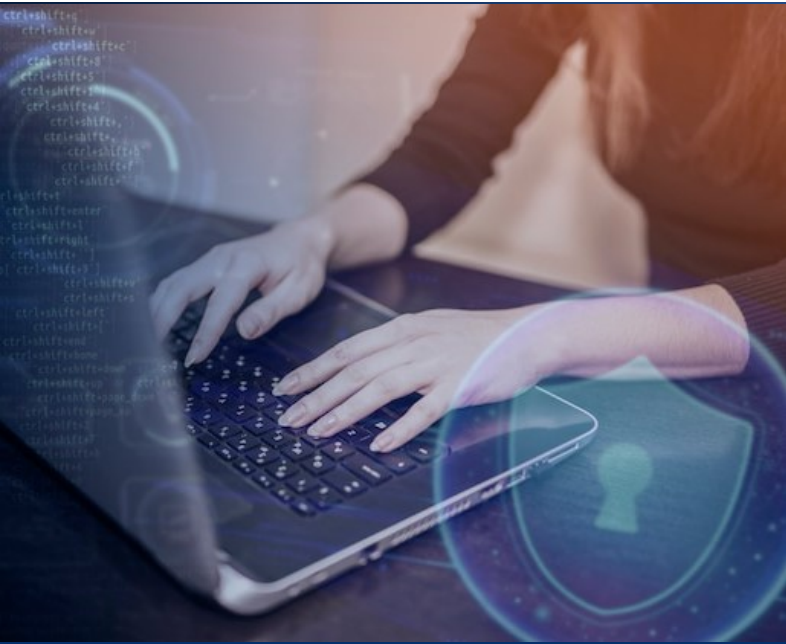
- A Threat Intelligence Platform (TIP) centralizuje zber údajov o hrozbách z mnohých zdrojov a formátov.
- **Typy threat Intelligence dát:**
 - Indicators of Compromise (IOC)
 - Tactics Techniques and Procedures (TTP)
 - Informácie o reputácii internetových cieľov alebo domén
- Organizácie môžu prispieť k CTI **zdieľaním** svojich údajov o narušeníach cez internet, zvyčajne prostredníctvom automatizácie
- Honeypots - simulované siete alebo servery, ktoré sú navrhnuté tak, aby prilákali útočníkov.
 - Informácie súvisiace s útokmi získané z honeypotov sa môžu zdieľať s predplatiteľmi CTI platformy.



Brandefense Digital Risk Protection Platform by Brandefense



<https://www.gartner.com/reviews/market/security-threat-intelligence-services>



Praktický checklist – Vulnerability Management

VM checklist

- **1. Identifikácia zraniteľností**
 - Určiť a inventarizovať všetky systémy, aplikácie a zariadenia v organizácii (CPE zoznam)
 - Nastaviť automatické skenovanie zraniteľností (napr. Nessus, GVM/OpenVAS, Qualys)
 - Definovať frekvenciu skenovania (napr. týždenne pre kritické systémy, mesačne pre menej kritické)
 - Prijímať a integrovať aktualizované feedy zraniteľností (NVD/CVE, SCAP, vendor advisories)

The screenshot displays the NetBox web interface. At the top, there's a search bar and navigation tabs for 'All Objects' and 'admin'. The main content area is divided into several sections:

- Organization:** Sites (30), Tenants (12)
- Inventory:** Racks (43), Device Types (22), Devices (88)
- Wireless:** Wireless LANs (1), Wireless Links (0)
- IPAM:** VRFs (1), Aggregates (1), Prefixes (7), IP Ranges (0), IP Addresses (11), VLANs (19)
- Power:** Power Panels (4), Power Feeds (48)
- Virtualization:** Clusters (33), Virtual Machines (180)
- Circuits:** Providers (9), Circuits (29)
- Connections:** Cables (115), Console (0), Interfaces (97), Power Connections (26)

Below these sections is a 'Change Log' table with columns for ID, Time, Username, Full Name, Action, Type, Object, and Request ID. It shows recent actions like 'Created' for DCIM objects.

The bottom part of the screenshot shows a dashboard with several widgets:

- Availability Map:** A grid of colored squares representing device status.
- Device summary table:** A table with columns for Total, Up, Down, Ignored, and Disabled for Devices and Services.
- Top CPU, Top Memory, Top Interfaces:** Line graphs showing resource usage for various devices and interfaces.
- Alerts:** A table showing system alerts with columns for Status, Rule, Hostname, Timestamp, Severity, Acknowledge, and Procedure.
- Eventlog:** A table showing system events with columns for Datetime, Hostname, Type, Message, and User.

VM checklist

- 2. Klasifikácia a hodnotenie rizík
 - Priradiť CVSS skóre alebo iný metrický systém k zisteným zraniteľnostiam
 - Identifikovať kritické systémy a dáta, aby sa určilo prioritizovanie opráv
 - Určiť rizikové kombinácie (napr. zraniteľnosť + dostupný exploit)

Operating System
Linux Kernel

Ports
443/tcp

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS **7.5**

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight
These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method
Checks previous collected cipher suites.

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution
Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References
cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872
url: <https://ssl-config.mozilla.org> , <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html> , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html> , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org> , <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014> , <https://sweet32.info>
cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K17/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

VM checklist

- 3. Prioritizácia a plánovanie opráv
 - Definovať kritériá pre urgentné opravy (napr. CVSS ≥ 7 , dostupný exploit, kritický systém)
 - Naplánovať opravy (patching, konfigurácia, mitigácia) podľa priorít
 - Dokumentovať plán opráv a zodpovednosti jednotlivých tímov

Summary

Vulnerability Scanner 1 of 8

Operating System: Linux Kernel

Ports: 443/tcp

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS 7.5

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight
These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method
Checks previous collected cipher suites.

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution
Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References
cve: CVE-2016-2183, CVE-2016-6329, CVE-2020-12872
url: <https://ssl-config.mozilla.org>, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>, https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html, <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>, <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>, <https://sweet32.info>
cert-bund: WID-SEC-2024-1277, WID-SEC-2024-0209, WID-SEC-2024-0064, WID-SEC-2022-2226, WID-SEC-2022-1955, CB-K21/1094, CB-K20/1023, CB-K20/0321, CB-K20/0314, CB-K20/0157, CB-K19/0618, CB-K19/0615, CB-K18/0296, CB-K17/1980, CB-K17/1871, CB-K17/1803, CB-K17/1753, CB-K17/1750, CB-K17/1709, CB-K17/1558, CB-K17/1273, CB-K17/1202, CB-K17/1196, CB-K17/1055, CB-K17/1026, CB-K17/0939, CB-K17/0917, CB-K17/0915, CB-K17/0877, CB-K17/0796, CB-K17/0724, CB-K17/0661, CB-K17/0657, CB-K17/0582, CB-K17/0581

Legend: High (red), Medium (yellow), Low (blue)

Score: 10



Quality of Detection

- **QoD** = skóre kvality detekcie jednotlivých nálezov v GVM
 - Každý NVT (Network Vulnerability Test) má priradené QoD skóre od 0 do 100
 - Vyššie skóre znamená väčšiu istotu, že detekcia je presná a nenastane falošný poplach
 - Napr.: QoD = 100 → vysoko presná detekcia, QoD = 50 → menej spoľahlivá, vyžaduje ďalšie overenie
- **Praktický význam:**
 - Pomáha tímom **prioritizovať opravy** podľa dôveryhodnosti zistených zraniteľností.
 - Znižuje čas strávený overovaním falošne pozitívnych nálezov

1 of 8

Operating System
Linux Kernel

Ports
443/tcp

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS **7.5**

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

EPSS (Maximum severity CVE)
Score: 0.31387
Percentile: 0.96634

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Insight
These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Detection Method
Checks previous collected cipher suites.

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution
Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References
cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872
url: <https://ssl-config.mozilla.org> , <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html> , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html> , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org> , <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014> , <https://sweet32.info>

cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K18/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

Feed a OID

Host	Port/Protocol	OID	QoD
None	443/tcp	1.3.6.1.4.1.25623.1.0.108031	98%

- **Greenbone Security Feed (GSF)**
 - pravidelne aktualizovaný balík informácií o zraniteľnostiach a testoch, ktorý používa GVM
 - Obsahuje
 - NVTs (Network Vulnerability Tests)
 - SCAP obsah (XCCDF/OVAL)
 - certifikačné checky
 - a ďalšie bezpečnostné informácie.
- **Typy feedov:**
 - **Community Feed** – bezplatný, menší a menej často aktualizovaný (50 000 NVT)
 - **Commercial / Greenbone Security Feed** – plná verzia, aktualizovaná denne, obsahuje tisíce NVT a rozšírený obsah SCAP (120 000)
- **Obsah feedu:**
 - **NVTs** – testy zraniteľností
 - **SCAP / OVAL / XCCDF** – pre compliance skeny
 - **Vendor advisories (oznámenia od výrobcu) / CVE mappings** – mapovanie testov na konkrétne CVE a produkty
- **OID je jedinečný identifikátor objektu používaný na:**
 - presnú identifikáciu konkrétneho testu zraniteľnosti (NVT – Network Vulnerability Test)
 - jeho výsledku
 - alebo iného objektu v databáze GVM
- **OID umožňuje:**
 - presne referencovať konkrétny test v reporte,
 - sledovať históriu nálezov,
 - automatizovane mapovať výsledky na patch alebo mitigation.
- **Formát OID je často hierarchický reťazec čísel, napr.**
1.3.6.1.4.1.25623.1.0.101234

EPSS score + percentile

EPSS (Exploit Prediction Scoring System)

- model vytvorený FIRST/NIST, ktorý predikuje pravdepodobnosť, že konkrétna zraniteľnosť (CVE) bude zneužitá v reálnom svete
 - NIST = „zdroj pravdy“ o zraniteľnostiach.
 - FIRST = „správca EPSS modelu“, ktorý tieto dáta používa a distribuuje skóre
- Cieľ: pomôcť tímom **prioritizovať** opravy podľa reálneho rizika, nielen podľa CVSS skóre

EPSS (Maximum severity CVE)

Score: 0.31387

Percentile: 0.96634

Score & Percentile

▪ Score

- Hodnota medzi 0 a 1, ktorá odhaduje pravdepodobnosť, že zraniteľnosť bude zneužitá v najbližšom časovom období (zvyčajne 30 dní)
- Vyššie skóre → vyššia pravdepodobnosť exploitácie

▪ Percentile:

- Porovnanie CVE s ostatnými zraniteľnosťami
- Napr. Percentile 90 znamená, že daná zraniteľnosť je **v top 10 % najpravdepodobnejšie zneužitelných zraniteľností**.
- Pomáha vizualizovať, ktoré CVE sú prioritou pre tím bezpečnosti

VM checklist

4. Remediácia

- Implementovať patch alebo mitigáciu podľa plánu
- Overiť, že zraniteľnosť bola úspešne opravená (re-scan)
- Aktualizovať inventár a evidenciu zraniteľností po oprave

Solution

Mitigation: The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

References

cve: CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872

url: <https://ssl-config.mozilla.org> , <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html> , https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html , <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html> , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html , <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org> , <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014> , <https://sweet32.info>

cert-bund: WID-SEC-2024-1277 , WID-SEC-2024-0209 , WID-SEC-2024-0064 , WID-SEC-2022-2226 , WID-SEC-2022-1955 , CB-K21/1094 , CB-K20/1023 , CB-K20/0321 , CB-K20/0314 , CB-K20/0157 , CB-K19/0618 , CB-K19/0615 , CB-K18/0296 , CB-K17/1980 , CB-K17/1871 , CB-K17/1803 , CB-K17/1753 , CB-K17/1750 , CB-K17/1709 , CB-K17/1558 , CB-K17/1273 , CB-K17/1202 , CB-K17/1196 , CB-K17/1055 , CB-K17/1026 , CB-K17/0939 , CB-K17/0917 , CB-K17/0915 , CB-K17/0877 , CB-K17/0796 , CB-K17/0724 , CB-K17/0661 , CB-K17/0657 , CB-K17/0582 , CB-K17/0581

IP adresa	Domain name	Dátum a čas zistenia zraniteľnosti	Názov zraniteľnosť	Závažnosť	Riešenie	Kto schválil akceptáciu (osoba)	Dôvod akceptácie	Kto vykonal mitigáciu (osoba)	Spôsob mitigácie	Dátum mitigácie/akceptácie
		22.09.2025 02:19:17	SSL/TLS: Server Certificate / C	Medium	v procese					
		22.09.2025 02:19:17	Non-Existent Page Physical P	Medium	v procese					
		22.09.2025 02:19:17	SSL/TLS: Deprecated TLSv1.0	Medium	v procese					
		22.09.2025 02:19:17	SSL/TLS: Certificate Signed U	Medium	v procese					

VM checklist



- **5. Monitorovanie a reporting**
 - Generovať pravidelné reporty pre vedenie (počet zraniteľností, stav opráv, trendy)
 - Monitorovať nové zraniteľnosti a exploit kity
 - Aktualizovať interné politiky a checklist podľa nových hrozieb a skúseností

1 Summary	3
1.1 Scan	3
1.2 Report	3
1.3 Results	4
2 Common Vulnerabilities	5
2.1 Top 10 vulnerabilities - High Severity	5
2.2 Top 10 vulnerabilities - Medium Severity	6
2.3 Top 10 vulnerabilities - Low Severity	7
3 Vulnerability Overview	8
3.1 Top 10 vulnerable Hosts	8
3.2 Network Topology	8
3.3 Top 10 vulnerable Operating Systems	9
3.4 Top 10 vulnerable ports	10
3.5 CVSS distribution for Ports	10
3.6 Top 10 Applications	11
3.7 CVSS distribution for Hosts	12
3.8 CVSS distribution for Vulnerabilities	12
4 Host Overview	13
4.1 Hosts by IP	13
4.2 Hosts by Severity	13
4.3 Known Hostnames	13

VM checklist

6. Integrácia do interných procesov

- Uistiť sa, že VM checklist je súčasťou change management procesu.
- Prepojiť s incident response, aby kritické zraniteľnosti vyvolali okamžitú reakciu.
- Zabezpečiť dokumentáciu a školenie tímov pre používanie checklistu.



00 - Procesný plán skenovania zraniteľností na UNIZA.docx



01 - Inštrukcie pre spracovanie záznamov o riešení zraniteľností.docx



02 - Šablóna pre evidenciu postupov na mitigáciu zraniteľností.docx



03 - Záznam o riešení zraniteľností_Sample Data.xlsx



ŽILINSKÁ UNIVERZITA
V ŽILINE

Procesný plán skenovania zraniteľností na UNIZA

Pracovná verzia vytvorená v rámci projektu Riadenie kybernetickej a informačnej bezpečnosti na UNIZA



ŽILINSKÁ UNIVERZITA
V ŽILINE

Procesný plán skenovania zraniteľností

Obsah

Účel dokumentu	
Rozsah dokumentu	
Normy a odporúčania	
Harmonogram skenovania	
Spustenie skenovania	
Možnosti doručenia a formát reportov	
Dôležité aspekty skenovania zraniteľností	
Záznam a evidencia riešenia zraniteľností	
Zodpovednosť	
Pilotná fáza	
Záver	
Prílohy	

Účel dokumentu

Tento dokument popisuje procesný plán pravidelného skenovania zraniteľností na UNIZA. Cieľom je zabezpečiť vyššiu úroveň kybernetickej bezpečnosti a ochrany informačných ak univerzity. V reakcii na nedávne udalosti, ako ransomware útoky na kataster nehnuteľno (2025), útok na UMB (2023), je nevyhnutné posilniť preventívne opatrenia pr kybernetickým hrozbám. V tomto prípade boli na útok zneužitú dlho známe zraniteľnosti, kt dokážu nástroje pre skenovanie zraniteľností odhaliť. Pravidelným skenovaním môžeme tie zraniteľnosti odhaliť a vyriešiť skôr, než ich potenciálny útočník môže zneužiť.

Rozsah dokumentu

Procesný plán sa vzťahuje na všetky fakulty, súčasti a pracoviská UNIZA, ktoré sú napojené univerzitnú IT infraštruktúru.





Krátka ukážka zisťovania zraniteľnosti systému

**Z verejne dostupných informácií na internete
a internetových vyhľadávačov**

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Zoznam domén registrovaných pre organizáciu (ŠGÚDŠ)

 Copilot 

Nepodarilo sa mi nájsť verejný zoznam domén registrovaných pre **Štátny geologický ústav Dionýza Štúra (ŠGÚDŠ)** priamo cez NIC.SK alebo iné verejné zdroje. Takéto informácie nie sú štandardne dostupné ako centralizovaný zoznam, pokiaľ organizácia sama nezverejní svoje domény.

Známe domény ŠGÚDŠ (overené z praxe):

Na základe predchádzajúcich technických analýz a verejne dostupných služieb sú známe tieto domény:

- **geology.sk** – hlavná doména ústavu
- **apl.geology.sk** – mapový portál (Aplikácie geologických údajov)
- **mapserver.geology.sk** – pravdepodobne interný alebo špecializovaný mapový server
- **geofond.geology.sk** – súvisiaci s geologickým fondom

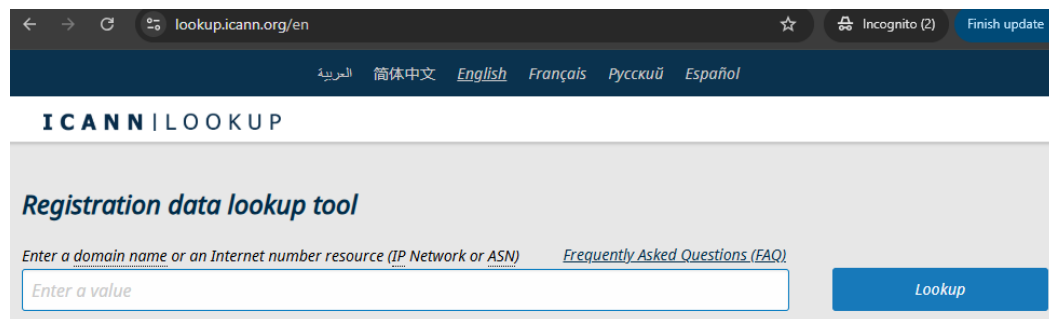
Tieto subdomény sú aktívne a prevádzkované ŠGÚDŠ, ale ich **IP adresy a rozsahy** nie sú verejne publikované.

Vyhľadávače informácií o doménach a IP adresách

WHOIS nástroje

ICANN Lookup

- **ICANN** (Internet Corporation for Assigned Names and Numbers) je **globálna autorita**, ktorá spravuje pridelenie domén a IP adres.
- Ich nástroj lookup.icann.org poskytuje **priamy prístup k oficiálnym WHOIS záznamom**.
- Je to najspoľahlivejší zdroj, pretože ICANN je **regulačný orgán** pre doménové mená.

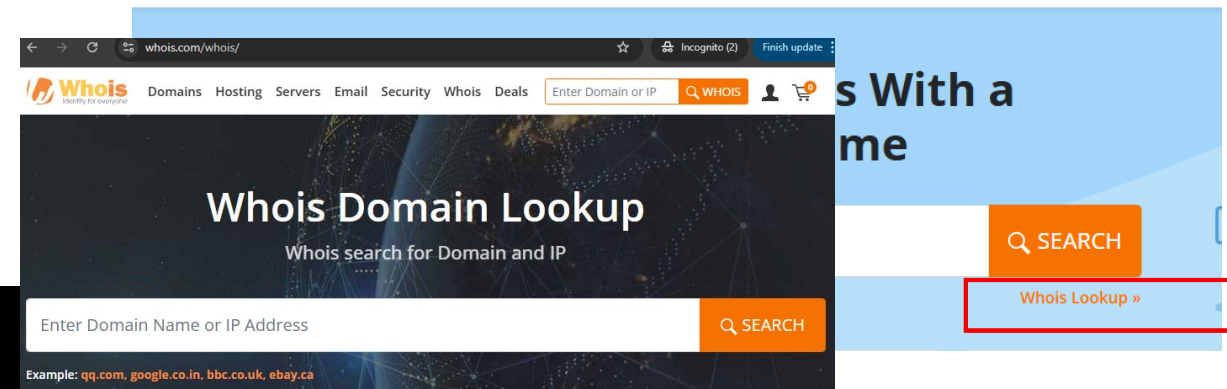


Je to užitočné pre:

- IT bezpečnostných expertov
- administrátorov sietí
- právnikov pri riešení sporov o domény
- bežných používateľov, ktorí chcú overiť dôveryhodnosť webu

Whois.com

- Whois.com je **dlhoročný a známy poskytovateľ WHOIS služieb**.
- Aj keď nie je regulačným orgánom ako ICANN, je **široko používaný** a má **prehľadné rozhranie**.
- Získava údaje z rôznych registrátorov a často poskytuje aj doplnkové informácie (napr. hosting, DNS, lokalita).
- <https://www.whois.com/whois/>



Zistime si logické (IP) adresy organizácie

Prieskum logických IP adries

← → ↻ 🌐 whois.com/whois/geology.sk



Domains Hosting Servers Email Security Whois Deals Enter [

geology.sk

Updated 1 second ago ↻

Domain:	geology.sk
Created:	2004-03-10
Valid Until:	2026-03-10
Updated:	2025-03-06
Domain Status:	ok
Nameserver:	ns.axonpro.sk
Nameserver:	ns2.axonpro.sk
Nameserver:	ns3.axonpro.sk
Domain registrant:	TTNY-0018
Name:	Štátny geologický ústav Dionýza Štúra
Organization:	Štátny geologický ústav Dionýza Štúra
Organization ID:	31753604
Phone:	+421.259375233
Email:	ladislav.nartinsky@geology.sk
Street:	Mlynská dolina 1
City:	Bratislava
Postal Code:	81704
Country Code:	SK
Authorised Registrar:	AXON-0001
Created:	2017-09-01
Updated:	2017-09-01

🖥️ Prikazový riadok

```
C:\Users\Jana>ping geology.sk
```

```
Pinging geology.sk [194.160.66.21] with 32 bytes of data:  
Reply from 194.160.66.21: bytes=32 time=4ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=3ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=7ms TTL=56  
Reply from 194.160.66.21: bytes=32 time=7ms TTL=56
```

Ping statistics for 194.160.66.21:

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

🖥️ Prikazový riadok - nslookup

```
Microsoft Windows [Version 10.0.19045.6216]  
(c) Microsoft Corporation. Všetky práva vyhradené.
```

```
C:\Users\Jana>nslookup  
Default Server: dns.google  
Address: 8.8.8.8
```

```
> set type=SOA  
> geology.sk  
Server: dns.google  
Address: 8.8.8.8
```

```
Non-authoritative answer:  
geology.sk  
    primary name server = geolsurv.geology.sk  
    responsible mail addr = postmaster.geology.sk  
    serial = 20240726  
    refresh = 10800 (3 hours)  
    retry = 3600 (1 hour)  
    expire = 604800 (7 days)  
    default TTL = 38400 (10 hours 40 mins)
```

🖥️ Prikazový riadok - nslookup

```
> set type=A  
> geolsurv.geology.sk  
Server: dns.google  
Address: 8.8.8.8  
  
Non-authoritative answer:  
Name: proxy.geology.sk  
Address: 194.160.66.28  
Aliases: geolsurv.geology.sk
```

WHOIS lookup

Zistenie rozsahu logických (IP) adries pre organizáciu



whois.com/whois/194.160.66.21

Whois Domains Hosting Servers Email Security Whois Deals

Whois IP 194.160.66.21

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '194.160.66.0 - 194.160.67.255'

% Abuse contact for '194.160.66.0 - 194.160.67.255' is 'abuse@sanet.sk'

inetnum:        194.160.66.0 - 194.160.67.255
netname:        GEOLOGY-DS-SK
descr:          State Geological Institute of Dionyz Stur
descr:          Slovakia
country:        SK
admin-c:        SK1370-RIPE
tech-c:         JB6619-RIPE
status:         ASSIGNED PA
mnt-by:         SWDB-SANET
mnt-lower:      SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified: 2007-12-11T20:04:22Z
source:         RIPE
```

```
person:         Juraj Baluch
address:        Mlynska dolina 1
address:        Bratislava
address:        817 04
address:        Slovakia
phone:          +421 2 5937 5248
fax-no:         +421 2 5477 1940
nic-hdl:        JB6619-RIPE
mnt-by:         SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified: 2008-10-22T14:16:36Z
source:         RIPE # Filtered
```

```
person:         Stefan Kacer
address:        Mlynska dolina 1
address:        Bratislava
address:        817 04
address:        Slovakia
phone:          +421 2 5937 5155
fax-no:         +421 2 5477 1940
nic-hdl:        SK1370-RIPE
mnt-by:         SWDB-SANET
created:        2007-12-11T19:56:10Z
last-modified: 2008-10-22T14:16:35Z
source:         RIPE # Filtered
```

```
% Information related to '194.160.0.0/17AS2607'
```

```
route:          194.160.0.0/17
descr:          SANET-AS2607-BLOCK
origin:         AS2607
mnt-by:         AS2607-MNT
mnt-lower:      AS2607-MNT
created:        2022-10-10T12:06:38Z
last-modified: 2022-10-10T12:06:38Z
source:         RIPE
```

```
% This query was served by the RIPE Database Query Service version 1.118.1 (BUSA)
```

Kto spravuje (takmer) všetky číselné identifikátory na internete – dôveryhodná autorita

IANA.org



The global coordination of the DNS Root, IP addressing, and other Internet protocol resources is performed as the Internet Assigned Numbers Authority (IANA) functions. [Learn more.](#)

Domain Names

Management of the DNS Root Zone (assignments of ccTLDs and gTLDs) along with other functions such as the .int and .arpa zones.

- Root Zone Management
- Database of Top Level Domains
- .int Registry
- .arpa Registry
- IDN Practices Repository

Number Resources

Coordination of the global IP and AS number spaces, such as allocations made to Regional Internet Registries.

- IP Addresses & AS Numbers
- Network abuse information

Protocol Assignments

The central repository for protocol name and number registries used in many Internet protocols.

- Protocol Registries
- Apply for an assignment
- Time Zone Database

Nie je oficiálnym zdrojom informácií pre EU... Ale poslúži nám, lebo poskytne viac...

https://whois.ipip.net/

AS2607 - SANET - Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET, SK

IP Address Ranges	Graph v4	Graph v6	Upstreams	Downstreams	IX	Whois
AS Number AS2607	AS Name SANET	Org Name Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET	Country Slovakia			
Registry ripe	RegDate	Updated 2018-11-22T15:27:18Z	AS2607 Looking Glass			
IPv4Prefixes 39	IPv6Prefixes 3	IPv4 NUMs 526,080	IPv6 NUMs (64) 4,294,967,296			

526,080 IPv4 Addresses

IPv4 Ranges IPv6 Ranges

192.108.132.0/24	✓	VSEBBNET
192.108.132.0/23	✓	VSEBBNET
192.108.133.0/24	✓	VSEBBNET
192.108.138.0/24	✓	SANET
192.108.138.0/23	✓	SANET
192.108.149.0/24	✓	UAKOMBONE
193.87.0.0/17	🔍 ✓	National Health Information Center
193.87.0.0/16	🔍 ✓	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
193.87.128.0/17	🔍 ✓	NBSNET
194.160.0.0/17	🔍 ✓	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
194.160.0.0/16	🔍 ✓	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete
194.160.128.0/17	🔍 ✓	SSKNM-SK

Reverzné záznamy na <https://whois.ipip.net/> Zisťovanie informácií

- 194.160.66.0/24
- 192.160.67.0/24

194.160.25.0/24	194.160.26.0/24	194.160.27.0/24
194.160.30.0/24	194.160.31.0/24	194.160.32.0/24
194.160.35.0/24	194.160.36.0/24	194.160.37.0/24
194.160.40.0/24	194.160.41.0/24	194.160.42.0/24
194.160.45.0/24	194.160.46.0/24	194.160.47.0/24
194.160.50.0/24	194.160.51.0/24	194.160.52.0/24
194.160.55.0/24	194.160.56.0/24	194.160.57.0/24
194.160.60.0/24	194.160.61.0/24	194.160.62.0/24
194.160.65.0/24	194.160.66.0/24	194.160.67.0/24
194.160.70.0/24	194.160.71.0/24	194.160.72.0/24
194.160.75.0/24	194.160.76.0/24	194.160.77.0/24

BGP Announced

AS	CIDR	Description
AS2607	194.160.0.0/17	SANET - Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET, SK
AS2607	194.160.0.0/16	SANET - Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET, SK

Real Time BGP Data

AS / Info	IP / Time	AS Path
Loading...		

Reverse DNS List (Total:255)

IP	Host	DateTime
194.160.66.1	1.geology.sk	2025-09-04 14:23:12
194.160.66.2	proxy.geology.sk	2025-09-04 14:23:12
194.160.66.3	3.geology.sk	2025-09-04 14:23:12
194.160.66.4	4.geology.sk	2025-09-04 14:23:12
194.160.66.5	5.geology.sk	2025-08-30 12:41:16
194.160.66.6	6.geology.sk	2025-09-04 14:23:12

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

<https://www.shodan.io/>

▪ Shodan.io

- špecializovaný vyhľadávač, ktorý umožňuje prehľadávať zariadenia pripojené k internetu
- na rozdiel od klasických vyhľadávačov ako Google, ktoré indexujú webové stránky, Shodan indexuje **internet vecí (IoT)** – teda:
 - servery
 - webkamery
 - smerovače
 - inteligentné zariadenia
 - priemyselné systémy a ďalšie.
- **Účel:**
 - Zisťovanie, aké zariadenia sú pripojené k internetu a aké služby poskytujú.
- **Použitie:**
 - Bezpečnostní experti ho využívajú na auditovanie sietí, hľadanie zraniteľností a monitorovanie zariadení.
- **Funkcie:**
 - Umožňuje filtrovať podľa IP adresy, portu, geografickej polohy, operačného systému, otvorených služieb a ďalších parametrov.
- **Riziká:**
 - Môže byť zneužitý na identifikáciu nezabezpečených zariadení, preto je dôležité správne konfigurovať a zabezpečiť sieťové zariadenia.



Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io

shodan.io/host/194.160.66.48

SHODAN Explore Downloads Pricing Search Account

194.160.66.48 Regular View Raw Data Timeline

// TAGS: eol-product // LAST SEEN: 2025-09-02

General Information

Hostnames	geology.sk 48.geology.sk
Domains	geology.sk
Country	Slovakia
City	Bratislava
Organization	State Geological Institute of Dionyz Stur
ISP	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET

Open Ports

80	443	1883	8000
----	-----	------	------

// 80 / TCP -70800581 | 2025-08-23T10:25:54.665599

nginx 1.20.2

Mapportal ŠGÚDŠ

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Sat, 23 Aug 2025 10:25:54 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Vyhľadanie informácií cez shodan.io (pokrač.)

shodan.io/host/194.160.66.48

Organization: **State Geological Institute of Dionyz Stur**

ISP: **Zdruzenie pouzivatelov Slovenskej akademickej datovej siete SANET**

ASN: **AS2607**

Vulnerabilities [All ports] [Latest]

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2023 (1)

CVE-2023-44487 **7.5** The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (1)

CVE-2021-3618 **7.4** ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MITM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

Server: nginx/1.20.2
Date: Sat, 23 Aug 2025 10:25:54 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
Etag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-CustomHeader,Ke
-Control,Content-Type
Accept-Ranges: bytes

Vulnerabilities

0 2 0 0 0

// 443 / TCP

nginx 1.20.2

Mapportal ŠGÚDŠ

HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Sun, 31 Aug 2025 14:54:37 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
Etag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-CustomHeader,Ke
-Control,Content-Type,Content-Range,Range
Access-Control-Expose-Headers: DNT,X-CustomHeader,ke
-Control,Content-Type,Content-Range,Range

Vyhľadávač pre zariadenia pripojené k internetu (vrátane ich zraniteľností)

Filter na zraniteľnosti

The screenshot shows a web browser window with the URL `shodan.io/search?query=vuln:CVE-2023-44487`. The browser's navigation bar includes tabs for 'Shodan', 'Maps', 'Images', 'Monitor', 'Developer', and 'More...'. Below the browser, the Shodan website interface is visible, featuring a search bar with the query `vuln:CVE-2023-44487` and a search button. A prominent error message is displayed in a red box, stating: **Error:** The "vuln" filter is only available to Academic users or Small Business API subscription and higher.

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

- NIST NVD (National Vulnerability Database) je oficiálna databáza kybernetických zraniteľností
 - spravovaná NIST (National Institute of Standards and Technology) v USA
 - zoznam známych zraniteľností softvéru a hardvéru, často označených identifikátorom CVE (Common Vulnerabilities and Exposures).
 - Pomáha organizáciám identifikovať a hodnotiť bezpečnostné riziká v ich systémoch.
 - Každá zraniteľnosť má priradené skóre CVSS (Common Vulnerability Scoring System), ktoré hodnotí jej závažnosť.
 - Úzko spolupracuje s MITRE (správcom CVE systému) a ďalšími bezpečnostnými komunitami.

The screenshot shows the NIST National Vulnerability Database search page. The browser address bar displays 'nvd.nist.gov/search'. The page header includes the NIST logo and 'Information Technology Laboratory'. The main heading is 'NATIONAL VULNERABILITY DATABASE'. A search bar is present, and a red box highlights the 'Vulnerabilities - CVE' button. Other buttons include 'Products - CPE' and 'Checklists - NCP'. The page also features a 'Search' section with the text 'Please make use of the interactive search interfaces to find information in the database!'.

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

Vyhľadávanie informácií o zraniteľnostiach

- CVE-2023-44487

The screenshot shows the NVD Vulnerability Search interface. The search bar contains the keyword "CVE-2023-44487". The search results table has the following columns: Identifier, CISA Key Info, Published Date, CNA, and Description. The first result is highlighted with a red box.

Identifier	CISA Key Info	Published Date	CNA	Description
CVE-2023-44487	✓	2023-10-10	MITRE	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

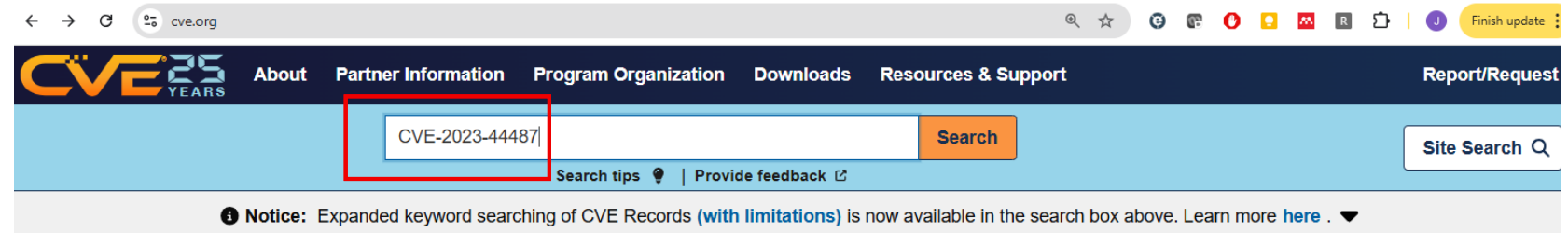
cve.org

- CVE Record User Guide

- <https://www.cve.org/CVERecord/UserGuide/#cve-key>

- Vyhľadávanie informácií o:

CVE-2023-44487



CVE™ Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There are currently over 292,000 CVE Records accessible via [Download](#) or [Keyword Search](#) above.

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of **CVE Numbering Authorities (CNAs)** and **Roots**.

[Learn More](#) [Become a Partner](#)

News

- [Searching for Patterns Now Available in "CVE List Keyword Search" on CVE.ORG Website](#)
- [Vulnerability Data Enrichment for CVE Records: 243 CNAs on the Enrichment Recognition List for September 2, 2025](#)
- [CVE Program Report for Quarter 2 Calendar Year \(Q2 CY\) 2025](#)
- [AxxonSoft Added as CVE Numbering Authority \(CNA\)](#)

NEWS ICONS

Access

- [List of Partners](#)
- [CNA Rules](#)
- [CVE Record Lifecycle](#)
- [CVEProject on GitHub for Development](#)
- [Idea tracker](#)

Learn

- [About CVE](#)
- [Process](#)
- [Program Organization](#)
- [CVE 25th Anniversary Report](#)
- [Related Efforts](#)
- [Terminology](#)
- [CVE Services for CNAs](#)

Report/Request

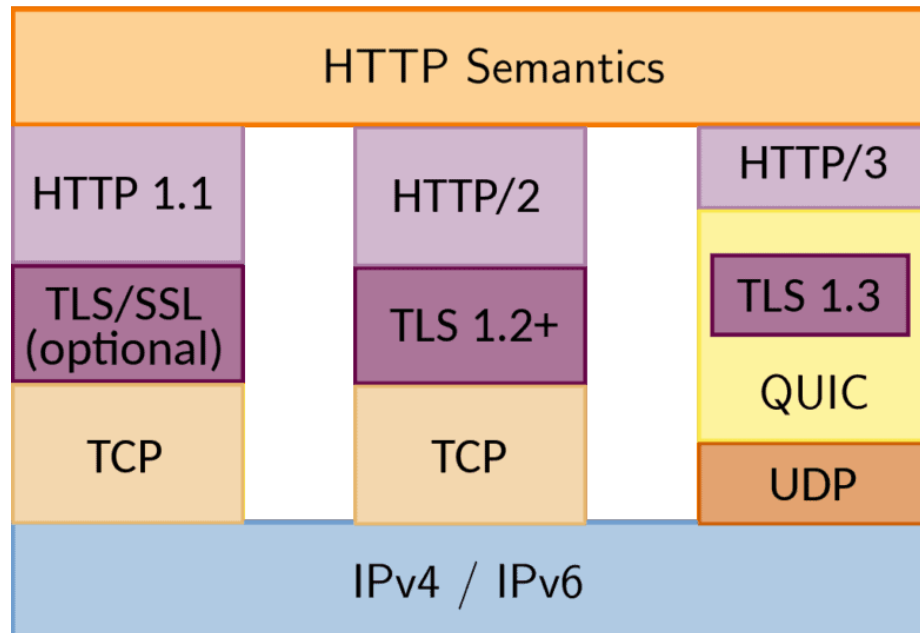
- [Report vulnerability/Request CVE ID](#)
- [Request CVE Record be published/updated](#)
- [Report the use of a reserved CVE ID](#)

Konkrétna ukážka pre zisťovanie zraniteľnosti systému

CVE-2023-44487

■ HTTP/3: Rýchlejší a bezpečnejší web

- <https://www.websupport.sk/podpora/kb/http3-rychlejsi-a-bezpecnejsi-web/>



CVE-2023-44487 **PUBLISHED** [View JSON](#) | [User Guide](#)

Required CVE Record Information

CNA: MITRE Corporation

Published: 2023-10-10 Updated: 2025-06-07

Description

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Product Status
[Learn more](#)

Information not provided

References 144 Total

- <https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73>

<https://www.cve.org/CVERecord?id=CVE-2023-44487>

Je viacero rôznych databáz zraniteľností

Zoznamy zraniteľností

CVE

Common Vulnerabilities and Exposures

- Medzinárodný štandard pre identifikáciu známych zraniteľností v softvéri.
- Každá zraniteľnosť má jedinečný identifikátor (napr. CVE-2023-12345).
- Spravuje ho organizácia MITRE Corporation v spolupráci s NIST.
- CVE záznam obsahuje:
 - stručný popis zraniteľnosti,
 - dátum zverejnenia,
 - odkazy na technické detaily (napr. NVD, vendor advisories).
- Používa sa v nástrojoch na správu zraniteľností, bezpečnostných skeneroch, SIEM systémoch atď.

<https://www.cve.org/>

KEV

Known Exploited Vulnerabilities

- Zoznam zraniteľností, ktoré sú **aktívne zneužívané v reálnom svete**.
- Spravuje ho **Cybersecurity and Infrastructure Security Agency (CISA)** v USA.
- KEV zoznam je podmnožinou CVE – obsahuje len tie CVE, ktoré sú **potvrdené ako aktívne zneužívané**.
- Slúži ako **prioritný zoznam pre patchovanie** – organizácie by mali riešiť KEV zraniteľnosti prednostne.
- Obsahuje:
 - CVE identifikátor,
 - dátum pridania do KEV,
 - požiadavku na mitigáciu (napr. deadline pre federálne agentúry v USA).

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Shodan.io/Pricing

Cena licencií na shodan.io

(len pre predstavu)

- Doživotná basic licencia (zaujímavá... ale dostupná iba v špeciálnych akciách, raz za X rokov)



Receipt from **Shodan, LLC.**

Receipt #1268-4168

AMOUNT PAID	DATE PAID	PAYMENT METHOD
\$5.00	Jul 17, 2023, 1:42:45 PM	MasterCard -

SUMMARY

Payment to Shodan, LLC.	\$5.00
Amount charged	\$5.00

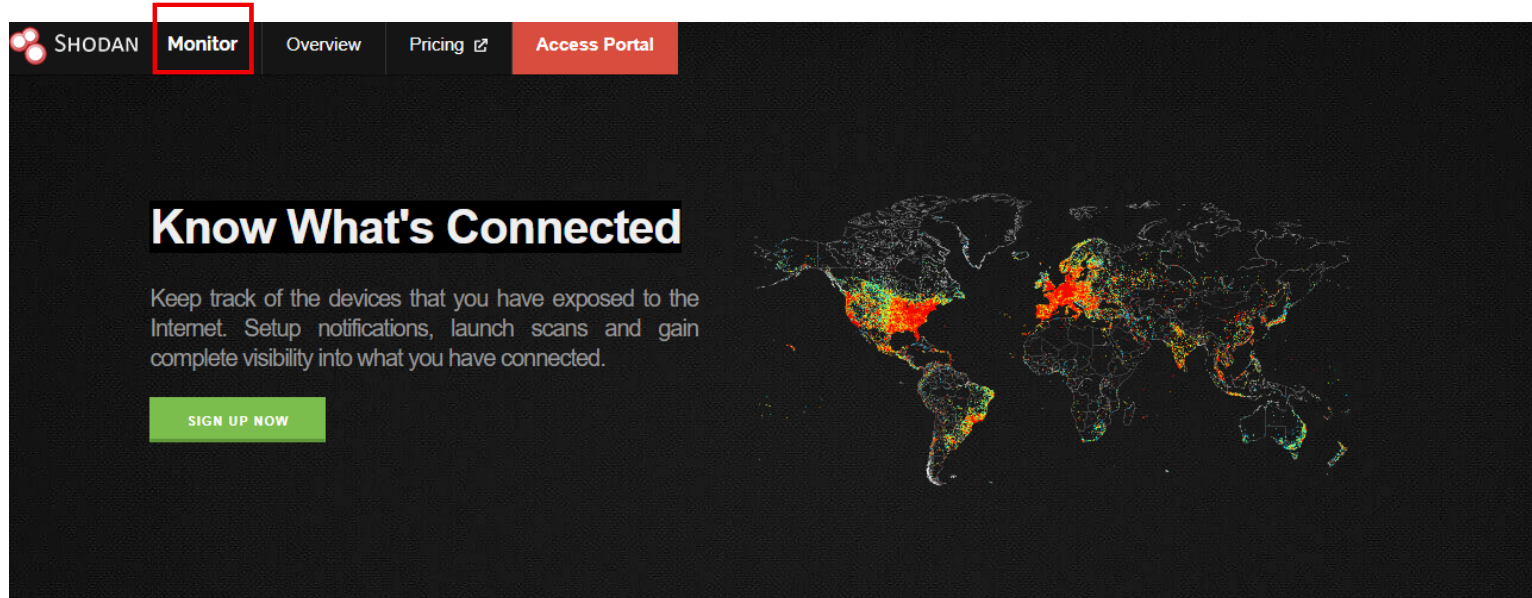
If you have any questions, contact us at support@shodan.io or call at +1 740-746-3261.

Choose Your Plan

No contracts. No setup fees. Cancel anytime.

<p>Freelancer</p> <p>\$69/month</p> <p>LOGIN TO SUBSCRIBE</p> <ul style="list-style-type: none"> ✓ Up to 1 million results per month* ✓ Scan up to 5,120 IPs per month ✓ Network Monitoring for 5,120 IPs <hr/> <ul style="list-style-type: none"> ✓ Access to most filters ✓ Allows paging through search results ✓ Basic access to the Streaming API ✓ Commercial Use <hr/> <ul style="list-style-type: none"> ✓ Grandfathered Pricing ✓ E-Mail support 	<p>Small Business</p> <p>\$359/month</p> <p>LOGIN TO SUBSCRIBE</p> <ul style="list-style-type: none"> ✓ Up to 20 million results per month* ✓ Scan up to 65,536 IPs per month ✓ Network Monitoring for 65,536 IPs <hr/> <ul style="list-style-type: none"> ✓ Access to most filters ✓ Allows paging through search results ✓ Basic access to the Streaming API ✓ Commercial Use <hr/> <ul style="list-style-type: none"> ✓ Grandfathered Pricing ✓ E-Mail support 🛡️ Vulnerability search filter 	<p>Corporate</p> <p>\$1099/month</p> <p>LOGIN TO SUBSCRIBE</p> <ul style="list-style-type: none"> 📶 Unlimited results per month* ✓ Scan up to 327,680 IPs per month ✓ Network Monitoring for 327,680 IPs <hr/> <ul style="list-style-type: none"> ✓ Access to all filters ✓ Allows paging through search results ✓ Basic access to the Streaming API ✓ Commercial Use <hr/> <ul style="list-style-type: none"> ✓ Grandfathered Pricing 👤 Premium Support 🛡️ Vulnerability search filter ✓ Batch IP Lookups 🔍 Tag Search Filter 🌐 InternetDB API Commercial Use 👤 Complementary Membership Upgrades
---	---	--

S liceniou: aj možnosť monitorovať (svoje) zariadenia



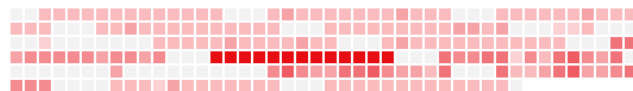
Network Monitoring Made Easy

Within 5 minutes of using Shodan Monitor you will see what you currently have connected to the Internet within your network range and be setup with real-time notifications when something unexpected shows up.



Small network

198.20.68.0/24 [↗](#)



Built to Scale

Whether you want to monitor 1 IP or you're an ISP with millions of customers - the Shodan platform was built to handle networks of all sizes without breaking a sweat.

Identifikácia zraniteľností systémov so shodan.io

Monitorovanie aktív (assets)

monitor.shodan.io/networks

Shodan Maps Images Monitor Developer More...

SHODAN Monitor Dashboard **Manage Assets** Events Log Settings

Manage Assets

ADD NETWORK ADD DOMAIN ADD SEARCH QUERY

geology.sk	194.160.66.48/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	
gymrk.sk	194.160.142.194/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	
sczsk.sk	195.146.133.107/32	1 IP	malware, open_database, ai, iot, end_of_life, internet_scanner, industrial_control_system, new_service, ssl_expired, vulnerable	

Monitorovanie aktív – alert o novej zraniteľnosti



Shodan Alert <no-reply@mg.shodan.io>
to me ▾

Sep 4, 2025, 4:02 PM (21 hours ago)



194.160.66.48

80 / tcp
Port

[geology.sk](#)
Asset Group

end_of_life
Trigger

nginx 1.20.2

```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Thu, 04 Sep 2025 13:44:23 GMT
Content-Type: text/html
Content-Length: 9619
Last-Modified: Wed, 06 Dec 2023 11:35:14 GMT
Connection: keep-alive
ETag: "65705c72-2593"
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type
Accept-Ranges: bytes
```

View Events

Add to Whitelist



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Správa zraniteľností a kybernetických hrozieb

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, <https://kc.uniza.sk/>

Jana.Uramova@fri.uniza.sk