Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riešenie incidentov

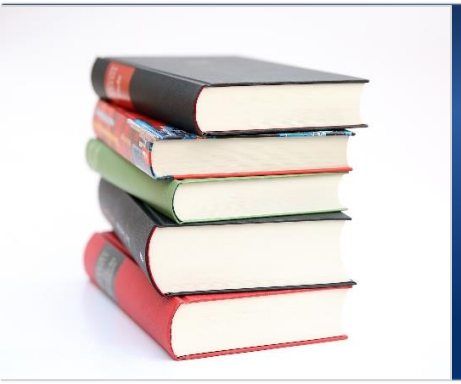
Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk



Ciele

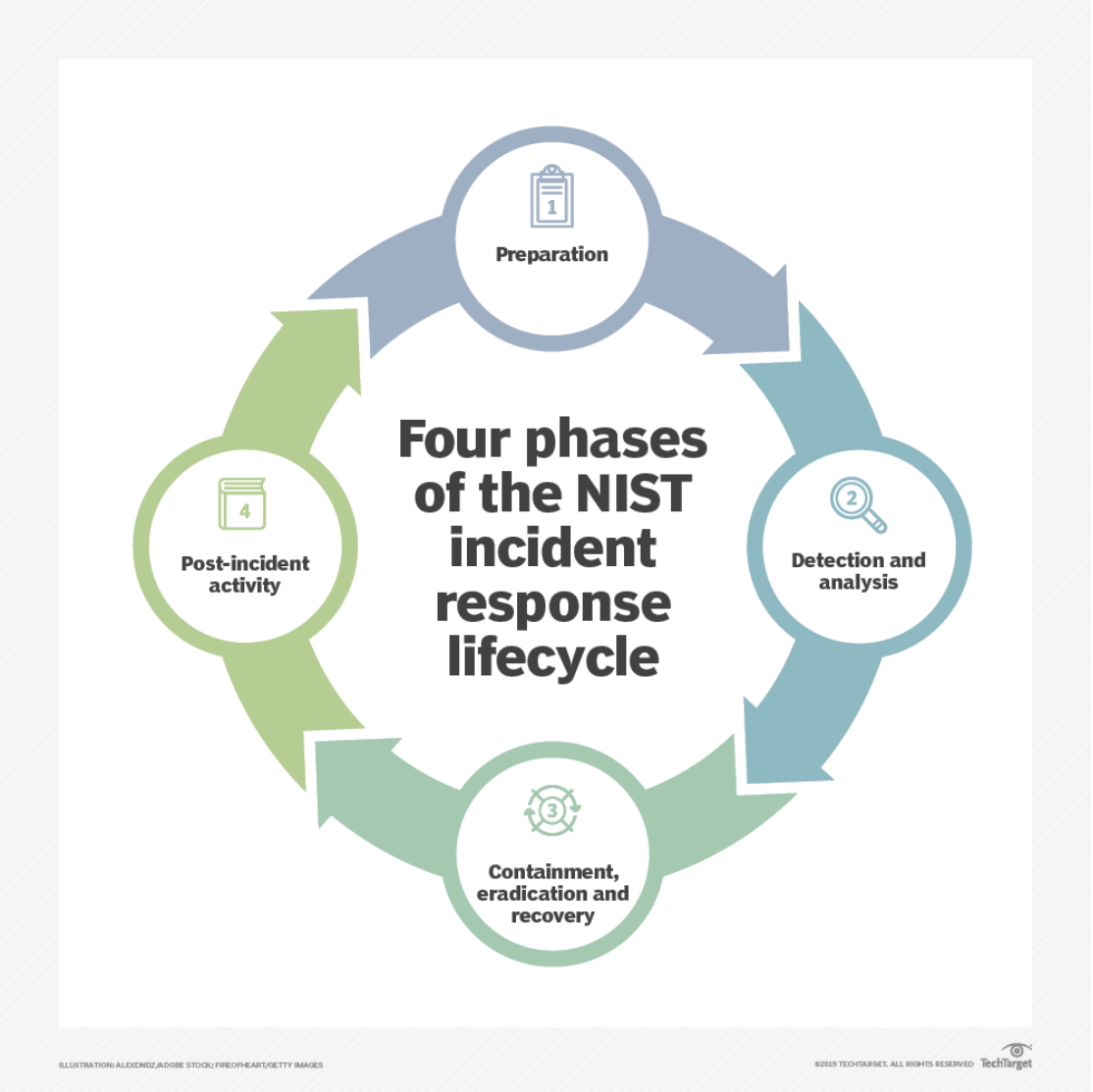
- Pochopiť proces riešenia kybernetických incidentov podľa metodiky NIST SP 800-61, vrátane jeho fáz – príprava, detekcia a analýza, reakcia, obnova a spätné vyhodnotenie.
- Predstaviť úlohu SOC centra v procese riešenia incidentov a jeho prepojenie s Incident Response(IR) tímami.
- Analyzovať a porovnať nástroje určené pre manažment incidentov (TheHive, DFIR-IRIS, RTIR, Znuny) z pohľadu ich funkcií, integrácií a vhodnosti pre SOC prostredie.
- Vysvetliť metodológiu Cyber Kill Chain a jej využitie pri identifikácii a zastavení kybernetických útokov v rôznych fázach.
- Zdôrazniť význam automatizácie, spolupráce a forenznej dokumentácie v procese Incident Response.

Proces riešenia incidentov

Proces riešenia incidentu

Proces riešenia incidentov vychádza z metodiky **NIST SP 800-61r2**, ktorá definuje štyri hlavné fázy:

- **Preparation (Príprava)** – pripravenosť, plánovanie a procesy.
- **Detection & Analysis (Detekcia a analýza)** – zisťovanie a hodnotenie incidentov.
- **Containment, Eradication & Recovery (Reakcia a obnova)** – izolácia, odstránenie a návrat do prevádzky.
- **Post-Incident Activity (Lessons Learned)** – spätné vyhodnotenie a zlepšovanie procesov.

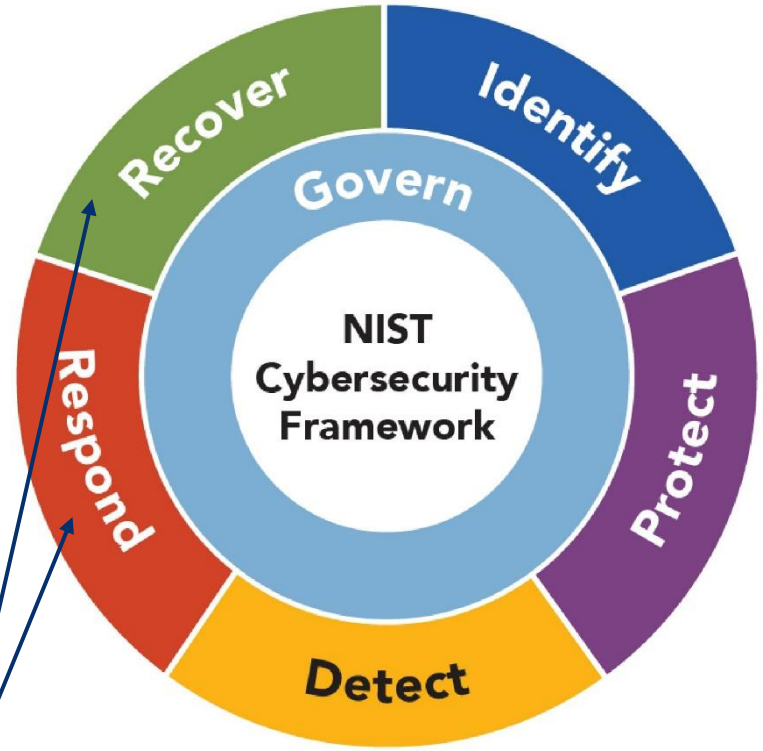


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prepojenie procesu riešenia incidentov s NIST CSF

NIST Cybersecurity Framework definuje 5 základných funkcií:

- **Identify** – identifikácia aktív, prostredia, rizík
- **Protect** – zavedenie bezpečnostných opatrení
- **Detect** – odhaľovanie anomálií a incidentov (monitoring).
- **Respond** – reakcia na incidenty
- **Recover** – obnova služieb a procesov



Proces riešenia incidentov zodpovedá najmä fáze **Respond** rámca NIST a čiastočne aj **Recover**.
V praxi sú tieto fázy podporené nástrojmi pre **evidenciu, koordináciu a správu incidentov** – napríklad **The Hive**, **DFIR-IRIS**, **RTIR** či **Znuny**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

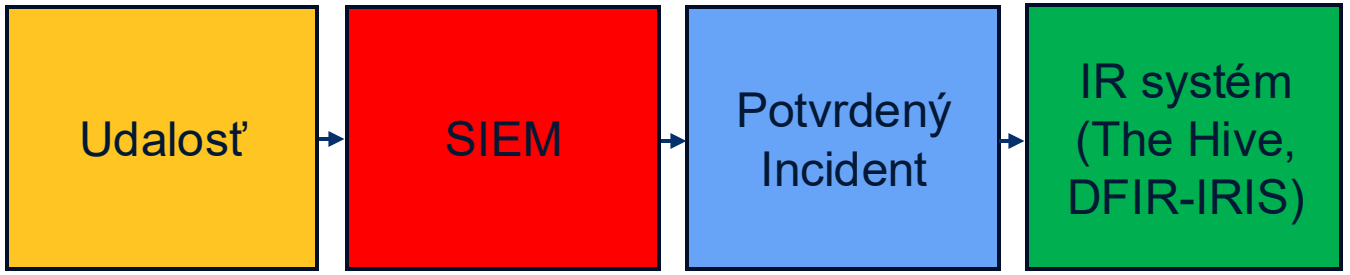
Prípravná fáza

- **Fáza Preparation (Príprava)** predstavuje základ procesu riešenia incidentov podľa metodiky **NIST SP 800-61r2**.
  Cieľom je pripraviť organizáciu, tím a technológie na efektívnu reakciu na bezpečnostné incidenty.
- **Definovanie politík a postupov** pre riadenie incidentov (Incident Response Plan, komunikačný plán, klasifikácia incidentov).
- **Zostavenie IR tímu** – určenie rolí (SOC, CIRT, manažér, forenzný analytik).
- **Zabezpečenie nástrojov a infraštruktúry** pre detekciu, evidenciu a reakciu (SIEM, TheHive, DFIR-IRIS, RTIR, Znuny).
- **Školenia a testovanie pripravenosti tímu** – simulácie incidentov, tabletop cvičenia.
- **Zber a aktualizácia kontaktov** – vnútorné a externé komunikačné kanály (CERT, dodávatelia, vedenie organizácie).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Identifikácia a detekcia incidentu

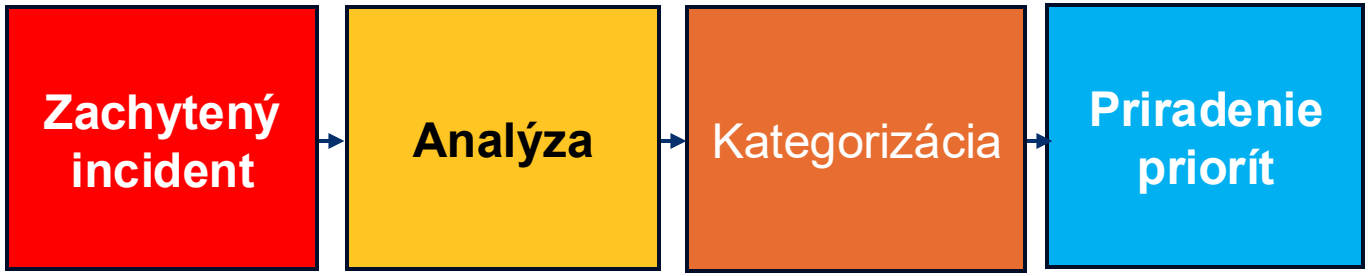
- Fáza detekcie a identifikácie predchádza samotnému procesu riešenia incidentov.
- V tejto fáze sa analyzujú bezpečnostné udalosti s cieľom zistiť, či ide o skutočný incident, ktorý sa má ďalej spracovať v IR systéme.
- SOC tím využíva nástroje ako SIEM, IDS/IPS, EDR, ktoré poskytujú vstupné dáta pre Incident Response.
- Potvrdený incident sa následne eviduje v nástroji IR (napr. TheHive, DFIR-IRIS).



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Analýza a posúdenie incidentu

- Po potvrdení incidentu nasleduje jeho analýza a klasifikácia podľa typu, rozsahu a dopadu.
- Cieľom je určiť zdroj útoku, postihnuté systémy, údaje a časovú os incidentu.
- Analytici využívajú nástroje na forenznú analýzu, prehľad logov, sieťovú analýzu a koreláciu dát.
- Správne vyhodnotenie incidentu umožňuje zvoliť primerané reakčné opatrenia a stanoviť prioritu riešenia.



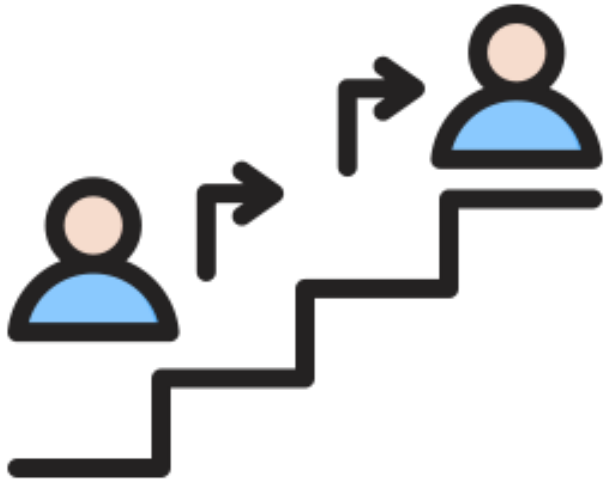
Reakcia na incident a jeho mitigácia

- Cieľom fázy reakcie je zastaviť a eliminovať aktívny kybernetický útok a minimalizovať jeho dopad.
- Zahŕňa izoláciu napadnutých systémov, prerušenie pripojení a zamedzenie ďalšiemu šíreniu útoku.
- Vykonávajú sa mitigačné opatrenia – odstránenie škodlivých súborov, blokovanie IP adries, zmena hesiel, vypnutie služieb.
- Incident Response tím dokumentuje všetky kroky v nástrojoch ako TheHive, DFIR-IRIS, RTIR alebo Znuny.
- Počas reakcie prebieha komunikácia s ďalšími tímami (napr. administrátori, CIRT, vedenie organizácie).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Eskalácia incidentu a rozdelenie úloh v tíme

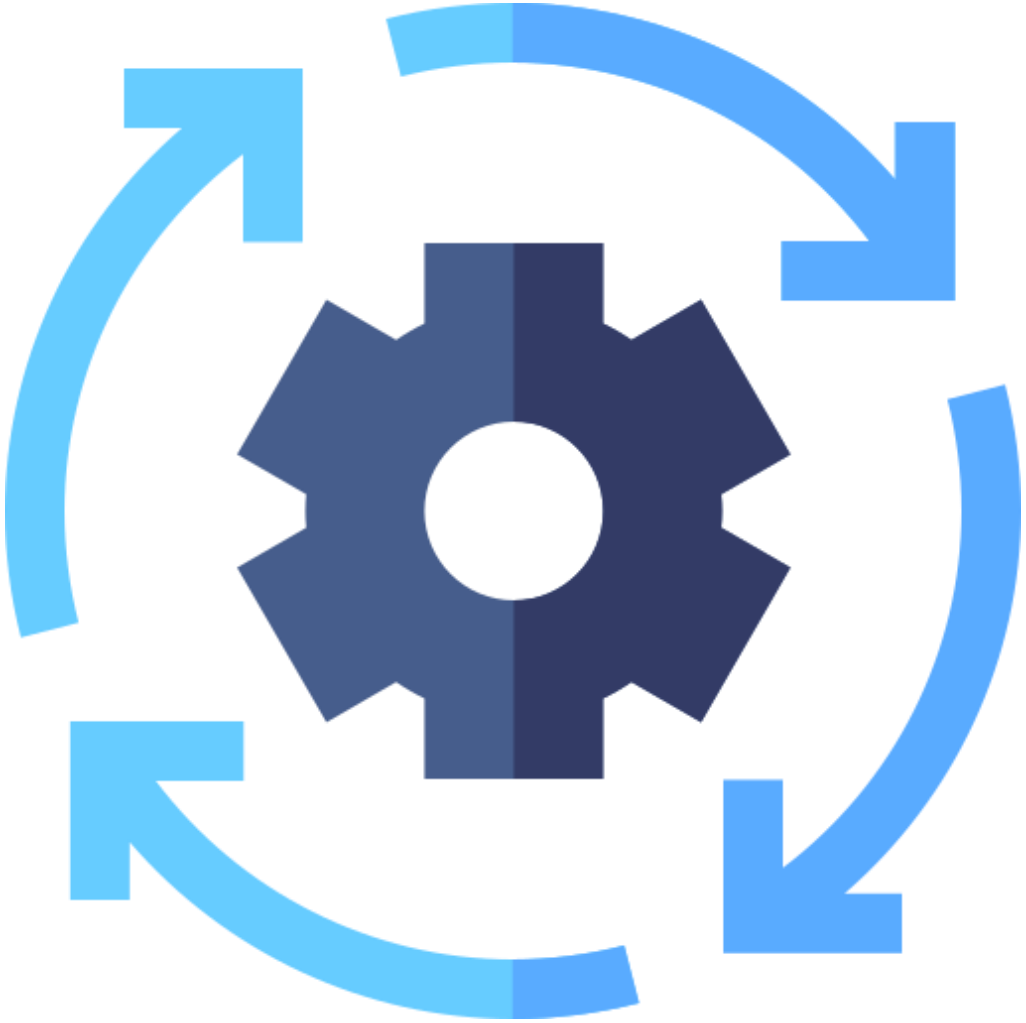
- Ak incident nemožno vyriešiť na základnej úrovni, dochádza k jeho **eskalácii na vyššiu úroveň odbornosti**.
- Cieľom eskalácie je zabezpečiť rýchle a efektívne riešenie zložitejších alebo kritických incidentov.
- Incident sa v rámci IR systému (napr. **TheHive, DFIR-IRIS**) priraďuje **špecializovanému analytikovi alebo tímu (Tier 2 / Tier 3 / CIRT)**.
- Počas eskalácie je kľúčová **koordinácia a komunikácia** medzi jednotlivými úrovňami tímu.
- Všetky kroky eskalácie sa **dokumentujú v IR nástroji**, aby bola zachovaná sledovateľnosť a kontinuita riešenia.



Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Obnova po incidente

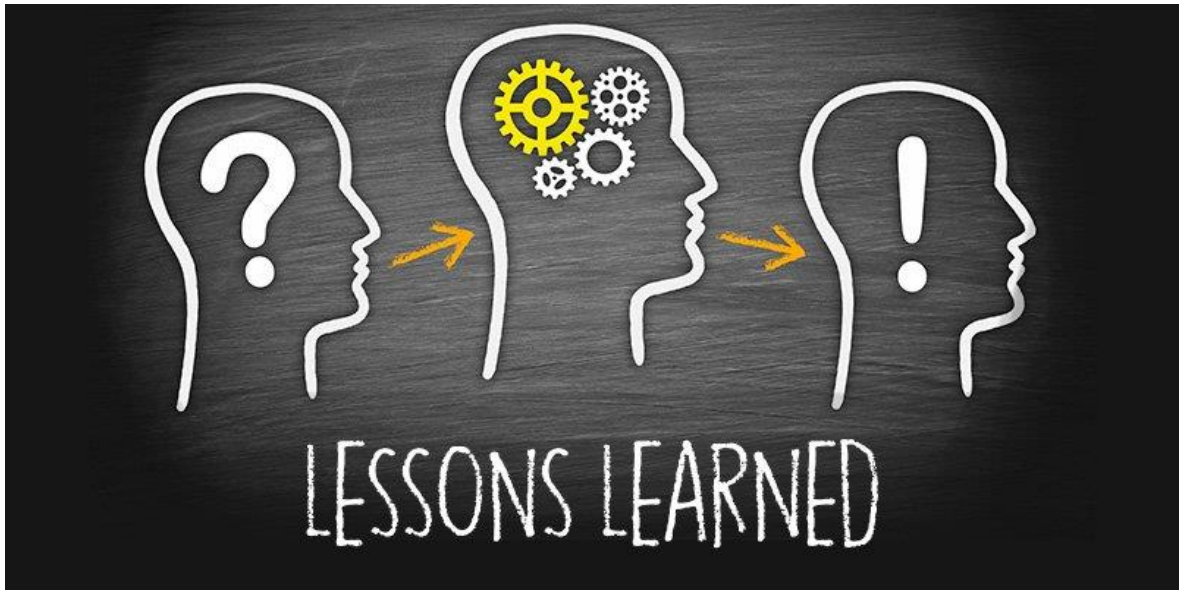
- Cieľom fázy obnovy je **obnoviť bežnú prevádzku systémov** po incidente a **overiť, že boli odstránené všetky hrozby**.
- Zahŕňa obnovenie služieb, dát, konfigurácií a pripojení v bezpečnom stave.
- Pred opätovným uvedením do prevádzky sa vykonáva **validácia a testovanie** systémov, aby sa zabránilo opakovaniu útoku.
- Všetky vykonané kroky a výsledky sa evidujú v IR nástrojoch (napr. *TheHive*, *DFIR-IRIS*).
- Po obnove sa pripravuje **záverečná správa o incidente**, ktorá slúži na zlepšenie procesov a prevencie budúcich útokov.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Spätná analýza incidentu (Lessons Learned)

- Cieľom **fázy Lessons Learned** je vyhodnotiť priebeh incidentu a prijať opatrenia na zlepšenie procesov.
- **Vyhodnotenie priebehu incidentu** – analýza krokov, ktoré boli vykonané počas detekcie, reakcie a obnovy.
- **Identifikácia silných a slabých stránok** – čo fungovalo dobre, čo je potrebné zlepšiť.
- **Tvorba „After Action Report (AAR)"** – dokumentácia priebehu, rozhodnutí a odporúčaní.
- **Aktualizácia plánov a postupov IR** – úprava Incident Response Plánu, playbookov, komunikačných procesov.
- **Zdieľanie poznatkov** – interné školenia, workshopy, alebo report pre manažment / CIRT.



Fáza Lessons Learned uzatvára Incident Response cyklus a zabezpečuje neustále zlepšovanie procesov a nástrojov organizácie.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Prepojenie SOC centra s procesom riešenia incidentov

Úloha SOC centra v procese riešenia incidentov

- SOC centrum (Security Operations Center) predstavuje kľúčový prvok v **procese monitorovania, detekcie a riadenia bezpečnostných incidentov**.
  Zabezpečuje **nepretržitý dohľad nad infraštruktúrou**, vyhodnocuje udalosti a poskytuje vstupy pre Incident Response tím.
- **Hlavné funkcie SOC:**
- **Zber a korelácia dát** – SIEM, log manažment, monitorovanie udalostí.
- **Detekcia a analýza incidentov** – vyhodnocovanie alertov, hľadanie hrozieb (Threat Intelligence).
- **Eskalácia a reakcia** – odovzdanie incidentu IR tímu (TheHive, DFIR-IRIS).
- **Reportovanie a komunikácia** – informovanie vedenia, tvorba reportov.
- **Znalostná báza a vývoj** – zlepšovanie detekcie, tvorba playbookov, aktualizácia politiky.

SOC centrum predstavuje **srdce kybernetickej obrany** organizácie – zhromažďuje informácie, vyhodnocuje incidenty a zabezpečuje efektívnu reakciu prostredníctvom IR tímov.

Nástroje pre riešenie incidentov

TheHive – úvod a účel

- **TheHive** je platforma pre riadenie a koordináciu kybernetických incidentov,
  - dostupná vo **voľne dostupnej open-source**
  - aj **komerčnej enterprise** verzii.
- Slúži ako **centrálna IR platforma**, ktorá umožňuje evidenciu, analýzu a koordináciu incidentov v rámci SOC a CSIRT tímov.
- Incidenty sú vedené vo forme **„cases“**, ktoré obsahujú:
  - artefakty,
  - IOC,
  - úlohy
  - a dokumentáciu priebehu vyšetrovania.
- Cieľom je:
  - **tímová spolupráca**,
  - prehľadný workflow
  - a **automatizácia reakčných procesov**.
- Platformu TheHive možno rozšíriť o doplnkové moduly, ako Cortex (automatizácia a analýza artefaktov) a MISP (Threat Intelligence a zdieľanie IOC).
- Ich prepojenie tvorí **integrovaný ekosystém pre Incident Response**, ktorý podporuje celý **životný cyklus riešenia incidentov**.

Architektúra a integrácie ekosystému TheHive

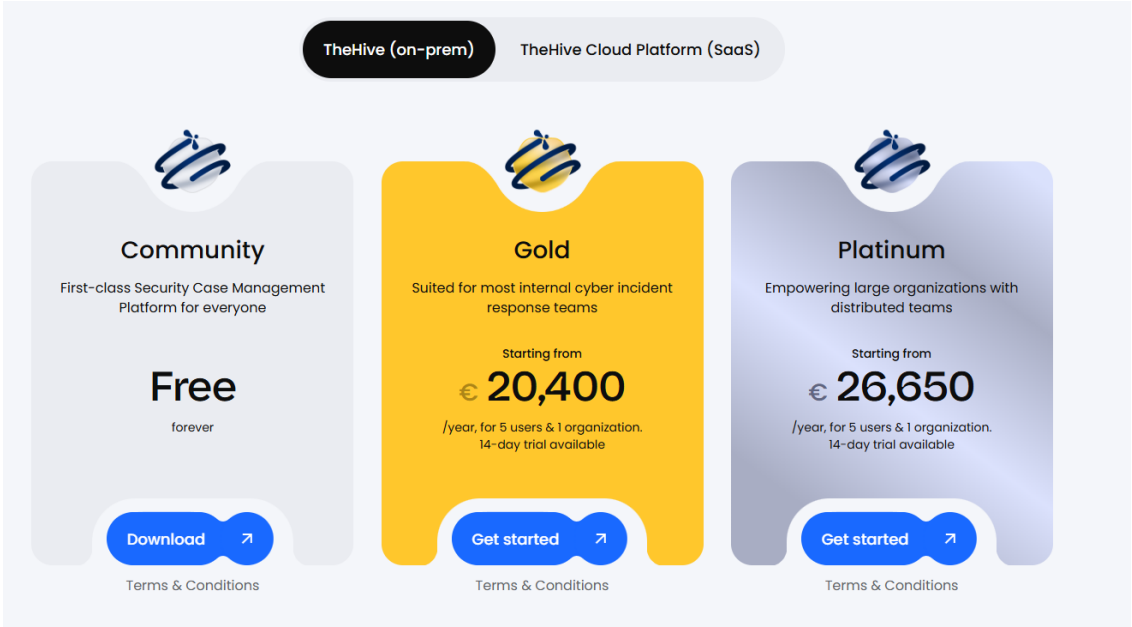
- **TheHive** je modulárne riešenie, ktoré umožňuje rozšírenie o doplnkové komponenty a integráciu s ďalšími bezpečnostnými systémami.
- Základ tvorí **TheHive Core**, ktorý slúži ako **c**entrálny bod pre správu incidentov a tímovú spoluprácu.
- Prostredníctvom REST API komunikuje s externými modulmi a nástrojmi ako:
  - **Cortex**
    - vykonáva automatizovanú analýzu artefaktov (hash, IP, URL, domény) pomocou analyzérov (napr. VirusTotal, AbuseIPDB, HybridAnalysis).
  - **MISP**
    - slúži ako **Threat Intelligence platforma** pre zdieľanie IOC, kampaní a TTPs a ich automatický import do prípadov v TheHive.
  - **SIEM a EDR systémy**
    - ako zdroje detekcie incidentov (napr. Splunk, Wazuh, SentinelOne, CrowdStrike).
  - **Integrácie s ticketovacími alebo e-mail systémami**
    - napr. Znuny, RTIR, ServiceNow, ktoré umožňujú automatizované vytváranie incidentov v TheHive.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje pre riešenie incidentov – TheHive

Vývoj a verzie TheHive platformy

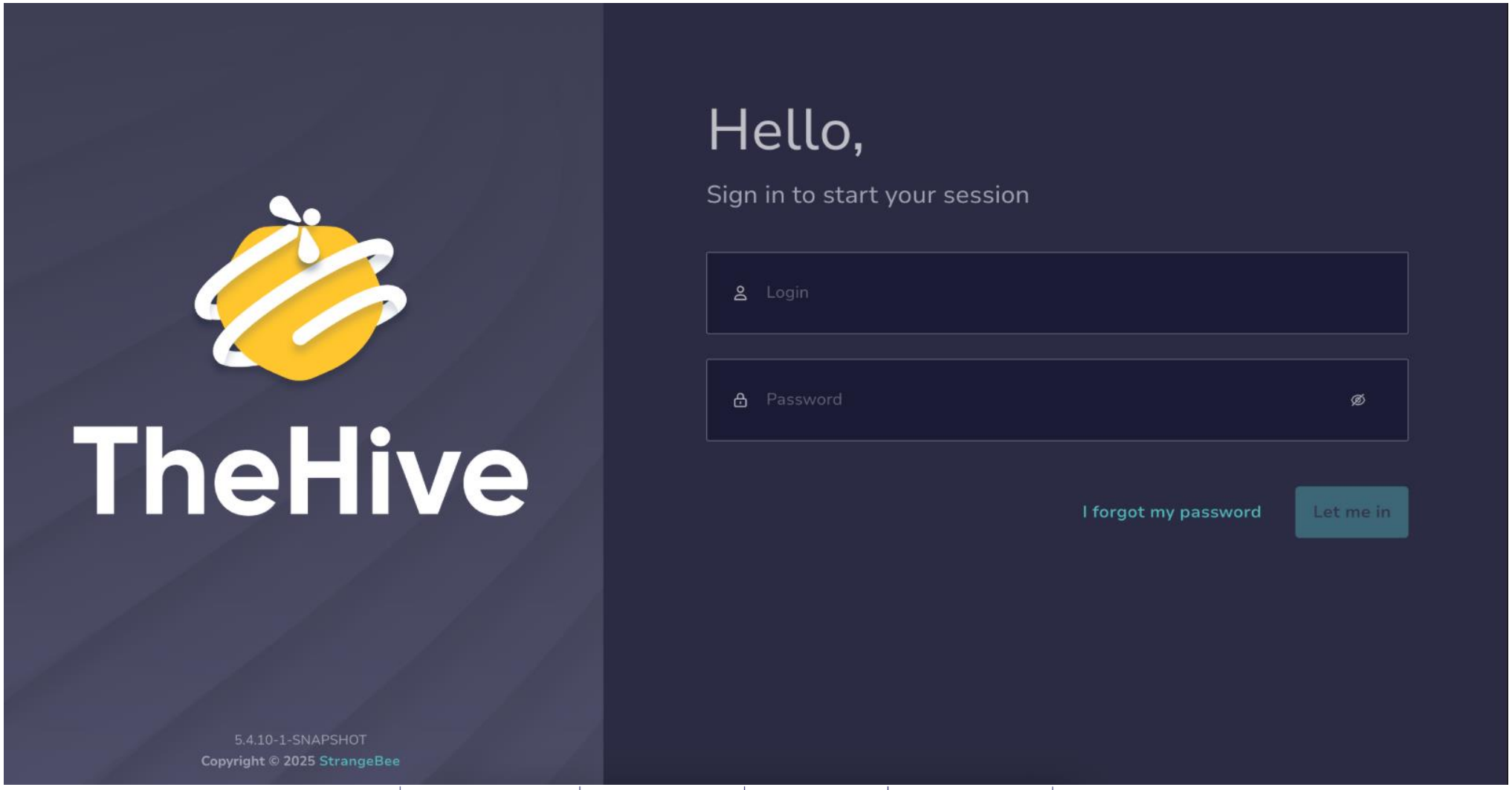
- **TheHive Project (verzia 3.x – 4.x)** – pôvodná open-source verzia spravovaná komunitou *TheHive Project*.
- **TheHive 5 / Enterprise (StrangeBee)** – aktuálna verzia vyvíjaná firmou *StrangeBee*, dostupná v edíciách:
  - **Community** – bezplatná, vhodná pre menšie tímy.
  - **Gold** – komerčná, s rozšírenou podporou a integráciami.
  - **Platinum** – pre veľké tímy a enterprise prostredia, s možnosťou SLA a multi-tenant správy.



FEATURES BY SERVICE LEVEL	Community	Gold	Platinum
Quotas			
NUMBER OF USERS	2	pay per user	pay per user
NUMBER OF ORGANIZATIONS	1	Pay per org (up to 5)	Pay per org
MULTI-TENANCY	–	✓	✓
CORTEX SERVERS	1	Up to 5	Unlimited
MISP SERVERS	1	Up to 5	Unlimited
Features			

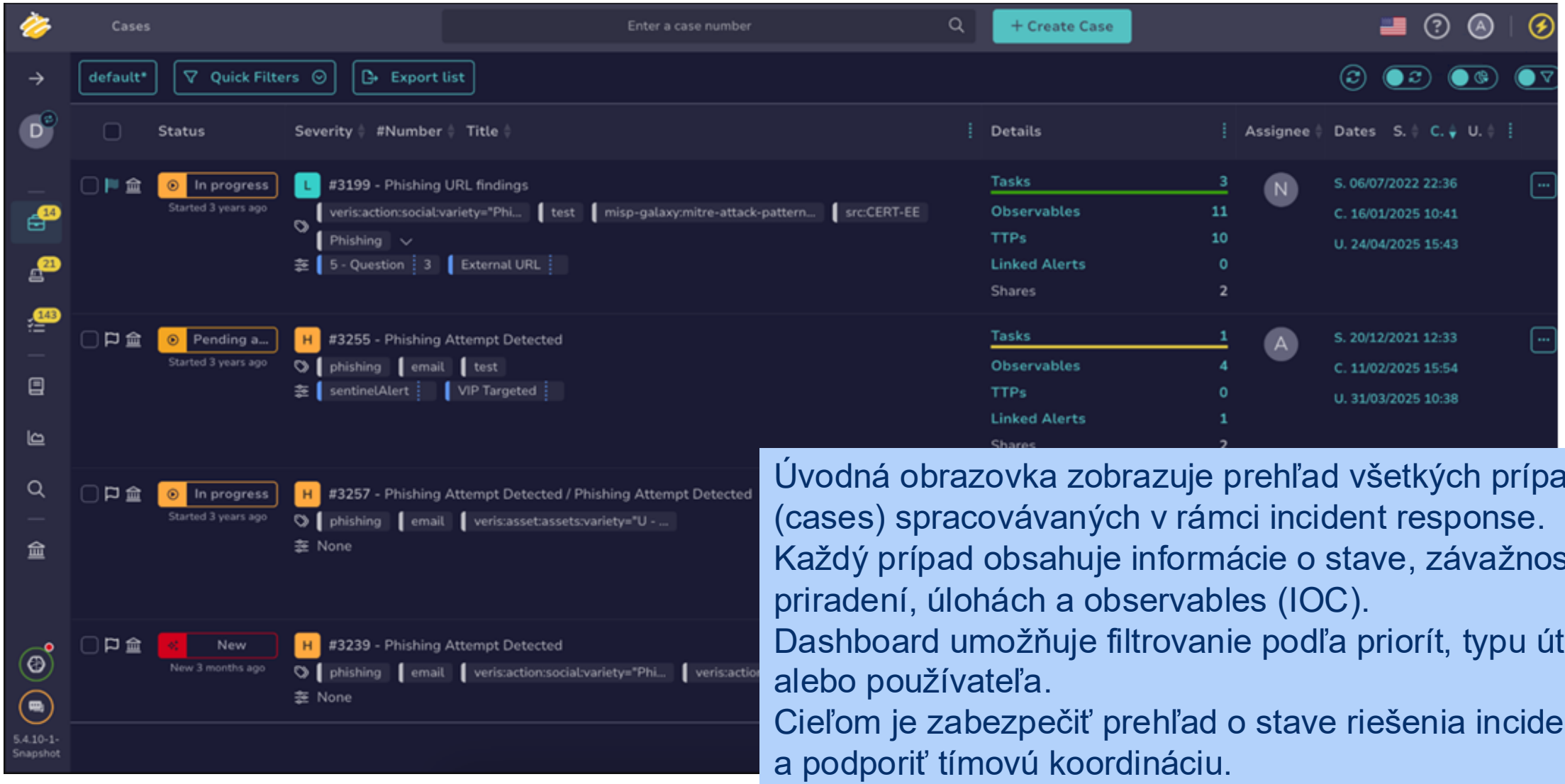
Nástroje pre riešenie incidentov – TheHive

Ukážka prostredia úvodná obrazovka



Nástroje pre riešenie incidentov – TheHive

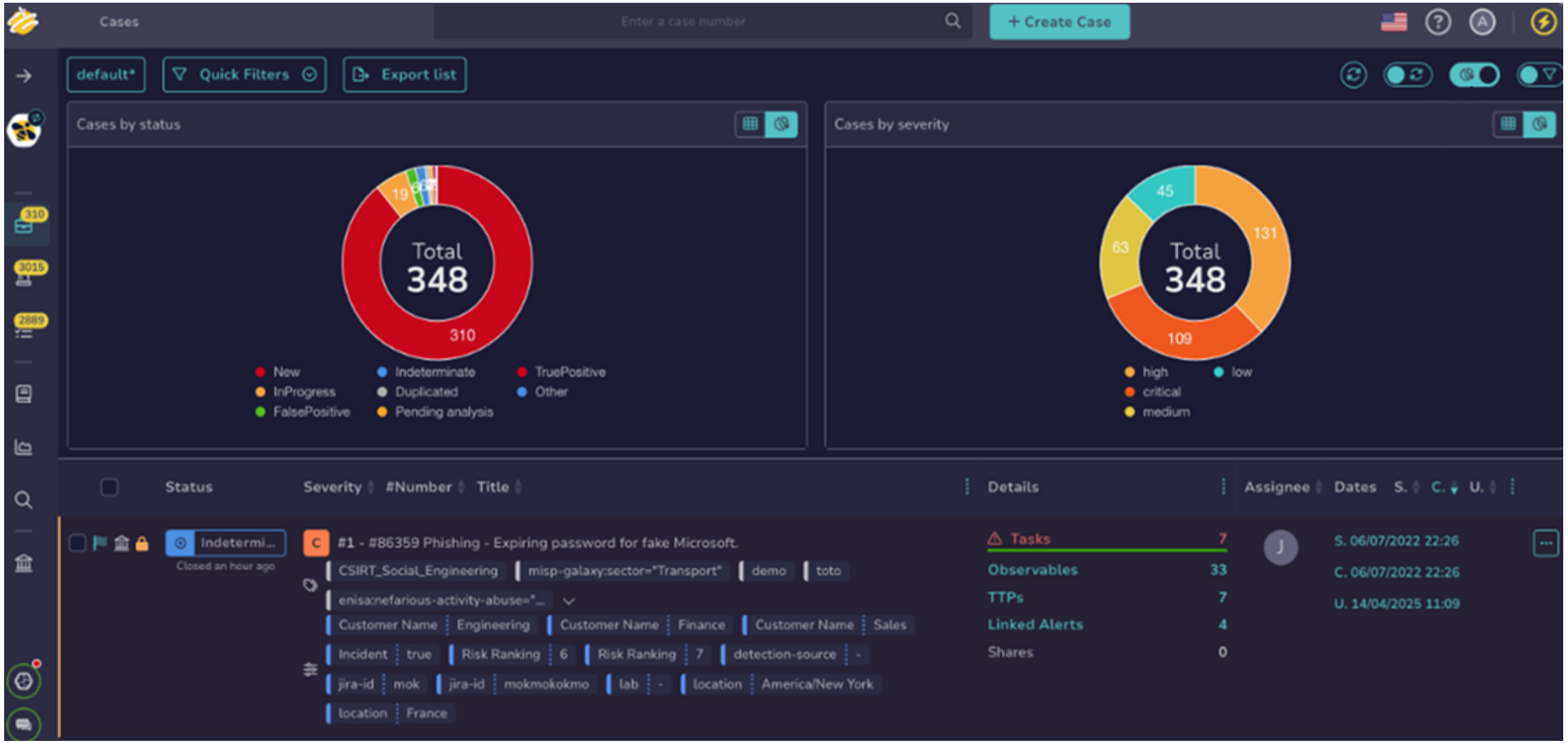
Prehľad prostredia (Dashboard) v TheHive



Úvodná obrazovka zobrazuje prehľad všetkých prípadov (cases) spracovávaných v rámci incident response.
Každý prípad obsahuje informácie o stave, závažnosti, priradení, úlohách a observables (IOC).
Dashboard umožňuje filtrovanie podľa priorít, typu útoku alebo používateľa.
Cieľom je zabezpečiť prehľad o stave riešenia incidentov a podporiť tímovú koordináciu.

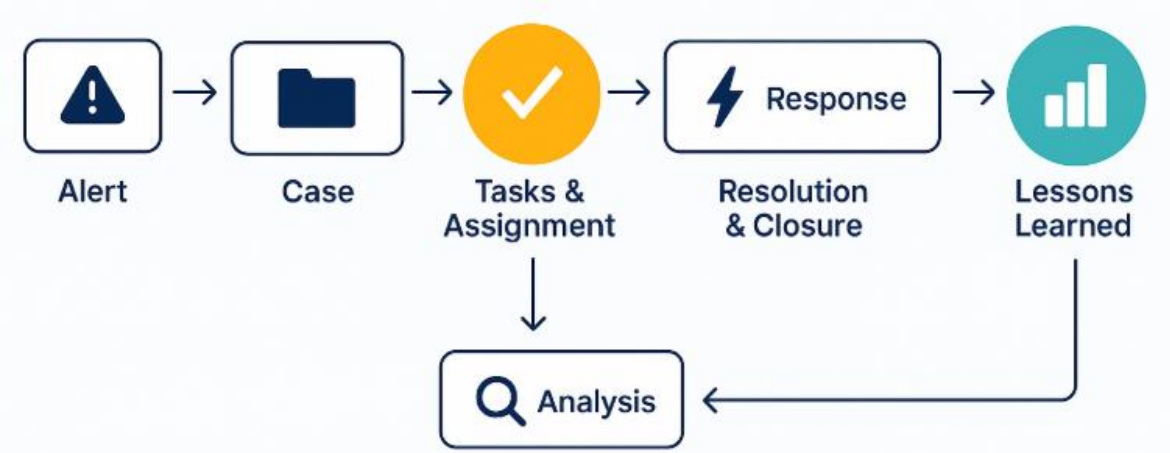
Nástroje pre riešenie incidentov – TheHive

Prehľad prostredia štatistiky v TheHive



Proces spracovania incidentu (Case Workflow)

- V systéme **TheHive** prebieha spracovanie incidentu ako ucelený proces, ktorý pokrýva všetky fázy riešenia kybernetických incidentov – od prijatia hlásenia až po jeho vyhodnotenie.
  - **1. Prijatie hlásenia (Alert)** – incident môže byť automaticky importovaný z detekčných systémov (napr. SIEM, IDS/IPS) alebo manuálne nahlásený operátorom.
  - **2. Vytvorenie prípadu (Case)** – z prijatého hlásenia sa vytvorí nový prípad, v ktorom sa zhromažďujú všetky informácie o incidente.
  - **3. Priradenie úloh a členov tímu (Tasks & Assignment)** – manažér incidentu rozdelí úlohy medzi analytikov a stanoví priority.
  - **4. Analýza artefaktov (Analysis)** – jednotlivé IOC (IP, hash, URL, e-mail) sa odosielajú na analýzu do modulu **Cortex** alebo porovnávajú s databázami hrozieb v **MISP**.
  - **5. Korelácia a reakcia (Response)** – výsledky analýzy sú využité na prijatie opatrení, eskaláciu prípadu alebo jeho mitigáciu.
  - **6. Uzavretie prípadu (Resolution & Closure)** – po odstránení hrozby sa prípad uzavrie a vytvorí sa záznam o priebehu vyšetrovania.
  - **7. Vyhodnotenie a zlepšenie (Lessons Learned)** – tím vyhodnotí postup, identifikuje rezervy a aktualizuje playbooky alebo politiky.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY

Výhody a nevýhody platformy TheHive

Výhody

- **Prehľadná IR platforma** – zjednocuje všetky fázy riešenia incidentu do jedného prostredia.
- **Otvorený ekosystém** – natívne integrácie s **Cortex** (automatizácia) a **MISP** (Threat Intelligence).
- **Flexibilná architektúra a REST API** – umožňuje jednoduché prepojenie so SIEM, EDR a ticketovacími systémami.
- **Spolupráca tímov** – umožňuje priraďovanie úloh, zdieľanie poznámok, alertov a audit trail.
- **Moderné rozhranie a prehľadné dashboardy** – vhodné pre rýchlu orientáciu a reporting.

Nevýhody

- **Chýba natívny ticketovací modul** – na komplexné riadenie požiadaviek je vhodné doplniť napr. **Znuny/RTIR**.
- **Zložitejšia prvotná konfigurácia** (vyžaduje znalosť Linuxu, Elasticsearch, konfigurácií API).
- **Niektoré funkcie (napr. multi-tenant, SLA)** sú dostupné len v platenej verzii.
- **Vyššia závislosť na externých moduloch** (Cortex, MISP), čo zvyšuje nároky na údržbu.

Nástroj RTIR

RTIR – úvod a účel

- **RTIR (Request Tracker for Incident Response)** je rozšírením systému **Request Tracker (RT)** určeným pre **CERT a CSIRT tímy**.
  Slúži na **správu a koordináciu kybernetických incidentov** prostredníctvom prepojených tiketov.
  - Každý incident je evidovaný ako **tiket (Request/Ticket)**, ktorý môže mať typ:
  - *Incident Report* – hlásenie o incidente,
  - *Incident* – hlavný tiket prípadu,
  - *Investigation* – vyšetrovanie alebo technická analýza,
  - *Block* – mitigácia (blokovanie IP, izolácia zariadenia).

RTIR umožňuje:

- príjem hlásení e-mailom alebo cez formulár,
- automatické vytváranie tiketov a ich prepojenie,
- spoluprácu analytikov a komunikáciu s externými subjektmi,
- sledovanie priebehu riešenia a vytváranie reportov.

Architektúra a možnosti integrácie systému RTIR

RTIR je modul postavený na platforme **Request Tracker (RT)**, ktorá beží na **Perl aplikácii s webovým rozhraním** a relačnou databázou (MySQL, PostgreSQL).

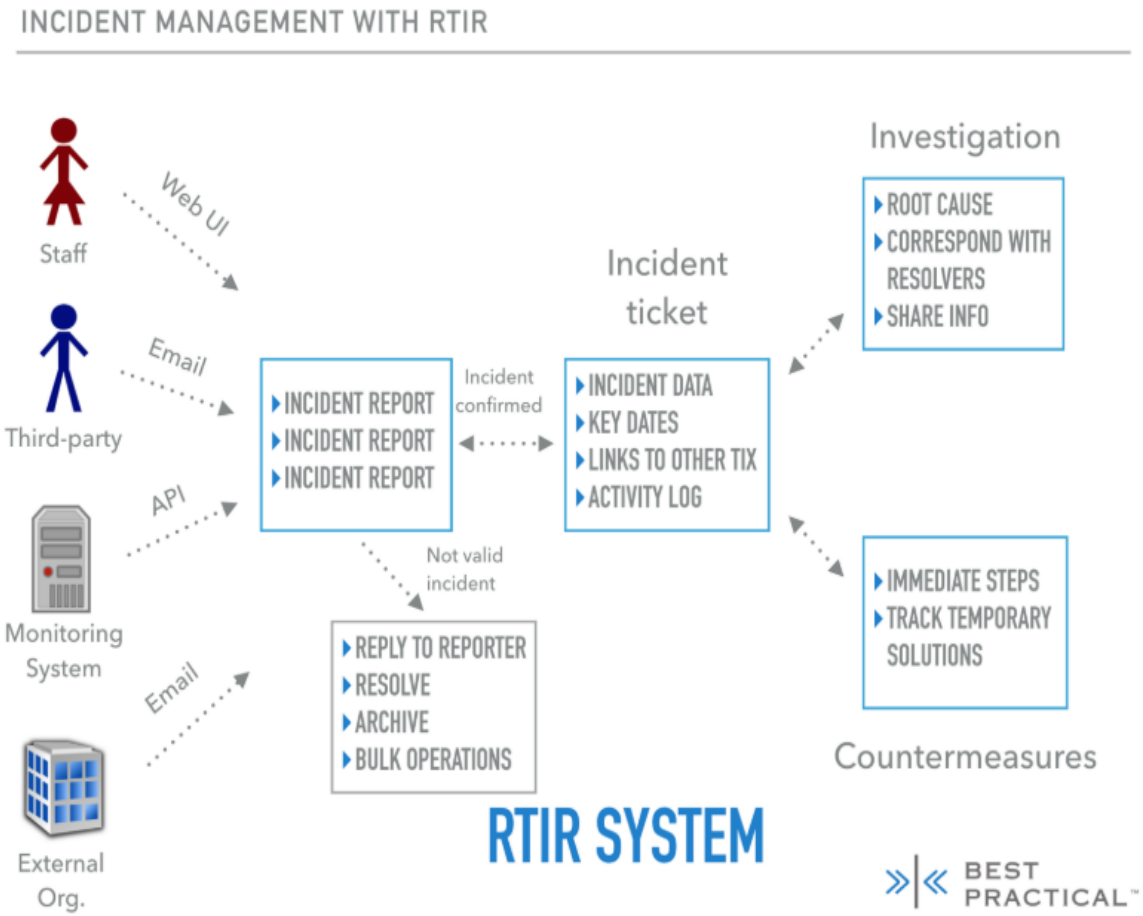
Architektúra systému využíva REST API, ktoré umožňuje prepojenie s externými detekčnými a analytickými nástrojmi.

Základné komponenty:

- **RT Core** – správa tiketov, workflow a používateľov,
- **RTIR module** – rozšírenie o incidentové typy (Incident, Report, Investigation, Block),
- **MailGate / REST API** – rozhranie pre automatický príjem hlásení, integráciu a správu tiketov.

Integrácie a prepojenia:

- **SIEM systémy** – automatizovaný import alertov ako incident reports (napr. Wazuh, Splunk, ELK).
- **EDR alebo IDS/IPS** – zasielanie detekcií e-mailom alebo cez API.
- **MISP (Threat Intelligence)** – možné prepojenie pomocou komunitných doplnkov alebo vlastných skriptov.
- **E-mail systémy** – plná integrácia – RTIR vie vytvárať a spracovávať incidenty prijaté e-mailom.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Incident management v RTIR

1

Príjem a nahlasovanie incidentov

Incidenty sú prijímané z rôznych zdrojov: interní zamestnanci prostredníctvom webového rozhrania, tretie strany cez e-mail, monitorovacie a detekčné systémy prostredníctvom API. Všetky počiatočné hlásenia sú evidované ako Incident Report tikety.

2

Validácia incidentu

V nasledujúcom kroku prebieha validácia incidentu, počas ktorej IR tím posudzuje, či nahlásená udalosť predstavuje skutočný bezpečnostný incident. V prípade, že sa nejedná o relevantný incident, tiket je uzavretý a archivovaný. Ak je incident potvrdený, postupuje sa do ďalšej fázy spracovania.

3

Vytvorenie hlavného incidentového tiketu

Po potvrdení vzniká hlavný Incident Ticket, ktorý slúži ako centrálny bod pre riadenie incidentu. Tento tiket obsahuje podrobné informácie o incidente, časové údaje, odkazy na súvisiace tikety a kompletný záznam aktivít počas riešenia. Incident Ticket tak prepája všetky informácie potrebné pre koordináciu riešenia.

4

Fáza vyšetrovania (Investigation)

Ďalšou fázou je vyšetrovanie (Investigation), v ktorej sa vykonáva analýza koreňovej príčiny incidentu, prebieha komunikácia s riešiteľskými tímami a dochádza k zdieľaniu informácií medzi členmi IR tímu s cieľom pochopiť príčinu a rozsah incidentu.

5

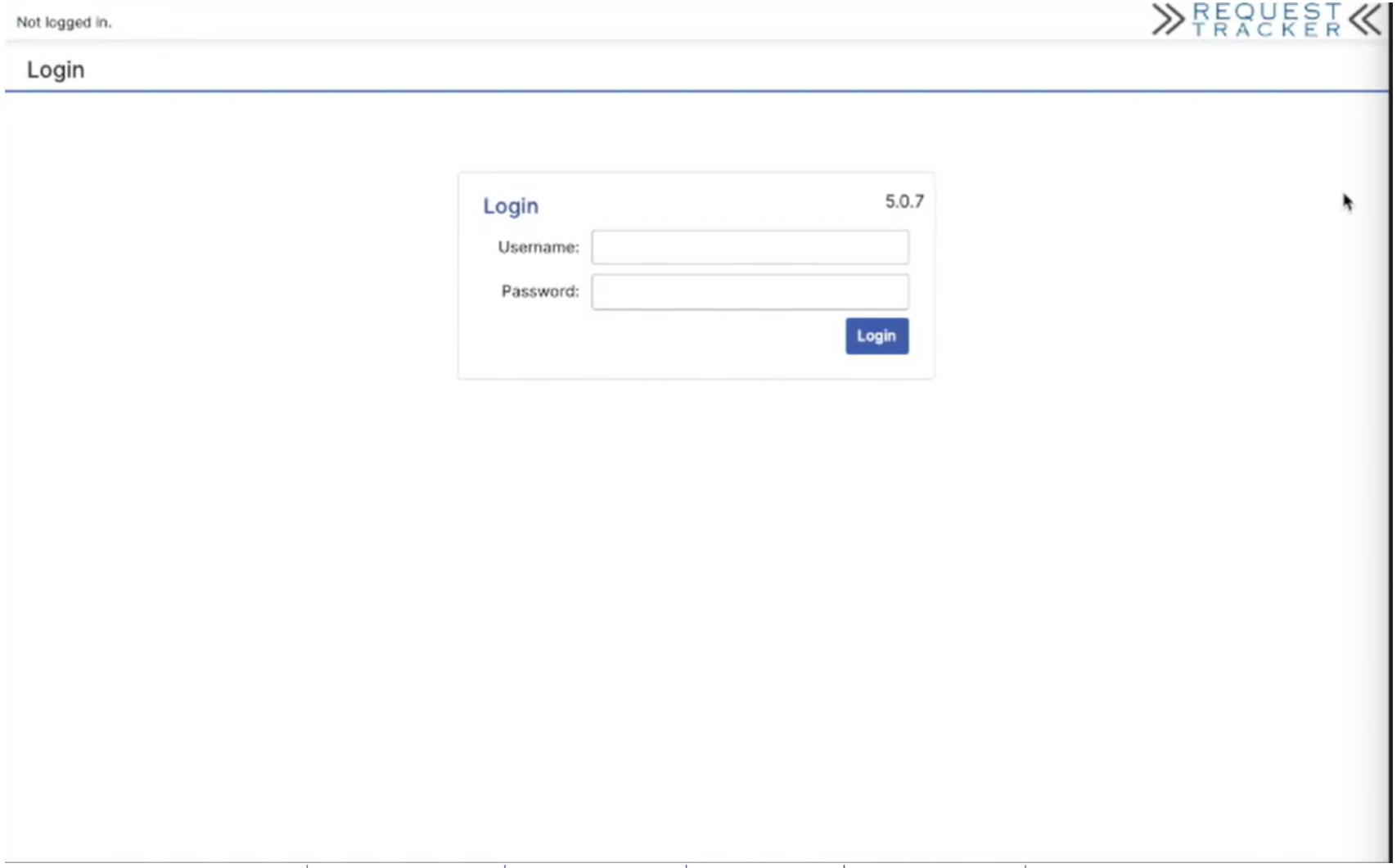
Implementácia opatrení (Countermeasures)

Záverečnou časťou procesu je implementácia opatrení (Countermeasures). V tejto fáze sa realizujú okamžité reakčné kroky na obmedzenie dopadu incidentu, sleduje sa účinnosť dočasných riešení a všetky vykonané opatrenia sú priebežne dokumentované.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

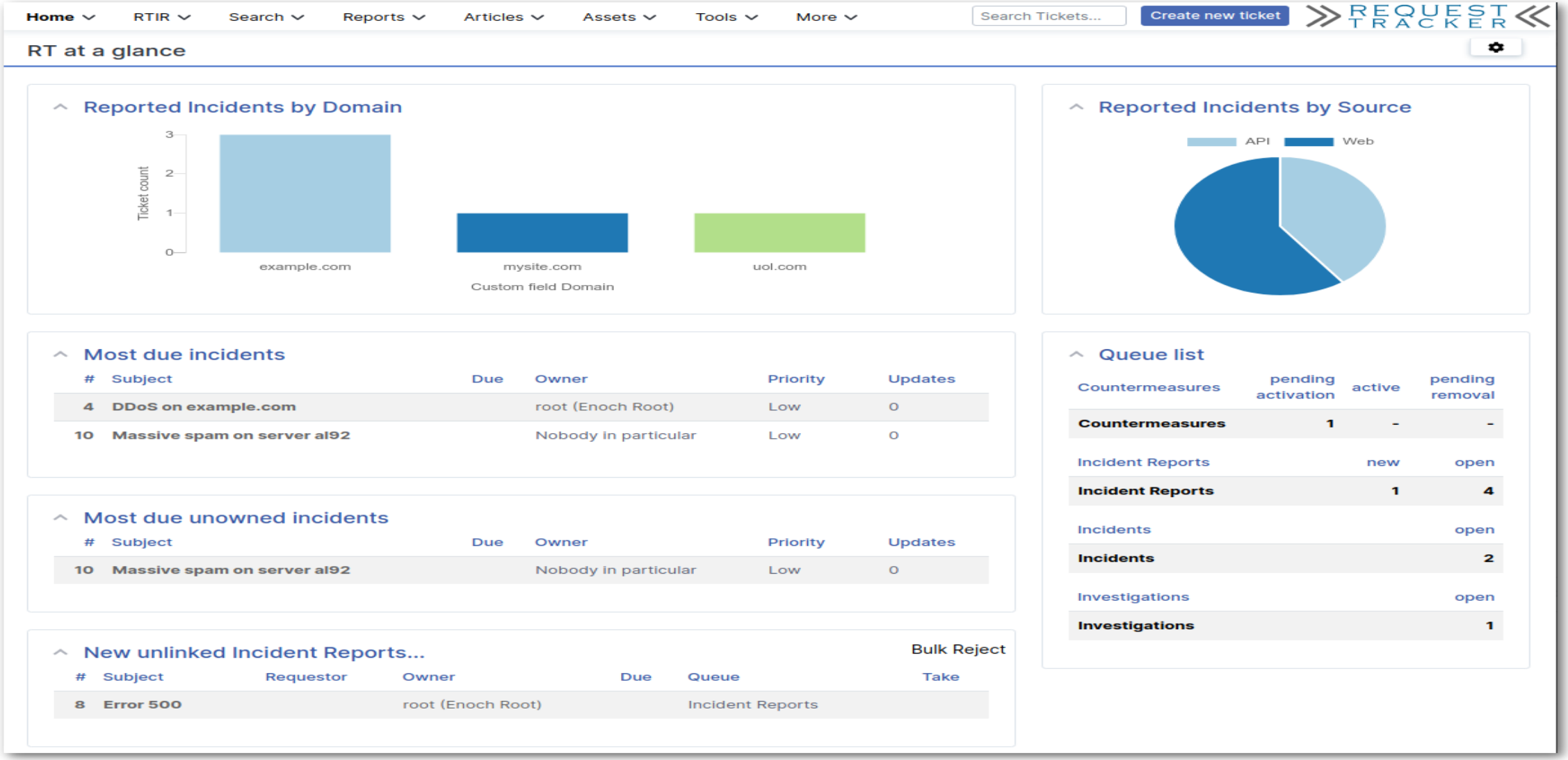
Nástroje pre riešenie incidentov – RTIR

Ukážka prostredia úvodná obrazovka



Nástroje pre riešenie incidentov – RTIR

Prehľad prostredia štatistiky v RTIR (Dashboard)



Nástroje pre riešenie incidentov – RTIR

Kľúčové funkcie RTIR Dashboardu (RT at a glance)

Dashboard „RT at a glance" poskytuje rýchly prehľad o aktuálnom stave incidentov a tiketov v systéme RTIR. Slúži ako úvodná obrazovka, ktorá analytikovi umožňuje okamžite vidieť najdôležitejšie informácie pre riadenie incidentov.

Reportované incidenty podľa domény/zdroja

Prehľady zobrazujú, z akých domén prichádzajú hlásenia a akým spôsobom boli prijaté (API, web, e-mail), čím pomáhajú identifikovať najčastejšie zdroje incidentov.

Incidenty s najbližším termínom riešenia

Zobrazuje tikety s blížiacim sa termínom, ich predmet, priradeného riešiteľa, prioritu a počet aktualizácií, umožňujúc efektívne určovanie priorít.

Incidenty bez priradeného riešiteľa

Upozorňuje na incidenty s blížiacim sa termínom, ktoré ešte nemajú priradeného riešiteľa, čím predchádza prehliadnutiu dôležitých úloh.

Nové neprepojené hlásenia incidentov

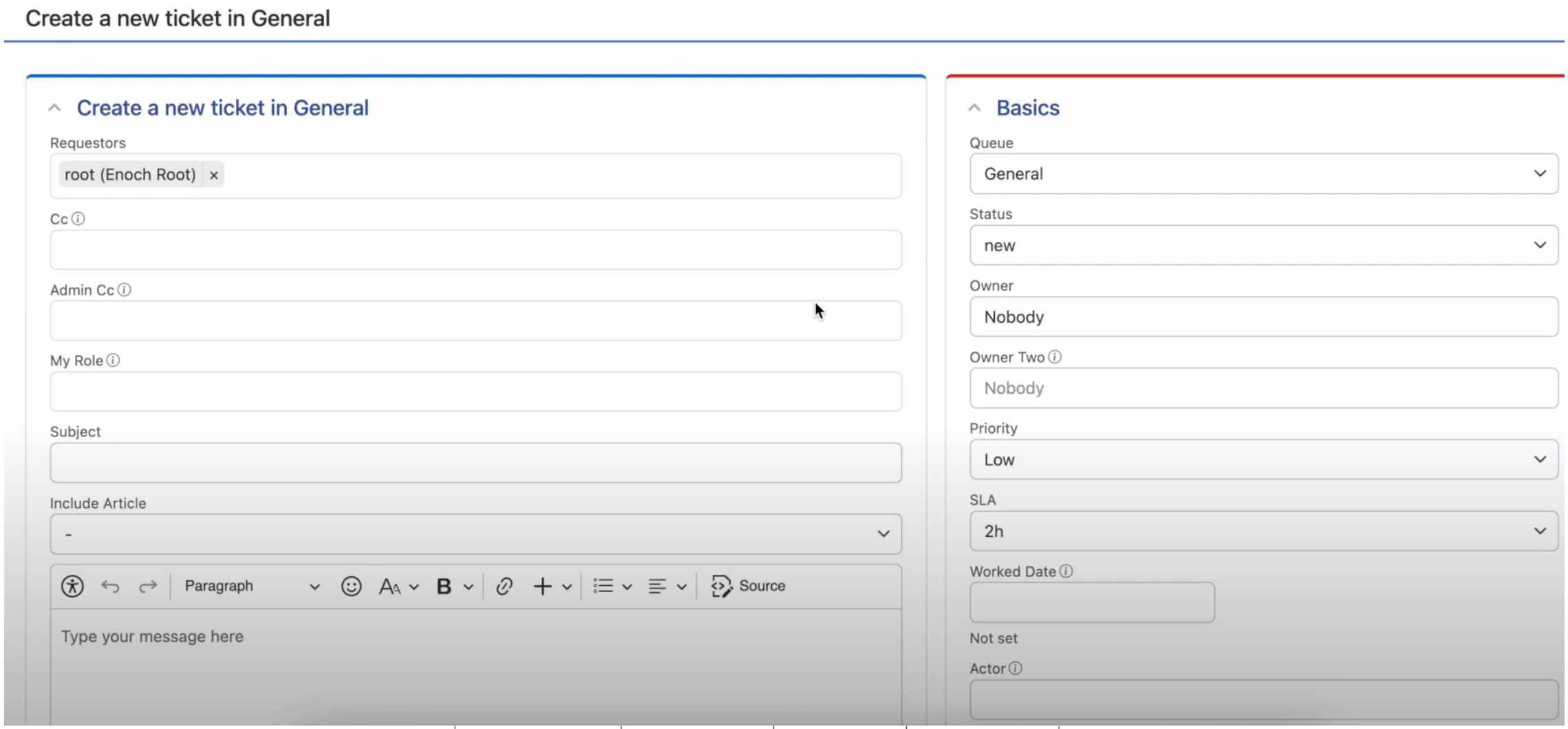
Hlásenia, ktoré ešte nie sú priradené ku konkrétnemu incidentu. Slúži na manuálne preverenie, zlúčenie alebo zaradenie do správneho frontu.

Zoznam frontov (stav frontov)

Zobrazuje aktuálny stav jednotlivých typov tiketov (Incident Reports, Incidents, Investigations, Countermeasures) vrátane počtu nových, otvorených a čakajúcich tiketov v každom fronte.

Nástroje pre riešenie incidentov – RTIR

Vytvorenie nového tiketu v RTIR



Spravovanie lístkov v RTIR

1

Metódy vytvorenia

Tiket v RTIR je možné vytvoriť:

- manuálne cez webové rozhranie,
- automaticky z e-mailov,
- integráciou s detekčnými systémami (napr. SIEM).

2

Základné atribúty tiketu

Každý tiket obsahuje:

- **Queue** – typ incidentu (Incident Report, Investigation, Block),
- **Status** – stav riešenia (new, open, resolved),
- **Owner** – zodpovedný analytik,
- **Priority a SLA** – závažnosť a čas reakcie.

3

Spracovanie a workflow

Interné workflow riešenia incidentu:

- Spracovanie tiketu,
- Prepojenie s ďalšími tiketmi,
- Vytvorenie incidentového prípadu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výhody a nevýhody systému RTIR

Výhody

- **Overený nástroj pre CSIRT/SOC tímy** – používaný v praxi mnohými národnými a univerzitnými CSIRT tímami.
- **Plne open-source** – bez licenčných poplatkov, on-premise inštalácia dostupná zdarma (len podpora a hosting sú platené).
- **Stabilné a spoľahlivé jadro** – postavené na platforme *Request Tracker (RT)* s dlhoročnou komunitou.
- **Flexibilný systém tiketov** – jasné rozdelenie incidentu do štyroch typov:
  Incident Report, *Incident*, *Investigation* a *Block* – uľahčuje koordináciu tímu.
- **Rozsiahle možnosti integrácie** – REST API, import alertov z *ELK/Wazuh*, export dát do *Elasticsearch*, komunitné moduly pre *MISP* a *CTI* (OpenCTI).
- **Automatizovaný e-mailový vstup** – nové tikety možno generovať priamo z e-mailov alebo systémových alertov.
- **Vhodný pre procesné riadenie incidentov a evidenciu komunikácie** – ideálny pre CSIRT organizácie, ktoré potrebujú auditovateľný proces.

Nevýhody

- **Zložitejšia implementácia a konfigurácia** – vyžaduje skúsenosti s *Perl, Apache, moduly RTIR*, databázami (*MySQL/PostgreSQL*).
- **Zastaranejšie používateľské rozhranie** – menej moderné oproti novším IR systémom (napr. DFIR-IRIS, TheHive).
- **Viacero tiketov na jeden incident** – znižuje prehľadnosť a zvyšuje administratívnu záťaž.
- **Menšia komunita pre bezpečnostné moduly** – väčšina integrácií (napr. MISP, Wazuh) funguje len cez komunitné skripty.
- **Obmedzená vizualizácia a reporting** – bez natívnych dashboardov, vizualizácie vyžadujú prepojenie s ELK alebo Grafana.
- **Vyššia náročnosť na správu servera** – potreba pravidelných aktualizácií a správy komponentov RT, RTIR a databázy.
- **Horšia a nejednotná dokumentácia** – často zastaraná, dopĺňaná komunitne.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

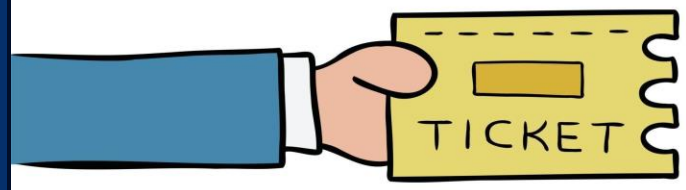
Nástroj ZNUNY

Znuny – úvod a účel

Znuny je open-source **ticketovací a ITSM systém**, ktorý vychádza z projektu **OTRS (Open Ticket Request System)**.

- Po ukončení vývoja OTRS Community Edition v roku 2020 vznikol **Znuny ako jeho aktívne udržiavaný nástupca**.
- Systém je určený na **správu požiadaviek, incidentov a komunikácie** – využíva sa v IT, helpdesk a bezpečnostných tímoch (vrátane SOC/CSIRT).
- V kontexte **Incident Response** môže Znuny slúžiť ako **centrálny systém na evidenciu, kategorizáciu a koordináciu incidentov** medzi používateľmi, administrátormi a analytikmi.
- Vďaka svojmu modulárnemu systému a REST API sa dokáže integrovať s ďalšími bezpečnostnými nástrojmi, ako napr. **TheHive, MISP, alebo SIEM platformy**.
- Existuje aj **komerčná verzia Znuny LTS**, ktorá ponúka dlhodobú podporu a rozšírené funkcie pre podnikové prostredia.

Znuny predstavuje univerzálny ticketovací nástroj, ktorý možno prispôsobiť pre potreby kybernetickej bezpečnosti. Poskytuje stabilnú platformu pre komunikáciu, koordináciu a správu incidentov v rámci SOC alebo ITSM prostredia.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra a možnosti integrácie systému Znuny

Znuny je postavené na **modulárnej architektúre**, ktorá umožňuje rozširovanie funkcií prostredníctvom doplnkov (add-ons) a integráciu s externými systémami.

Platforma beží na **Perl aplikácii** s **webovým rozhraním** a **relačnou databázou** (MySQL, PostgreSQL).

Komunikáciu a automatizáciu umožňuje **REST API**, cez ktoré možno prijímať alebo spracovávať požiadavky (incidenty, úlohy, notifikácie).

Základné komponenty:

- **Znuny Core** – správa tiketov, používateľov a workflow.
- **Generic Interface (REST / SOAP)** – rozhranie pre prepojenie s inými systémami (napr. SIEM, MISP, EDR).
- **Mail Gateway** – spracovanie e-mailov, automatické vytváranie alebo aktualizácia tiketov.
- **Scheduler / Daemons** – automatické úlohy (eskalácie, SLA, upozornenia).

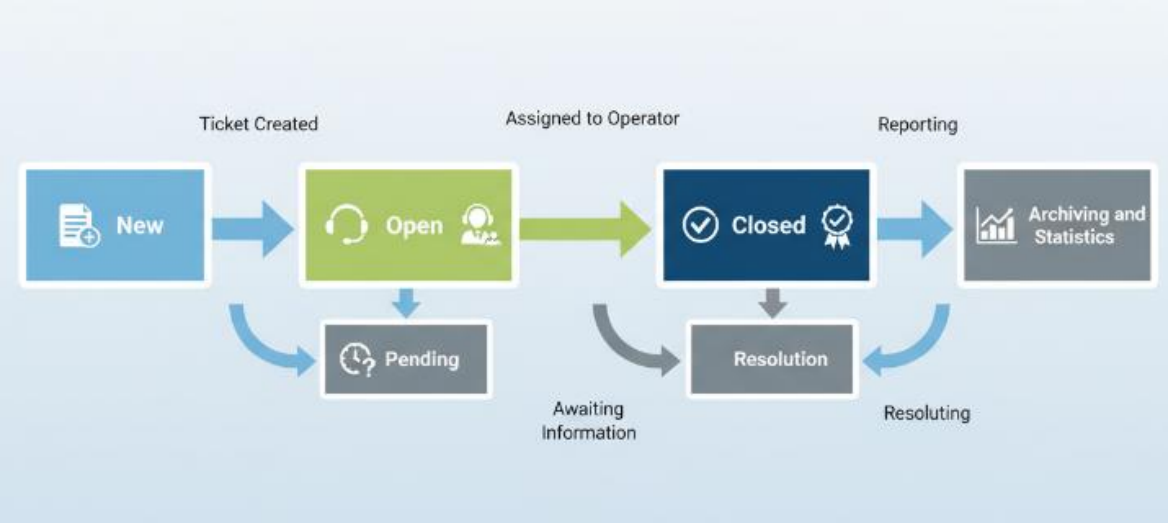
Integrácie:

- **SIEM a EDR systémy** – automatizovaný import incidentov (napr. Wazuh, Splunk, ELK).
- **MISP** – zdieľanie a import IOC prostredníctvom REST API alebo skriptov.
- **TheHive / Cortex** – obojsmerná výmena údajov o incidentoch a artefaktoch.
- **Ticketing a Helpdesk systémy** – integrácia s externými helpdesk riešeniami (napr. GLPI, RTIR).

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Životný cyklus ticketu v systéme Znuny

- **1. Vytvorenie tiketu (New):**
  Tiket vzniká po prijatí požiadavky – automaticky cez e-mail, API alebo manuálne používateľom.
  Systém mu priradí stav **New** a základné informácie (žiadateľ, priorita, téma).
- **2. Otvorenie a spracovanie (Open):**
  Po priradení operátorovi sa tiket presunie do stavu **Open**.
  V tejto fáze prebieha komunikácia so žiadateľom a riešenie incidentu.
- **3. Čakajúci stav (Pending reminder / auto):**
  Ak systém čaká na doplnenie údajov, potvrdenie alebo uplynutie času SLA, tiket sa presunie do stavu **Pending**.
  Tento stav môže byť automaticky ukončený po uplynutí času (pending auto).
- **4. Uzavretie prípadu (Closed):**
  Po vyriešení problému alebo potvrdení od používateľa sa tiket presunie do stavu **Closed**.
  Všetky správy, prílohy a kroky riešenia zostávajú archivované.
- **5. Archivácia a štatistiky:**
  Uzavreté tikety možno ďalej analyzovať, filtrovať alebo používať na reportovanie výkonnosti tímu SOC.



Prehľad prostredia štatistiky v Znuny (Dashboard)

Dashboard Znuny poskytuje centralizovaný prehľad o stave tiketov a aktivitách používateľov. Umožňuje rýchlu orientáciu v aktuálnych incidentoch a podporuje operatívne riadenie.

Sledovanie tiketov v reálnom čase

Rýchly prehľad o tiketoch podľa stavov: New, Open, Reminder, Escalated, Closed. Pomáha okamžite vidieť, čo je nové, čo čaká a čo je eskalované.

Štatistiky a prehľad výkonnosti

Zobrazuje počty vytvorených a uzavretých tiketov za posledné dni a trendy riešenia. Vhodné pre priebežné hodnotenie záťaže tímu.

Pokročilé filtrovanie

Možnosť filtrovať tikety podľa fronty, stavu, typu alebo priority čo uľahčuje zameranie sa na najdôležitejšie incidenty.

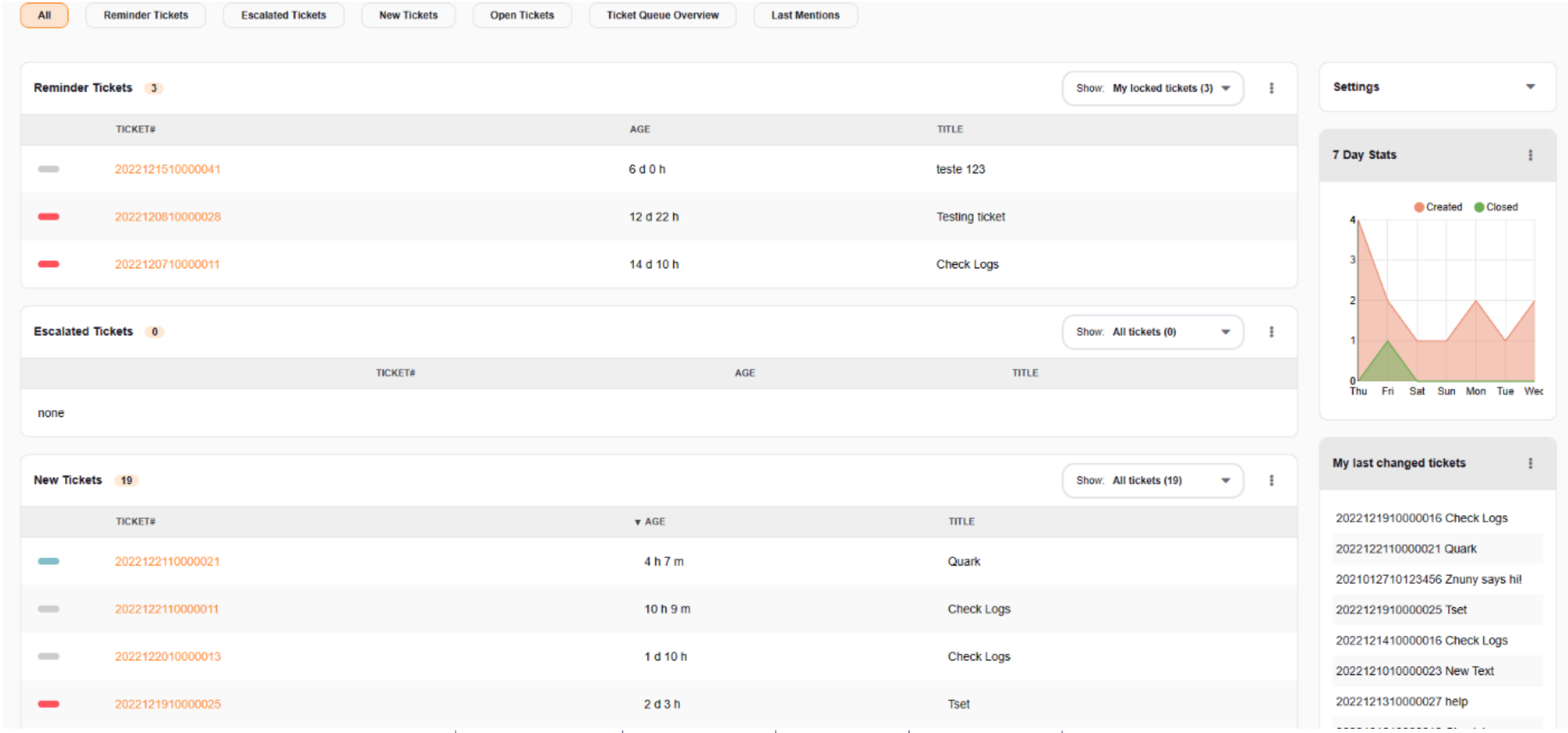
Podpora riadenia incidentov

Prehľad posledných zmien, aktivity používateľov a grafické štatistiky. Podporuje operatívne rozhodovanie aj reporting pre manažment.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje pre riešenie incidentov – Znuny

Prehľad prostredia štatistiky v Znuny (Dashboard)



Nástroje pre riešenie incidentov – Znuny

Výhody a nevýhody systému Znuny

Výhody:

- **Stabilná a overená platforma** – vychádza z OTRS, dlhodobo používaná v praxi.
- **Open-source a bez licencie**, dostupná aj v LTS verzii s podporou.
- **Flexibilný tiketovací systém** – vhodný pre správu incidentov aj IT požiadaviek.
- **Rozsiahle možnosti integrácie** – REST API, e-mail, prepojenie s TheHive alebo MISP.
- **Užívateľsky prispôsobiteľné rozhranie** – možnosť vlastných dashboardov a filtrov.

Nevýhody:

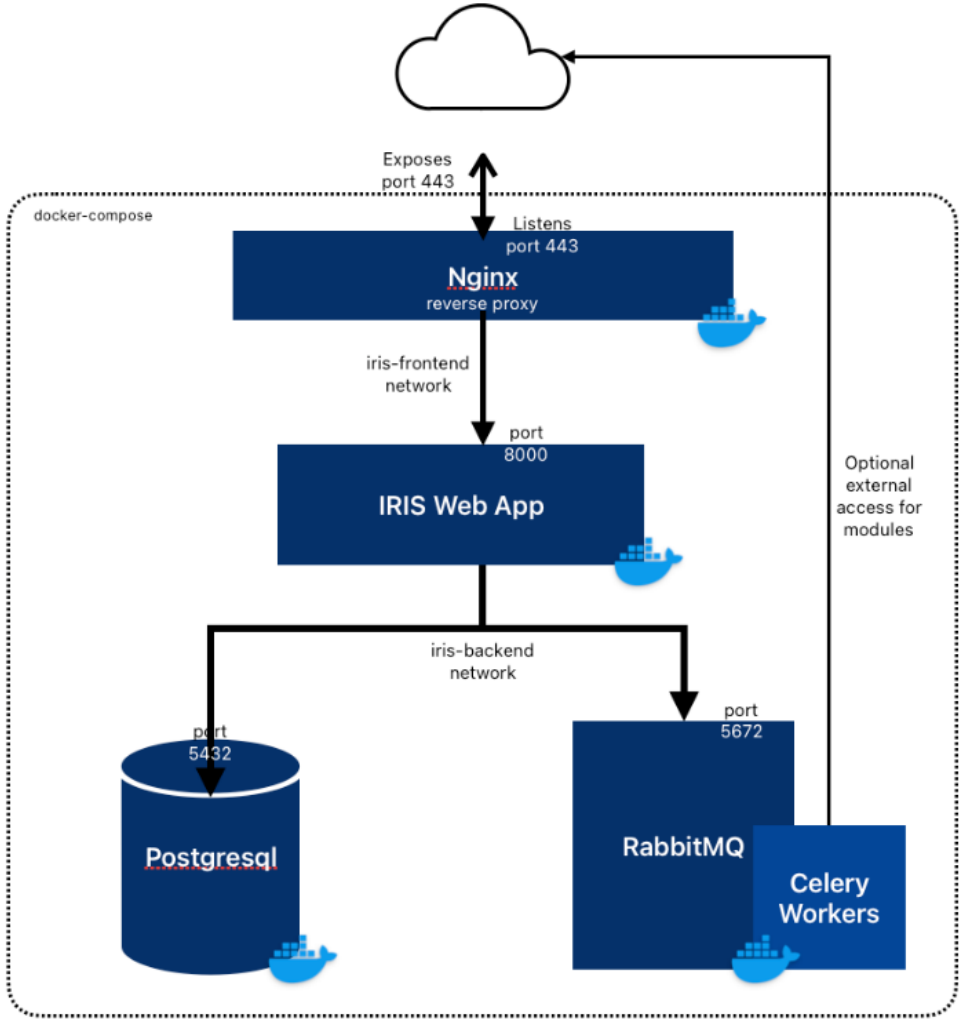
- **Nie je natívny IR (Incident Respond) nástroj**
  chýba vstavaná podpora pre prácu s IOC, artefaktmi či analytické IR funkcie (ktoré majú napr. TheHive alebo DFIR-IRIS).
- **Práca s IOC je možná len cez integrácie**
  Znuny nevie IOC spracovať samostatne; MISP / TheHive / Cortex sú potrebné ako doplnky.
- **Menej automatizácie a IR workflow**
  automatizované playbooky, korelácia artefaktov, timeline incidentu a behaviorálna analýza chýbajú.
- **Zložitejšia počiatočná konfigurácia a správa**
  množstvo modulov, perl prostredie, manuálne úpravy.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroj DFIR-IRIS

DFIR-IRIS – úvod a účel v procese riešenia incidentov

- **DFIR-IRIS** (*Digital Forensics and Incident Response – Incident Response Investigation System*)
  je open-source platforma určená pre **komplexné riadenie a dokumentáciu kybernetických incidentov**.
- Slúži ako **centrálny systém IR manažmentu**, ktorý prepája fázy **detekcie, analýzy, reakcie a reportingu** v rámci incidentu.
- Umožňuje **zaznamenávať priebeh vyšetrovania**, priraďovať úlohy členom tímu, spravovať dôkazy a artefakty, a vytvárať **automatizované reporty**.
- DFIR-IRIS podporuje **multi-user prístup**, auditovanie zmien a **forenznú dokumentáciu** jednotlivých krokov v riešení incidentu.
- Systém bol navrhnutý pre použitie v **SOC, CSIRT a DFIR tímoch** a spája funkcie manažmentu incidentov s forenznou analýzou.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra a integrácie DFIR-IRIS

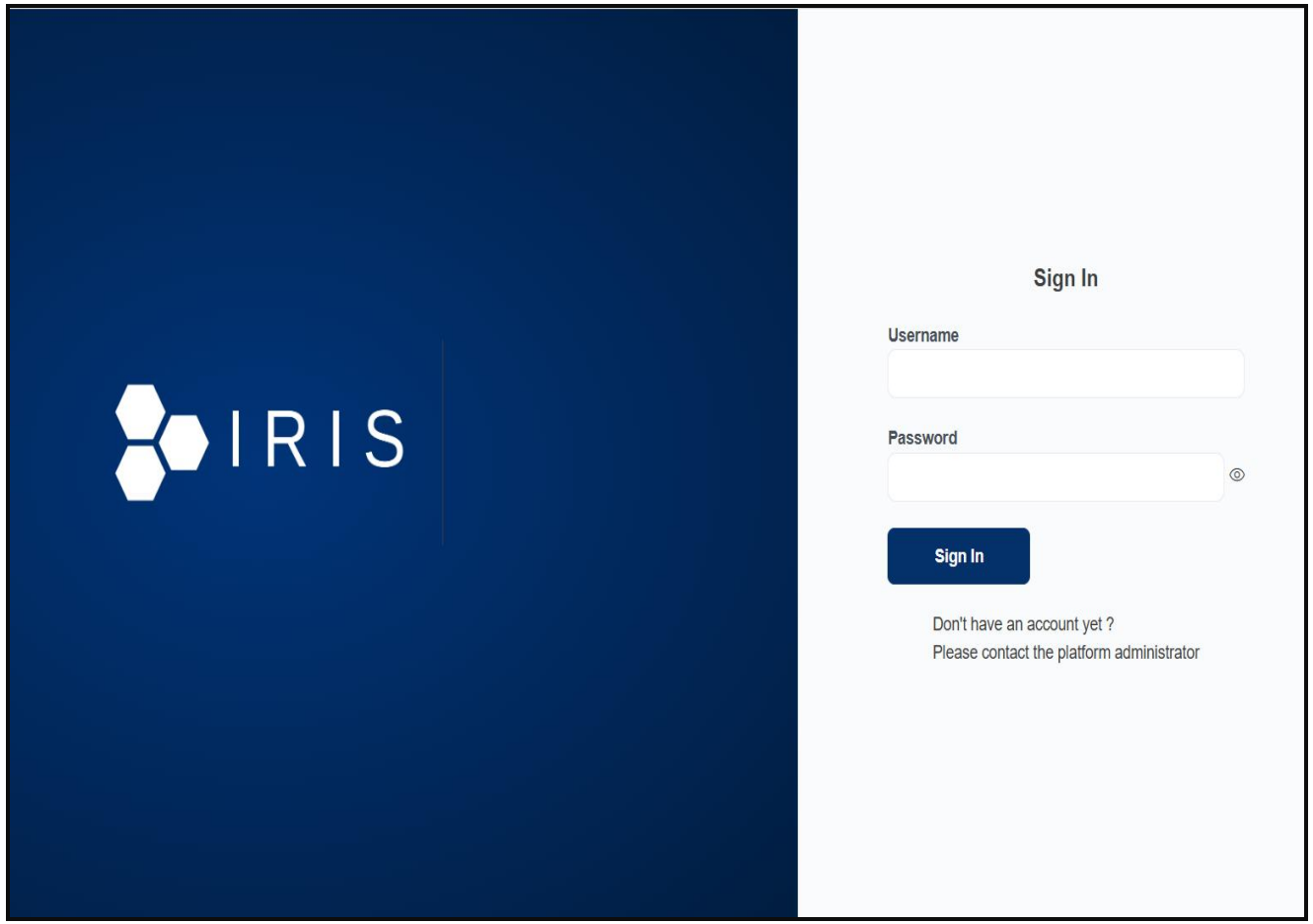
- DFIR-IRIS je postavený na **modulárnej architektúre**, ktorá umožňuje prepojenie s externými nástrojmi prostredníctvom **REST API**.
- Systém integruje dáta z **detekčných nástrojov** (napr. SIEM, IDS/IPS, Wazuh, ELK), ktoré môžu priamo vytvárať incidenty (cases).
- Podporuje **automatizáciu a obohacovanie údajov** cez nástroje ako:
  - **MISP** – import a spracovanie IOC, Threat Intelligence.
  - **Cortex** – spúšťanie analyzérov a playbookov na analýzu artefaktov.
- DFIR-IRIS využíva **PostgreSQL databázu** pre dáta a **RabbitMQ** pre správu správ medzi službami.
- Dáta je možné exportovať alebo vizualizovať pomocou **ELK Stacku** či **Grafany**.
- Integrácia prebieha obojsmerne – výsledky analýz sa ukladajú späť do systému ako **artefakty alebo dôkazy**.

DFIR-IRIS možno nasadiť ako samostatný nástroj alebo integrovať do existujúceho SOC ekosystému.Jeho otvorené REST API umožňuje prepojenie s nástrojmi ako MISP, Cortex, Wazuh či ELK Stack, čím pokrýva celý cyklus Incident Response.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

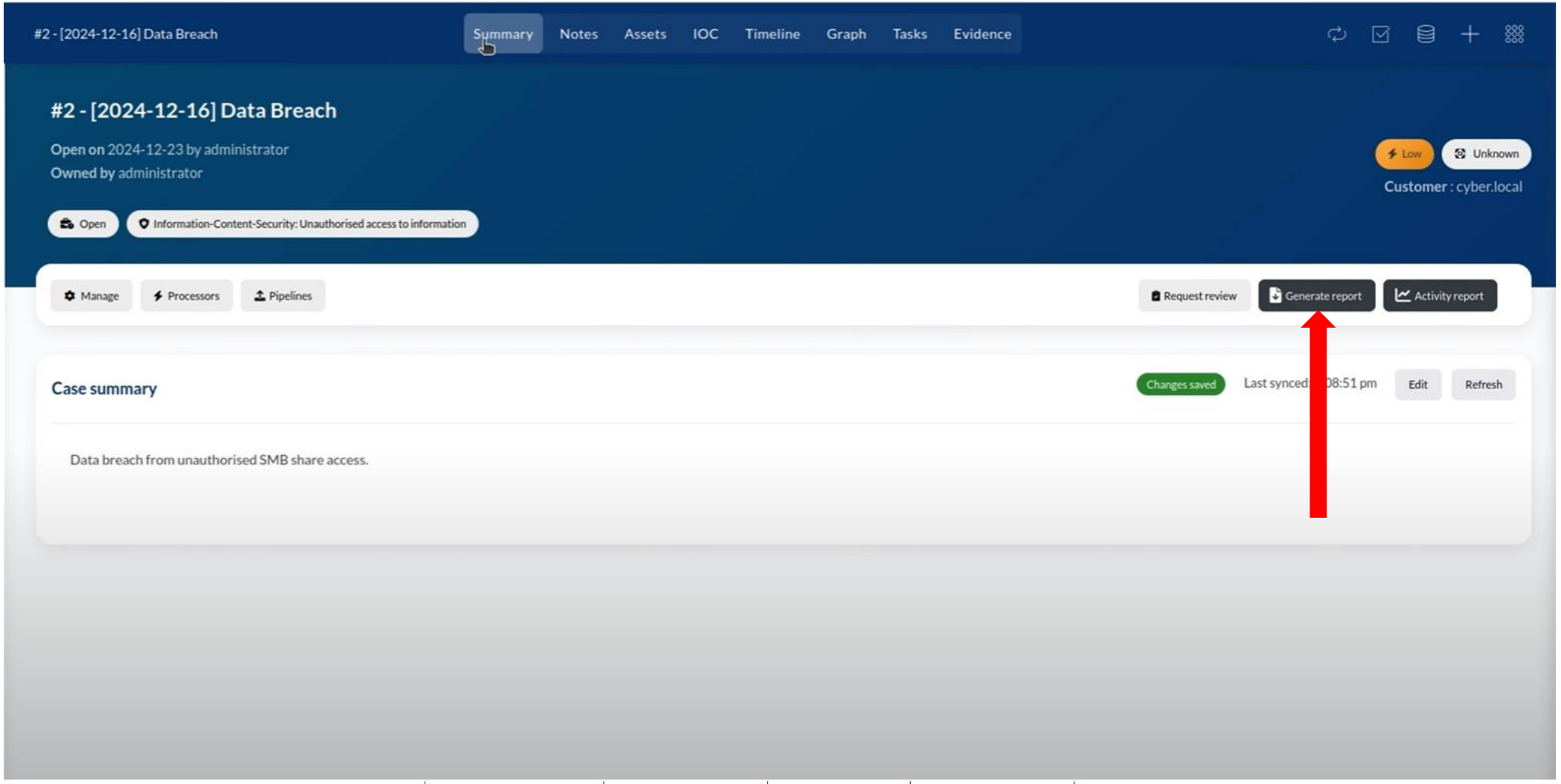
DFIR-IRIS inštalácia

- Inštalácia systému **DFIR-IRIS** prebieha jednoducho pomocou nástroja **Docker Compose**.
  Aplikácia je distribuovaná ako kontajnerové riešenie, ktoré obsahuje všetky potrebné súčasti – webové rozhranie, databázu, správu správ a procesné služby.
- Postup inštalácie je nasledovný:
  Najskôr je potrebné naklonovať oficiálny repozitár príkazom
  git clone https://github.com/dfir-iris/iris-web.git
- následne prejsť do vytvoreného priečinka pomocou **cd iris-web**.
- V ďalšom kroku sa stiahnu všetky potrebné kontajnery príkazom **docker compose pull**, čím sa načítajú najnovšie verzie jednotlivých služieb (Nginx, PostgreSQL, RabbitMQ a Celery Workers).
- Nakoniec sa aplikácia spustí príkazom **docker compose up –d** ktorý zabezpečí jej spustenie na pozadí.
- Po prvom spustení sa automaticky vytvorí administrátorský účet, pričom prihlasovacie údaje sa zobrazia v konzole.
- Po úspešnej inštalácii je DFIR-IRIS dostupný prostredníctvom webového prehliadača na adrese **https://<IP_adresa_servera>** (predvolene na porte **443**).



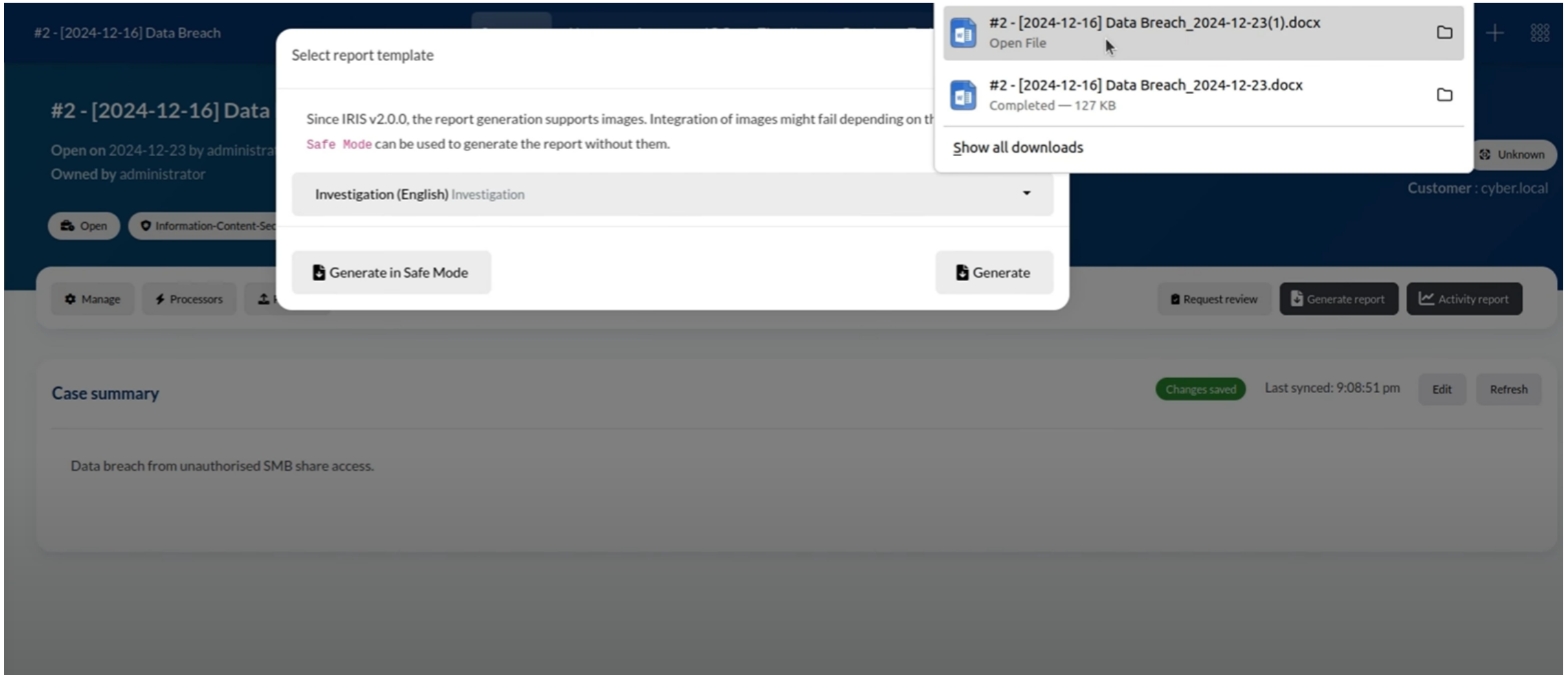
Nástroje pre riešenie incidentov – DFIR-IRIS

Správa incidentu a generovanie reportu



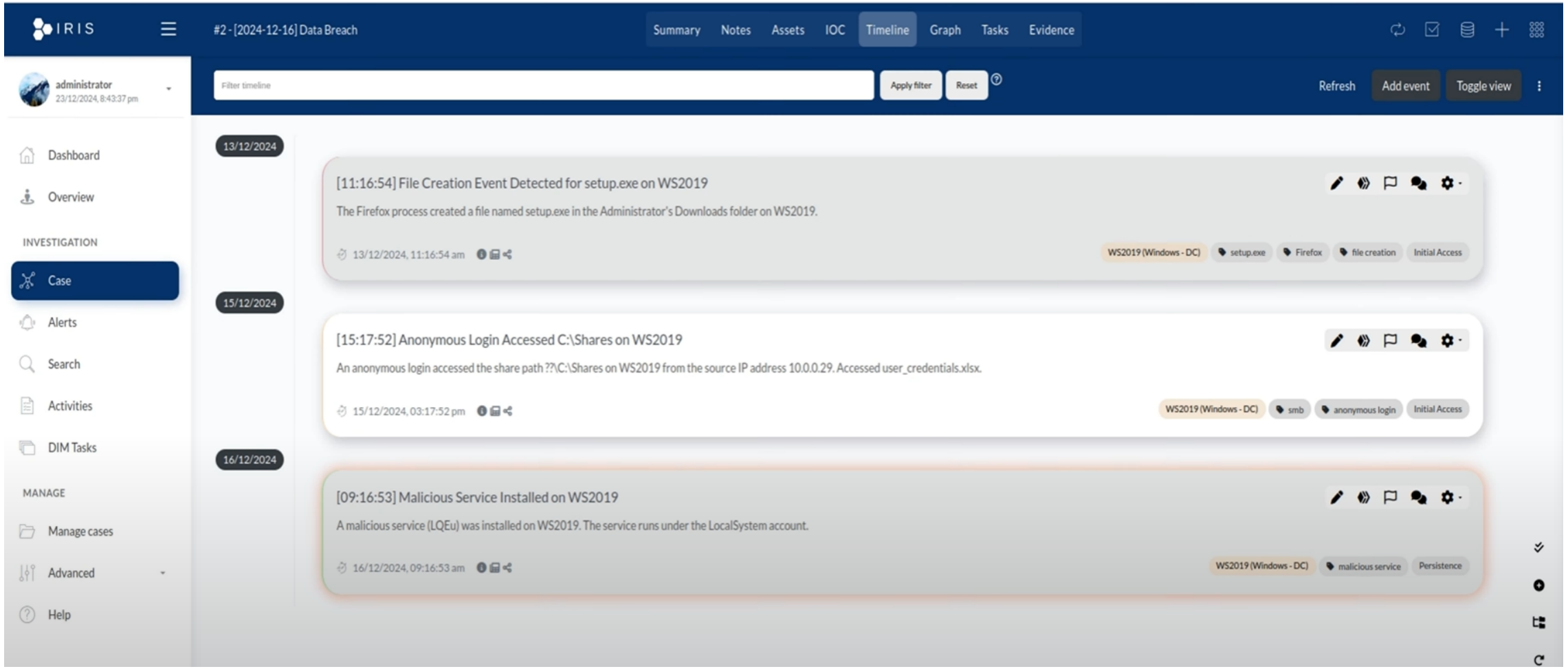
Nástroje pre riešenie incidentov – DFIR-IRIS

Tvorba výstupov a dokumentácie incidentov



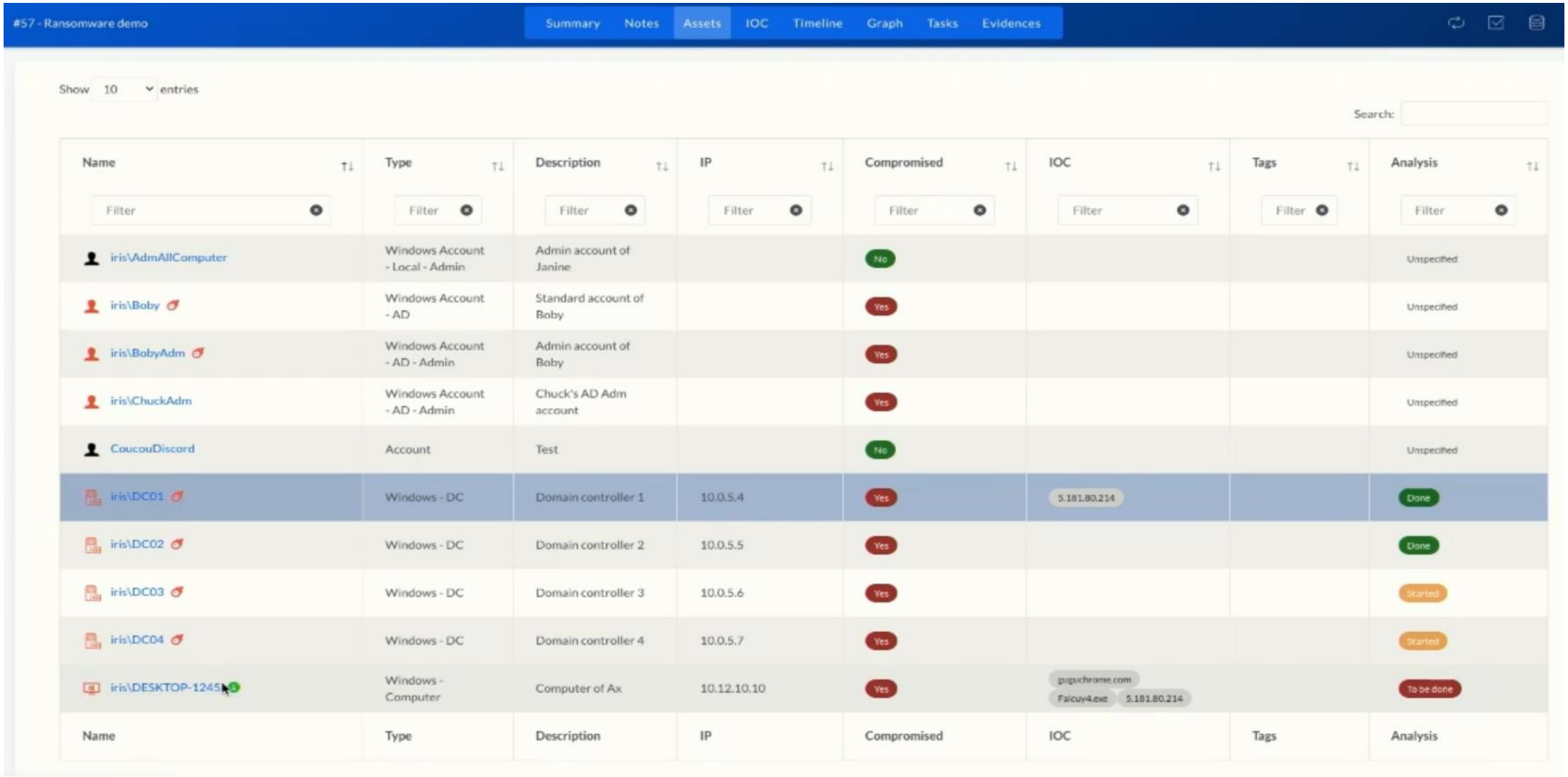
Nástroje pre riešenie incidentov – DFIR-IRIS

Časová os incidentu v DFIR-IRIS



Nástroje pre riešenie incidentov – DFIR-IRIS

Prehľad aktív a používateľských účtov



Ako funguje pridávanie assetov

- Po potvrdení bezpečnostného incidentu je v nástroji DFIR-IRIS možné identifikovať a evidovať aktíva a používateľské účty, ktoré boli incidentom ovplyvnené. Tieto aktíva je možné do systému pridávať manuálne alebo ich importovať automaticky.

A) Manuálne pridávanie aktív a účtov

Analytik môže počas vyšetrovania manuálne pridávať kľúčové informácie o aktívach a účtoch, najmä:

- Zariadenie alebo meno používateľa (napr. iris\DC01)
- Typ (napr. Windows - DC, Linux)
- IP adresa
- Popisok (Description)
- Stav kompromitácie

Tento prístup je dôležitý najmä pri spracovaní údajov z logov, forenzných analýz alebo EDR reportov.

B) Automatizovaný import prostredníctvom API

DFIR-IRIS poskytuje REST API, ktoré umožňuje automatizovaný import aktív z rôznych externých zdrojov:

- **SIEM** (napr. Splunk, ELK)
- **EDR** (napr. CrowdStrike, SentinelOne)
- **MISP** (pre koreláciu IOC)
- **CMDB / systémy správy aktív** (napr. ServiceNow, GLPI)
- Možný Import údajov vo formáte **CSV**.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Zhodnotenie nástrojov

Zhodnotenie nástrojov

Zoznam definovaných kritérií

Zoznam definovaných kritérií

	názov kritéria	stručný popis	vysvetlenie priradenia bodov
1	Tvorba a správa prípadov (cases) s úlohami a detailmi	Možnosť vytvárať incidenty ako prípady s úlohami, popisom a atribútmi.	1 = Iba jednoduchý záznam; 5 = Komplexné prípady s úlohami, atribútmi, väzbami.
2	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Možnosť sledovať IOC ako súčasť prípadu.	1 = Žiadna podpora pre IOC; 5 = Plná správa IOC vrátane stavu, histórie a väzieb.
3	Prepojenie medzi prípadmi na základe spoločných indikátorov	Automatická alebo manuálna identifikácia súvisiacich incidentov.	1 = Žiadna podpora prepájania; 5 = Automatická korelácia na základe IOC, času, typov útokov.
4	Kategorizácia incidentov pomocou tagov	Možnosť kategorizovať incidenty pomocou štítkov/tagov.	1 = Bez tagovania; 5 = Pokročilé tagovanie s podporou filtrov a štatistík.
5	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov.	1 = Manuálne pridávanie údajov; 5 = Automatické enrichovanie cez API/CTI.
6	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi	Možnosť prispôsobiť platformu podľa potrieb organizácie.	1 = Bez možnosti úprav; 5 = Vysoká miera konfigurovateľnosti, UI pre šablóny a workflow.

Zhodnotenie nástrojov

Porovnanie hodnotenia nástrojov

		Kritériá pre nástroj pre Evidenciu a s							
		Tvorba a správa prípadov (cases) s úlohami a detailmi	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Prepojenie medzi prípadmi na základe spoločných indikátorov	Kategorizácia incidentov pomocou tagov	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi
dostupné riešenia	TheHive	5	5	5	5	5	5	5	4
	RTIR	4	3	2	3	3	3	4	2
	DFIR-IRIS	5	5	4	5	4	4	5	4
	Znuny	4	2	2	4	2	5	5	4

Prepočet so zohľadnením váh jednotlivých kritérií

		Kritériá pre nástroj pre Evidenciu a s								
		Tvorba a správa prípadov (cases) s úlohami a detailmi	Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Prepojenie medzi prípadmi na základe spoločných indikátorov	Kategorizácia incidentov pomocou tagov	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	**výsledný súčet pre dané riešenie**
	váhy	0,08	0,07	0,07	0,06	0,08	0,07	0,06	0,06	
dostupné riešenia	TheHive	0,4	0,35	0,35	0,3	0,4	0,35	0,3	0,24	4,89
	RTIR	0,32	0,21	0,14	0,18	0,24	0,21	0,24	0,12	3,14
	DFIR-IRIS	0,4	0,35	0,28	0,3	0,32	0,28	0,3	0,24	4,52
	Znuny	0,32	0,14	0,14	0,24	0,16	0,35	0,3	0,24	3,75

Cyber Kill Chain

Čo je Cyber Kill Chain?

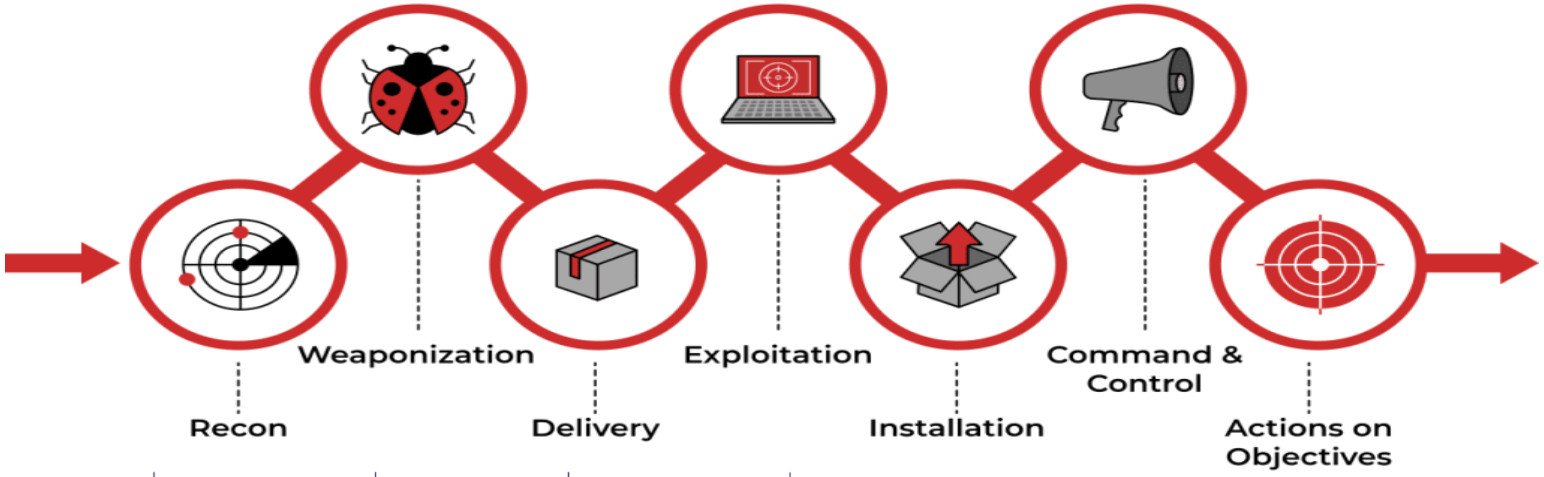
Model vyvinutý spoločnosťou *Lockheed Martin* na pochopenie a prerušenie kybernetických útokov.

Popisuje **7 krokov**, ktoré útočník bežne vykonáva – od prieskumu až po dosiahnutie cieľa.

Pomáha organizáciám **mapovať správanie útočníka** a nasadzovať detekcie či obranu v každej fáze.

Prečo je dôležitý?

- Umožňuje *proaktívne* reagovať – útok sa dá zastaviť už v počiatočnej fáze.
- Poskytuje štruktúru pre *Incident Response, Threat Hunting* aj *Security Monitoring*.
- Uľahčuje prepojenie s rámcami ako **MITRE ATT&CK** alebo **NIST CSF**.



Fázy útoku podľa modelu Cyber Kill Chain

1. Reconnaissance (Prieskum)
Útočník zbiera informácie o cieľoch, systémoch a používateľoch (OSINT, sieťové skeny, sociálne siete).

2. Weaponization (Vytvorenie nástroja)
Spojenie exploitov s payloadom – napr. vytvorenie infikovanej prílohy alebo webu.

3. Delivery (Doručenie)
Odovzdanie škodlivého obsahu cieľu – e-mail, web, USB, dodávateľský reťazec.

4. Exploitation (Zneužitie)
Využitie zraniteľnosti alebo sociálneho inžinierstva na spustenie škodlivého kódu.

5. Installation (Inštalácia)
Zavedenie malvéru do systému a získanie trvalého prístupu.

6. Command & Control (C2)
Napadnutý systém nadväzuje spojenie s útočníkom a prijíma príkazy.

7. Actions on Objectives (Cieľ útoku)
Útočník dosahuje svoj cieľ – exfiltrácia dát, šifrovanie (ransomware), sabotáž.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad útoku (phishing → exploit → exfiltrácia)

- **1) Phishingový e-mail — 14:23**
  E-mail so škodlivou prílohou alebo odkazom odoslaný zamestnancovi.
  Detekcia: kontrola obsahu e-mailu, sandboxing príloh, URL filtering.
  Mitigácia: e-mailová brána so sandboxom, školenia používateľov, DMARC/DKIM/SPF.

- **2) Spustenie exploitu — 14:28**
  Používateľ otvorí prílohu alebo klikne na link; exploit spustí škodlivý kód a útočník získa prístup.
  Detekcia: behaviorálna detekcia na endpointoch (EDR), monitoring procesov, SIEM alerty.
  Mitigácia: patch management, application whitelisting, EDR automatická izolácia.

- **3) Krádež dát (exfiltrácia) — 14:35**
  Citlivé súbory sú odoslané na server útočníka alebo do cloudového úložiska.
  Detekcia: monitorovanie egress traffic, DLP, netflow/anomaly detection.
  Mitigácia: egress filtering, DLP blokovanie, segmentácia siete, obnovy zo záloh.

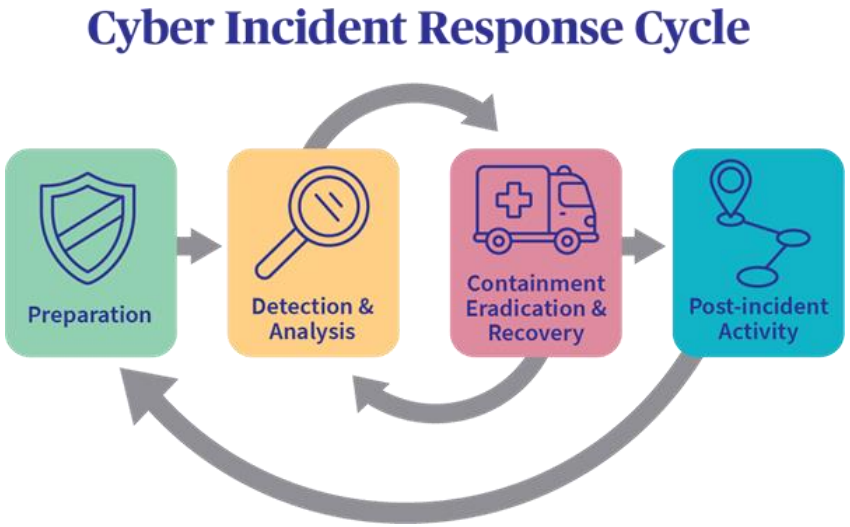
Cyber Kill Chain

Detekcia a reakcia v jednotlivých fázach

Fáza (CKC)	Indikátory / IOC	Nástroje a detekcia	Reakcia / Mitigácia
Reconnaissance	Skenovanie portov, neznáme dopyty DNS, OSINT aktivity	IDS/IPS, firewall logy, netflow analýza, threat intel	Blokovanie IP, rate limiting, honeypot, monitoring
Weaponization	Neznáme makrá, payloady, zbalené archívy	Sandbox, AV, statická/dynamická analýza, YARA	Analýza vzoriek, IOC feed aktualizácia, blokovanie hashov
Delivery	Phishing e-maily, podozrivé URL, neobvyklé prílohy	E-mail gateway, SIEM, EDR, URL filtering	Blokovanie e-mailov/domén, školenie používateľov
Exploitation	Neočakávané procesy, exploit logy, zmeny oprávnení	EDR, SIEM korelácia, patch monitoring	Patchovanie, izolácia zariadenia, eradikácia hrozby
Installation	Nové služby, registry kľúče, persistence artefakty	EDR, Sysmon, autoruns monitoring	Odstránenie malwaru, reimage, zmena hesiel
Command & Control (C2)	Beaconing, DNS tunneling, neobvyklé outbound spojenia	NTA/NDR, DNS logs, proxy, threat intel feedy	Blokovanie domén/IP, sinkholing, segmentácia siete
Actions on Objectives	DLP alerty, exfiltrácia dát, neobvyklé veľké prenosy	DLP, SIEM, EDR, NetFlow	Izolácia systému, blokovanie prenosu, incident response, obnovy

Ako Cyber Kill Chain korešponduje s NIST IR procesom

Cyber Kill Chain fáza	Popis	NIST Incident Response fáza	Typická aktivita / reakcia
Reconnaissance	Útočník zbiera informácie o cieľoch	**Identify**	Asset inventory, znižovanie expozície, OSINT monitoring
Weaponization	Príprava nástroja, exploit + payload	**Protect**	Antivírus, e-mail filtering, zabezpečenie dodávateľov
Delivery	Doručenie payloadu (phishing, web, USB)	**Protect / Detect**	E-mail gateway, sandbox, SIEM alerty
Exploitation	Spustenie exploitu / získanie prístupu	**Detect / Respond**	EDR detekcia, izolácia hosta, patchovanie
Installation	Inštalácia malwaru, persistence	**Respond**	Eradikácia malwaru, forenzná analýza, obnovenie systému
Command & Control (C2)	Komunikácia s útočníkom	**Respond / Contain**	Blokovanie C2, sinkholing, segmentácia siete
Actions on Objectives	Exfiltrácia dát, sabotáž, ransom	**Recover / Improve**	Obnovenie dát, reporting, lessons learned, policy update



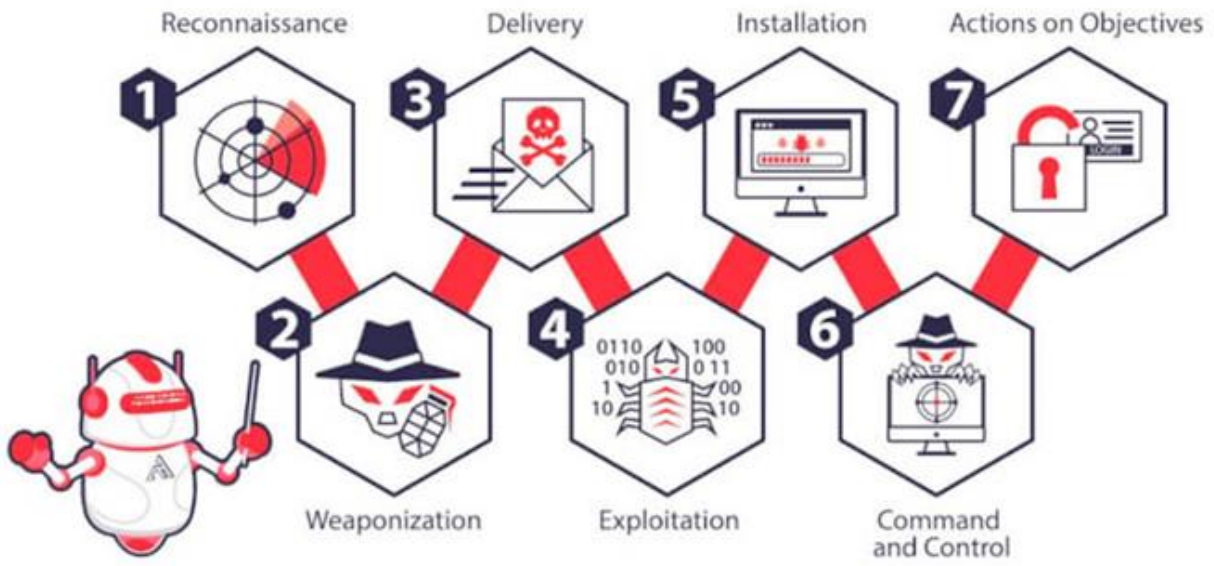
Zhrnutie časti – Cyber Kill Chain

Cyber Kill Chain je model, ktorý pomáha pochopiť a prerušiť kybernetický útok v každej jeho fáze.

Popisuje **7 fáz útoku** – od prieskumu (*Reconnaissance*) až po dosiahnutie cieľa (*Actions on Objectives*).

Každá fáza predstavuje príležitosť na **detekciu a reakciu** – čím skôr sa útok identifikuje, tým menšie sú škody.

- **Prepojenie s rámcami NIST IR a MITRE ATT&CK**
  umožňuje lepšiu automatizáciu a efektívnejšiu obranu.
- **Praktické využitie:**
  SOC, *Threat Hunting*, *Incident Response* a bezpečnostné cvičenia.
- **Cieľ modelu:**
  Transformovať reakcie z reaktívnych na **proaktívne a prediktívne**.



Každý článok reťazca, ktorý sa podarí prerušiť, môže zastaviť útok

Otvorená reflexia

1. Prvým krokom pri riešení kybernetického incidentu je identifikácia a potvrdenie incidentu, až potom nasleduje jeho obsahovanie a mitigácia.

A) Pravda

B) Nepravda

2. Ktoré kroky patria do procesu riešenia bezpečnostných incidentov podľa bežných rámcov (napr. NIST, SANS)?

A) Príprava a plánovanie

B) Detekcia a analýza

C) Obsahovanie, eradikácia a obnovenie

D) Audit finančných výkazov

Otvorená reflexia

3.Po detekcii ransomware útoku na firemné servery, čo sú vhodné okamžité kroky SOC tímu?

A) Odpojiť infikované zariadenia od siete

B) Spustiť zálohovanie infikovaných súborov

C) Identifikovať zdroj útoku a zasiahnuté systémy

D) Pokúsiť sa vyjednávať s útočníkom bez analýzy

4.Ktoré nástroje môžu SOC tímu pomôcť pri riešení kybernetických incidentov?

A) SIEM (Security Information and Event Management)

B) SOAR (Security Orchestration, Automation, and Response)

C) EDR (Endpoint Detection and Response)

D) Textový editor

Otvorená reflexia

5. Čo je cieľom modelu Cyber Kill Chain? (1 správne)

a) Zmapovať kroky útočníka a zastaviť útok v ktorejkoľvek fáze
b) Určiť postup obnovy po incidente
c) Získať prístupové údaje útočníka
d) Overiť funkčnosť antivírusu

6.Ktoré nástroje patria medzi Incident Response platformy? (2 správne)

a) TheHive
b) DFIR-IRIS
c) Wireshark
d) Metasploit

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

Riešenie incidentov

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk