Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výhody SOC centier

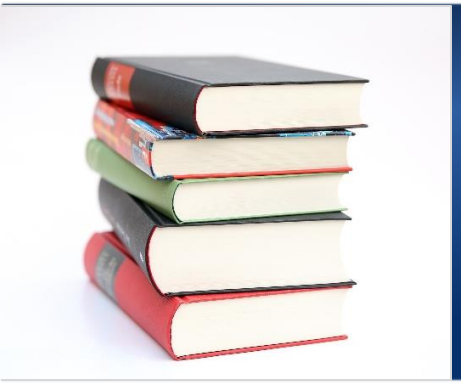
Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk



Ciele

- Porozumieť tomu, čo je SOC a prečo je dôležitý
- Predstaviť rôzne typy SOC centier a oblasti, v ktorých sa používajú
- Predstaviť nástroje používané v SOC (SIEM, SOAR, EDR…)
- Vysvetliť roly v SOC centre
- Vysvetliť prínosy SOC pre organizáciu a kybernetickú bezpečnosť

Úvod do témy

Network and Information security Directive

Smernica NIS

- Európska komisia v rámci stratégie kybernetickej bezpečnosti EÚ navrhla
  - smernicu EU Network and Information Security (NIS)
- Smernica NIS (pozri EU 2016/1148) je **prvou časťou celoeurópskej legislatívy v oblasti kybernetickej bezpečnosti**
  - Cieľom je zvýšiť kybernetickú bezpečnosť v celej EÚ.
  - Smernica NIS bola prijatá v roku **2016** a následne, keďže ide o smernicu EÚ, každý členský štát EÚ začal prijímať vnútroštátne právne predpisy, ktoré sa riadia smernicou alebo ju „transponujú“.
    - Smernice EÚ poskytujú krajinám EÚ určitú mieru flexibility, aby mohli zohľadniť vnútroštátne podmienky, napríklad opätovné využitie existujúcich organizačných štruktúr alebo zosúladenie s existujúcimi vnútroštátnymi právnymi predpismi.
    - Vnútroštátna implementácia členskými štátmi EÚ sa uskutočnila **9. mája 2018**.
      - U nás – skoro všetko je datované k **1.4.2018** – zákony, vyhlášky, vznik orgánov, samostatných útvarov, ...
        - Zákon o KB 69/2018 Z.z., Vyhláška 362/2018 Z.z.
  - NIS 2 v platnosti od 14.12.2022
    - náš Zákon o KB v SR bol podľa nej novelizovaný, rovnako aj vyhláška
      - Novelizácia zákona o KB, 366/2024 Z. z., účinnosť od 1.1.2025
      - Vyhláška NBU o bezpečnostných opatreniach 227/2025 Z. z., účinnosť od 1.9.2025

Smernica NIS

- Európska komisia udržiava mapu ktorá zobrazuje stav implementácie smernice NIS členskými štátmi EU.

Členské štáty	• vypracovať národné stratégie kybernetickej bezpečnosti • **národný CSIRT**, **vykonávať kybernetické cvičenia** • spolupráca medzi štátmi / **EU CSIRT sieťou**, **strategic NIS cooperation group, …** • identifikovať **Operators of Essential Services (OES)** v kritických sektoroch: energetika, doprava, bankovníctvo, finančný sektor, zdravotníctvo, vodohospodárstvo, digitálna infraštruktúra, a **Digital Service Providers (DPS)** (online trhoviská, cloudové a online vyhľadávače), a dohliadať na bezpečnosť
OES operators	• **prijať** minimálne **bezpečnostné opatrenia** • **hlásenie** významných **incidentov**.
DPS providers	• **dodržiavať** tieto bezpečnostné a oznamovacie **požiadavky**

Sectors of OES and types of digital services in the scope of the NIS Directive

OESs Operators of Essential Services = prevádzkovatelia základných služieb

DSPs Digital Service Providers = prevádzkovatelia digitálnych služieb

Aký je rozdiel?

CERT vs. CSIRT vs. CIRT vs. SOC

Authorized to Use CERT℠
CERT is a mark owned by
Carnegie Mellon University

- CSIRT - computer security incident response team
- CIRT - computer incident response team or, less frequently, cybersecurity incident response team
- CERT - computer emergency response (or readiness) team
- CSIRT, CIRT and CERT sa v tejto oblasti často používajú zameniteľne
  - CSIRT a CIRT sú takmer vždy skoro ekvivalentné; v podstate sú to synonymá
    - Organizácia môže uprednostňovať jednu alebo druhú formu na základe jazyka alebo štýlu organizácie
  - Carnegie Mellon University – nie iba definície:
    - „CSIRT je konkrétna organizačná jednotka (t. j. jeden alebo viac zamestnancov), ktorá je poverená koordináciou a podporou reakcie na udalosť alebo incident v oblasti počítačovej bezpečnosti."
    - “CERT” je registrovaná ochranná známka spoločnosti Carnegie Mellon University.
      - Jednotkám CSIRT, ktoré majú rovnakú zodpovednosť za budovanie bezpečnosti siete a zariadení, sa odporúča požiadať o súhlas na prijatie označenia „CERT“ v ich názve.
      - SK-CERT národná jednotka je vlastníkom certifikátu, ktorý ju oprávňuje používať CERT v jej mene.

SK NBÚ CERT

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

Certifikácie CSIRT tímov

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

- "**CERT**" je registrovaná ochranná známka spoločnosti **Carnegie Mellon University**
  - Jednotkám CSIRT, ktoré majú rovnakú zodpovednosť za budovanie siete a zabezpečenie zariadení, sa odporúča požiadať o súhlas, aby mohli prijať „CERT" vo svojom mene.
  - SK-CERT je vlastníkom certifikátu
- **Trusted Introducer Service (TI)**
  - medzinárodná organizácia spravujúca databázu CSIRTs a CERTs
  - národná jednotka SK-CERT sa 26. marca 2020 stala certifikovaným členom
- **Forum of Incident Response and Security Teams (FIRST)**
  - medzinárodná konfederácia tímov pre riešenie počítačových incidentov
  - hlavným cieľom FIRST je vytvoriť prostredie pre efektívne riešenie kybernetických bezpečnostných incidentov, ktoré umožní
    - výmena informácií, nástrojov, metodík a osvedčených postupov medzi členmi FIRST
  - 23. apríla 2018 sa národná jednotka SK-CERT stala členom FIRST

CERT vs. CSIRT vs. CIRT vs. SOC

SOC má širší rozsah

- SOC vo všeobecnosti zahŕňa viacero aspektov bezpečnostných operácií, zatiaľ čo CSIRTs, CERTs a CIRTs sa zameriavajú najmä na **reakciu na incidenty**.
- Do pôsobnosti SOC môže patriť funkcia reakcie na incidenty (buď úplne, alebo čiastočne), ako aj iné úlohy. SOC môže napríklad:
  - zahŕňať monitorovacie operácie a kontroly, napríklad:
    - systém detekcie narušenia
    - systém prevencie narušenia
    - správu bezpečnostných udalostí
  - dohliadať na vyhodnocovanie prevádzkovej a bezpečnostnej telemetrie a zhromažďovania informácií
  - riadiť úlohy, ako je
    - správa identít a autorizácia,
    - údržba súborov pravidiel brány firewall a filtrovania (kontrola aj správa zmien)
    - forenzná analýza a podpora vyšetrovania
    - alebo akýkoľvek iný aspekt prevádzkovej bezpečnosti.

-> telemetria je proces zhromažďovania, prenosu a analýzy dát z rôznych zariadení a systémov na diaľku

Čo je to Security Operations Center (SOC)?

Operačné centrum kybernetickej bezpečnosti (SOC)

- **Security Operations Center (Operačné centrum kybernetickej bezpečnosti, SOC)**
  - je interný alebo externý tím odborníkov na bezpečnosť v oblasti kybernetickej bezpečnosti,
    - ktorý nepretržite monitoruje celú **infraštruktúru IT** organizácie
    - s cieľom odhaliť udalosti týkajúce sa kybernetickej bezpečnosti v reálnom čase
    - a čo najrýchlejšie a najúčinnejšie ich riešiť.

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

Funkcie Operačného centra kybernetickej bezpečnosti

- **Monitorovanie 24/7** (continuous monitoring)
- **Detekcia hrozieb a incidentov** (threat detection)
- **Reakcia na incident** (incident response)
- **Obnova po incidente** (recovery)
- **Forenzná analýza** (forensics & analysis)
- **Proaktívny Threat hunting**
- **Dodržiavanie legislatívy a auditov (compliance)**
- **Centralizovaná správa bezpečnosti**

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

Funkcie Operačného centra kybernetickej bezpečnosti

Monitorovanie 24/7

- **SOC nepretržite sleduje všetky časti infraštruktúry:**
  - servery, sieťové zariadenia, firewally
  - cloudové prostredie, koncové zariadenia, databázy
  - logy z aplikácií a operačných systémov
- **Cieľom je čo najskôr identifikovať anomáliu, podozrivú aktivitu alebo známky útoku**
- **Na monitorovanie IT infraštruktúry sa používajú rôzne technológie, vrátane:**
  - SIEM (zbiera a vyhodnocuje logy)
  - IDS/IPS (detekcia pokusov o prienik)
  - EDR (monitorovanie koncových bodov)

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

Detekcia hrozieb a incidentov

- **SOC vyhodnocuje bezpečnostné udalosti a odhaľuje:**
  - Pokusy o prístup k službám,
  - Neštandardnú sieťovú prevádzku,
  - Anomálie v správaní používateľa
  - Malware / ransomvér
  - Zraniteľnosti a zlé konfigurácie
  - Úniky dát
  - Podozrivé priradenia privilegovaných účtov.

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

Reakcia na incident

- **Po detegovaní incidentu nasleduje:**
  - **Klasifikácia a prioritizácia**
    - Určí sa kritickosť incidentu (High / Medium / Low)
    - Definuje sa rozsah problému: koľko systémov / účtov je ovplyvnených
    - Priradí sa typ incidentu (malware, ransomvér, únik dát, neoprávnený prístup…)
  - **Izolácia (containment)**
    - Odpojenie postihnutého zariadenia od siete
    - Zablokovanie IP adresy útočníka na firewalle
    - Zastavenie škodlivých procesov
    - Zastavenie aplikácie alebo služby
  - **Eliminácia hrozby (erradication)**
    - Odstránenie malvéru, škodlivých súborov
    - Odstránenie zraniteľností (patch, zmena konfigurácie)
    - Aktualizácia firewallu, SIEM pravidiel

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

- **Ciel obnovy je vrátiť systémy do normálnej prevádzky ako pred útokom**
- **Obnova zahŕňa:**
  - Odstránenie škodlivého kódu (malware, ransomvér, backdoor)
  - Obnova dát zo záloh (backup, snapshoty, cloud)
  - Kontrola integrity systémov (overenie, že útočník nezanechal prístup)
  - Vrátenie služieb do normálneho režimu bez rizika opakovania útoku
  - Komunikácia s vedením alebo zákazníkmi (ak boli ovplyvnení)

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

Forenzná analýza

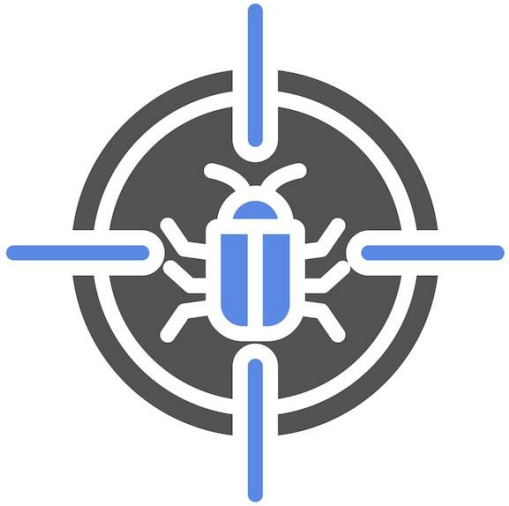
- **Analyzujeme ako incident vznikol a čo útočník urobil**
- **Analyzujeme logy zo systémov** (SIEM, endpoint, firewall, cloud logy)
- **Snažíme sa zistiť entry point** (kde sa útočník dostal dovnútra)
- **Zachytávame dôkazy** (diskové obrazy, pamäť, sieťová komunikácia)
- **Zisťujeme úmysel útočníka** (exfiltrácia dát, ransomvér, sabotáže)
- Spracujeme **dokumentáciu incidentu** pre manažment, auditorov alebo políciu
- Výsledkom je **Incident Report**, ktorý obsahuje informácie o tom:
  - Čo sa stalo
  - Ako sa to stalo
  - Čo robiť aby sa to neopakovalo

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

•Proaktívny Threat Hunting

- **SOC centrum** tu nečaká na alarm, ale **aktívne prehľadáva prostredie**:
  - Hľadá nezvyčajné správanie používateľov (anomálie)
  - Porovnáva dianie v sieti s databázami hrozieb (IOC, TTP z MITRE ATT&CK)
  - Hľadá stopy útočníka (napr. malware, command & control komunikáciu)

- Pri **Threat Huntingu** hľadáme veci ako napr.:
  - Pokusy o laterálne šírenie cez sieť (winrm, rdp, smb)
  - Vytváranie nových lokálnych admin účtov
  - Prístup z neznámej / neobvyklej geografickej lokality



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

Dodržiavanie legislatívy a auditov

- **SOC centrum** zabezpečuje, že organizácia bude dodržiavať legislatívu:
  - **NIS2**
  - **GDPR**
  - **ISO 27001**, **CSIRT požiadavky**, **auditné štandardy**

- Pre organizácie, zaradené pod **smernicu NIS2** je nutné **každé 2 roky** vykonať **povinný bezpečnostný audit**
- Pri **ISO/IEC 27001** sa očakáva že organizácia vykoná:
  - **Interný audit** – minimálne 1× ročne
  - **Externý certifikačný audit –** každé 3 roky
  - **Dozorný audit** (kontrolný audit certifikácie) – raz za rok

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

Centralizovaná správa bezpečnosti

- Účelom **SOC centra** je mať všetky **bezpečnostné dáta** na **jednom mieste**
- **SOC centrum** zhromažďuje **logy** a **incidenty** z rôznych systémov:
  - Servery
  - Sieťové zariadenia (firewall, IDS/IPS)
  - Počítače a endpointy (EDR/XDR)
  - Cloud (Office365, Azure, AWS)
- Všetko smeruje do **SIEM systému**, ktorý:
  - Centralizuje logy
  - Vyhodnocuje vzťahy medzi udalosťami (korelácia)
  - Upozorňuje na incidenty

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

Prečo vznikol SOC?

Hlavné dôvody vzniku SOC

- **IT prostredie** je dnes príliš rozsiahle, rýchle a komplexné a útoky sú oveľa sofistikovanejšie než boli v minulosti.
- Nárast počtu **kybernetických útokov**
- Organizácie nemali prehľad o tom čo sa v ich sieti deje
- **Incidenty** sa riešili až keď spôsobili škody
- Nástup novej legislatívy (**NIS2**)

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

Nárast incidentov

- V období od júla 2023 do júna 2024 agentúra **ENISA** (European Union Agency for Cybersecurity) zaznamenala **11 079 kybernetických incidentov**, z čoho **322 incidentov bolo zameraných na viacero členských štátov EÚ**.
- Najčastejšie zaznamenanými typmi útokov boli **DDoS a ransomware**, ktoré spolu tvorili viac ako polovicu všetkých incidentov.
- Najviac napádanými sektormi boli verejná správa, doprava a finančný sektor.

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

Technológie používané v SOC

Aké technológie SOC používa?

- Úlohou **SOC centra** je nepretržité sledovanie toho čo sa deje v sieťovej infraštruktúre, odhaľovanie hrozieb a reagovanie na incidenty
- Pre plnenie týchto úloh používa SOC rôzne technológie
- **Kľúčové technológie** pre fungovanie SOC centra sú:
  - **SIEM** (Security Information and Event Management)
  - **SOAR** (Security Orchestration, Automation and Response)
  - **EDR/XDR** (Endpoint/Extended Detection and Response)
  - **IDS/IPS** (Intrusion Detection System) / (Intrusion Prevention System)
  - **Threat Intelligence**

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

Technológie používané v SOC

Aké technológie SOC používa?

1. SIEM (Security Information and Event Management)	• Centralizuje logy, analyzuje udalosti a generuje bezpečnostné alerty na základe korelácií.
2. Log Management	• Zbieranie, ukladanie a normalizácia logov zo systémov, aplikácií a infraštruktúry.
3. IDS/IPS (Intrusion Detection/Prevention Systems)	• Detekcia alebo prevencia škodlivej aktiviy v sieťovej komunikácii podľa vzorov a anomálií.
4. NDR (Network Detection and Response)	• Pokročilá analýza sieťového trafficu pomocou behaviorálnej detekcie a strojového učenia.
5. EDR (Endpoint Detection and Response)	• Monitorovanie a analýza aktivít na koncových zariadeniach s detekciou hrozieb a možnosťou reakcie.
6. XDR (Extended Detection and Response)	• Integruje dáta zo SIEM, EDR, NDR, cloudov a identity pre jednotnú detekciu a odpoveď.
7. NGAV (Next-Gen Antivirus)	• Proaktívna ochrana endpointov založená na správaní, AI a detekcii anomálií.
8. SOAR (Security Orchestration, Automation and Response)	• Automatizácia reakcií na incidenty a orchestrácia medzi rôznymi bezpečnostnými systémami.
9. Vulnerability Management	• Identifikácia, hodnotenie a prioritizácia zraniteľností v systémoch a sieťach.
10. Patch Management	• Riadenie a aplikácia aktualizácií a bezpečnostných opráv v celom prostredí.

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

Technológie používané v SOC

Aké technológie SOC používa?

11. IAM (Identity and Access Management)	• Správa používateľských identít, autentifikácie a prístupových práv.
12. PAM (Privileged Access Management)	• Kontrola, audit a zabezpečenie účtov s vysokými oprávneniami (admin/root).
13. UEBA (User and Entity Behavior Analytics)	• Analýza správania používateľov a systémov s cieľom detegovať anomálie a insider hrozby.
14. DLP (Data Loss Prevention)	• Ochrana pred únikom dát monitorovaním, detekciou a blokovaním rizikového správania.
15. CASB (Cloud Access Security Broker)	• Kontrola bezpečnosti pri prístupe k cloudovým aplikáciám a SaaS službám.
16. CSPM (Cloud Security Posture Management)	• Monitorovanie konfigurácií cloudových služieb a odhaľovanie nesprávnych nastavení.
17. CIEM (Cloud Infrastructure Entitlement Management)	• Riadenie cloudových oprávnení a identifikácia nadmerných alebo rizikových prístupov.
18. CWPP (Cloud Workload Protection Platform)	• Ochrana workloadov (VM, kontajnerov, serverless) počas behu aj pri nasadení.
19. CNAPP (Cloud-Native Application Protection Platform)	• Komplexná ochrana cloudu kombinujúca CSPM, CIEM, CWPP a ďalšie funkcie.
20. E-mail Security / SEG	• Analýza a filtrovanie škodlivých e-mailov, phishingu a príloh.

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

Aké technológie SOC používa?

21. Proxy / Secure Web Gateway	• Monitoruje a filtruje webový traffic, blokuje škodlivé webstránky a downloady.
22. Firewally / Next-Gen Firewally	• Kontrolujú sieťovú komunikáciu na základe politík, aplikácií a hrozbovej inteligencie.
23. Threat Intelligence (CTI)	• Získavanie informácií o hrozbách, IOC, taktikách a aktéroch útokov pre detekciu.
24. Sandbox / Malware Analysis	• Bezpečné spustenie podozrivých súborov na analýzu ich správania.
25. DFIR (Digital Forensics & Incident Response)	• Forenzná analýza systémov, sietí a zariadení počas šetrenia incidentov.
26. Network Forensics	• Detailná analýza sieťovej komunikácie kvôli rekonštrukcii útokov.
27. Configuration Management / CMDB	• Evidencia aktív a konfigurácií, ktorá pomáha SOC-u identifikovať rizikové zmeny.
28. Monitoring and Observability	• Meranie výkonu systémov, sieťovej prevádzky a zber telemetrie pre detekciu problémov.
29. Incident Management and Ticketing	• Sledovanie životného cyklu incidentov, ich priraďovanie a dokumentácia.
30. Backup & Recovery	• Zabezpečenie rýchlej obnovy pri ransomvéri alebo stratách dát počas incidentu.

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

Aké technológie SOC používa?

31. Zero Trust Security	• Model bezpečnosti, ktorý nepredpokladá dôveru ani vo vnútornej sieti.
32. Microsegmentation	• Delenie siete na menšie časti, čím sa minimalizuje laterálny pohyb útočníkov.
33. NAC (Network Access Control)	• Riadenie toho, kto sa môže pripojiť k sieti, a kontrola bezpečnostného stavu zariadení.
34. MDM/MAM (Mobile Device/App Management)	• Zabezpečenie mobilných zariadení a aplikácií používaných v organizácii.
35. Encryption / Key Management	• Ochrana dát šifrovaním a riadenie kryptografických kľúčov.

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

SIEM (Security Information and Event Management)

- **Centrálna platforma**, ktorá zbiera, ukladá a vyhodnocuje logy zo všetkých systémov v organizácii
- SOC centrá potrebujú **SIEM** preto, aby porozumeli údajom, ktoré generujú firewally, sieťové zariadenia, systémy na zistenie narušenia bezpečnosti a ostatné zariadenia
- Systémy **SIEM** zhromažďujú a filtrujú, detegujú, klasifikujú a vyšetrujú hrozby
- Taktiež môžu použiť zdroje na implementáciu preventívnych akcií a poukázať na budúce hrozby
- Úlohou **SIEM** je aj uchovávanie logov pre audity (**NIS2, GDPR, ISO 27001**)

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

Nástroje pre SIEM

- **Open – Source:**
  - Wazuh
  - Security Onion
- **Proprietárne:**
  - ELK (Elastic Stack)
  - Microsoft Sentinel
  - Splunk
  - IBM Qradar
  - LogRhythm
  - OpenEDR

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

Technológie používané v SOC

Nástroje pre SIEM

Open-source

- **Wazuh**
- **OSSIM** (Open Source SIEM)
- **OpenSearch + OpenSearch Dashboards** (fork Elasticu)
- **Apache Metron** (už neudržiavané, ale open-source)
- **Prelude OSS**
- **SIEMonster Community Edition** (open-source zostava komponentov)
- **MozDef** (Mozilla Defense Platform)

Proprietárny

- **IBM QRadar**
- **Micro Focus ArcSight**
- **LogRhythm SIEM**
- **RSA NetWitness**
- **McAfee Enterprise Security Manager (ESM)**
- **Exabeam SIEM / Exabeam Fusion**
- **Securonix Next-Gen SIEM**
- **Splunk Enterprise Security (ES) –** nie Splunk Free
- **Rapid7 InsightIDR**
- **Sumo Logic Enterprise Security**
- **Snowflake Security Lake** (ako SIEM modul / riešenie)
- **Devo SIEM**
- **Chronicle SIEM** (Google)
- **Hunters AI SIEM**

Proprietárny s free verziou

- **Splunk Free** (obmedzené na 500 MB logov/deň, bez enterprise funkcií)
- **Graylog Open / Graylog Free Edition** (komerčný, ale má free verziu s limitmi)
- **Elastic Stack** (Elastic License Basic) (základ zadarmo, pokročilé SIEM funkcie sú platené)
- **Sumo Logic Free Tier** (obmedzený retenčný čas)
- **Logz.io Free Tier** (ELK-based, limitované množstvo dát)
- **AlienVault USM Anywhere Free Trial / Essentials** (nie plne free, ale existujú dlhodobé low-tier free možnosti s limitmi)
- **QRadar Community Edition** (obmedzenia: <=50 EPS, <=5k assets)IBM QRadar

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

SOAR (Security Orchestration, Automation and Response)

- Technológie **SOAR** integrujú **spravodajské informácie** o hrozbách a automatizujú pracovné postupy vyšetrovania incidentov a reakcie na ne, na základe **postupových manuálov** vytvorených **bezpečnostným tímom**
- **SOAR využíva nástroje na:**
  - Zhromažďovanie údajov o výstrah z každého komponentu systému
  - Skúmanie, posudzovanie a vyšetrovanie bezpečnostných incidentov
  - Automatizáciu komplexných pracovných postupov reakcie na incidenty. Tieto postupy umožňujú rýchlejšiu reakciu a prispôsobiteľné stratégie obrany
  - Automatickú reakciu na konkrétne hrozby. Používa na to preddefinované scenáre a postupnosti krokov (tzv. playbooks). Tieto materiály sa môžu spúšťať automaticky na základe vopred definovaných pravidiel alebo ich môžu spúšťať bezpečnostní pracovníci.

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

Nástroje pre SOAR

- **Open – Source:**
  - TheHive + Cortex
  - Shuffle
- **Proprietárne:**
  - Splunk SOAR
  - Palo Alto Cortex XSOAR
  - Microsoft Sentinel SOAR

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

Technológie používané v SOC

Nástroje pre SOAR

Open-source

- **Shuffle SOAR (open-source edition)**
  Kompletné severless SOAR riešenie (kontajnery alebo cloud funkcie), workflow engine, integrácie.
- **DFF (Digital Forensics Framework)** – *čiastočne SOAR prvky*
  Primárne forenzný nástroj, ale umožňuje automatizované workflow.
- **Walkoff (od US Navy, už neudržiavané, ale open-source)**
  Open SOAR engine, stále funkčný v starších verziách.

Proprietárny

- **Palo Alto Cortex XSOAR**
- **Splunk SOAR (ex-Palo Alto Phantom)** – komerčný
- **IBM Resilient (IBM Security QRadar SOAR)**
- **Siemplify SOAR (Google Chronicle SOAR)**
- **DFLabs IncMan SOAR**
- **Swimlane**
- **ServiceNow Security Incident Response (SIR)** – SOAR modul
- **LogRhythm SmartResponse** *(SOAR modul)*
- **ReliaQuest (ex-Highlander SOAR)**
- **Tines (automatizačná bezpečnostná platforma)**
- **Rapid7 InsightConnect** *(primárne platené)*
- **D3 Security SOAR**
- **Securonix SOAR**
- **ThreatConnect SOAR**
- **FortiSOAR** (Fortinet)

Proprietárny s free verziou

- **Splunk SOAR Community Edition (ex-Phantom Community).**
  Bezplatná staršia edícia, limitovaná API a funkciami.
- **Tines Free Tier**
  Obmedzený počet automatizácií a workflow.
- **Rapid7 InsightConnect Trial / Limited**
  Nie je zadarmo, ale existuje dlhodobá „community/training“ licencia.

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

EDR (Endpoint Detection and Response)

- Nástroj na **detekciu a reakciu** na útoky na **koncových zariadeniach** (endpointoch)
- **Koncové zariadenia** sú zariadenia ako:
  - Notebook
  - Desktop
  - Server
  - Mobil
  - Cloudový VM.

- **Hlavé úlohy**, ktoré vykonáva **EDR** sú:
  - Monitoruje správanie zariadení v reálnom čase
  - Deteguje podozrivú aktivitu (napr. ransomware, proces injection)
  - Umožňuje analýzu incidentu (timeline, procesy, sieťová komunikácia)
  - Umožňuje reakciu na útok (izolovať endpoint od siete, zabiť proces, odstrániť súbory)

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

Technológie používané v SOC

Nástroje pre EDR/XDR

- **EDR:**
  - CrowdStrike Falcon Insight
  - SentinelOne
  - Microsoft Defender for Endpoint
- **XDR:**
  - Microsoft Defender XDR
  - CrowdStrike Falcon XDR
  - Palo Alto Cortex XDR
  - Wazuh XDR

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

Technológie používané v SOC

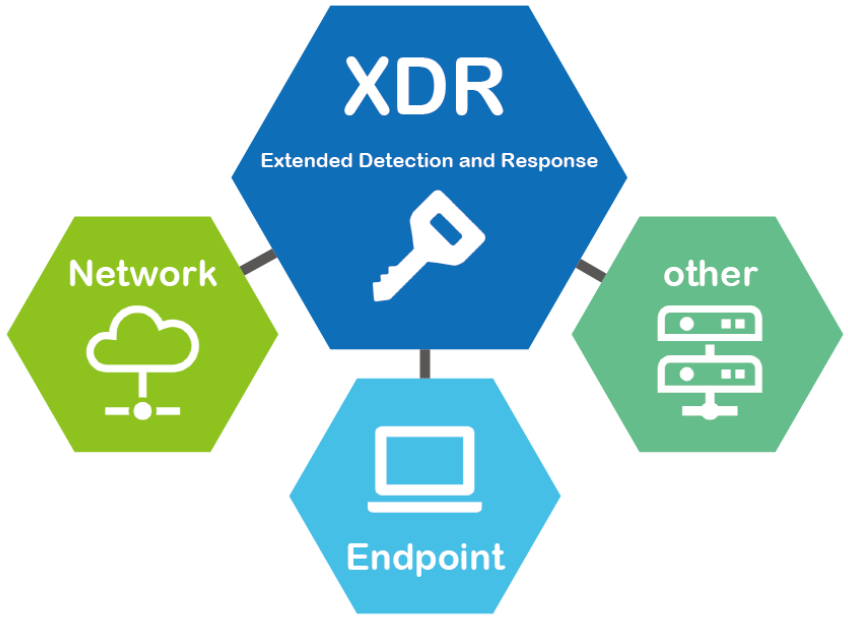
Nástroje pre EDR

Open-source	Proprietárny	Proprietárny s free verziou
• Wazuh EDR • OpenEDR (Comodo) • Falco (CNCF)	• CrowdStrike Falcon Insight / Complete • SentinelOne Singularity XDR/EDR • Palo Alto Cortex XDR • Trellix/McAfee Endpoint Security & EDR • Trend Micro Apex One / Vision One • Cisco Secure Endpoint (ex-AMP) • Check Point Harmony Endpoint • FireEye Endpoint Security (Trellix) • ESET Enterprise Inspector (EEI) • Bitdefender GravityZone EDR • Kaspersky EDR Expert • Sophos Intercept X Advanced with EDR • Fortinet FortiEDR • Cybereason EDR • VMware Carbon Black EDR • Heimdal EDR • Elastic EDR (pri enterprise licencii) • RSA NetWitness Endpoint	• Microsoft Defender for Endpoint – Free built-in (Windows Security) • Elastic Security – Free & Basic tier • CrowdStrike Falcon Free Trial / Falcon Go limited • SentinelOne Free Trial • Cybereason Free Trial • FortiEDR Free Trial

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

XDR (Extended Detection and Response)

- **Rozšírený EDR**, ktorý prepája dáta z viacerých bezpečnostných technológií
- Namiesto sústredenia sa len na **endpointy**, XDR zbiera dáta z:
  - Endpointov (EDR)
  - Siete (firewally / IDS / IPS)
  - Cloudových služieb (Azure/M365, AWS, Google Cloud)
  - Aplikácií a identít (IAM, AD, e-mail systémy)
- **XDR** koreluje dáta z celého prostredia



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

Technológie používané v SOC

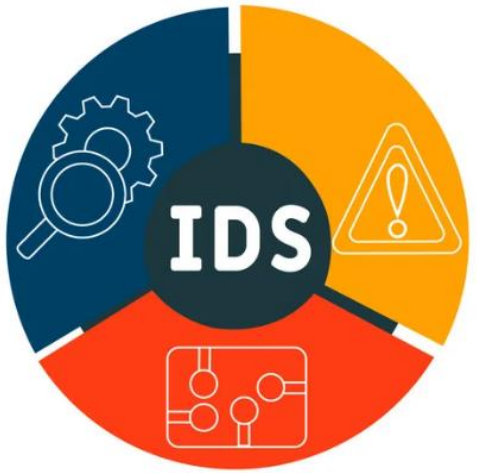
Nástroje pre XDR

Open-source	Proprietárny	Proprietárny s free verziou
• Wazuh EDR • OpenEDR (Comodo) • Falco (CNCF)	• Palo Alto Networks Cortex XDR • CrowdStrike Falcon XDR • SentinelOne Singularity XDR • Trend Micro Vision One XDR • Microsoft Defender XDR • Fortinet FortiXDR • Sophos XDR • Cisco XDR • Check Point Infinity XDR • Trellix XDR (McAfee + FireEye) • Elastic XDR (enterprise edícia) • RSA NetWitness XDR • Cybereason XDR • Exabeam Fusion XDR • Securonix Unified Defense SIEM (XDR funkcionalita) • Rapid7 InsightXDR • ESET XDR (v rámci ESET PROTECT Elite)	• Microsoft Defender XDR – Free Core • Elastic Security XDR – Free/Basic licencia • Trend Micro Vision One – Free Trial / Developer Edition • CrowdStrike Falcon XDR – Free Trial / Falcon Go limitované • SentinelOne Singularity – Free Trial • Cybereason XDR – Free Trial • Sophos XDR – Free Trial

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

IDS / IPS (Intrusion Detection / Prevention System)

- IDS je systém na **detekciu narušenia** (prieniku) do siete alebo systému
- IDS analyzuje **sieťovú komunikáciu** alebo **logy** a hľadá:
  - Známe útoky (pomocou signatúr)
  - Anomálie v správaní (neštandardná prevádzka)
  - Pokusy o zneužitie zraniteľností
- IPS je systém na **prevenciu narušenia** – aktívne blokuje útoky.
- **IPS dokáže:**
  - Blokovať sieťovú komunikáciu,
  - Zablokovať IP adresu útočníka,
  - Ukončiť reláciu,
  - Upraviť firewall pravidlo.



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

Nástroje pre IDS / IPS

- Suricata
- Snort
- Zeek
- Security Onion (SIEM + IDS + IPS)

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

Technológie používané v SOC

Nástroje pre IDS/ISP

Open-source

- **Snort (open-source verzia)**
- **Suricata**
- **Zeek (ex-Bro)**
  IDS (behaviorálna analýza, nie IPS)
- **OSSEC / Wazuh HIDS**
  host-based IDS
- **Security Onion** (platforma obsahujúca Suricata + Zeek + ďalšie)
- **Prelude OSS**
- **Sagan IDS**
- **Maltrail IDS**
- **AIDE / Samhain**
  host-based integrity & IDS

Proprietárny

- **Cisco Firepower Threat Defense (FTD)**
- **Palo Alto Networks Threat Prevention (IPS modul)**
- **Fortinet FortiGate IPS**
- **Check Point IPS / ThreatCloud**
- **McAfee Network Security Platform (NSP)**
- **Trend Micro TippingPoint**
- **Juniper SRX IPS**
- **WatchGuard IPS**
- **IBM Security Network IPS (GX Series – legacy)**
- **Hillstone Networks IPS**
- **HP TippingPoint (legacy)**
- **Forcepoint IPS**

Proprietárny s free verziou

- **Snort Subscriber Rules Free Tier**
  Snort je open-source, ale existuje aj komerčná verzia pravidiel.
- **Suricata – ETOpen Ruleset (free)**
  Open-source engine s voľným pravidlovým setom; platené pravidlá sú komerčné od ETPro.
- **Cisco Firepower – Evaluation License**
- **Palo Alto Threat Prevention – Trial (30 dní)**
- **Fortinet FortiGate IPS – Free trial / limited features in FortiOS free VM**
  Virtuálna verzia má niektoré IPS funkcie v obmedzenom režime.

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

Threat Intelligence (CTI – Cyber Threat Intelligence)

- Je to **proces** zberu, analýzy a distribúcie informácií o kybernetických hrozbách, útočníkoch a ich technikách.
- Výsledkom sú **informácie**, ktoré pomáhajú organizácii **predchádzať útokom** alebo na ne **rýchlejšie reagovať**.

Technológie používané v SOC

Nástroje pre Threat Inteligence

Open-source

- **MISP** (Malware Information Sharing Platform)
- **OpenCTI** (od LEXSI / OASIS, open-source)
- **Yeti** (Your Everyday Threat Intelligence)
- **Open Threat Exchange (OTX) –** open community feed
- **Hail a TAXII** (open-source TAXII server)
- **Cortex & TheHive** (open-source IR + analyzéry IOCs)
- **IntelMQ** (CTI pipeline framework)
- **STIX/TAXII** open-source implementácie
- **Maltrail** (open-source threat feed + IDS)
- **Zeek Intel Framework** (open intelligence ingestion)

Proprietárny

- **Recorded Future Intelligence Cloud**
- **ThreatConnect (Enterprise TI)**
- **Anomali ThreatStream**
- **Flashpoint CTI**
- **Intel 471**
- **Group-IB Threat Intelligence**
- **Kaspersky Threat Intelligence Portal (KTI full)**
- **CrowdStrike Falcon Intelligence (premium)**
- **Palo Alto Unit42 Intelligence**
- **FireEye/Mandiant Threat Intelligence**
- **Cisco Talos Intelligence (enterprise subscription)**
- **Fortinet FortiGuard Threat Intelligence Service**
- **Check Point ThreatCloud Intelligence**
- **Secureworks Counter Threat Unit (CTU)**
- **Securonix Threat Intelligence platform**

Proprietárny s free verziou

- **VirusTotal –** Free Community Edition
  Základné zisťovanie hashov, URL, súborov.
- **AlienVault OTX** – Free Community Feed
  Komerčný ekosystém, ale s veľkou free komunitnou časťou.
- **IBM X-Force Exchange** – Free Tier
- **Recorded Future –** Free Browser Extension + Limited Community Access
- **Cisco Talos –** Free Intelligence Portal
- **Kaspersky TI** – Free Tools
- **Hybrid Analysis** (by CrowdStrike) – Free Community
- **Any.run –** Free Interactive Malware Analysis (limitovaná)
- **AbuseIPDB** – Free Tier

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

Typy SOC centier

Typy modelov SOC centra

- **Interné SOC centrum** (Internal SOC)
- **Externé SOC centrum** (Outsourced SOC, External SOC, SOC as a Service)
- **Globálne SOC centrum** (Global alebo Command SOC)
- **Spolu riadené SOC centrum** (Co - Managed SOC)
- **Hybridné SOC centrum** (Hybrid SOC)
- Okrem týchto modelov SOC centier existujú ešte iné centrá a služby, ktoré sa nachádzajú v rovnakej oblasti kybernetickej bezpečnosti ako SOC centrá.
- Sú to napr.:
  - **Poskytovateľ riadených bezpečnostných služieb** (MSSP, Managed Security Service Provider)
  - **Riadená detekcia a odpoveď** (MDR, Managed Detection and Response)

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

Typy SOC centier

Interné SOC centrum

- SOC centrum je plne **interné**, pričom vlastníkom a prevádzkovateľom je **daný podnik**
- Zamestnáva **vlastných** SOC analytikov (**Tier 1–3**), forenzných špecialistov, SOC manažéra
- Prevádzkuje svoje **vlastné nástroje** (SIEM, SOAR, EDR/XDR)
- Reaguje na incidenty bez tretích strán, priamo v rámci organizácie.

- **Výhody**:
  - Firma má plnú kontrolu nad dátami a procesmi
  - Nižšie riziko úniku citlivých dát
  - SOC tím veľmi dobre pozná prostredie a procesy organizácie
- **Nevýhody**:
  - Investícia do ľudí (analytici, inžinieri, manažér SOC)
  - Investícia do technológií (SIEM, SOAR, EDR/XDR)
  - Prevádzka 24/7
  - Je potrebné nájsť špecialistov v oblasti kybernetickej bezpečnosti

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

Interné SOC centrum

- Tento typ SOC centa sa najčastejšie používa v sektoroch, kde sú **vysoké požiadavky na bezpečnosť, dostupnosť** a **legislatívu**:
  - Finančný sektor (banky, poisťovne)
  - Energetika (elektrina, voda, plyn, ...)
  - Verejná správa, zdravotníctvo
  - Telekomunikácie a doprava
  - Veľké podniky s rozsiahlym IT

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

Typy SOC centier

Externé SOC centrum

- **Neprevádzkuje** ho organizácia, ale **prenajíma** si ho od špecializovaného poskytovateľa (outsourcing).
- Služba sa najčastejšie označuje ako **SOCaaS** (SOC as a Service) alebo **Managed SOC**
- Poskytovateľ zabezpečuje nástroje, ľudí aj procesy
- Všetky logy a bezpečnostné udalosti sa odosielajú do SOC poskytovateľa
- Poskytovateľ analyzuje incidenty a informuje o nich zákazníka
- Pri závažných incidentoch rieši eskaláciu a navrhne kroky na odstránenie

- **Výhody**:
  - Nižšie vstupné náklady (firma neplatí vlastný tím, stroje ani licencie)
  - Rýchle nasadenie
  - Prístup k expertom a najnovším technológiám
  - 24/7 monitoring
- **Nevýhody**:
  - Menšia kontrola nad dítami
  - Potreba riešiť SLA (Service Level Agreement)
  - Menšia znalosť interného prostredia organizácie

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

Externé SOC centrum

- Tento typ SOC centra **najčastejšie** používajú
  - Malé a stredné podniky (obmedzený rozpočet)
  - Firmy bez vlastného bezpečnostného oddelenia
  - Startupy
  - Firmy, ktoré musia splniť legislatívu (NIS2), ale nechcú investovať do vlastnej prevádzky

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

Typy SOC centier

Globálne SOC centrum

- Je to **centrálna entita** (hlavné SOC centrum), ktorá riadi a koordinuje činnosti **menších** SOC centier v rámci väčšej organizácie alebo regiónu
- Je to **najvyšší level** SOC modelu
- **Riadi** a **koordinuje** bezpečnosť naprieč regiónmi / časovými zónami
- Sleduje infraštruktúru všetkých pobočiek firmy
- Poskytuje **monitoring 24/7/365** kombináciou regionálnych SOC centier.
- Využíva sa tam, kde jedna organizácia funguje vo viacerých časových pásmach a potrebuje centrálnu bezpečnostnú kontrolu:
  - Nadnárodné korporácie (Microsoft, Amazon, ...)
  - Banky a poisťovne s pobočkami v rôznych krajinách
  - Globálne logistické firmy a dopravné spoločnosti
  - Poskytovatelia cloudových služieb a telekomunikácie

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

Spolu riadené SOC centrum

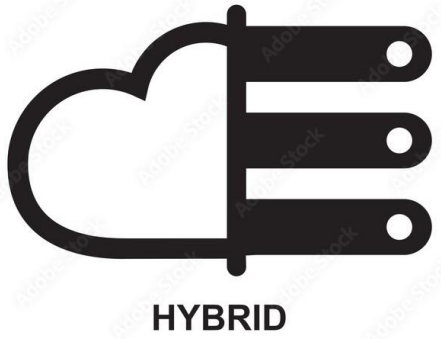
- **Interné** IT oddelenie podniku spolupracuje s **externým** SOC centrom
- **Spoločne** spravujú potreby kybernetickej bezpečnosti
- Organizácia si **zachová kontrolu** nad bezpečnosťou, ale externý partner jej pomáha s monitoringom, technológiami a analytikmi.
- **Tento spôsob sa používa keď**:
  - Organizácia má interné IT/SOC, ale nemá kapacitu na monitorovanie 24/7
  - Má vlastný SIEM, ale potrebuje expertov na ďalšiu analýzu
  - Chce si zachovať vlastníctvo dát (na rozdiel od plného outsourcingu)
  - Nechce budovať drahé 24/7 smeny (Tier 1), ale chce mať pod kontrolou Tier 2/3

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

Typy SOC centier

Hybridné SOC centrum

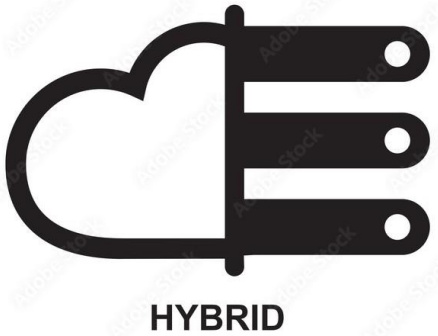
- Je to model prevádzky SOC centra, kde sa **kombinuje interný** SOC tím organizácie s **externým** poskytovateľom služieb
- Firma má kontrolu nad dátami a incidentami, ale využíva externých expertov, nástroje a podporu
- **Externý partner:**
  - Poskytuje SIEM, SOAR,
  - Analyzuje logy,
  - Filtruje alerty,
  - Monitoruje prevádzku 24/7,
  - Dodáva know-how, ...
- **Interný tím organizácie:**
  - Pozná prostredie firmy a biznis procesy,
  - Rozhoduje o reakcii na incidenty,
  - Rieši lokálne zásahy a kritické incidenty,
  - Definuje politiky a priority



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

Hybridné SOC centrum

- **Hybridné SOC centrum sa používa vtedy keď:**
  - organizácia chce kontrolu nad bezpečnostnými dátami, ale nemá dostatok ľudí
  - ide o firmy v kritickej infraštruktúre, kde externé SOC centrum nemôže rozhodovať samostatne
  - spoločnosti prechádzajú transformáciou a budujú vlastné SOC centrum, ale potrebujú podporu

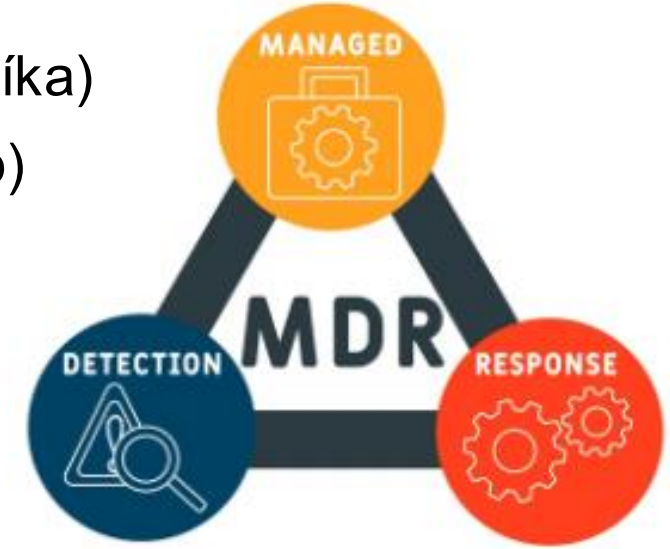


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy SOC centier

Riadená detekcia a odpoveď (MDR)

- MDR je bezpečnostná služba zameraná na detekciu a reakciu
- Zameriava sa primárne na **koncové zariadenia** (notebooky, počítače, servery), využíva nástroje na **EDR / XDR**
- Pracovníci, ktorý vykonávajú túto službu **preskúmajú** anomálie, **odstránia** falošné poplachy a **reagujú** na hrozby v mene klienta, ktorý si platí za ich služby.
- MDR **deteguje** hrozby a útoky (ransomvér, phishing, malware)
- Aktívne **zasahuje** pri incidente (izoluje zariadenie, blokuje útočníka)
- **Vykonáva** Threat Hunting (proaktívne hľadanie skrytých hrozieb)
- Po vyriešení incidentu poskytuje odporúčania na zlepšenie bezpečnosti



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

Poskytovateľ riadených bezpečnostných služieb (MSSP)

- MSSP je **externý poskytovateľ** bezpečnostných služieb, ktorý pre organizáciu **monitoruje a spravuje** bezpečnostné technológie:
  - Firewally
  - VPN
  - IDS/IPS
  - Antivírus
  - Sieťové zariadenia

- MSSP na rozdiel od MDR **nereaguje** na útoky a ani **nehľadá** hrozby
- **MSSP iba informuje** zákazníka o detegovaných incidentoch, odstránenie, **analyzovanie a následná obnova je plne v rukách zákazníka**

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

Typy SOC centier

Rozdiel medzi MDR, MSSP a SOC

Funkcionalita	MDR	MSSP	SOC
Monitorovanie koncových zariadení (EDR/XDR)	**Áno** – hlavná funkcia	Nie	Čiastočne (ak má EDR integráciu)
Monitorovanie siete	Nie	**Áno** – základná úloha	**Áno**
Monitorovanie celej infraštruktúry	Nie	Nie	**Áno** – kompletný prehľad
Korelácia logov (SIEM)	Nie	Nie	**Áno** – jadro činnosti
Reakcia na incidenty (Incident Response)	**Áno** – aktívne zasahuje	Obmedzene – väčšinou len upozorní	**Áno** – plnohodnotné IR
Aktívne zastavenie útoku (containment)	**Áno**	Nie	**Áno**, ak má EDR/SOAR
Thread Hunting	**Áno** – kľúčová činnosť	Nie	**Áno** – pri vyšších leveloch SOC
Forenzná analýza útoku	**Áno**	Nie	**Áno**
Analýza hrozieb (Threat Intelligence)	**Áno**	Obmedzene	**Áno**
Správa a archivácia logov	Nie	Nie	**Áno**
Správa bezpečnostných zariadení (FW, IPS, VPN…)	Nie	**Áno**	Nie (iba kontrola a dohľad)
Tvorba bezpečnostných politík	Nie	**Áno** – ako súčasť služieb	**Áno** (interný SOC)
Odporúčania po incidente (Security Posture)	**Áno**	Obmedzene	**Áno**
Poskytuje SIEM	Nie	Nie	Môže (ak ide o externý/managed
Poskytuje EDR/XDR	**Áno** (je to základ)	Nie	Nie (ale integruje s EDR)
24/7 monitoring	Áno (zamerané na endpointy)	Obvykle Áno	Áno
Nahrádza interný IT tím	Nie	**Môže**	Nie
Zodpovednosť za bezpečnosť prostredia	Zdieľaná	Zdieľaná	**Interná alebo externá (podľa typu**

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

Poskytovatelia SOCaaS vo svete

- **Arctic Wolf Networks** (USA)
- **Secureworks** (USA) - globálny poskytovateľ s platformou Taegis
- **Alert Logic** (USA) - Cloud-zameraný SOCaaS poskytovateľ
- **eSentire** - špecialista na SOCaaS a Threat-Hunting tím
- **Trustwave** - poskytuje SOC služby aj Threat-Hunting
- **N-iX** - (Ukrajina / Európa)
- **Fortinet** (USA) - ponúka službu FortiGuard SOCaaS
- **Palo Alto Networks**
- **Rapid7** - SOCaaS + platforma Insight.
- **Cloudflare**
- **CITIC Telecom CPC** - globálne pokrytie, SOCaaS služba
- **Soitron Security** - pôsobí v strednej Európe
- **VOID SOC** - slovenský poskytovateľ (časť Soitron skupiny) v oblasti SOC
- **Netsurion**
- **TechMagic** - ukrajinský poskytovateľ SOCaaS.
- **Infopulse** - globálny vendor s SOCaaS službami
- **Dataprise** – USA, SOCaaS poskytovateľ
- **CyberDuo** - USA, SOCaaS poskytovateľ
- **UnderDefense** - USA, SOCaaS poskytovateľ

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

Slovenský poskytovatelia SOCaaS

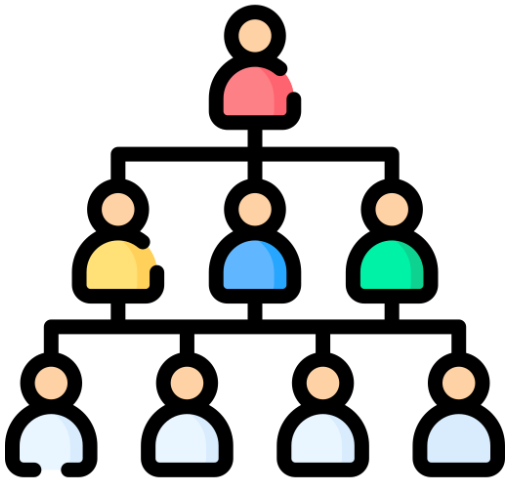
- **Binary Confidence s.r.o. – Bratislava**
  - Špecializovaná kyberbezpečnostná firma, vlastné SOC centrum (BINCONF CDC)
- **SOITRON, s.r.o. – Bratislava (void SOC)**
  - Veľký integrátor; má vlastné bratislavské SOC, poskytuje „SOC ako služba“ s 24/7 monitoringom a tímom analytikov
- **IstroSec s.r.o. – Bratislava (Petržalka)**
  - Čisto bezpečnostná firma; robí managed defense/monitoring prostredníctvom vlastného SOC tímu, plus IR, threat hunting, CISO-as-a-service
- **WDS Solutions s.r.o. – Trenčín**
  - IT spoločnosť s bezpečnostnou divíziou; ponúka priamo službu „SOC as a Service“ (monitoring, reakcia, DFIR)
- **iServices (iS SOC as a Service)**
  - Slovenská firma zameraná na správu infraštruktúry a kybernetickú bezpečnosť; má produkt „iS SOC as a Service“ ako komplexný bezpečnostný monitoring
- **Orange Slovensko, a.s. – Bratislava**
  - Telekomunikačný operátor; pre biznis segment ponúka „SOC ako služba“, teda 24/7 monitoring a analýzu incidentov ako managed službu
- **Alanata a.s. – Bratislava**
  - Poskytuje Managed XDR a SOC as a Service
- **Aricoma Slovakia – Bratislava**
  - Slovenská entita skupiny Aricoma
- **TÜV SÜD Slovakia s.r.o.**
  - Popri auditoch a certifikácii prevádzkuje manažovaný SOC pre IT/OT, vrátane špecializovaného SOC pre zdravotnícke zariadenia

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

Role v SOC centre

SOC tím

- Zamestnanci SOC centra sú rozdelený do úrovní **podľa zodpovedností a odbornosti**
- SOC tím delíme do nasledujúcich úrovní:
  - **Úroveň 1** – Analytik výstrah (SOC Analyst)
  - **Úroveň 2** – Riešiteľ incidentov (Incident Responder)
  - **Úroveň 3** – Hľadač hrozieb (Threat Hunter / Forenzný špecialista)
  - **SOC manažér**



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

Úroveň 1 – Analytik výstrah (alertov)

- Monitoruje prichádzajúce výstrahy
- Ak zistí že výstraha **je pravdivá**:
  - Spraví základné opatrenia na zmiernenie dopadov danej hrozby
  - Alebo ak je to potrebné, predá riešenie hrozby pracovníkovi 2. úrovne
- Ak zistí že incident **je nepravdivý**:
  - Aktualizuje systém pre detekciu incidentov, ktorý danú výstrahu vygeneroval
- Ak incident **nedokáže vyriešiť** predá hrozbu pracovníkovi 2

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

Úroveň 2 – Riešiteľ incidentov

- **Rieši incidenty**, ktoré mu odovzdá Analytik výstrah
- **Skúma** incidenty do hĺbky
- **Navrhne**, ako by sa mal problém riešiť
- **Reaguje** na incident
- **Odporučí** nápravu
- **Dokumentuje** incident

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

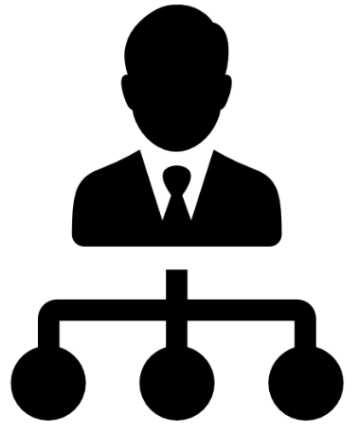
Úroveň 3 – Hľadač hrozieb

- Je to **expert v oblasti** sietí, koncových zariadení, hrozieb, informácií o hrozbách a reverzného inžinierstva malvéru
- Sleduje procesy malvéru s cieľom určiť jeho vplyv, a ako ho možno odstrániť (vrátane preventívnych opatrení)
- Je **hlboko zapojený** do hľadania potenciálnych hrozieb a implementácie nástrojov na detekciu hrozieb
- **Proaktívne hľadá** kybernetické hrozby, ktoré sú prítomné v sieti, ale ešte neboli detegované.

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

SOC manažér

- Spravuje **všetky zdroje** v SOC centre
- **Slúži ako bod kontaktu** pre organizácie, zákazníkov
- Implementujte štandardizované prevádzkové postupy (Standard Operating Procedures, SOPs) pre proces riešenia incidentov, ktoré usmerňujú analytikov prostredníctvom postupov triedenia a reakcie.
- Zodpovedá za reporty pre vedenie a komunikáciu pri veľkých incidentoch.



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

Zhrnutie výhod SOC centra

Výhody SOC centra pre organizáciu

- **Nepretržité monitorovanie 24/7** – včasná detekcia hrozieb a minimalizácia dopadov incidentov
- **Rýchla reakcia na bezpečnostné incidenty** – izolácia napadnutých zariadení, odstránenie hrozby, obnova prevádzky
- **Forenzná analýza incidentov** – zistenie príčiny útoku, vstupného bodu a návrhy preventívnych opatrení
- **Proaktívne hľadanie hrozieb (Threat Hunting)** – odhaľuje útoky ešte pred tým, než spôsobia škodu
- **Centralizovaná správa bezpečnosti** – všetky logy, udalosti a dáta sú na jednom mieste
- **Automatizácia a rýchlejšia reakcia** vďaka nástrojom ako SIEM, SOAR a EDR/XDR
- **Podpora legislatívy a auditov** – NIS2, GDPR, ISO 27001, interné a externé audity
- **Zníženie finančných a prevádzkových rizík** – menej prestojov, menšie škody po incidente

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

Otvorená reflexia

- **Aká je hlavná úloha SOC centra?** (1 správna)
  - a) Vyvíjať nové IT systémy
    b) Monitorovanie IT infraštruktúry a reagovať na bezpečnostné incidenty
    c) Riadi len prevádzku firewallov a nastavovanie sieťových pravidiel
    d) Analyzuje dáta o incidentoch, ale zásah a reakciu vždy prenecháva externým dodávateľom
- **Ktoré z nasledujúcich tvrdení patria medzi výhody SOC centra?** (2 správne)
  - a) Nepretržité monitorovanie 24/7
    b) Znižuje finančné a prevádzkové riziká organizácie
    c) Odhaľuje incidenty až po tom, čo spôsobia škodu
    d) Zákazníkom poskytuje lacnejšie licencie

Otvorená reflexia

- **Ktorá technológia zabezpečuje centralizované zbieranie logov a ich vyhodnocovanie?** (1 správna)
  - a) CRM
    b) SIEM
    c) VPN
    d) Office365
- **Ktorá z možností najlepšie vystihuje forenznú analýzu v SOC?** (1 správna)
  - a) Kontrola účtovníctva firmy
    b) Analýza incidentu, hľadanie vstupného bodu a návrh opatrení
    c) Tvorba marketingových reportov
    d) Automatická aktualizácia softvéru

Otvorená reflexia

- **Ktorá z nasledujúcich činností je mimo primárneho pôsobenia SOC centra?** (1 správna)
  - a) Korelácia bezpečnostných udalostí z rôznych systémov pomocou SIEM
    b) Hľadanie vstupného bodu útoku a vytvorenie Incident Reportu
    c) Nastavovanie finančného rozpočtu organizácie a plánovanie investičných rozhodnutí
    d) Izolácia napadnutého zariadenia od siete počas incidentu

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

Výhody SOC centier

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