**PRÍSTUP K PROJEKTU**

(Verzia dokumentu v1.01/07\_2021)

Identifikovanie požiadaviek **na technickú časť riešenia**

**Identifikácia projektu**

|  |  |
| --- | --- |
| **Povinná osoba** | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| **Názov projektu** | Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS) |
| **Zodpovedná osoba za projekt** | Mgr. Filip Tubler |
| **Realizátor projektu** | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| **Vlastník projektu** | Ing. Martin Florián, PhD. |

**Schvaľovanie dokumentu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Položka** | **Meno a priezvisko** | **Organizácia** | **Pracovná pozícia** | **Dátum** | **Podpis**  (alebo elektronický súhlas) |
| Vypracoval | Filip Tubler | MIRRI | Gestor pre Investíciu 6 | 27.10.2023 |  |

\*Pôvodná verzia dokumentu bola z hľadiska dôvernosti informačných aktív klasifikovaná na stupeň „CHRÁNENÉ“ podľa vyhlášky Národného bezpečnostného úradu z 11. decembra 2018 č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov a podľa smernice Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 13/2021 zo dňa 22. októbra 2021 o inventarizácii a ochrane informačných aktív Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Z dôvodu zverejnenia dokumentácie v METAIS a vyššie uvedenej klasifikácie dokumentu sú vybrané textové a obrázkové časti redigované.

**OBSAH**

[1. POPIS ZMIEN DOKUMENTU 3](#_Toc150461134)

[1.1 História zmien 3](#_Toc150461135)

[2. ÚČEL DOKUMENTU 4](#_Toc150461136)

[2.1 Konvencie používané v dokumentoch – označovanie požiadaviek 4](#_Toc150461137)

[3. POPIS NAVRHOVANÉHO RIEŠENIA 4](#_Toc150461138)

[3.1 Modul 1 - Early Warning System (EWS) 5](#_Toc150461139)

[3.2 Modul 2 - Vládny SOC 6](#_Toc150461140)

[3.2.1 Fáza 1 6](#_Toc150461141)

[3.2.2 Fáza 2 – plánované kapability nezaradené do projektu 8](#_Toc150461142)

[3.3 Modul 3 - Monitorovacie nástroje na OVM 8](#_Toc150461143)

[4. ARCHITEKTÚRA RIEŠENIA PROJEKTU 9](#_Toc150461144)

[4.1 Biznis vrstva 9](#_Toc150461145)

[4.1.1 Aktuálny stav biznis architektúry 9](#_Toc150461146)

[4.1.2 Budúci stav Biznis architektúry 11](#_Toc150461147)

[4.2 Aplikačná vrstva 13](#_Toc150461148)

[4.2.1 Aktuálny stav aplikačnej architektúry 13](#_Toc150461149)

[4.2.2 Budúci stav aplikačnej architektúry 14](#_Toc150461150)

[4.2.3 Rozsah informačných systémov 17](#_Toc150461151)

[4.2.4 Využívanie nadrezortných centrálnych blokov a podporných spoločných blokov (SaaS) 17](#_Toc150461152)

[4.2.5 Prehľad plánovaného využívania podporných spoločných blokov (SaaS) 18](#_Toc150461153)

[4.2.6 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky – spoločné moduly 18](#_Toc150461154)

[4.2.7 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky - modul procesnej integrácie a integrácie údajov (IS CSRÚ) 18](#_Toc150461155)

[4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ 18](#_Toc150461156)

[4.2.9 Konzumovanie údajov z IS CSRÚ 18](#_Toc150461157)

[4.3 Dátová vrstva 18](#_Toc150461158)

[4.3.1 Údaje v správe organizácie 18](#_Toc150461159)

[4.3.2 Dátový rozsah projektu 19](#_Toc150461160)

[4.3.3 Kvalita a čistenie údajov 19](#_Toc150461161)

[4.4 Referenčné údaje 19](#_Toc150461162)

[4.4.1 Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné 19](#_Toc150461163)

[4.4.2 Identifikácia údajov pre konzumovanie alebo poskytovanie údajov do/z CSRU 19](#_Toc150461164)

[4.5 Otvorené údaje 19](#_Toc150461165)

[4.6 Analytické údaje 19](#_Toc150461166)

[4.7 Moje údaje 19](#_Toc150461167)

[4.8 Prehľad jednotlivých kategórií údajov 19](#_Toc150461168)

[4.9 Technologická vrstva 19](#_Toc150461169)

[4.9.1 Prehľad technologického stavu 19](#_Toc150461170)

[4.9.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky 20](#_Toc150461171)

[4.9.3 Návrh riešenia technologickej architektúry 20](#_Toc150461172)

[4.9.4 Využívanie služieb z katalógu služieb vládneho cloudu 22](#_Toc150461173)

[4.9.5 Jazyková lokalizácia 22](#_Toc150461174)

[4.10 Bezpečnostná architektúra 22](#_Toc150461175)

[5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY 26](#_Toc150461176)

[6. ZDROJOVÉ KÓDY 26](#_Toc150461177)

[7. PREVÁDZKA A ÚDRŽBA 26](#_Toc150461178)

[7.1 Prevádzkové požiadavky 26](#_Toc150461179)

[7.1.1 Úrovne podpory používateľov: 26](#_Toc150461180)

[7.2 Požadovaná dostupnosť pre jednotlivé bezpečnostné nástroje: 27](#_Toc150461181)

[7.2.1 Dostupnosť (Availability) 27](#_Toc150461182)

[7.2.2 RTO (Recovery Time Objective) 27](#_Toc150461183)

[7.2.3 RPO (Recovery Point Objective) 28](#_Toc150461184)

[8. POŽIADAVKY NA PERSONÁL 28](#_Toc150461185)

[9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU 28](#_Toc150461186)

[10. PRÍLOHY 29](#_Toc150461187)

# POPIS ZMIEN DOKUMENTU

## História zmien

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia | Dátum | Zmeny | Meno |
| v0.1 | 30.11. 2022 | Vytvorenie dokumentu | Filip Tubler |
| v0.2 | 30.04. 2023 | Nová architektúra TO BE riešenia – variant nový SOC | Filip Tubler |
| v0.3 | 30.09. 2023 | Aktualizácia architektúry TO BE riešenia – variant využitia kapacít aktuálneho SOC na NASES | Filip Tubler |
| v1 | 23.10.2023 | Aktualizácia technologickej a bezpečnostnej architektúry a harmonogramu. | Filip Tubler |

# ÚČEL DOKUMENTU

Dokument **Prístup k projektu** je určený pre iniciačnú fázu **v súlade s vyhláškou č. 85/2020 Z. z. o riadení projektov**  a slúži na rozpracovanie detailných informácií prípravy projektu z pohľadu budúceho stavu a navrhovaného riešenia tak, aby mohol byť projekt schválený a začal proces verejného obstarávania a následný prechod do realizačnej fázy projektu.

## Konvencie používané v dokumentoch – označovanie požiadaviek

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek sú rozdelené na funkčné, nefunkčné a technické. Podskupiny v hlavných kategóriách je možné rozšíriť v závislosti od potrieb projektu, napríklad:

Funkčné požiadavky používajú konvenciu:

*RF\_xxx*

* *RF – funkčná požiadavka*
* *xxx – číslo požiadavky*

Nefunkčné a technické požiadavky používajú konvenciu:

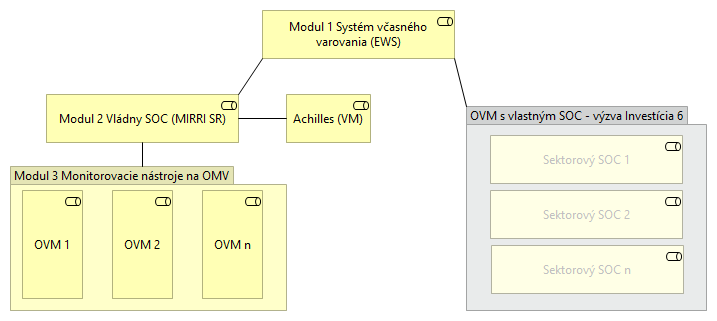
*RNF\_xxx*

* *RNF – nefunkčná požiadavka*
* *xx – číslo požiadavky*

Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.

# POPIS NAVRHOVANÉHO RIEŠENIA

Naplnenie cieľov projektu bude zabezpečené prostredníctvom niekoľkých samostatných častí, ktoré vzájomnou integráciou vytvoria jeden ekosystém. Celé navrhované riešenie pozostáva z troch modulov. Schéma prezentujúca zloženie projektu je znázornená na obrázku nižšie. Centrálna časť riešenia **Systému včasného varovania - Early Warning System (EWS) (Modul 1)** umožní skrátiť čas detekcie a reakcie na kybernetické bezpečnostné incidenty a umožní zbierať, vyhodnocovať a poskytovať informácie o aktuálnych kybernetických bezpečnostných hrozbách. Tieto informácie budú zbierané prostredníctvom **bezpečnostných nástrojov nasadených v internej infraštruktúre pripojeného subjektu verejnej správy (Modul 3)** a zabezpečeným spojením budú dáta posielať do spoločného **pracoviska SOC (Modul 2)** prevádzkovaného Národnou agentúrou pre sieťové a elektronické služby (NASES) a Vládnou jednotkou CSIRT. Ďalšie informácie o kybernetických bezpečnostných incidentoch budú zbierané z ostatných SOC-ov budovaných v prostredí verejnej správy, pôjde najmä o tzv. sektorové dohľadové centrá, ktoré budú pripojené do systému včasného varovania. Budovanie tzv. sektorových SOC bude podporené na základe Výzvy na predkladanie žiadostí o poskytnutie prostriedkov mechanizmu na Podporu budovania bezpečnostných dohľadových centier v prostredí verejnej správy. **Projekt nepočíta s vlastným alebo externým vývojom navrhovaného riešenia**, ale s kombináciou a vzájomnou integráciou viacerých tzv. krabicových riešení.



*Obrázok 1: Štruktúra projektu*

## Modul 1 - Early Warning System (EWS)

Modul predstavuje tzv. dáždnik navrhovaného riešenia. Jednotlivé funkcie modulu budú dodávané prostredníctvom VJ CSIRT, nainštalovaných technológií a definovaných procesov, ktoré tvoria interne procesy v rámci systému včasného varovania, ale aj nastavenie procesov medzi EWS a jednotlivými OVM zapojenými do EWS. Uvedené funkcie a služby budú dodávané subjektom, ktoré: 1) spadajú pod monitoring Vládneho SOC, ale aj 2) pre subjekty, ktoré bezpečnostný monitoring neprevádzkujú alebo 3) majú prevádzkovaný a postupne budovaný bezpečnostný monitoring pre svoje lokálne potreby (v schéme vyššie označované ako Sektorové SOC). Funkcie budú koncipované tak, aby mohli byť dodávané centrálne, zvyšovali úroveň zabezpečenia, umožnili poskytovať preventívne varovania, zdieľanie informácií a skúseností medzi pracoviskami SOC, prinášali väčšiu visibilitu, maximalizovali automatizáciu a pomáhali k efektívnemu a čo najkratšiemu riešeniu bezpečnostných incidentov. Plánované funkcie modulu EWS:

1. **Ohlasovanie bezpečnostného incidentu**

Služba umožní vytvorenie platformy pre rýchle a ucelené nahlásenie bezpečnostného incidentu. Reportovaný incident bude možné klasifikovať a sprístupniť len požadovaným OVM na základe definovaných prístupových oprávnení, čo garantuje automatické priradenie konkrétnych podmienok na reakciu a vyriešenie SOC tímom, prípadne VJ CSIRT. V prípade, že vznik incidentu bude možné očakávať aj v iných OVM, EWS bude pomocou implementovaných procesov OVM informovať a umožní incidentu predísť (včasné varovanie).

1. **Distribúcia indikátorov možnej kompromitácie (Indicators of Compromise – IoC)**

Indikátory kompromitácie pomáhajú pri včasnom odhaľovaní a predchádzaní sieťových útokov, prieniku škodlivého softvéru alebo inej škodlivej činnosti. Hľadaním indikátorov kompromitácie môžu organizácie včas identifikovať narušenie bezpečnosti a začať s nápravnými opatreniami, aby zabránili kybernetickým útokom dosiahnuť svoj konečný cieľ. Vďaka distribúcii IoC aj do všetkých OVM so zriadenými sektorovými SOC bude maximalizovaný úžitok z knižníc IoC, čo prináša aj možnosť samostatne včas odhaliť možné narušenie bezpečnosti aj bez zapojenia do centrálneho SOC riešenia.

1. **Tvorba a udržovanie Mapy hrozieb**

Threat mapa poskytuje komplexný prehľad jednotlivých taktík, techník a procedúr (TTP), ktoré môže použiť útočník a pripravuje tak vstupy pre SOC tím, ktorý na základe kritickosti TTP priorizuje tvorbu detekčných scenárov. Threat mapa a detekčné scenáre budú poskytované aj pre OVM, ktoré nebudú monitorované vládnym SOC tímom, čo im umožní zamerať sa na hrozby, ktoré sú pre daný subjekt z pohľadu útočníka najviac relevantné a tým pádom zefektívniť reakciu na incidenty.

1. **Poskytovanie Threat intelligence (TI) feedov**

Poskytovanie relevantných Threat Intelligence feedov pre SIEM riešenia a iné bezpečnostné technológie, v ktorých následne SOC tím vyvíja detekčné pravidlá obohatené o kontext z TI.

1. **Monitoring digitálnej stopy pre jednotlivé OVM**

Monitorovanie internetu a alertovanie v prípade detekcie citlivých informácií. Príkladom môže byť monitoring internetových stránok, darknetu alebo falošných účtov sociálnych médií, ktoré sa snažia impersonifikovať zamestnancov, nadväzovať kontakty a následne využívať techniky sociálneho inžinierstva. Detekcia škodlivých URL, ktoré sú publikované na profiloch sociálnych sietí jednotlivých OVM. Útoky, ktoré pomáha monitoring digitálnej stopy odhaliť, môžu predstavovať napr. phishing, kompromitácia prihlasovacích údajov, únik citlivých dát, typosquatting atď.

1. **Impersonifikovanie VIP zamestnancov jednotlivých OVM**

Monitoring falošných profilov a účtov VIP zamestnancov, ktoré môžu byť použité na rôzne techniky zneužívané útočníkmi.

1. **Monitoring relevantných uniknutých dát**

Monitoring uniknutých dát, ktoré sa týkajú interných IT prostriedkov - hostnames, užívateľské účty, názvy IT komponentov. Na základe detegovaných dát môže následne bezpečnostné dohľadové centrum v spolupráci s CSIRT tímom okamžite vykonať nápravné opatrenia.

1. **Pravidelné reporty na základe zdrojov z Threat Intelligence platformy**

Príprava a distribúcia reportov týkajúcich sa prehľadu o útočníkoch, ich motivácii a cieľoch. Reporty budú koncipované na manažérskej aj technologickej úrovni. Manažment môže vďaka TI reportu presnejšie zamerať svoje aktivity, projekty a re-prioritizovať nasadzovanie jednotlivých technológií, procesov alebo opatrení.

1. **Knižnica informácií o útočníkoch**

Poskytovanie relevantných informácií o útočníkoch a ich akciách v minulosti, vrátane ich spôsobu výkonu útoku (modus operandi).

1. **Služba upozornenia na zraniteľnosti**

Služba upozornenia na zraniteľnosti informuje organizáciu zapojenú do EWS o najnovších hrozbách a zraniteľnostiach. Organizácia môže identifikovať zraniteľné technológie, ktoré používa, čo umožňuje výstražnému systému, aby proaktívne informoval o nových zraniteľnostiach špecifických pre infraštruktúru organizácie a adresoval kritické zraniteľnosti spustením dedikovaného procesu, ktorý slúži na okamžitú nápravu kritických zraniteľností.

1. **Zber, analýza a dodávanie Techník, taktík a procedúr (TTP)**

Príprava relevantných TTPs, ktoré sú používané veľkými hackerskými skupinami alebo tzv. APT skupinami a následná distribúcia pre pripravovaný Red Team. Red teaming prestavuje samostatnú službu, ktorá preverí pripravenosť organizácie na reálne hackerské útoky. Službu bude možné poskytovať až po úspešnej implementácii a ladení bezpečnostných nástrojov.

1. **Komunikácia bezpečnostného povedomia na OVM**

Komunikácia bezpečnostného povedomia na OVM zapojených do EWS na základe existujúcich incidentov a prebiehajúcich kampaní. O cielenú útočnú kampaň ide vtedy, keď aktér hrozby aktívne a dôsledne cieli na kompromitáciu organizácie. Aktér hrozby je koordinovaný a cieľavedomý vo svojom útoku proti organizácii. Spoločnosť zasiahnutá cielenou útočnou kampaňou by mohla utrpieť neúnosné finančné straty a poškodenie reputácie. Zvýšené povedomie o cielenej útočnej kampani môže minimalizovať riziko a dopad pre organizáciu.

1. **Poskytnutie podpory ostatným zložkám subjektu pri riešení vzniknutých bezpečnostných incidentov**

V prípade, že dané OVM nemá dostatočné kapability pre riešenie bezpečnostného incidentu, VJ CSIRT môže pomôcť s koordináciou priradením vhodných expertov z konkrétnych oblastí (pre OVM vo svojej konštituencii už danú službu VJ CSIRT poskytuje). OVM bude mať prehľad o reakčnej dobe podľa jednotlivých úrovní kritickosti.

1. **Manažment technológií**

EWS bude centrálne zabezpečovať obstaranie a prevádzku technológií potrebných pre prevádzku uvedených funkcií. Prevádzka bude garantovaná internými ľudskými zdrojmi s potrebnými support zmluvami zo strany dodávateľov a výrobcov jednotlivých technológii.

1. **Prevádzka platformy na ohlasovanie bezpečnostných incidentov**

Nahlasovanie incidentov OVM cez Service Desk a komunikácia ohľadom incidentov s OVM. Riešenie bude umožňovať OVM nahlasovať reálne alebo potenciálne bezpečnostné incidenty a zároveň komunikovať s úradmi ohľadom priebehu riešenia týchto incidentov.

1. **Vyhodnocovanie podaných a automaticky generovaných hlásení**

Vyhodnocovanie eskalovaných bezpečnostných incidentov cez prevádzkovanú platformu.

1. **Informovanie o bezpečnostných incidentoch**

Distribúciu relevantných informácií o bezpečnostných incidentoch zložkám subjektu a ďalším spolupracujúcim subjektom. Informované subjekty môžu informácie využiť v technologickej rovine na identifikáciu opatrení, ktoré zabránia vzniku incidentu v OVM, ale aj pri manažérskych rozhodnutiach, kde môžu informácie slúžiť na prevenciu proti hrozbám typu insider threat, únik citlivých informácií, atď.

1. **Koordinácia opatrení pre OVM**

EWS odporučí a v prípade potreby môže koordinovať realizáciu a zdieľanie proaktívnych opatrení zameraných na zníženie rizika hrozieb ako aj reaktívnych opatrení pri výskyte incidentov.

**Základné aplikačné/technologické komponenty modulu EWS**

Vyššie uvedené funkcie EWS budú garantované technologickými prostriedkami, ktoré budú prevádzkované pod správou EWS v úzkej spolupráci s Vládnym SOC.

1. Threat Intelligence platforma
2. MISP – Malware Information Sharing Platform & Threat Sharing

Nepriamo budú využité aj ďalšie komponenty:

1. SOAR
2. ServiceDesk

## Modul 2 - Vládny SOC

Cieľom plánovaného riešenia je dobudovať také komponenty **Vládneho SOC**, ktoré sa budú zameriavať predovšetkým na nástroje, technológie a spôsobilosti, ktoré pomáhajú bezpečnostným expertom monitorovať, analyzovať, reagovať na bezpečnostné incidenty a posielať relevantné údaje do systému včasného varovania. Vládny SOC bude technologicky, procesne a personálne integrovaný s EWS. Budovanie modulu Vládny SOC nadväzuje na už existujúce riešenie. To predstavuje spoločné pracovisko SOC prevádzkované špecialistami NASES a VJ CSIRT (podrobnejší opis v kapitole 4). Navrhované riešenie počíta s rozširovaním aktuálneho riešenia a to v dvoch fázach v závislosti od základných funkcií a služieb SOC až po veľmi pokročilé funkcie, ktoré nie sú predmetom predloženého projektu a do úvahy pripadajú až po úspešnej implementácii prvotnej fázy. V nasledujúcej časti sú špecifikované funkcie obsiahnuté v danej fáze budovania SOC aj s predpokladanou veľkosťou jednotlivých tímov, ktoré sú obsadené internými odbornými kapacitami NASES a VJ CSIRT.

### Fáza 1

Fáza predstavuje postupnú implementáciu kľúčových technológií, procesov a obsadzovanie rolí potrebných pre rozširovanie kapacít a služieb Vládneho SOC, ktoré budú pre monitorované subjekty poskytované jednotným prístupom z dôvodu zachovania rovnakých bezpečnostných štandardov. Implementácia jednotlivých technológií môže prebiehať paralelne. Podobný prístup platí aj pre obsadzovanie rolí, kde sa nepredpokladá zavedenie všetkých tímov od začiatku projektu, ale budú budované a obsadzované postupne. Jednotlivé roly môžu byť po dobu projektu obsadzované externými spolupracovníkmi a postupne internalizované. Tento prístup zabráni komplikovanému procesu najímania interných zamestnancov, kde môže dôjsť k dlhým posunom z dôvodu nízkej saturácie trhu, ale aj vysokej špecifickosti rolí. Jednotlivé tímy obsahujú roly, ktoré budú pripravovať, vykonávať a dodávať služby poskytované vládnym SOC-om a sú rozdelené podľa zaužívanej praxe pre prevádzku obdobných bezpečnostných tímov.

* Ľudské zdroje

V nasledujúcej tabuľke sú uvedené roly špecialistov pre SOC a stručný opis ich základných činností

|  |  |
| --- | --- |
| **Funkcia** | **Popis činností** |
| Onboarding tím | Centrálny tím, ktorý zabezpečuje integráciu zdrojov logov z jednotlivých OVM čerpajúcich služby Vládneho SOC. Nastavenie integrácie, normalizácie a parsovania logov (syntaktická analýza textu) z jednotlivých OVM podľa definovaného zoznamu „povinných logov“. Tím je zodpovedný za doručenie logov do SIEM-u a korektné nastavenie zdrojov logovania. |
| Analytici L1, L2 | Tím analytikov L1 kontroluje výstrahy/udalosti a prideľuje im relevantnosť a naliehavosť (triáž zaznamenaných udalostí a incidentov). Spravuje tickety pre výstrahy, ktoré signalizujú incident a vyžadujú kontrolu úrovne 2 a reakciu na incident. Tím analytikov L2 vyhodnocuje eskalované tickety eskalované analytikmi úrovne L1. Využíva informácie o vznikajúcich hrozbách na identifikáciu postihnutých systémov a rozsahu útoku. Vykonáva reakciu na detegované udalosti. Kontroluje a zhromažďuje údaje o aktívach v týchto systémoch na účely ďalšieho vyšetrovania a riadi činnosti pre nápravu funkčností. |
| SOC špecialista: Use case manažment tím | Use case manažment tím zodpovedá za vývoj a doručenie detekčných scenárov podľa definovanej Threat mapy. Testuje a nasadzuje detekčné scenáre do produkčného prostredia SIEM. Spolupracuje s Onboarding tímom a definuje, ktoré logy/eventy sú potrebné pre dostatočné pokrytie definovaných hrozieb v Threat mape. Spolupracuje s analytikmi na zlepšovaní kvality používaných detekčných scenárov – whitelisting, false positive reduction, zmena tresholdov, atď. |
| SOC špecialista: Threat Intelligence tím | Threat Intelligence tím spravuje dostupné zdroje údajov spravodajských informácií o hrozbách, overuje ich relevantnosť a zabezpečuje správu Threat Intelligence platformy a platformy MISP. Vyhľadáva a identifikuje skryté hrozby pomocou najnovších informácií o hrozbách. |
| Tím reakcie na incidenty | Tím reakcie na incidenty zabezpečuje vyšetrovanie incidentov a v spolupráci s analytikmi vytvára a rozvíja procesy a postupy SOC. Riadi riešenie kritických incidentov a je zodpovedný za nepretržité aktívne vyhľadávanie hrozieb. Tím riadi proces reakcie na identifikovaný incident, ktorý zahŕňa identifikáciu útoku, pochopenie jeho závažnosti a stanovenie priorít, vyšetrenie a zmiernenie útoku, obnovenie operácií a prijatie opatrení, aby sa incident neopakoval. |
| Manažment zraniteľností | Úlohou tímu je analyzovať aktuálny stav manažmentu zraniteľností v rámci jednotlivých OVM. Pripravuje hodnotenie pravdepodobnosti zneužitia zraniteľnosti. Integruje výsledky skenov do SIEM-u a poskytuje výsledky pre Threat Intelligence tím. Odporúča pre OVM nápravné opatrenia na odstraňovanie zraniteľností. Overuje odstraňovanie zraniteľností. |
| Platform support tím | Tím pre technickú a technologickú podporu, ktorý ma na starosti chod, údržbu a aktualizáciu nástrojov a systémov. Pripravuje dokumentáciu, ktorú môžu potrebovať iní členovia tímu. Vytvára riešenia a nástroje, ktoré pomáhajú organizáciám riešiť prerušenie prevádzky. |

Tabuľka č. 1 Odhadované ľudské zdroje pre Vládny SOC

* Základné nástroje vládneho SOC a ich vlastnosti

Nasledujúce nástroje sú základným prvkom budovania bezpečnostného monitoringu v prostredí verejnej správy. V časti popis je uvedené zhrnutie ich najvýznamnejších vlastností. Nie všetky z nižšie uvedených nástrojov bude potrebné v navrhovanom riešení implementovať, vzhľadom na skutočnosť, že niektoré nástroje sú už v súčasnom stave implementované.

|  |  |
| --- | --- |
| **Nástroj** | **Opis** |
| Centrálne riešenie správy bezpečnostných informácií a udalostí (SIEM) - implementované | Poskytuje monitorovanie, analýzu a výstrahy udalostí v reálnom čase. Komponenty SIEM môžu zahŕňať agregáciu údajov, spravodajstvo o hrozbách, koreláciu, strojové učenie, výstrahy, ovládacie panely, súlad, uchovávanie údajov a forenzné funkcie. Aktuálna forma licencovania umožňuje škálovanie nástroja s ohľadom na postupné pripájanie nových užívateľov – OVM. Nástroj je aktuálne implementovaný a integrovaný s riešením SOAR. K nástroju sú v rámci súčasných licenčných podmienok dostupné dostatočné kapacity pre monitoring (s výnimkou HW kapacít) a aj ďalšie virtuálne kolektory a procesory potrebné pre zber a spracovanie logov na nových organizáciách. |
| Bezpečnostná organizácia, automatizácia a odozva (SOAR) - implementované | Technológie, ktoré organizáciám umožňujú zhromažďovať vstupy monitorované tímom bezpečnostných operácií. Napríklad výstrahy zo systému SIEM a iných bezpečnostných technológií – kde je možné vykonávať analýzu a triedenie incidentov využitím kombinácie ľudskej a strojovej sily – pomáhajú definovať, uprednostňovať a riadiť štandardizované aktivity reakcie na incidenty. Nástroje SOAR umožňujú organizácii definovať analýzu incidentov a postupy automatickej odozvy vo formáte digitálneho pracovného toku. Automatizácia eskalovaných incidentov zo strany SOC predstavuje esenciálny prvok pre schopnosť SOC efektívne reagovať na množstvo detekovaných bezpečnostných incidentov. SOAR platforma umožňuje definovaním workflow zrýchlenie reakcie a prináša časový priestor pre bezpečnostných analytikov zameriavať sa na pokročilé incidenty, ktoré vyžadujú rozsiahlu analýzu. |
| Bezpečnostný nástroj 1 |  |
| Bezpečnostný nástroj 2 |  |
| Bezpečnostný nástroj 3 |  |
| Integrovanie technológií do centrálneho riešenia SIEM | Integrovanie jednotlivých technológií vo forme logov, ktoré sú nevyhnutné pre poskytnutie viditeľnosti v procese detekcie, incident response a iných SOC procesov (napr. forenzná analýza). Zdroje logov poskytujú možnosť korelácie pre tvorbu detekčných scenárov. Kvalita SOC služieb je závislá na integrovaní vhodných technológií-logov. Integrácia je definovaná podľa priorít a následne bude každá technológia pripojená podľa definovaného projektového plánu. Pre všetky monitorované OVM sú stanovené rovnaké minimálne zdroje logov (tzv. mandatory logsources) integrované do SIEM |
| Bezpečnostný nástroj 4 |  |
| Forenzná analýza | Jednotka CSIRT už aktuálne disponuje nástrojmi a špecialistami pre vykonávanie forenzných úkonov, ktoré sú nevyhnutné pre prípad vyšetrovania incidentu a identifikovania vykonaných akcií útočníka. Forenzný a Malvér analytický tím VJ CSIRT bude automaticky dodávať služby L3 v rámci Vládneho SOC. |

Tabuľka č. 2 Navrhované nástroje vládneho SOC-u a ich opis

### Fáza 2 – plánované kapability nezaradené do projektu

* Purple teaming – spoločná aktivita Red team | Blue team (SOC) a OVM – úzko spolupracujú s cieľom zlepšiť schopnosti tímov prostredníctvom kontinuálnej spätnej väzby a prenosu znalostí.
* Analýza a vyšetrovanie incidentov – forenzné skúmanie s cieľom určiť zdroj incidentu alebo hrozby a rozsah, v akom útočníci infiltrovali a ovplyvnili informačné systémy. V tomto prípade sa jedná o implementáciu najmodernejších nástrojov s podporou AI, inovovanie postupov a metód vyšetrovania incidentov k už existujúcim nástrojom a postupom.
* Obnova a náprava – získanie stratených alebo ukradnutých údajov a preskúmanie toho, aké aktíva boli ohrozené, ako aj riešenie slabých miest a úprava nástrojov a postupov na monitorovanie a upozorňovanie na bezpečnosť.
* Disassembler a technológie ladenia – pomáhajú tímom SOC pri spätnom inžinierstve a analýze zložitých binárnych súborov na určenie účelu hrozby, funkčnosti a schopností.
* Medziplatformové získavanie obrazov hardvéru a softvéru – zabezpečte získavanie forenzných obrazov diskov a pamäte naprieč operačnými systémami.
* Hardvér pre mobilné získavanie – získava forenzné snímky/obrazy z mobilných zariadení a vykonáva analýzu na účely vyšetrovania.
* Cloud-based Acquisition Solutions – zhromažďuje údaje zo služieb tretích strán, ako sú Amazon Web Services, Microsoft 365, Google, iCloud, Facebook, Instagram a Twitter, a vykonáva analýzu údajov.
* Možnosti vzdialeného zberu údajov – sťahovanie artefaktov, systémových informácií a forenzných obrazov na diaľku bez potreby lokálneho prístupu.
* Kontrola verejne publikovaných zdrojových kódov ISVS.

## Modul 3 - Monitorovacie nástroje na OVM

Bezpečnostný monitoring nie je možné realizovať bez vhodne zvolených technológií, ktorých úlohou je zber, analýza a vyhodnocovanie dát a následná reakcia na hrozbu. V rámci projektu budú preto nasadené a na Vládny SOC napojené **Monitorovacie nástroje na OVM**. V budúcom riešení sa plánuje implementácia rôznych bezpečnostných nástrojov, ich následná vzájomná kombinácia a integrácia s cieľom komplexnejšieho pokrytia celej IT infraštruktúry OVM a lepšej viditeľnosti. Uvedený prístup má za cieľ zvýšiť kvalitu bezpečnostného monitoringu. Nasledujúca tabuľka uvádza nástroje, ktoré budú nasadené v prostredí OVM a ďalšie nástroje, ktoré v prípade už existujúcich riešení bude možné využívať pre bezpečnostný monitoring.

|  |  |
| --- | --- |
| **Monitorovací nástroj** | **Popis** |
| Bezpečnostný nástroj 1 |  |
| Bezpečnostný nástroj 2 |  |
| Bezpečnostný nástroj 3 |  |
| Bezpečnostný nástroj 4 |  |
| **Nasledujúce nástroje budú použité pre potreby zvýšenia úrovne monitoringu len ak ich už OVM používa** | |
| Sieťové IDS/IPS | Systémy pre detekciu (prevenciu) vniknutia monitorujú sieťovú prevádzku a vykonávajú jej analýzu z hľadiska známok možných prienikov, ako sú pokusy o zneužitie a incidenty, ktoré môžu byť bezprostrednou hrozbou pre sieť. Prevencia narušenia je proces vykonávania detekcie narušenia a následného zastavenia zistených incidentov, čo sa zvyčajne vykonáva zahodením paketov alebo ukončením relácií. Tieto bezpečnostné nástroje sú dostupné ako systémy detekcie prienikov (IDS) a systémy prevencie prienikov (IPS), ktoré sú súčasťou bezpečnostných opatrení pre detekciu a zastavenie potenciálnych incidentov v sieti. |
| UEBA | Analýza správania používateľov a entít (UEBA), známa aj ako analýza správania používateľov (UBA), je proces zhromažďovania informácií o udalostiach v sieti, ktoré generujú používatelia. Po zhromaždení a analýze, sú tieto informácie použité na detekciu použitia skompromitovaných prihlasovacích údajov, bočného pohybu (lateral movement) a iného škodlivého správania. |
| DLP | Prevencia straty údajov (DLP) predstavuje technológie, ktoré vykonávajú kontrolu obsahu aj kontextovú analýzu údajov odosielaných prostredníctvom aplikácií na odosielanie správ, ako sú e-maily a okamžité správy, v pohybe po sieti, pri používaní na kontrolovanom koncovom zariadení, a v pokoji na lokálnych súborových serveroch alebo v cloudových aplikáciách a cloudových úložiskách. Tieto riešenia vykonávajú reakcie založené na politike a pravidlách definovaných tak, aby riešili riziko neúmyselného alebo náhodného úniku alebo exponovania citlivých údajov mimo autorizovaných kanálov.  Technológie DLP sú rozdelené do dvoch kategórií – Enterprise DLP a Integrated DLP. Zatiaľ čo riešenia Enterprise DLP sú komplexné a zabalené v softvéri agentov pre desktopy a servery, fyzických a virtuálnych zariadeniach na monitorovanie sietí a e-mailovej prevádzky alebo softvérových zariadeniach na zisťovanie údajov, integrované DLP je obmedzené na zabezpečené webové brány (SWG), zabezpečené e-mailové brány ( SEG), produkty na šifrovanie e-mailov, platformy na správu podnikového obsahu (ECM), nástroje na klasifikáciu údajov, nástroje na vyhľadávanie údajov a nástroje pre riadenie cloudového prístupu (CASB). |
| Web content filter / Proxy | Proxy na filtrovanie obsahu je proxy server, server fungujúci ako sprostredkovateľ medzi dvoma počítačmi, ktorý filtruje prenášaný obsah a obmedzuje prístup k nežiaducemu, zakázanému alebo nebezpečnému obsahu. Organizácie sa môžu rozhodnúť použiť proxy na filtrovanie obsahu na kontrolu toho, čo si ľudia prezerajú v ich zariadeniach. Okrem filtrovania obsahu môže proxy tiež zachytiť malvér, vírusy a iný nežiaduci softvér a odstrániť ich skôr, ako sa dostanú do siete. |
| Web Application Firewall (WAF) | WAF pomáha chrániť webové aplikácie filtrovaním a monitorovaním obsahu HTTP komunikácie medzi webovou aplikáciou a internetom. Zvyčajne chráni webové aplikácie pred útokmi, ako je cross-site forgery, cross-site-scripting (XSS), vkladanie súborov a vkladanie SQL výrazov. |
| Mobile device management (MDM) | Správa mobilných zariadení (MDM) je softvér, ktorý umožňuje IT oddeleniu organizácie automatizovať, ovládať a zabezpečovať administratívne politiky na prenosných počítačoch, smartfónoch, tabletoch alebo akomkoľvek inom zariadení pripojenom k sieti organizácie.  Správa mobilných zariadení zvyčajne nasadzuje súhrn organizačných politík a certifikátov, konfigurácií na zariadení, aplikácií, back-endového softvéru a hardvéru na správu zariadení koncových používateľov. Cieľom správy mobilných zariadení je maximalizovať podporu zariadení, organizačné funkcie a bezpečnosť. |

Tabuľka č. 3 Monitorovacie nástroje na OVM

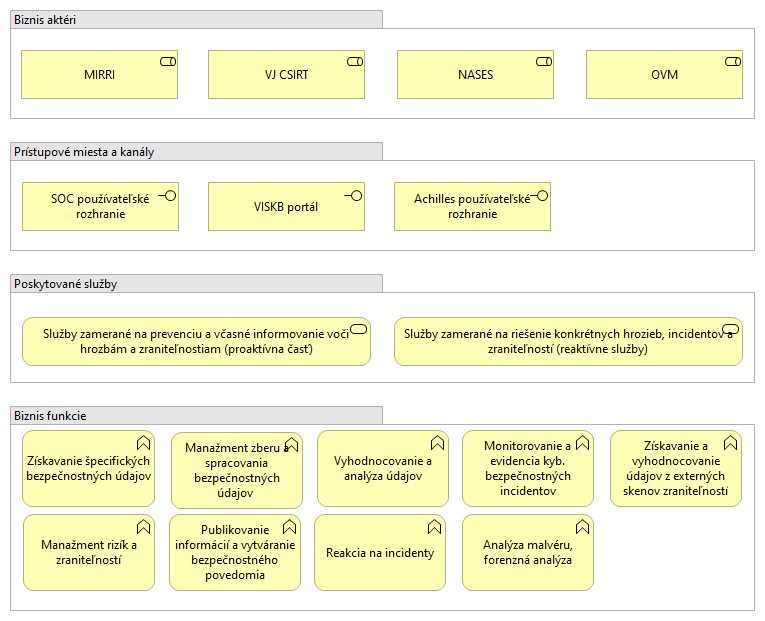
# ARCHITEKTÚRA RIEŠENIA PROJEKTU

## Biznis vrstva

### Aktuálny stav biznis architektúry

V rámci súčasného stavu biznis architektúry riešeného projektu boli identifikovaní nasledujúci biznis aktéri a ich role:

* **MIRRI** – subjekt zabezpečujúci plánovanie, riadenie, koordinovanie a zvyšovanie kybernetickej a informačnej bezpečnosti a ochranu ISVS, orgán vedenia, vykonávanie kontrol podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe (ITVS) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, overovania súladu a príprava stanovísk k zisteniam z bezpečnostných kontrol vybraných OVM;
* **VJ CSIRT (CSIRT.SK)** - vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Vykonáva oprávnenia podľa § 23 a 23a zákona č. 95/2019 Z. z. o ITVS. Spolu s NASES sa podieľa na prevádzke SOC;
* **NASES** – subjekt zabezpečujúci prevádzku siete Govnet, základných služieb a manažment údajov získavaných a spracovaných „vládnym SOC“ a vybraných IS v prostredí VS, ktoré poskytujú špecifické bezpečnostné dáta. Prevádzkuje HW a SW časť SOC;
* **OVM** – orgány verejnej moci sú prevádzkovatelia a používatelia IS v prostredí VS. Zabezpečujú manažment bezpečnostných údajov spravovaných IS, vytváranie a aktualizáciu analýzy rizík, zoznamu aktív, CMDB atď. v zmysle zákona o ITVS a zákona o KB a prislúchajúcich vyhlášok.



Obrázok 1: Biznis architektúra súčasného stavu

Jednotliví aktéri môžu pristupovať k funkciám a bezpečnostným údajom na základe definovaných právomocí prostredníctvom nasledujúcich kanálov:

* **VISKB portál** – portál zabezpečujúci nahrávanie údajov zo samostatného klientskeho modulu, zadávanie a úpravu zbieraných údajov prostredníctvom webového rozhrania pre organizácie, ktoré nemajú nasadený samostatný klientsky modul a vypĺňanie dotazníkov k bezpečnostným otázkam týkajúcich sa organizácií a ich aktív;
* **SOC používateľské rozhranie** – používateľské rozhranie bezpečnostného dohľadového centra poskytujúce manažment a analýzu získaných bezpečnostných údajov cez technológiu SIEM, SOAR a Service Desk;
* **Achilles používateľské rozhranie** – Achilles (cez svoj komponent COC) poskytuje rozhranie pre používateľa a rozhranie pre administrátora, kde sú pokročilé možnosti autorizácie a manažmentu skenerov zraniteľnosti. Používateľmi a administrátormi sú zamestnanci VJ CSIRT, ktorí realizujú skenovanie zraniteľností OVM z vonkajšieho prostredia a ich následnú validáciu.

V súčasnosti sú poskytované nasledovné služby (tieto služby sú poskytované len oprávneným subjektom a zamestnancom daných subjektov):

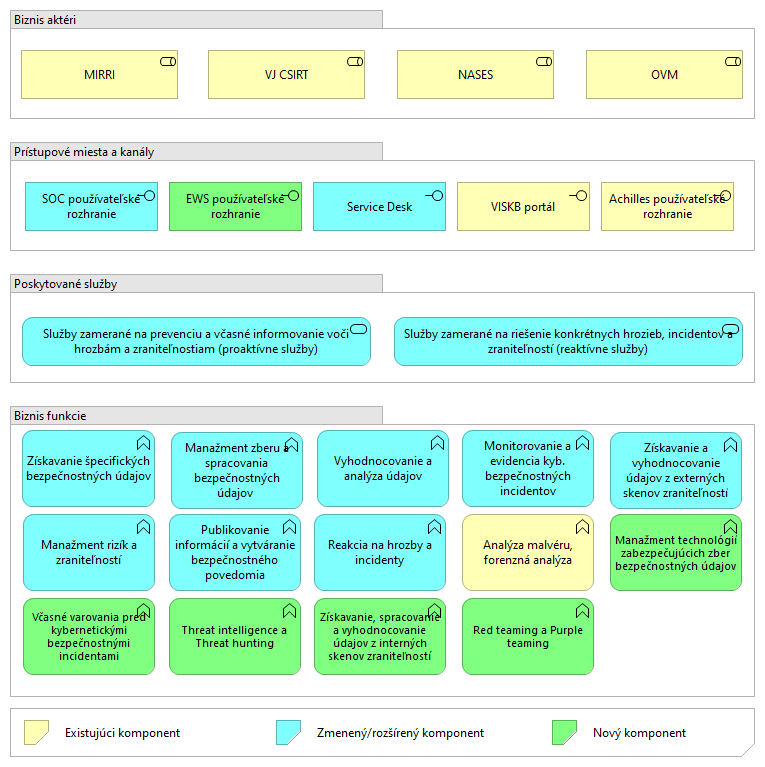
* **Služby zamerané na prevenciu a informovanie voči hrozbám a zraniteľnostiam** – služby poskytované zainteresovaným OVM s cieľom predchádzania kybernetickým bezpečnostným incidentom, ktoré sú zároveň spojené s vytváraním bezpečnostného povedomia. Služba informovania o identifikovaných zraniteľnostiach sa aktuálne realizuje formou newslettru zasielaného emailom.
* **Služby zamerané na riešenie konkrétnych hrozieb, incidentov a zraniteľností** – VJ CSIRT aktuálne poskytuje reaktívne služby na základe vyžiadania od organizácií vo svojej konštituencii. V súlade s tým automaticky vykonáva podporu pri riešení konkrétnych vzniknutých bezpečnostných incidentov, ktoré sú detegované v infraštruktúre OVM, s cieľom minimalizácie škôd a následkov. Základné služby bezpečnostného monitoringu sú v súčasnosti poskytované pre MIRRI, NASES, Govnet a niektoré OVM v obmedzenom rozsahu (monitorovaná len časť aktív).

Biznis funkcie v kontexte súčasného stavu sú nasledovné:

* **Získavanie špecifických bezpečnostných údajov** – špecifické bezpečnostné údaje sú odosielané a čiastočne centralizované, následne prebieha spracovanie a vyhodnocovanie týchto získaných údajov. V súčasnom stave sú získavané rôzne údaje organizácií ako napr. informácie o aktívach organizácie, evidencie bezpečnostných a iných auditov, údaje o kybernetických incidentoch (napr. systémom VISKB);
* **Manažment zberu a spracovania bezpečnostných údajov** – zber, evidencia a spracovanie bezpečnostných údajov získavaných monitorovacími nástrojmi na základe rôzne definovaných parametrov a konfigurácií (realizuje sa v prostredí MIRRI, NASES a u vybraných OVM v obmedzenom rozsahu;
* **Vyhodnocovanie a analýza údajov** – bezpečnostné údaje, ktoré sú zozbierané sú ďalej analyzované. vyhodnocované a klasifikované na základe definovaných kritérií a metrík, avšak častokrát nie sú využívane sofistikované metódy na identifikáciu pokročilejších bezpečnostných hrozieb a zraniteľnosti. Údaje sú vyhodnocované manuálne, automatizovane, resp. kombináciou týchto dvoch prístupov;
* **Monitorovanie a evidencia kybernetických bezpečnostných incidentov** – monitorovanie informácií o aktivitách na koncových zariadeniach a v sieťovej prevádzke s cieľom identifikácie potencionálnych hrozieb a evidencia prípadných vzniknutých bezpečnostných incidentov. V súčasnom stave prebieha monitorovanie len prostredia MIRRI, NASES a na vybraných OVM v obmedzenom rozsahu (monitorovaná len časť aktív);
* **Získavanie, spracovanie a vyhodnocovanie údajov z externých skenov zraniteľností** – komplexné externé skenovanie zraniteľnosti systémom Achilles na základe rôznych parametrov (frekvencia, typ vyhľadávaných zraniteľnosti atď.) a spracovanie týchto údajov do požadovanej formy. V súčasnom stave sa realizuje overovanie zraniteľností dostupných zo siete internet na množine OVM (cca. 150 subjektov). Vyhodnocovanie a validácia získaných údajov prebieha na základe rôzne definovaných parametrov s cieľom identifikácie hrozieb a zraniteľnosti zo získaných údajov. V súčasnom stave vyhodnocovanie údajov prebieha manuálne a v nedostatočnej miere;
* **Manažment rizík a zraniteľností** – evidencia rizík a zdieľanie informácií o zistených rizikách a zraniteľnostiach. V súčasnom stave táto agenda prebieha decentralizovane a bez podpory nástrojov threat intelligence a ďalších zdrojov;
* **Publikovanie informácií a vytváranie bezpečnostného povedomia** – v súčasnom stave publikovanie informácií prebieha v obmedzenom režime na webe csirt.gov.sk. Primárne sa jedná o publikovanie informácií o kritických zraniteľnostiach;
* **Reakcia na hrozby a incidenty –** VJ CSIRT aktuálne poskytuje len služby incident response a incident handling na základe vyžiadania zo strany OVM spadajúceho do konštituencie VJ CSIRT. Reakcia na incident nie je automatizovaná a reakčný čas nereflektuje súčasné požiadavky;
* **Analýza malvéru a forenzná analýza –** v aktuálnom stave je VJ CSIRT plne vybavená po technickej a personálnej stránke na realizáciu špecifických činností slúžiacich na identifikáciu typu, funkcionalít a chovania malvéru, vyhodnocovanie možných detekčných mechanizmov alebo identifikáciu možnosti narušiť chod škodlivého kódu. V prípade forenznej analýzy sú poskytované činnosti získavania digitálnych stôp so zachovaním chain of custody, analýzy digitálnych stôp a vypracovanie správ, reportov a posudkov.

### Budúci stav Biznis architektúry

Biznis architektúra budúceho stavu reflektuje zámer projektu, ktorým je posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov. Na úrovni biznis aktérov v budúcom stave nedochádza k zmenám. Z pohľadu prístupových miest a kanálov realizáciou projektu dôjde k zmenám a doplneniu funkcionalít používateľského rozhrania pre SOC, pričom vzniknú nové prístupové miesta pre lokálnych bezpečnostných špecialistov na OVM zapojených do monitoringu. Zároveň vznikne novo-vybudované používateľské rozhranie pre EWS a Service Desk. V prípade Service Desk sa nejedná o vývoj nového komponentu. Už dnes slúži prioritne na nahlasovanie prevádzkových incidentov pre organizácie využívajúce služby vládnej siete Govnet. Do Service Desk tak pribudne ďalšia funkcionalita na nahlasovanie kybernetických bezpečnostných incidentov a bude sprístupnená pre osoby zodpovedajúce za kybernetickú bezpečnosť na OVM zapojené do bezpečnostného monitoringu.



Obrázok 2: Biznis architektúra budúceho stavu

Zásadné zmeny v rámci navrhovaného projektu a riešenia sa dotknú nasledovných biznis funkcií:

* **Získavanie špecifických bezpečnostných údajov** – získavanie bezpečnostných údajov bude v budúcom stave rozšírené o nové zdroje dát, ktoré budú poskytovať vyššiu mieru tzv. viditeľnosti do prostredia monitorovaných OVM a s tým spojený väčší rozsah bezpečnostných údajov, ktoré budú môcť byť detailne analyzované a vyhodnocované. Z dôvodu nastavenia a implementácie jednotných štandardov na kvalitu a rozsah bezpečnostného monitoringu bude stanovený minimálny rozsah zdrojov logov, ktoré bude musieť monitorovaný subjekt posielať do centrálneho riešenia monitoringu.
* **Manažment zberu a spracovanie bezpečnostných údajov** – bezpečnostné údaje budú zbierané na základe definovaných kritérií a spracované do požadovaného formátu na základe sofistikovaných metód s cieľom zavádzania čo najvyššej miery automatizácie v oblasti včasnej identifikácie potencionálnych hrozieb, resp. útokov.
* **Vyhodnocovanie a analýza údajov** – centralizované vyhodnocovanie a analýza údajov získaných z viacerých zdrojov s cieľom identifikácie potencionálnych zraniteľností, resp. hrozieb. Vyhodnocovanie a analýza budú vykonávané najmodernejšími technológiami využívajúce napríklad prvky strojového učenia a umelej inteligencie za účelom, korelácie rôznych dát, presnejšej detekcie s minimalizáciou tzv. false positive ratio, teda podielu falošne pozitívnych výsledkov, ktoré majú negatívne dopady na efektívnosť práce analytikov a ďalších špecialistov na SOC a monitorovaných OVM.
* **Monitorovanie a evidencia kybernetických bezpečnostných incidentov** – monitorovanie, evidencia a zdokumentovanie bezpečnostných incidentov, ktoré vznikli v minulosti s cieľom predchádzania podobných incidentov v budúcnosti v súlade s klasifikáciou TTPs.
* **Získavanie a vyhodnocovanie údajov získaných z externých skenov zraniteľností** – integrácia výstupov z externých skenov monitorovaných OVM realizovaných prostredníctvom systému Achilles do platformy SOAR pre OVM zapojené do EWS.
* **Manažment rizík a zraniteľností** – manažment rizík a zraniteľností bude realizovaný kombináciou výsledkov interných a externých skenov v súlade s vyhodnocovaním na základe CVE (Common Vulnerabilities and Exposures) framework cez SOAR, kde budú zraniteľnosti evidované a kontinuálne sledovaný stav riešenia identifikovaných rizík a zraniteľností na monitorovaných OVM.
* **Publikovanie informácií a vytváranie bezpečnostného povedomia** - údaje budú zdieľané a publikované viacerými spôsobmi. Jednu kategóriu predstavujú zdieľané údaje z OVM a tvorba reportov, ktoré budú zapojené do systému včasného varovania. Druhou kategóriou je publikovanie verejne dostupných informácií na webstránke VJ CSIRT a/alebo do centrálneho portálu KB na základe definovaného formátu a štruktúry, ktorý bude vytvorený v rámci Reformy č. 4: Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (ITVS).
* **Reakcia na hrozby a incidenty** – rozšírenie funkcií v budúcom stave umožní pomocou najmodernejších technológií vykonávať rýchle reakcie na detegované hrozby a incidenty. Riešenie umožní vykonávať automatizovaný aj manuálny výkon reakcie SOC špecialistom (alebo aj interným bezpečnostným tímom) v reálnom čase za účelom minimalizovať dopady a následky kybernetických incidentov. Okrem reakcie nástroje umožnia aj spätné vyšetrovanie a popísanie priebehu incidentu.

Realizáciou projektu vzniknú tieto nové biznis funkcie:

* **Manažment technológií zabezpečujúcich zber bezpečnostných údajov** – implementáciou nového riešenia sa umožní centrálny manažment technológií (bezpečnostných nástrojov) používaných na zabezpečenie monitoringu na jednotlivých OVM, ktoré bude spravovať SOC, čo prispeje k zabezpečeniu rovnakých štandardov a postupov pri nastavovaní politík, ladení a správe týchto nástrojov.
* **Včasné varovanie pred kybernetickými bezpečnostnými incidentami** – rozšírené zdroje údajov a ich automatizované spracovanie a vyhodnocovanie umožní generovať včasné varovania pre OVM zapojené do EWS na základe detailnej dátovej analýzy získaných dát z koncových zariadení, siete, manažmentu zraniteľností a ďalších spravodajských údajov.
* **Threat intelligence a Threat hunting** – v budúcom riešení vznikne platforma integrujúca viacero zdrojov spravodajských údajov. Riešenie je navrhnuté tak, aby zhromažďovalo, agregovalo a organizovalo informácie o hrozbách z viacerých zdrojov a formátov. Platforma Threat intelligence umožní prostredníctvom EWS jednoducho zdieľať údaje o hrozbách s ostatnými OVM a bezpečnostnými dohľadovými centrami. Nové funkcionality budú zabezpečovať monitorovanie uniknutých dát OVM zapojených do EWS, vytváranie prehľadov hrozieb, distribúciu indikátory kompromitácie (IoC) do monitorovacích systémov, vytvárať hypotézy a realizovať threat hunting, teda proces proaktívneho a opakovaného prehľadávania záznamov s cieľom odhaliť a izolovať pokročilé hrozby, ktoré neboli identifikované existujúcimi bezpečnostnými riešeniami.
* **Získavanie, spracovanie a vyhodnocovanie údajov zo skenov zraniteľností** – navrhovaným riešením vznikne nová biznis funkcia v podobe možnosti získavania, spracovania a vyhodnocovania dát z interných skenov zraniteľností monitorovaných OVM. Tým sa doplnia údaje systému Achilles, ktorý už v súčasnosti skenuje a analyzuje zraniteľnosti na úrovni verejných IP adries. V prípade veľkého množstva identifikovaných kritických položiek je kľúčovou funkciou pre faktické odstránenie zraniteľností prioritizácia, ktorá zohľadňuje aj ďalšie dôležité parametre než len CVSS. Predovšetkým poskytuje aktuálne informácie z Threat Intelligence, informácie o možnosti zneužitia a definuje jej náročnosť alebo spresňuje typ zraniteľného systému.
* **Red teaming a Purple teaming** – nové bezpečnostné nástroje v budúcom riešení vytvoria predpoklad pre vykonávania Red teamimg-u, ktorý využíva známe taktiky, techniky a procedúry (TTP) na simuláciu reálnych kybernetických hrozieb na základe bezpečnostného profilu OVM. Cieľom Red teamu je okrem overenia úrovne kybernetickej bezpečnosti organizácie pomôcť obrannému tímu organizácie detegovať kybernetický útok a reagovať naň. Zámerom je simulovať realistický útok na organizáciu, ktorý je založený na relevantných hrozbách a TTP pre organizáciu. Pri tejto simulácií je cieľom taktiež preveriť bezpečnostné opatrenia, technológie, procesy, bezpečnostný tím organizácie a identifikovať možné nedostatky. Red teaming sa obyčajne vykonáva bez znalosti bezpečnostného tímu organizácie s výnimkou vybraných zamestnancov.

Predstaveným projektom a navrhnutým riešením sa zároveň zásadne rozširujú poskytované služby v oblasti kybernetickej bezpečnosti. Projektom sa priamo vytvoria podmienky pre poskytovanie nových proaktívnych služieb a zvýšenie kvality a dostupnosti tzv. reaktívnych služieb, teda služieb zameraných na riešenie konkrétnych hrozieb, incidentov a identifikovaných zraniteľností. Zoznam služieb systému včasného varovania (EWS) a bezpečnostného dohľadového centra rozdelené na proaktívnu a reaktívnu časť sú zosumarizované v Projektovom zámere.

## Aplikačná vrstva

### Aktuálny stav aplikačnej architektúry

Súčasný stav aplikačnej architektúry pozostáva z dvoch hlavných komponentov, ktoré sa rozvíjali ako nezávislé. Prvým komponentom je bezpečnostné dohľadové centrum (SOC), ktoré spoločne prevádzkuje NASES a VJ CSIRT. Pre svoju činnosť a poskytovanie služieb je pre SOC nevyhnutné použitie viacerých nástrojov, ktoré predstavujú preexistentný obchodne dostupný softvér. Pracovisko poskytuje služby bezpečnostného monitoringu prioritne pre svoje potreby, čiže pre infraštruktúru NASES so sieťou Govnet a prostredie MIRRI SR. Služby v obmedzenom režime a rozsahu sú poskytované aj pre ďalšie vybrané OVM. Tomu zodpovedá aj aktuálna aplikačná architektúra SOC, ktorá pozostáva z nasledujúcich nástrojov:

1. Centrálne nasadené na SOC:
   1. **SIEM (Centrálne riešenie správy bezpečnostných informácií a udalostí)** – riešenie disponuje dostatočnou licenciou pre škálovanie a jeho využitie pre zabezpečenia monitorovania ďalších OVM. Do SIEM sú integrované len vybrané logy z niektorých technológií;
   2. **SOAR (Bezpečnostná organizácia, automatizácia a odozva)**;
2. Monitorovacie nástroje:
   1. **Bezpečnostný nástroj 1** – nasadené len v prostredí NASES a MIRRI
   2. **Bezpečnostný nástroj 2** – nasadené len v určitých častiach infraštruktúry a len niektorých z vybraných OVM
   3. **SIEM kolektory** – zber a parsovanie logov z vybraných systémov a endpointov

Súčasťou SOC sú aj aplikácie používané pre potreby služieb L3, ktoré poskytuje VJ CSIRT. Jedná sa o súbor nástrojov a aplikácií v rámci malware a forenzného laboratória VJ CSIRT, ako napr. sandbox, virtualizačná platforma, software na správu imageov, analyzačný software (dokumenty, spustiteľne súbory, atď.), dekompilačné nástroje, debuggeri, nastroj na monitorovanie prevádzky v malware labe, software na akvizíciu a extrakciu dát a vytváranie kópií, software na mobilnú analýzu, software na analýzu dátových úložísk a pamäťových médií, alebo software na analýzu sieťovej prevádzky.

Druhým komponentom je systém Achilles, ktorého hlavný riadiaci komponent bol vyvinutý výlučne internými kapacitami VJ CSIRT, vrátane integrácie využívaných systémov a slúži na vyhľadávanie zraniteľných miest a proaktívne odhaľovanie zraniteľností u viac než 150 orgánov verejnej správy. Vďaka systému Achilles prebieha pravidelné skenovanie systémov spravidla na mesačnej báze, vedie sa automatická štatistika odhalených zraniteľností s komplexným prehľadom o ich časovom výskyte a ich odstraňovaní. Systém **Achilles** v súčasnosti pozostáva z viacerých SW komponentov a je prevádzkovaný on-premise v rámci serverovej infraštruktúry VJ CSIRT na virtuálnych strojoch a skladá sa z nasledujúcich častí:

* **Cyber Operation Center (COC)** - Riadiaci komponent prostredia a systému Achilles, ktorý bol vyvinutá v rámci VJ CSIRT R&D (Research and Development);
* **Skener zraniteľností** – v súčasnosti je ako hlavný skener využívaný Nessus - skener zraniteľností systémov a aplikácií;
* **Security Incident Response Platform (SIRP)** – tiketovací systém a zároveň systém na riešenie incidentov a bezpečnostných prípadov, ktoré si vyžadujú analytickú časť, v súčasnosti zabezpečený pomocou platformy TheHive, ktorá umožňuje korelovať incident s proaktívnou časťou systému Achilles, a teda prinášať dôležité informácie pri riešení incidentov. Prináša výborné výsledky pri riešení viacerých verejných či neverejných incidentov. Táto korelácia je možná na základe vytvorenej vlastnej taxonómie pozostávajúcej z názvov organizácií v konštituencii. Na tejto platforme boli vyvinuté aj vlastné Cortex respondery umožňujúce integráciu s COC;
* **Databázový komponent** – použitý je open-source nástroj Elasticsearch, ktorý ukladá záznamy o zraniteľnostiach vo forme logových záznamov. V súčasnosti sú logy normalizované v COC aplikácii a software Logstash momentálne na normalizáciu logov nie je využívaný;
* **Vizualizačný komponent** – použitý je open-source nástroj Kibana, v ktorom prebiehajú pokročilé dátové a analytické vizualizácie. Zahŕňa niekoľko tzv. dashboardov, v ktorých je viditeľný najmä vývoj zraniteľností za ľubovoľné časové pásmo, vývoj opravených zraniteľností, najčastejšie zraniteľnosti a ich kategórie, zraniteľnosti s dostupným exploitom v relácii s rizikovým faktorom zraniteľností, organizácie s najviac zraniteľnosťami, služby a otvorené porty daných IP adries a ďalšie;
* Zoznam skenovaných subjektov, ktorý pozostáva z údajov vo Vládnom informačnom systéme kybernetickej bezpečnosti (VISKB). Obsahuje subjekty patriace do konštituencie VJ CSIRT a konkrétne ich IP adresy, prípadne celé adresné rozsahy a domény.

Aktuálne je naplánovaný ďalší rozvoj systému Achilles. Ten však nie je predmetom predloženého projektu. Rozvoj je nutný za účelom navýšenia kapacít pre možnosť skenovania vyššieho počtu inštitúcii (cieľ 500 do roku 2026), zvýšenia kvality validácie výsledkov a vyššej miery automatizácie.

N/A

Obrázok 3: Aplikačná architektúra súčasného stavu

### Budúci stav aplikačnej architektúry

V budúcom stave, vďaka realizácii tejto investície, dôjde z pohľadu aplikačnej architektúry k viacerým zmenám. Vznikne nový komponent Systém včasného varovania (EWS) a zároveň dôjde k úpravám, resp. doplneniu funkcionalít už existujúceho komponentu bezpečnostného dohľadového centra (SOC) a rozšírenie integrácií s cieľom centralizovaného zberu, vyhodnocovaniu údajov z relevantných zdrojov a rýchlej reakcie.

N/A

Obrázok 4: Aplikačná architektúra budúceho stavu

Hlavným komponentom navrhovaného budúceho riešenia bude novo-vytvorený systém **EWS**, ktorý bude na zabezpečenie kybernetickej bezpečnosti využívať pri monitoringu prevádzky pravidelne aktualizovanú databanku informácií o rizikách zloženú kombinovane z rôznych zdrojov a z vlastného výskumu alebo iných zdrojov VJ CSIRT takým spôsobom, aby poskytoval čo možno najširšie, vždy aktuálne informácie o hrozbách a skracoval priemerný čas identifikácie kybernetických bezpečnostných incidentov. EWS bude centralizovaným komponentom v oblasti kybernetickej bezpečnosti štátnych organizácií, na ktorý sa budú integrovať ďalšie systémy poskytujúce jednak metaúdaje o systémoch (VISKB) so systémom Achilles a jednak monitorované a spracované údaje z jednotlivých OVM (Vládny SOC a iné sektorové SOC-y zapojené do EWS na úrovni niektorých rezortov).

EWS bude vytvorený s možnosťou prepojenia na externé systémy, resp. systémy, ktoré nie sú pod správou VJ CSIRT/MIRRI alebo NASES:

* **Sektorové SOC (finančne podporené z výzvy Investície 6 POO)** – systémy implementované na vybraných OVM s cieľom zberu údajov o prevádzke IT systémov v reálnom čase, rozpoznávanie anomálnych aktivít, poskytnutie možnosti skorej detekcie a prípravu protiopatrení na zabezpečenie kybernetickej bezpečnosti a predchádzanie bezpečnostným incidentom;
* **JISKB** (Jednotný informačný systém kybernetickej bezpečnosti) – systém budovaný NBÚ, ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT.

Základ budúcej aplikačnej architektúry EWS tvorí Threat intelligence platforma (TIP), ktorá spolu s open-source platformou MISP zabezpečujú kľúčové biznis funkcie a služby systému včasného varovania (kapitola 3.1 – modul 1). Architektúra budúceho stavu TIP a MISP je znázornená na nasledujúcom obrázku. V prípade TIP bude EWS v pozícii tzv. MSSP (Managed Security Service Provider), v preklade poskytovateľ spravovaných bezpečnostných služieb. Integrácia uvedených aplikácií do celého prostredia EWS a Vládneho SOC je prezentovaná v high-level architektúre budúceho stavu (obrázok 5).

N/A

 Obrázok 5: Aplikačná architektúra budúceho stavu TIP a MISP

Cieľom budúceho riešenia je zásadné rozšírenie komponentu **Vládny SOC.** Z pohľadu aplikačnej architektúry sa rozšírenie bude zameriavať predovšetkým na nástroje a technológie, ktoré pomáhajú bezpečnostným expertom monitorovať, analyzovať a rýchlo reagovať na bezpečnostné incidenty a posielať relevantné údaje do systému včasného varovania. Vládny SOC bude aplikačne, technologicky, personálne a organizačne integrovaný s EWS.

Existujúce nástroje bez zásadných zmien:

* **SOAR (Bezpečnostná organizácia, automatizácia a odozva) -** technológia umožňujúca zhromažďovať vstupy monitorované tímom bezpečnostných operácií. Napríklad výstrahy zo systému SIEM a ďalších bezpečnostných nástrojov, kde je možné vykonávať analýzu a triedenie incidentov využitím kombinácie ľudskej a strojovej sily. SOAR pomáha definovať, uprednostňovať a riadiť štandardizované aktivity reakcie na incidenty. SOAR umožňuje organizácii definovať analýzu incidentov a postupy odozvy vo formáte digitálneho pracovného toku. V prípade budúceho riešenia budú nevyhnutné integrácie SOAR s ďalšími novo implementovanými bezpečnostnými nástrojmi, zadefinovanie workflow-ov a odladenie nástroja.

Existujúce nástroje s potrebou rozšírenia alebo zmien:

* **SIEM (Centrálne riešenie správy bezpečnostných informácií a udalostí)** – nástroj zabezpečuje monitorovanie, analýzu a výstrahy v reálnom čase. Aktuálne riešenie disponuje dostatočnou licenciou pre škálovanie a jeho využitie pre zabezpečenia monitorovania ďalších OVM. Rozšírenie spočíva s nutnosti rozšírenia centrálnej časti a implementácie nových kolektorov a procesorov logov na OVM, ktoré budú využívať služby bezpečnostného monitoringu. Pôjde o virtuálne appliance (podrobnejšie v technologickej architektúre). Rozšírenie SIEM zároveň spočíva v integrácii ďalších bezpečnostných nástrojov za účelom zvýšenia tzv. vizibility do monitorovanej infraštruktúry a potrebou obohacovania udalosti o údaje z externých zdrojov, čo umožňuje presnejšie vyhodnocovanie „skóre rizika“, z ktorého je možné ľahko prioritizovať kroky vedúce k vyriešeniu indikovaných hrozieb a incidentov.
* **Bezpečnostný nástroj 1 -** aktuálne je nástroj nasadený len v prostredí MIRRI a NASES. Zmena vyplýva z obstarania a nasadenia nového jednotného nástroja, ktorý bude reflektovať požadované funkčné požiadavky s plnou podporou multitenantného riešenia.
* **Bezpečnostný nástroj 2** – aktuálne je nástroj nasadený len v niektorých častiach infraštruktúry niektorých OVM, ktoré už využívajú služby bezpečnostného monitoringu zo strany NASES a VJ CSIRT. Na tieto prípady sa budúce riešenie aplikačnej architektúry nevzťahuje. Zmena vyplýva z obstarania a nasadenia nového jednotného nástroja, ktorý bude vyhovovať zadefinovaným funkčným požiadavkám. Nástroj bude nasadený v multitenantnom režime (jedno OVM predstavuje jeden tenant) za účelom ochrany údajov v súlade s GDPR a s centrálnou konzolou na pracovisku SOC.

Nové nástroje v prostredí SOC:

* **Bezpečnostný nástroj 3** – rozšírenie bezpečnostných nástrojov o ďalšiu technológiu vychádza z koncepcie skvalitňovania bezpečnostného monitoringu kombináciou viacerých nástrojov a ich vzájomnou integráciou so SIEM. Z pohľadu SOC sú hlavnými výhodami nástroja: zníženie času detekcie a rýchla reakcia. Nástroj sa zároveň vyznačuje menej zložitým nasadením a nižšími prevádzkovými nákladmi. Technológia bude nasadená na OVM, ktoré budú monitorované vládnym SOC. Architektúra vyžaduje multitenantnosť s centrálnou správou na SOC.
* **Bezpečnostný nástroj 3** **–** aktuálne neexistujúci nástroj, ktorý môže organizáciám umožniť kontrolovať, či ich siete, systémy a aplikácie majú bezpečnostné slabiny. Do nástroja bude doplnená integrácia o výsledky zo systému Achilles.

N/A

*Obrázok 6: Governance model budúceho stavu podľa použitých nástrojov*

Ako súčasť projektu je cieľom na spolupracujúcich OVM nasadiť **Monitorovacie nástroje** s vyústením do vládneho SOC (uvedené vyššie). Okrem toho bude zber udalostí z lokálnych aj vzdialených zdrojov log záznamov a normalizácia logov do požadovaného formátu zabezpečovaná prostredníctvom SIEM kolektorov. Tie budú nasadené vo virtualizačnom prostredí bez potreby ďalšieho obstarávania keďže aktuálna licencia technológie SIEM umožňuje umiestňovanie ľubovoľného množstva virtuálnych kolektorov.

Nasledujúce nástroje budú použité pre potreby zvýšenia úrovne monitoringu len ak nimi už OVM disponuje (neplánujú sa obstarávať a nasadiť na OVM ako súčasť projektu, ale ak ich OVM získa z iných zdrojov, bude možná integrácia počas trvania zmluvy o poskytovaní služieb EWS a SOC):

|  |  |
| --- | --- |
| **Nástroj** | **Popis** |
| Sieťové IDS/IPS | Systémy pre detekciu (prevenciu) vniknutia monitorujú sieťovú prevádzku a vykonávajú jej analýzu z hľadiska známok možných prienikov, ako sú pokusy o zneužitie a incidenty, ktoré môžu byť bezprostrednou hrozbou pre sieť. Prevencia narušenia je proces vykonávania detekcie narušenia a následného zastavenia zistených incidentov, čo sa zvyčajne vykonáva zahodením paketov alebo ukončením relácií. Tieto bezpečnostné nástroje sú dostupné ako systémy detekcie prienikov (IDS) a systémy prevencie prienikov (IPS), ktoré sú súčasťou bezpečnostných opatrení pre detekciu a zastavenie potenciálnych incidentov v sieti. |
| UEBA | Analýza správania používateľov a entít (UEBA), známa aj ako analýza správania používateľov (UBA), je proces zhromažďovania informácií o udalostiach v sieti, ktoré generujú používatelia. Po zhromaždení a analýze, sú tieto informácie použité na detekciu použitia skompromitovaných prihlasovacích údajov, bočného pohybu (lateral movement) a iného škodlivého správania. |
| DLP | Prevencia straty údajov (DLP) predstavuje technológie, ktoré vykonávajú kontrolu obsahu aj kontextovú analýzu údajov odosielaných prostredníctvom aplikácií na odosielanie správ, ako sú e-maily a okamžité správy, v pohybe po sieti, pri používaní na kontrolovanom koncovom zariadení, a v pokoji na lokálnych súborových serveroch alebo v cloudových aplikáciách a cloudových úložiskách. Tieto riešenia vykonávajú reakcie založené na politike a pravidlách definovaných tak, aby riešili riziko neúmyselného alebo náhodného úniku alebo exponovania citlivých údajov mimo autorizovaných kanálov.  Technológie DLP sú rozdelené do dvoch kategórií – Enterprise DLP a Integrated DLP. Zatiaľ čo riešenia Enterprise DLP sú komplexné a zabalené v softvéri agentov pre desktopy a servery, fyzických a virtuálnych zariadeniach na monitorovanie sietí a e-mailovej prevádzky alebo softvérových zariadeniach na zisťovanie údajov, integrované DLP je obmedzené na zabezpečené webové brány (SWG), zabezpečené e-mailové brány (SEG), produkty na šifrovanie e-mailov, platformy na správu podnikového obsahu (ECM), nástroje na klasifikáciu údajov, nástroje na vyhľadávanie údajov a nástroje pre riadenie cloudového prístupu (CASB). |
| Web content filter / Proxy | Proxy na filtrovanie obsahu je proxy server, server fungujúci ako sprostredkovateľ medzi dvoma počítačmi, ktorý filtruje prenášaný obsah a obmedzuje prístup k nežiaducemu, zakázanému alebo nebezpečnému obsahu. Organizácie sa môžu rozhodnúť použiť proxy na filtrovanie obsahu na kontrolu toho, čo si ľudia prezerajú v ich zariadeniach. Okrem filtrovania obsahu môže proxy tiež zachytiť malvér, vírusy a iný nežiaduci softvér a odstrániť ich skôr, ako sa dostanú do siete. |
| Web Application Firewall (WAF) | WAF pomáha chrániť webové aplikácie filtrovaním a monitorovaním obsahu HTTP komunikácie medzi webovou aplikáciou a internetom. Zvyčajne chráni webové aplikácie pred útokmi, ako je cross-site forgery, cross-site-scripting (XSS), vkladanie súborov a vkladanie SQL výrazov. |
| Mobile device management (MDM) | Správa mobilných zariadení (MDM) je softvér, ktorý umožňuje IT oddeleniu organizácie automatizovať, ovládať a zabezpečovať administratívne politiky na prenosných počítačoch, smartfónoch, tabletoch alebo akomkoľvek inom zariadení pripojenom k sieti organizácie.  Správa mobilných zariadení zvyčajne nasadzuje súhrn organizačných politík a certifikátov, konfigurácií na zariadení, aplikácií, back-endového softvéru a hardvéru na správu zariadení koncových používateľov. Cieľom správy mobilných zariadení je maximalizovať podporu zariadení, organizačné funkcie a bezpečnosť. |

Tabuľka č. 4 Príklady monitorovacích nástrojov na OVM

N/A

*Obrázok 7: Architektúra budúceho stavu podľa použitých nástrojov*

### Rozsah informačných systémov

Niektoré systémy, ktoré budú súčasťou navrhovaného riešenia nebudú evidované v MetaIS z dôvodu, že sa jedná o bezpečnostné systémy, ktoré sú prvkom kritickej infraštruktúry.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Kód ISVS**  *(z MetaIS)* | **Názov ISVS** | **Modul ISVS**  *(zaškrtnite ak ISVS je modulom)* | **Stav ISVS** | **Typ ISVS** | **Kód nadradeného ISVS**  *(v prípade zaškrtnutého checkboxu pre modul ISVS)* |
| N/A  *(Systém je v utajenom režime (nie je evidovaný v MetaIS)* | Bezpečnostné dohľadové centrum |  | Prevádzkovaný a plánujem rozvoj | Vyberte jednu z možnostíVyberte jednu z možností |  |
| isvs\_11534 | Systém vyhľadávania zraniteľností -Achilles |  | Prevádzkovaný a plánujem rozvoj | Agendový |  |

Tabuľka č.5 Prehľad dotknutých informačných systémov v projekte – súčasný stav

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Kód ISVS** *(z MetaIS)* | **Názov ISVS** | **Modul ISVS**  *(zaškrtnite ak ISVS je modulom)* | **Stav IS VS** | **Typ IS VS** | **Kód nadradeného ISVS**  *(v prípade zaškrtnutého checkboxu pre modul ISVS)* |
| projekt\_2167 | Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS) |  | Plánujem budovať | Agendový |  |
| isvs\_11534 | Systém vyhľadávania zraniteľností -Achilles |  | Prevádzkovaný a plánujem rozvíjať | Agendový |  |
| N/A  *(Systém je v utajenom režime (nie je evidovaný v MetaIS)* | Bezpečnostné dohľadové centrum |  | Prevádzkovaný a plánujem rozvíjať | Vyberte jednu z možností |  |

Tabuľka č.6 Prehľad budovaných/rozvíjaných ISVS v projekte – budúci stav

### Využívanie nadrezortných centrálnych blokov a podporných spoločných blokov (SaaS)

Systémy používané v kontexte tohto projektu nebudú využívať nadrezortné centrálne bloky ani podporné spoločné bloky vzhľadom na to, že sa v identifikovaných procesoch, ktoré projekt pokrýva nemajú opodstatnenie a ani relevantný prínos.

### Prehľad plánovaného využívania podporných spoločných blokov (SaaS)

Systémy používané v kontexte tohto projektu nebudú využívať podporné spoločné bloky vzhľadom na to, že sa v identifikovaných procesoch, ktoré projekt pokrýva nemajú opodstatnenie a ani relevantný prínos.

### Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky – spoločné moduly

Systémy používané v kontexte tohto projektu nebudú využívať nadrezortné centrálne bloky – spoločné moduly vzhľadom na to, že sa v identifikovaných procesoch, ktoré projekt pokrýva nemajú opodstatnenie a ani relevantný prínos.

### Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky - modul procesnej integrácie a integrácie údajov (IS CSRÚ)

Implementované systémy nebudú integrované na Modul procesnej integrácie a integrácie údajov.

### Poskytovanie údajov z ISVS do IS CSRÚ

Implementované systémy nebudú poskytovať žiadne údaje do IS CSRÚ vzhľadom na údaje bezpečnostného charakteru s ktorými budú pracovať.

### Konzumovanie údajov z IS CSRÚ

Implementované systémy nebudú konzumovať údaje z IS CSRU vzhľadom k tomu, že v identifikovaných procesoch, ktoré projekt pokrýva nemajú opodstatnenie a ani relevantný prínos.

## Dátová vrstva

### Údaje v správe organizácie

**Modul 1 - EWS**

Na strane VJ CSIRT a NASES bude EWS zbierať a pracovať s dátami z/zo:

* Threat intelligence a verejne dostupných (OSINT) zdrojov, databáz prihlasovacích údajov;
* IoC a ďalšie zdroje pochádzajúce z vlastnej činnosti VJ CSIRT;
* Systému Achilles o zistených kritických zraniteľnostiach zo skenerov zraniteľnosti;
* Adresné varovania o zero-day zraniteľnostiach podľa používaného SW;
* VISKB ako databáza subjektov. Informácie, ktoré VISKB spracúva od OVM, ktorú sú v konštituencii VJ CSIRT:
  + Základné údaje o organizácii;
  + Kontaktné údaje;
  + IPv4 adresy;
  + IPv6 adresy;
  + Doménové mená;
  + Informácie o sieťových službách;
  + Informácie o softvéroch v organizácii;
  + Aktíva organizácie;
  + Klasifikácia a kategorizácia IS a sietí;

Na strane zapojených subjektov v tzv. Vládnom alebo inom sektorovom SOC bude EWS zbierať a pracovať s dátami z/zo:

* Implementovaných bezpečnostných nástrojov;
* Log manažmentu/SIEM;
* Vyhodnocovania anomálií zachytených pri bezpečnostnom monitoringu v SOC (ich porovnanie, resp. zdieľanie rules, use case-ov);
* Kybernetických bezpečnostných incidentov;
* Ďalšími zdrojmi informácií pochádzajúcich z monitorovaných systémov na strane OVM.

**Modul 2 – Vládny SOC**

Rozsah zbieraných údajov súvisiacich s bezpečnosťou infraštruktúry OVM musí byť zabezpečený minimálne v rozsahu tzv. povinných zdrojov logov, ktoré budú definované v zmluve o poskytovaní služieb pre všetky OVM jednotne. V prípade ak OVM už disponuje inými bezpečnostnými nástrojmi, údaje, ktoré generujú môžu byť tiež integrované.

Rozsah údajov môže byť ďalej doplnený napríklad o:

* Kompletný záznam sieťovej aktivity;
* Dešifrovanú komunikáciu na aplikačnej vrstve.

### Dátový rozsah projektu

V budúcom stave sa predpokladá využívanie dát zo systémov VISKB, Achilles, bezpečnostných dohľadových centier, threat intelligence platforiem a ďalších verejne dostupných (OSINT) zdrojov.

### Kvalita a čistenie údajov

V rámci projektu a jeho výstupov nebude riadenie dátovej kvality, čistenie údajov.

## Referenčné údaje

Implementované riešenie nebude poskytovať žiadne referenčné údaje vzhľadom na povahu údajov, s ktorými systémy budú pracovať.

### Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné

Implementované riešenie nebude poskytovať žiadne referenčné údaje vzhľadom na povahu údajov, s ktorými systémy budú pracovať.

### Identifikácia údajov pre konzumovanie alebo poskytovanie údajov do/z CSRU

Implementované riešenie nebude konzumovať ani poskytovať údaje do/z CSRU.

## Otvorené údaje

Implementované riešenie nebude poskytovať žiadne otvorené údaje vzhľadom na citlivosť bezpečnostných údajov, s ktorými systémy budú pracovať.

## Analytické údaje

Implementované riešenie nebude poskytovať žiadne analytické údaje vzhľadom na povahu a citlivosť údajov, s ktorými systémy budú pracovať.

## Moje údaje

Implementované riešenie nebude poskytovať žiadne Moje údaje vzhľadom na povahu a citlivosť údajov, s ktorými systémy budú pracovať.

## Prehľad jednotlivých kategórií údajov

V zmysle vyššie uvedeného sa v súvislosti s projektom nebudú vyhlasovať žiadne nové typy údajov.

## Technologická vrstva

### Prehľad technologického stavu

Súčasná technologická vrstva sa detailne nepopisuje, pretože v prípade rozširovania a dopĺňania Modulu 2 – Vládny SOC bolo aktuálne technologické riešenie navrhované a implementované v utajovanom režime. Jednotlivé riešenia na centrálnej úrovni Vládneho SOC sú kombináciou fyzického a virtualizovaného prostredia. V prípade NASES je technologická a aplikačná vrstva Vládneho SOC oddelená od ostatnej prevádzkovanej infraštruktúry najmä z bezpečnostných a operatívnych dôvodov (bližšie opísané v časti bezpečnostná architektúra). Podobne je riešená aj technologická a aplikačná vrstva VJ CSIRT v rámci infraštruktúry MIRRI SR.

Systém Achilles je z pohľadu umiestnenia HW/SW, prevádzky (dostupnosť, patchovanie, LCM), administrácie z pohľadu bezpečnosti a samotného prístupu do systému plne v zodpovednosti VJ CSIRT. Technologická vrstva systému Achilles je špecifikovaná v [METAIS](https://metais.vicepremier.gov.sk/detail/Projekt/5e3a4cb3-d396-40b2-b36c-1339e672b8f9/cimaster?tab=documentsForm).

Vlastná infraštruktúra poskytuje pre celé aktuálne riešenie bezpečnostného monitoringu:

* Systémové prostredie ako sú operačné systémy, virtualizácia, clustering, loadbalancing, adresárové služby;
* Databázové prostredie;
* Súborové služby;
* Infraštruktúrne a sieťové prostredie;
* Prezentačné a portálové služby;
* Bezpečnosť;
* Prevádzkové prostredie;
* Testovacie prostredie;
* Zálohovanie.

### Požiadavky na výkonnostné parametre, kapacitné požiadavky

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Jednotky** | **Predpokladaná hodnota** | **Poznámka** |
| Počet interných používateľov (NASES, VJ CSIRT) | Počet |  |  |
| Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení | Počet |  |  |
| Počet externých používateľov (internet) | Počet |  |  |
| Počet externých používateľov používajúcich systém v špičkovom zaťažení – administrátori OVM zapojené do EWS | Počet |  |  |
| Dátová priepustnosť technológie SIEM - events per second | EPS |  |  |
| Dátová priepustnosť ďalších nástrojov | Byte/sekunda |  |  |

Tabuľka č.7 Prehľad vybraných kapacitných a výkonových požiadaviek na EWS – budúci stav

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Jednotky** | **Predpokladaná hodnota** | **Poznámka** |
| Očakávaný príjem dát (data ingest) | GB/deň |  |  |
| Počet event per second | EPS |  |  |
| Počet používateľov SIEM riešenia | Počet |  |  |
| Celkový počet pracovných staníc | Počet |  |  |
| Počet používateľov | Počet |  |  |
| Počet aktívnych koncových zariadení v sieti (PC, ntb, tel., servery,...) | Počet |  |  |
| Počet serverov (fyzických aj virtuálnych spolu) | Počet |  |  |
| Odhad sieťovej prevádzky vo vnútri organizácie | Gbps |  | Priemerná hodnota pre 1 OVM |

Tabuľka č.8 Prehľad vybraných kapacitných a výkonových požiadaviek na bezpečnostné nástroje – budúci stav

### Návrh riešenia technologickej architektúry

**Technologická architektúra EWS**

Budúci stav technologickej architektúry EWS počíta s implementáciou a nasadením jednotlivých nástrojov do existujúceho riešenia. Kľúčovým nástrojom EWS bude threat intelligence platforma, ktorá može byť nasadená ako SaaS (Software as a Service) alebo lokálne riešenie s požadovanou konektivitou do cloudového prostredia vendora. V budúcom stave je zámerom nasadiť technológiu ako SaaS, čo umožní konektivitu do cloudovej aplikácie výrobcu cez internet. Uvedeným riešením sa eliminujú potreby inštalácie a prevádzky aplikácie na vlastných zariadeniach.

Open-source platforma MISP slúži pre zdieľanie artefaktov, taktík, techník a procedúr o kybernetických útokoch, teda zdroje z Threat intelligence. Platformu MISP používajú aj organizácie ako napríklad NATO, Europol, Interpol alebo bankové inštitúcie. V budúcom stave sa implementáciou novej threat intelligence platformy rozšíri architektúra MISP serverov. K aktuálnym MISP serverom bude pridaný ďalší centrálny MISP EWS server pre TIPs využívaný primárne pre EWS a Vládny SOC.

N/A

Obrázok 8 Návrh riešenia technologickej architektúry EWS z pohľadu MISP a TIP

Centrálna časť (tzv. riadiaca alebo management) jednotlivých aplikácií a nástrojov na zabezpečovanie služieb bezpečnostného monitoringu a včasného varovania bude nasadená a prevádzkovaná v samostatnej bezpečnostnej časti NASES na dedikovaných fyzických a virtuálnych serveroch (obrázok 9). Pripájaním nových subjektov a nasadením ďalších bezpečnostných nástrojov bude nutné rozšírenie výkonov spojených so spracovaním, vyhodnocovaním a uložením dát. Vzhľadom na dostatočné skúsenosti a prevádzku aktuálneho riešenia bezpečnostného centra bude za uvedenú časť zodpovedať tím SOC. Aktuálne prevádzkuje celé riešenie SIEM, SOAR a on-premise niektoré bezpečnostné nástroje využívané primárne pre monitoring. Z dôvodu požiadaviek na multitenantné riešenie za účelom zachovania bezpečnosti a dôvernosti údajov bude pre lokálne bezpečnostné tímy (OVM) umožnený prístup do tzv. lokálnej konzoly. Okrem toho budú v centrálnej správe ajkonzoly na správu ďalších nástrojov. NASES okrem toho už v súčasnom stave plne zodpovedá za prevádzku a ďalší vývoj nástroja Service Desk, ktorý je predpripravený aj pre potreby Vládneho SOC.

V prípade VJ CSIRT sa v budúcom stave technologickej architektúry nič nemení. Zmeny v architektúre systému Achilles budú riešené implementáciou iného projektu.

V prípade OVM, ktoré budú využívať služby bezpečnostného dohľadového centra bude technologická architektúra bezpečnostného monitoringu riešená prostredníctvom samostatného dedikovaného HW a SW. Tieto technológie budú umiestnené v prostredí OVM a z bezpečnostných dôvodov odčlenené od internej IT infraštruktúry. Serverové riešenie pre OVM bude pozostávať do serveru, procesorov, RAM, SSD diskov, zdrojov a ďalších nevyhnutných komponentov. Okrem toho budú pre potreby samostatnej infraštruktúry EWS v OVM umiestnené aj ďalšie sieťové prvky.

Základným komponentom virtualizačnej platformy je softvérová vrstva tzv. hypervízor, ktorá je nainštalovaná na fyzický hardvér a zabezpečuje vlastnú virtualizáciu prostriedkov. Okrem tejto základnej funkcionality tento komponent zabezpečuje aj ďalšie funkcionality: bezvýpadková prevádzka virtuálnych strojov; migrácia virtuálnych serverov počas behu; podpora šifrovania virtuálnych strojov; distribuované rozdelenie záťaže medzi jednotlivými hypervízormi - automatická migrácia virtuálneho stroja v prípade preťaženia jedného z hypervízorov resp. jedného z dátových úložísk; optimalizácie fyzickej pamäte - transparent page sharing, memory compression, memory balooning, RAM Overcommittment (presiahnutie veľkosti fyzickej RAM); rezervácia procesorového výkonu a pamäte; vytvárania skupín virtuálnych strojov, ktoré musia resp. nesmú za každých okolností bežať súčasne na jednom hypervízore; zabezpečuje sieťové prepojenie medzi jednotlivými virtuálnymi strojmi a prepojenie týchto strojov s prostredím mimo hypervízora.

N/A

Obrázok 9 Technologická architektúra riešenia

Konkrétne fyzické umiestnenie jednotlivých technologických komponent bude definované v projektovom pláne. Pre jednotlivé nástroje je preferované prevádzkovanie on-premise, resp. hybridné. Niektoré nástroje budú komunikovať s centrálnou konzolou umiestnenou v cloude výrobcu. V prípade použitia cloudových služieb výrobcu technológie, musia byť splnené všetky požiadavky kladené na samotné zabezpečenie cloudu a GDPR. Zároveň musí spĺňať štandardy v súlade s medzinárodne platnou normou ISO/IEC 27017 (Opatrenia informačnej bezpečnosti v cloudových službách) a normou ISO/IEC 27018 Požiadavky na ochranu PII (osobne identifikovateľné informácie).

**Vysoká dostupnosť**

Technická implementácia riešenia bude realizovaná vo vysokej dostupnosti (HA). Platí teda aktuálny stav a riešenie, ktoré už bolo navrhnuté pri budovaní SOC s technológiou SIEM a SOAR v predchádzajúcom projekte. Vzhľadom na platný režim utajenia tohto riešenia nie je možné poskytnúť podrobnejší opis. Použité sú/budú nasledujúce prístupy:

* Aktívne-pasívne klastrovanie: Na vytvorenie failover riešenia pri zlyhaní pre systémy EWS a Vládny SOC bude použité aktívne-pasívne klastrovanie. To znamená, že jedno z dátových centier funguje ako primárne (aktívne) miesto a druhé dátové centrum funguje ako sekundárne (pasívne) miesto. V normálnej prevádzke sa o všetku návštevnosť a spracovanie stará aktívna lokalita. V prípade poruchy prevezme a riadi prevádzku pasívne miesto.
* Synchrónna replikácia: Pre databázový komponent systému EWS a SOC bude použitá synchrónna replikácia na udržiavanie kópií údajov v reálnom čase v oboch dátových centrách. Uvedený prístup zabezpečí, že ak jedno dátové centrum zlyhá, druhé prevezme kontrolu bez straty dát.
* Mechanizmy Heartbeat a failover: Na detekciu zlyhaní sa použije mechanizmus Heartbeat medzi dvoma dátovými centrami. V prípade zlyhania možno použiť mechanizmus núdzového prepnutia na automatické prepnutie prevádzky do sekundárneho dátového centra, čo je možné buď pomocou virtuálnych adries IP alebo pomocou mechanizmov prepnutia pri zlyhaní založených na DNS.
* Redundancia siete: Aby sa zabezpečilo, že systém zostane dostupný aj v prípade zlyhania siete, je dôležité implementovať redundanciu siete pomocou viacerých sieťových prepojení a smerovacích protokolov. K tomu je možné pristúpiť pomocou redundantných sieťových rozhraní alebo pomocou agregačných a smerovacích protokolov, ako sú VRRP alebo OSPF. To pomáha zaistiť, že systém zostane pripojený k sieti, aj keď jedno zo sieťových spojení zlyhá.

### Využívanie služieb z katalógu služieb vládneho cloudu

Riešenie nebude využívať žiadne služby z katalógu služieb vládneho cloudu.

### Jazyková lokalizácia

Nasadené nástroje spolu so všetkými návodmi a vstupným zaškolením budú v anglickom alebo slovenskom jazyku.

## Bezpečnostná architektúra

Z dôvodu povahy a obsahu projektu a nadväznosti na bezpečnostnú architektúru už existujúceho riešenia (v režime utajenia) nie je možné detailnejšie špecifikovať bezpečnostnú architektúru súčasného a budúceho stavu.

N/A

*Obrázok 10 Bezpečnostná architektúra riešenia*

Implementované riešenia budú v súlade s nasledujúcimi princípmi bezpečnej architektúry.

Ide najmä o nasledovné princípy:

* Obrana do hĺbky - v systéme informačných technológií (IT) sú umiestnené viaceré vrstvy bezpečnostných kontrol (obrana). Jeho zámerom je poskytnúť redundanciu v prípade zlyhania bezpečnostnej kontroly alebo zneužitia zraniteľnosti, ktorá môže pokryť aspekty personálnej, procedurálnej, technickej a fyzickej bezpečnosti počas trvania životného cyklu systému.
* Rozčlenenie - je umiestnenie riadenia prístupu medzi rôzne podsiete, aby sa obmedzila komunikácia medzi systémami a službami a aby sa identifikovali neočakávané komunikácie, ktoré môžu byť znakom útoku. V každej sieti sú systémy a služby, ktoré by spolu nikdy nemali komunikovať.
* Princíp najmenších privilégií – predstavuje prístup „need-to-know“. Používatelia a technologické komponenty by mali by ste mať len takú úroveň prístupov a oprávnení, aby vedeli vykonať svoju prácu a nič navyše.
* Segregácia oprávnení - systém by mal pred udelením povolení objektu zabezpečiť splnenie viacerých podmienok. Kontrola prístupu len za jednej podmienky nemusí byť adekvátna pre dostatočne silné zabezpečenie. Ak softvérový systém z veľkej časti pozostáva z jedného komponentu, nemožno implementovať myšlienku viacerých kontrol na prístup k rôznym komponentom. Rozdelenie softvéru do samostatných komponentov, ktoré vyžadujú viacnásobné kontroly prístupu, môže zabrániť útoku alebo potenciálne zabrániť útočníkovi prevziať kontrolu nad celým systémom.
* Sprostredkovaný prístup - je založený na centralizácii bezpečnostných kontrol na ochranu skupín aktív alebo bezpečnostných domén. Sprostredkovaný prístup je realizovaný bezpečnostnými riešeniami, ktoré pracujú v mene aktív, ktoré majú chrániť a sprostredkúvajú dôveryhodné vzťahy medzi bezpečnostnými doménami.
* Všetky zdroje údajov a výpočtové služby sa považujú za zdroje. Sieť môže byť zložené z viacerých tried zariadení. Organizácia sa tiež môže rozhodnúť klasifikovať zariadenia v osobnom vlastníctve ako zdroje, ak majú prístup k zdrojom organizácie.
* Všetka komunikácia medzi bezpečnostnými nástrojmi, centrálnou časťou a OVM pripojenými do systému včasného varovania je zabezpečená. Všetka komunikácia bude prebiehať najbezpečnejším dostupným spôsobom, chrániť dôvernosť a integritu a požadovať autentifikáciu iniciátora komunikácie.
* Prístup k jednotlivým zdrojom organizácie sa poskytuje na základe jednotlivých relácií (session). Dôveryhodnosť žiadateľa je vyhodnotená pred udelením prístupu. Prístup by mal byť pridelený s ohľadom na princíp najmenších oprávnení potrebných na výkon úlohy. Autentifikácia a autorizácia prístupu k jednému zdroju automaticky neudelí prístup k inému zdroju.
* Princíp najmenších oprávnení je využitý pre obmedzenie viditeľnosti a prístupu.
* Organizácia monitoruje a meria integritu a bezpečnosť všetkých vlastnených aj pridružených aktív. Žiadnemu aktívu sa inherentne nedôveruje. Organizácia hodnotí bezpečnostný stav aktíva pri vyhodnocovaní požiadavky na prístup k zdroju. S aktívami, o ktorých sa zistilo, že majú narušenú bezpečnosť, majú známe zraniteľnosti a/alebo nie sú spravované organizáciou, sa môže zaobchádzať odlišne (vrátane odmietnutia všetkých pripojení k zdrojom organizácie) ako zariadenia vo vlastníctve alebo spojené s organizáciou, ktoré sa považujú za najbezpečnejšie.
* Organizácia zhromažďuje čo najviac informácií o aktuálnom stave aktív, sieťovej infraštruktúry a komunikácií a využíva ich na zlepšenie svojej úrovne bezpečnosti. Organizácia by mal zbierať údaje o stave zabezpečenia majetku, sieťovej prevádzke a žiadostiach o prístup, spracovávať tieto údaje a využívať získané poznatky na zlepšenie vytvárania a vynucovania bezpečnostnej politiky.

Implementované riešenia budú dodržiavať nasledovné požiadavky:

**Autentifikácia**

Existuje niekoľko riešení autentifikácie, ktoré možno použiť pre komponenty riešenia EWS:

* Autentifikácia na základe hesla: Zahŕňa použitie hesla na overenie identity používateľa. Heslá by mali byť silné a jedinečné.
* Dvojfaktorové overenie (2FA): Zahŕňa použitie druhej formy overenia okrem hesla, ako je kód odoslaný do telefónu alebo biometrický sken. Pomáha to zvýšiť bezpečnosť pridaním ďalšej vrstvy autentifikácie.
* Autentifikácia verejným kľúčom: Zahŕňa použitie páru verejného a súkromného kľúča na overenie identity používateľa. Súkromný kľúč je udržiavaný v tajnosti, zatiaľ čo verejný kľúč sa používa na overenie identity používateľa.
* Jednotné prihlásenie (SSO): Jednotné prihlásenie umožňuje používateľom používať jednu sadu poverení na prístup k viacerým aplikáciám a systémom. To môže pomôcť zjednodušiť proces overovania a zvýšiť bezpečnosť znížením počtu hesiel, ktoré si používatelia musia zapamätať.
* Celkovo je dôležité používať robustné riešenia autentifikácie, aby sa zabezpečilo, že ku komponentom riešenia EWS budú mať prístup iba oprávnení používatelia.

**Autorizácia**

Existuje niekoľko rôznych možností implementácie autorizácie pre riešenie EWS v závislosti od konkrétnych potrieb a požiadaviek organizácie. Niektoré možnosti, ktoré možno stoja za zváženie, zahŕňajú:

* Riadenie prístupu na základe rolí: Zahŕňa priradenie konkrétnych rolí alebo povolení používateľom a umožnenie prístupu iba k určitým zdrojom alebo funkciám na základe týchto rolí. Môže to byť dobrý spôsob, ako zabezpečiť, aby používatelia mali prístup len k zdrojom a funkciám, ktoré sú relevantné pre ich pracovné povinnosti.
* Zoznamy riadenia prístupu (Access Lists): Zahŕňa to vytvorenie zoznamu konkrétnych používateľov alebo skupín, ktorí majú povolený prístup k určitým zdrojom alebo funkciám, a odmietnutie prístupu každému, kto nie je na zozname. Môže to byť dobrý spôsob, ako zabezpečiť, aby k citlivým zdrojom alebo funkciám mali prístup iba oprávnení používatelia.

**Riadenie prístupu**

Existuje niekoľko rôznych možností, ktoré možno zvážiť pri implementácii vysoko bezpečnej kontroly prístupu v riešení a ich vzájomné kombinácie:

* Riadenie prístupu na základe rolí: Zahŕňa priradenie konkrétnych rolí alebo povolení používateľom a umožnenie prístupu iba k určitým zdrojom alebo funkciám na základe týchto rolí. Môže to byť dobrý spôsob, ako zabezpečiť, aby používatelia mali prístup len k zdrojom a funkciám, ktoré sú relevantné pre ich pracovné povinnosti.
* Zoznamy riadenia prístupu: Zahŕňa to vytvorenie zoznamu konkrétnych používateľov alebo skupín, ktorí majú povolený prístup k určitým zdrojom alebo funkciám, a odmietnutie prístupu každému, kto nie je na zozname. Môže to byť dobrý spôsob, ako zabezpečiť, aby k citlivým zdrojom alebo funkciám mali prístup iba oprávnení používatelia.
* Politiky riadenia prístupu: Zahŕňa to vytváranie špecifických politík, ktoré určujú, kto má povolený prístup k určitým zdrojom alebo funkciám a za akých okolností. Toto môže byť podrobnejší a flexibilnejší prístup k riadeniu prístupu, pretože umožňuje vytvárať prispôsobené politiky, aby vyhovovali špecifickým potrebám organizácie.
* Segmentácia siete: Zahŕňa rozdelenie siete do rôznych segmentov alebo zón a použitie rôznych kontrol prístupu na každý segment. Môže to byť dobrý spôsob, ako zabezpečiť, aby boli citlivé zdroje alebo funkcie izolované od zvyšku siete a prístup k nim mali len oprávnení používatelia.

**Sieťová komunikácia**

Všetky komponenty EWS a Vládneho SOC musia komunikovať iba bezpečnými sieťovými protokolmi. Existujú rôzne bezpečné sieťové protokoly, ktoré možno použiť v riešení EWS na zabezpečenie dôvernosti, integrity a dostupnosti komunikácie medzi rôznymi komponentmi, ako napr.:

* HTTPS: HTTPS (Hypertext Transfer Protocol Secure) je zabezpečená verzia HTTP, ktorá sa používa na prenos údajov cez internet. Používa šifrovanie na zabezpečenie údajov prenášaných medzi webovým serverom a klientom, ako je napríklad webový prehliadač.
* SSH: SSH (Secure Shell) je zabezpečený sieťový protokol používaný na vzdialené pripojenie a správu zariadení cez sieť. Používa šifrovanie na zabezpečenie komunikácie medzi klientom a serverom.
* VPN: VPN (Virtual Private Network) je sieť, ktorá umožňuje používateľom bezpečne sa pripojiť k súkromnej sieti cez internet. Používa šifrovanie na zabezpečenie komunikácie medzi klientom a serverom VPN.
* SFTP: SFTP (SSH File Transfer Protocol) je bezpečný protokol používaný na prenos súborov cez sieť. Používa šifrovanie na zabezpečenie komunikácie medzi klientom a serverom.
* TLS: TLS (Transport Layer Security) je bezpečný sieťový protokol používaný na vytvorenie bezpečnej komunikácie medzi dvoma systémami. Bežne sa používa na zabezpečenie komunikácie medzi webovými servermi a klientmi, ako sú webové prehliadače.

**Vzdialený prístup**

Vzdialený prístup do riešenia EWS musí byť adekvátne zabezpečený:

* Používanie silných, jedinečných hesiel: Je dôležité používať silné a jedinečné heslá pre všetky účty vzdialeného prístupu. To môže pomôcť zabrániť neoprávnenému prístupu do siete.
* Dvojfaktorové overenie: Užívatelia musia poskytnúť dve formy identifikácie, ktoré sú nevyhnutné k prístupu.
* Používanie sietí VPN: Virtuálne privátne siete (VPN) budú použité na zabezpečenie pripojení vzdialeného prístupu. Siete VPN šifrujú údaje prenášané medzi vzdialeným zariadením a sieťou, čo sťažuje neoprávneným používateľom zachytenie údajov.
* Zavedenie kontroly prístupu: Budú zavedené kontroly prístupu, ako je autentifikácia používateľov a kontroly prístupu na základe rolí, aby sa zabezpečilo, že do siete budú mať prístup len oprávnení používatelia.
* Monitorovanie aktivity vzdialeného prístupu: Bude monitorovaná aktivita vzdialeného prístupu vrátane zaznamenávania všetkých pokusov o vzdialený prístup a pravidelnej kontroly denníkov. To môže pomôcť identifikovať akúkoľvek podozrivú alebo neoprávnenú aktivitu.

**Ochrana údajov**

Údaje riešenia EWS a Vládneho SOC musia byť chránené počas uskladnenia aj počas prenosu:

* Šifrovanie: Ide o kódovanie údajov takým spôsobom, aby k nim mal prístup iba niekto s príslušným dešifrovacím kľúčom. Toto možno použiť na zabezpečenie dát pri prenose (napr. cez sieť) a dát v pokoji (napr. na serveri alebo úložnom zariadení).
* Bezpečné komunikačné protokoly: Zahŕňa to používanie protokolov ako SSL/TLS na zabezpečenie prenosu údajov. Tieto protokoly používajú šifrovanie a ďalšie bezpečnostné opatrenia na ochranu údajov pri ich prenose cez sieť.
* Kontroly prístupu: Zahŕňa to implementáciu opatrení, ako je autentifikácia používateľov, kontroly prístupu na základe rolí a zoznamy kontroly prístupu na obmedzenie prístupu k údajom len pre oprávnených používateľov.
* Zálohovanie a obnova dát: Zahŕňa vytváranie pravidelných záloh dát a implementáciu plánu obnovy dát v prípade katastrofy alebo straty dát.

**Logovanie**

V riešení EWS a SOC, ktoré zahŕňajú bezpečnostný monitoring ďalších OVM na Slovensku je dôležitým prvkom vysoká dôveryhodnosť a transparentnosť. Z tohto princípov vypláva nutnosť implementovať robustné nastavenia auditu, aby sa zabezpečilo, že sa všetky relevantné aktivity zaznamenávajú a dajú sa v prípade potreby spätne skontrolovať. Auditovanie sa bude týkať nasledujúcich oblastí:

* Auditovanie aktivity používateľa: Zahŕňa zaznamenávanie všetkých akcií vykonaných používateľmi, ako sú prihlásenia, prístup k súborom a prístup k prostriedkom. Logovanie aktivity používateľov je kľúčové pri sledovaní aktivity používateľov a identifikácii akejkoľvek podozrivej alebo neoprávnenej aktivity.
* Auditovanie aktivity systému: Zahŕňa protokolovanie všetkých aktivít na úrovni systému, ako sú systémové prihlásenia, zmeny konfigurácie a systémové chyby. Tento prístup je dôležitý pri sledovaní zmien v systéme a pri identifikácii akýchkoľvek problémov.
* Audit sieťovej aktivity: Zahŕňa protokolovanie všetkej sieťovej aktivity, ako sú vzory premávky, pokusy o pripojenie a prístup k prostriedkom. Ide o dôležitý prvok pri sledovaní používania siete a identifikácii akejkoľvek podozrivej alebo neoprávnenej aktivity.
* Auditovanie udalostí zabezpečenia: Zahŕňa zaznamenávanie všetkých udalostí súvisiacich so zabezpečením, ako sú protokoly brány firewall, protokoly detekcie narušenia a protokoly antivírusov. Predstavuje nutnosť pri identifikácii a reakcii na bezpečnostné hrozby a incidenty priamo v systéme EWS a samotnom SOC.

**Synchronizácia času**

Všetky komponenty riešenia musia byť časovo synchronizované. Presná synchronizácia času je dôležitá pre bezpečnosť z niekoľkých dôvodov:

* Audit a protokolovanie: Mnoho bezpečnostných systémov sa spolieha na presné časové pečiatky na zaznamenávanie udalostí a sledovanie aktivity. Ak časové pečiatky nie sú presné, môže byť ťažké identifikovať postupnosť udalostí alebo určiť správny čas incidentu.
* Detekcia narušenia: Niektoré systémy detekcie narušenia používajú na identifikáciu podozrivej aktivity časové vzory. Ak systémové hodiny nie sú synchronizované, môže byť pre systém ťažké presne rozpoznať prieniky.
* Digitálne podpisy: Digitálne podpisy sa spoliehajú na presné časové pečiatky na overenie pravosti dokumentu alebo správy. Ak časové pečiatky nie sú presné, môže byť ťažké overiť pravosť podpisu.
* Uplynutie platnosti hesla: Niektoré systémy používajú heslá založené na čase, ktorých platnosť vyprší po určitom čase. Ak hodiny nie sú synchronizované, môže byť ťažké určiť, kedy platnosť hesla vypršala.
* Celkovo je presná časová synchronizácia dôležitá pre bezpečnosť, pretože pomáha zabezpečiť, aby bezpečnostné systémy boli schopné správne fungovať a presne sledovať a monitorovať aktivitu.

Implementované riešenia budú v súlade s dotknutými právnymi normami a zároveň s technickými normami, ktoré stanovujú úroveň potrebnej bezpečnosti IS, pre manipuláciu so samotnými dátami, alebo technické/technologické/personálne zabezpečenie samotnej výpočtovej techniky/HW vybavenia. Ide najmä o:

* Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe;
* Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti;
* Zákon č. 45/2011 Z. z. o kritickej infraštruktúre;
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy;
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy;
* Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov;
* Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov);
* Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

# ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Kód projektu**  *(z MetaIS)* | **Názov projektu** | **Termín ukončenia projektu** | **Popis závislosti** |
| MIRRI SR | N/A | Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy | 05/2023 | Projektom sa rozvíja systém VISKB, ktorý bude integrovaný previazaný so systémom Achilles. Overené zraniteľnosti z Achilla budú použité pre EWS. |
| MIRRI SR/NASES | N/A | Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe | 03/2023 | Projektom sa rozvíja kapacita a rozsah poskytovaných služieb SOC vybudovaného z Národného systému, ktorý bude integrovaný do riešenia EWS. |
| MIRRI SR | projekt\_2056 | Zvýšenie spôsobilostí VJ CSIRT | 11/2024 | Projekt využije údaje z rozšírenej kapacity a automatizácie systému Achilles, ktorý skenuje zraniteľnosti OVM z vonkajšieho prostredia. Projekt tiež využije optimalizáciu a automatizáciu workflowov pri činnosti incident response tímov VJ CSIRT. |

Tabuľka č. 9 Prehľad projektov, ktoré sú v štádiu vývoja alebo v korelácii s pripravovaným projektom

# ZDROJOVÉ KÓDY

Nerelevantné, pretože žiadne zdrojové kódy sa projektom nevytvárajú.

# PREVÁDZKA A ÚDRŽBA

Minimálna doba udržateľnosti projektu je 5 rokov, teda 60 mesiacov. Udržateľnosť projektu znamená udržanie (zachovanie) výsledkov realizovaného projektu. Vzhľadom na predpoklad použitia viacerých preexistentných riešení od rôznych vendorov je v budúcej SLA nevyhnutné zabezpečiť podporu prevádzky (vendor supportov) pre jednotlivé bezpečnostné komponenty riešenia samostatne. Predpokladané finančné nároky na zabezpečenie podpory prevádzky sú uvedené v CBA (hárky TCO TO BE). Predmetná kalkulácia nezahŕňa bežné opravy súvisiace s mimozáručnými poruchami. V karte Moduly\_CBA boli navýšené percentuálne podiely aplikačnej podpory a rozvoja z dôvodu nutnosti pravidelne obnovovať licencie jednotlivých bezpečnostných nástrojov a ďalšieho SW. So zámerom zníženia cien obstarávaných licencií je cieľom ich nákup v režime: licencia na 3 roky s následnou možnosťou opcie predĺženia o ďalšie 2 roky.

## Prevádzkové požiadavky

### Úrovne podpory používateľov:

V prípade **OVM** zapojených do systému včasného varovania a vládneho SOC bude Help Desk realizovaný systémom Service Desk

cez 3 úrovne podpory, s nasledujúcim označením:

* **L1 podpora** (Level 1) - jednotný kontaktný bod predstavujú interní zamestnanci EWS SOC, ktorí zároveň prijímajú hlásenia o kybernetických bezpečnostných incidentoch a tvoria L1 podpory pre prevádzku siete Govnet. alebo platform support tím špecialistov.
* **L2 podpory** (Level 2, postúpenie požiadaviek od L1) - vybraná skupina špecialistov pre jednotlivé bezpečnostné nástroje na strane dodávateľa SW a licencií.
* **L3 podpory** (Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore bude zabezpečovať výrobca jednotlivých bezpečnostných nástrojov.

**Definícia:**

* **Podpora L1 (podpora 1. stupňa)** - začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.
* **Podpora L2 (podpora 2. stupňa)** – riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.
* **Podpora L3 (podpora 3. stupňa)** - Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobťažnejších Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.

**Pre služby sú definované takéto SLA:**

* Help Desk je dostupný cez Service Desk a pre vybrané skupiny užívateľov cez telefón a email. Prevádzkové incidenty sú tiež evidované v Service Desk.
* Dostupnosť L1, L2 a L3 podpory pre bezpečnostné nástroje je v režime 24/7 (24 hodín x 7 dní v týždni).

**Riešenie prevádzkových incidentov – SLA parametre**

Za prevádzkový incident je považovaná chyba používaného bezpečnostného nástroja, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou. Presné parametre riešenia prevádzkových incidentov medzi prijímateľmi služieb EWS a Vládneho SOC budú predmetom individuálnych vzájomných zmlúv o zapojení do systému včasného varovania a bezpečnostnom monitoringu.

## Požadovaná dostupnosť pre jednotlivé bezpečnostné nástroje:

|  |  |  |
| --- | --- | --- |
| ***Popis*** | ***Parameter*** | ***Poznámka*** |
| **Prevádzkové hodiny** | 24 hodín | 24 hodín počas pracovných dní, víkendov a sviatkov |
| **Servisné okno** | 10 hodín | od 19:00 hod. - do 5:00 hod. počas pracovných dní |
| 24 hodín | od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov  Servis a údržba sa bude realizovať mimo pracovného času. |
| **Dostupnosť produkčného prostredia** | 99% | * 99% z 24/7/365 t.j. max ročný výpadok je 3,65 dňa * Maximálny mesačný výpadok je 7,3 hodiny. * Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni. * Nedostupnosť systémov sa počíta od nahlásenia incidentu Zákazníkom (čiže špecialistami EWS a SOC v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase 24 hodín počas pracovných dní, víkendov a sviatkov). Do dostupnosti systémov nie sú započítavané servisné okná a plánované odstávky. |

### Dostupnosť (Availability)

Dostupnosť (Availability) znamená, že dáta alebo iné zariadenie sú prístupné v okamihu jej potreby. Vyjadruje sa v percentách dostupného času. Pre tento projekt je navrhnutá dostupnosť na úrovni:

* ***99% dostupnosť****znamená výpadok 3,65 dňa.*

### RTO (Recovery Time Objective)

RTO (Recovery Time Objective) je jeden z ukazovateľov dostupnosti dát. RTO vyjadruje množstvo času potrebné pre obnovenie dát a celého prevádzky nedostupného systému (softvér). RTO bude riešené formou tradičného zálohovania a obnovy a definované pri realizácií projektu. Navrhované RTO je 1 hodina.

### RPO (Recovery Point Objective)

RPO (Recovery Point Objective) je jeden z ukazovateľov dostupnosti dát. RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta. RPO bude riešené formou tradičného zálohovania a obnovy a definované pri realizácií projektu. Očakáva sa nulová strata údajov. Navrhované RPO je 24 hodín dozadu.

# POŽIADAVKY NA PERSONÁL

V rámci projektu bude vytvorený projektový tím v zložení:

* Projektový manažér;
* Kľúčový používateľ NASES;
* Kľúčový používateľ VJ CSIRT;
* Vlastník procesov NASES;
* Vlastník procesov VJ CSIRT;
* IT analytik;
* IT architekt;
* Manažér kvality;
* Manažér kybernetickej a informačnej bezpečnosti;
* SOC špecialista;
* Špecialista na manažment zraniteľností;
* Špecialista pre riešenie kybernetických incidentov;
* Bezpečnostný analytik L1/L2 – NASES;
* Integračný špecialista bezpečnostných nástrojov – NASES;
* Platform support – NASES;
* Špecialista pre onboarding – NASES.

Do projektu môžu byť zapojené aj ďalšie potenciálne roly a to predovšetkým v kontexte realizácie modulu Vládny SOC.

# IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude implementovaný v zmysle vyhlášky č. 85/2020 Z. z. o projektovom riadení bez rozdelení na viaceré inkrementy. Rozdelenie na inkrementy v projekte nie je možné vzhľadom na požiadavky inkrementu definovaných vyhláškou, podľa ktorých nie je možné realizovať viaceré inkrementy súbežne. Vzhľadom na charakter a rozsah projektu budú jednotlivé moduly, ktoré spolu vytvárajú jeden inkrement realizované paralelne v zmysle prístupu k implementácii jednotlivých častí projektu.

Realizačná fáza projektu bude rozdelená na 4 etapy:

* Analýza a dizajn
* Nákup HW, SW a služieb
* Implementácia a testovanie
* Nasadenie a post-implementačná podpora

V rámci high-level harmonogramu (obrázok 11 nižšie) sú pre lepšiu prehľadnosť samostatne naplánované fáza nasadenia a fáza testovania. V prípade všetkých modulov budú paralelne prebiehať analýza a dizajn spolu s nákupom HW, SW a služieb. Počas prípravy projektovej dokumentácie a CBA už boli špecifikované požiadavky na jednotlivé bezpečnostné nástroje a ďalšie technológie čo umožní spustiť proces obstarávania v krátkom časovom horizonte po schválení projektu. Obdobne bude riešená aj etapa implementácia a testovanie.

**Prístup k implementácii jednotlivých modulov projektu**

Modul 1: Vybudovanie Systému včasného varovania (EWS – Early Warning System)

* Riešenie bude implementované kombináciou externého dodávateľa a internými kapacitami na strane NASES a VJ CSIRT;
* Vzhľadom na krátky časový priestor na implementáciu riešenia (obmedzený termínmi stanovenými v POO) budú niektoré etapy realizačnej fázy časovo prekrývať. V rámci Detailného návrhu riešenia (DNR) budú dizajnované väčšie funkčné celky, ktoré bude možné a aj potrebné implementovať paralelne (napr. inštalácia, integrácie do centrálnych platforiem SIEM/SOAR, prepojenie na sektorové SOC, konfigurácia a testovanie a podobne).

Modul 2: Rozšírenie služieb a spustenie bezpečnostného monitoringu prostredníctvom tzv. Vládneho SOC

* Modul Vládny SOC bude implementovaný kombináciou viacerých externých dodávateľov a interných zamestnancov, resp. externých špecialistov na kybernetickú bezpečnosť na strane VJ CSIRT a NASES.
* Implementácia bude prebiehať v súlade s plánom nasadenia bezpečnostných nástrojov na OVM (Modul 3). Nasadenie nástrojov bude prebiehať po jednotlivých OVM zapojených do EWS a SOC od najmenších po najväčších (podľa počtu koncových zariadení). Po nasadení každej technológie na OVM prebehne integrácia na centrálne riešenie (centrálne manažment platformy) vo Vládnom SOC.

Modul 3: Nasadenie bezpečnostných nástrojov na OVM

* Pripájanie OVM (tzv. onboarding) do EWS a Vládneho SOC bude realizované kombináciou viacerých externých dodávateľov (prioritne SW nástroje) a internými zamestnancami NASES a VJ CSIRT postupnou detailnou analýzou IT infraštruktúry jednotlivých OVM, dizajnovaním, implementáciou, nasadzovaním, konfiguráciou a ladením nasadených nástrojov.
* V celom procese implementácie bezpečnostných nástrojov na OVM bude nevyhnutná participácia interných IT a bezpečnostných tímov.
* Nasadeniu nástrojov na OVM bude predchádzať podpísanie investičnej zmluvy a zmluvy o bezpečnostnom monitoringu, ktorá bude určovať rozsah monitoringu a teda aj výber nástrojov.
* Postupnosť nasadenia podľa nástrojov bude určená v podrobnom implementačnom pláne od nástrojov najmenej náročných na implementáciu po tie najzložitejšie, ktoré vyžadujú náročnejšiu analýzu a návrh.

Súčasťou etapy implementácia a testovanie vo všetkých moduloch budú aj školenia špecialistov na kybernetickú bezpečnosť na EWS, Vládnom SOC a zamestnancov na OVM zodpovedných za administráciu bezpečnostných nástrojov.

*Obrázok 11 Harmonogram realizačnej fázy projektu*

# PRÍLOHY

Dokument neobsahuje dodatočné prílohy.

**Koniec dokumentu**