V15 SW komponenty
KPB5 – Realizácia riešenia; typ – zoznam; mesiac odovzdania – M20

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY | ŽILINSKÁ UNIVERZITA V ŽILINE Fakulta riadenia a informatiky | BRAIN:IT

Zoznam komponentov

Názov komponentu	Aplikácia	Verzia	Licencia	Primárne nasadenie	Aplikačná vrstva
ELK Stack	SIEM	Release 8.x	MIT License	Docker / OpenStack (PoC)	Docker / Docker Compose
Shuffle	SOAR	Release 2.1.0	GNU Affero General Public License	Docker / OpenStack (PoC)	Docker
Wazuh	EDR	Version 4.14	GPLv2	Docker / OpenStack (PoC)	Docker
Greenbone Community edition	Skener zraniteľností	Version 24.10	Creative Commons Attribution Share Alike 4.0 International	Docker / OpenStack (PoC)	Docker
OpenCTI	CTI	Version 6.9.0	Apache 2.0 license	Docker / OpenStack (PoC)	Docker Compose
MISP	CTI	Version: 2.5.28	AGPL-3.0 license	Docker / OpenStack (PoC)	Docker Compose
GLPI	Asset management	Version 10.0.16	GPL-3.0	Docker / OpenStack (PoC)	Docker
NetBox	Asset management / IPAM/DCIM	Version 4.5	Apache 2.0 license	Docker / OpenStack (PoC)	Docker
DFIR IRIS	Ticketing	Version 2.4.20	LGPL-3.0 license	Docker / OpenStack (PoC)	Docker
DFIR IRIS	Evidencia, správa incidentov	Version 2.4.20	LGPL-3.0 license	Docker / OpenStack (PoC)	Docker
Kibana (ELK)	Reportovanie	Version 9.2.3	Apache 2.0-license	Docker / OpenStack (PoC)	Docker
Wiki.js	Znalostna databáza	Version 2.5	AGPL-v3 License	Docker / OpenStack (PoC)	Docker

Popis nástrojov

Oblasť / Funkcia (SOC)	Komponent (produkt)	Edícia / Verzia	Účel v SOCaaS	Kľúčové vlastnosti (capability)	Vstupy (zdroje dát)	Výstupy (artefakty)	Integrácie / API	Nasadenie	Uloženie dát / retencia	Prístupy & RBAC	Prevádzka (owner)	Poznámky / Riziká
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)	podľa implementácie	Centrálna agregácia, indexácia a korelácia logov + vyhľadávanie a analýza	Zber dát (Logstash ingest pipeline/data ingestion), normalizácia, korelácia udalostí, alerting, indexácia a vyhľadávanie (Elasticsearch databáza), vizualizácia (Kibana dashboards), škálovateľnosť, retencia a archivácia logov	Systémové logy, sieťové logy, logy z cloudových systémov, endpoint logy, logy z IAM systémov, aplikačné logy, Netflow, IPS/IDS systémy, syslog, Windows eventy, Wazuh alerts,...	indexy/normalizované logy, detekčné pravidlá, alerty, dashboardy, reporty, exporty dát	REST API, Beats/Agent, syslog, webhooky (podľa stacku)	self-hosted (VM/Docker/K8s)	Lokálna DB (Elasticsearch cluster), JSON logy (indexy); retencia konfigurovateľná	Používateľské roly, práva na indexy/dashboardy/alerty, práva na správu indexov, pravidiel	SOC tím (bezpečnostní analytici) + SOC manažér	Nároky na úložisko/výkon; treba riešiť životný cyklus indexov a zálohy
SOAR	Shuffle	podľa implementácie	Orchestrácia a automatizácia reakcií (playbooky), prepájanie jednotlivých komponentov v SOCaaS	Orchestrácia nástrojov (API integrácie s ostatnými SOC komponentami), automatizácia krokov a reakcie (workflow/playbooky)	Alerty zo SIEM systémov (ELK/Wazuh), alerty z EDR systémov, dáta z CTI systémov (OpenCTI/MISP), tickety z DFIR IRIS API webhooky	Spustené akcie (responce), záznamy o vykonaní, vytvorené a obohatené incidenty/tickety, výstupy z playbookov	REST API, webhooky, konektory	self-hosted (Docker/K8s)	Databáza (JSON formát), retencia konfigurovateľná	Roly pre tvorbu/spúšťanie workflow a playbookov, správu integrácií	SOC bezpečnostný inžinier+ SOC manažér	Dôležité ošetriť prístup k API kľúčom, vyššia záťaž pri paralelných playbookoch, Single point of failure pre automatizáciu
EDR	Wazuh	podľa implementácie	Endpoint monitoring/detekcie a základná reakcia + posielanie udalostí do SIEM	Ochrana a monitoring na koncových bodoch, HIPS/HIDS funkcionalita FIM, detekcie, analýza logov, audit systémov, podniknutie základných response kroky	Endpoint telemetria (procesy, služby), OS logy, aplikačné logy, FIM, integrity events	Bezpečnostné alerty, endpoint logy incident events, telemetria do SIEM, informácie o stave koncových zariadení (endpoint)	Wazuh API, integrácia na Elastic/Logstash, syslog	self-hosted (manager + agents, VM)	Wazuh indexy (JSON formát), databáza, retencia konfigurovateľná (zosúladenie so SIEM)	Roly/Používatelia (Wazuh UI/Elastic), práva na čítanie alertov, vyšetrovanie, práva na správu agentov, pravidiel	SOC tím (špecialista na EDR bezpečnosť) + SOC bezpečnostný inžinier	Vyššia záťaž na koncových zariadeniach (endpointoch), veľké množstvo logov, nastavenia privilégií na koncových hostoch
Skener zraniteľností	Greenbone Community Edition (GVM)	Community	Pravidelné skenovanie infra/servisov a reporting zraniteľností, identifikácia slabín v systémoch + podpora prioritizácie opráv (patching-u)	Skenovanie sietí, CVE skenovanie a detekcia, reporting a prioritizácia zraniteľností, hodnotenie zraniteľností (CVSS)	Informácie o aktívach (IP adresy, rozsahy, hostname), CVE/NVT feedy, prístupové údaje	Nálezy zraniteľností, reporty, exporty, zoznamy nájdených CVE, vyhodnotenie rizika (CVSS)	GMP API, exporty (CSV/XML), napojenie cez automatizáciu	self-hosted (VM/Docker)	Databáza so scan výsledkami; JSON/XML formát retencia konfigurovateľná	Používatelia/role v GVM, práva na čítanie reportov, práva na spúšťanie skenov,	SOC tím (špecialista na zraniteľnosti) + SOC manažér	Community edícia môže mať limity v aktualizáciách/komforte; treba nastaviť okná skenov a dopad na sieť, možná záťaž na sieť a skenované systémy
CTI	OpenCTI	podľa implementácie	Zber a analýza informácií o hrozbách, poskytovanie kontextu k jednotlivým incidentom. Správa, korelácia a obohacovanie alertov/incidentov.	Modelovanie hrozieb (STIX), obohacovanie dát, analýza a vizualizácia vzťahov (attack chain/attack vector/threat actor/campaign tracking), TAXII/API integrácie	Externé CTI feedy (TAXII, API), MISP, manuálne vloženie z externých zdrojov, OSINT zdroje	Model hrozieb (CTI entity, väzby, vzťahy), obohatené IOCs, exporty (STIX, TAXII), vizualizácie (grafy)	REST/GraphQL API, konektory, STIX/TAXII (podľa modulov)	self-hosted (Docker/K8s)	Databáza (napr. Elastic/Neo4j podľa setupu); retencia konfigurovateľná	Roly (RBAC)+ TLP obmedzenia	SOC tím (špecialista na CTI/ CTI analytik)	Dôležité nastaviť kvalitu zdrojov, deduplikáciu, kvôli zahľteniu úložiska;
CTI	MISP	podľa implementácie	Zber a analýza informácií o hrozbách, poskytovanie kontextu k jednotlivým incidentom. Správa, korelácia a obohacovanie alertov/incidentov.	Zdielanie atribútov/IOCs, real-time event-based CTI, automatický import/export informácií (CTI feeds), označovanie, organizácia a komunitné zdieľanie informácií (pomocou TLP), TAXII/API integrácie	IoC feedy, externé zdroje (OpenCTI platforma), malware sandbox, manuálne zadané vstupy	IoC feedy pre SIEM/SOAR/EDR, exporty STIX/JSON/CSV, CTI eventy	REST API, exporty (STIX), možné TAXII (podľa konfigurácie)	self-hosted (VM/Docker)	Databáza udalostí/atribútov (IoC eventy - JSON formát); retencia konfigurovateľná	Role-based prístup (RBAC), sharing pravidlá, TLP obmedzenia	SOC tím (špecialista na CTI/ CTI analytik)	Citlivé na správne nastavenie sharingu (čo sa môže zdieľať von),
Asset management	GLPI	podľa implementácie	Evidencia aktív, CMDB/ITSM evidencia, väzba na vlastníkov a služby	Inventarizácia hardvéru/ softvéru, CMDB, životný cyklus a riadenie aktív, možnosť vyhľadávania 'nových' aktív (discovery plugins), prepojenie na ticketing systém, prepojenie na používateľské, vlastnícke a organizačné väzby	Discovery nástroje, manuálne vstupy od používateľov, integrácia s inými asset managemnt systémymi (Netbox)	Zoznam aktív, vlastníci, vzťahy medzi aktívami, CMDB dáta, atribúty pre skeny/detekcie	REST API, import/export	self-hosted (Docker/K8s)	Databáza; relačné dáta (CMDB záznamy), retencia konfigurovateľná podľa interných pravidiel	Roly pre jednotlivé prístupy a oprávnenia, práva na správu aktív	IT/Asset tím / SOC bezpečnostný inžinier (admin)	Kvalita CMDB je kľúčová pre skeny a priorizáciu incidentov, občasné problémy so synchronizáciou pri integráciach
Asset management / IPAM/DCIM	NetBox	podľa implementácie	Evidencia a správa aktív obohatená o riadenie sieťovej infraštruktúry	Riadenie sieťových aktív a služieb, IPAM, DCIM, aktuálny centralizovaný inventár (Source of truth), modelovanie a vizualizácia topológie siete, exporty	Discovery nástroje, SNMP, manuálne vstupy, integrácia (Ansible, Terraform), CMDB (GLPI sync)	IP rozsahy, topológia siete, inventár infraštruktúry, mapovanie infraštruktúry pre SOC (API dáta/ source of truth)	REST API, webhooks	self-hosted (Docker)	Databáza; relačné dáta (IP, zariadenia, topológia), retencia konfigurovateľná podľa interných pravidiel	Roly pre jednotlivé prístupy a oprávnenia, práva na správu aktív	Network/Infra tím, IT/Asset tím / SOC bezpečnostný inžinier (admin)	Treba udržiavať aktuálnosť – inak skeny/monitoring míňajú cieľ
Ticketing	DFIR IRIS	podľa implementácie	Správa ticketov, požiadaviek a úloh SOC (triage, eskalácie, SLA), pridefovanie úloh a zodpovednosti	Case/ticket manažment, incident workflow, manažment úloh, priradenie a eskalácia incidentu, integrácia so SIEM a SOAR, vstupy do auditného hodnotenia, šablóny prípadov	Dáta o incidentoch (alerty) zo SIEM/SOAR, dôkazy (logy),CTI kontext, EDR alerty, manuálne vytvorenie vstupov	Tickety, stavy riešenia, audit trail, úlohy a workflow	API, webhooky (podľa možnosti), integrácia so SOAR	self-hosted (VM/Docker)	Databáza prípadov, JSON formát + relačné dáta; retencia konfigurovateľná	Roly (analyst/lead/admin), práva na čítanie incidentov, práva na prácu na prípade incidentu, práva na schvaľovanie	SOC tím (bezpečnostní analytici) + SOC manažér	Dôležité je jednotné pomenovanie a workflow (stavové modely), záťaž pri veľkom počte ticketov
Evidencia, správa incidentov	DFIR IRIS	podľa implementácie	Centrálna evidencia incidentov a dôkazov (case management), riadenie životného cyklu incidentov (eskalácia, dokumentácia a uzatvorenie)	Evidencia incidentov, riadenie životného cyklu incidentov, uchovávanie dôkazov a artefaktov, časová os incidentu, chain-of-custody, reporting incidentov	Exporty z ELK/Wazuh/Greenbone, tickety, dôkazy z vyšetrovania, CTI kontext, EDR artefakty	Zápisy z incidentov, evidenčné záznamy, dôkazy, export pre audit	API, import/export	self-hosted (VM/Docker)	Databáza + úložisko príloh (záznamy z incidentov + dôkazy); retencia podľa politiky	Roly (analyst/lead/admin), práva na čítanie incidentov, práva na prácu na prípade incidentu, práva na schvaľovanie	SOC tím (bezpečnostní analytici) + SOC manažér	Treba nastaviť pravidlá práce s dôkazmi a citlivými dátami, možné zahľtenie veľkým objemom dát
Reporting	Kibana (ELK)	podľa ELK	Vizualizácie, prehľady, dashboardy a reporty pre SOC tím, manažment a audit	Real-time a historické vizualizácie a dashboardy (grafy, heatmapy), export reportov, prístup na základe rolí a opravnení (role-based prístup), custom reporting	Indexy v Elasticsearch, alerty (SIEM), EDR dáta (Wazuh indexy), skeny zraniteľností, aplikačné metriky	Vizualizácie a dashboardy (grafy/ teplotné mapy), exporty reportov	REST API (Kibana/Elastic), integrácia v rámci ELK	súčasť ELK (VM/Docker/K8s)	Dáta v Elasticsearch databáze; retencia podľa SIEM politiky	Roly a oprávnenia naviazané na Elasticschearch, práva dashboardy	SOC tím (bezpečnostní analytici) + SOC manažér	Pozor na prístup k citlivým indexom; prístup k SIEM dátam, oddeliť view pre rôzne publikum
Knowledge portál	Wiki.js	podľa implementácie	Znalostná báza (runbooky, postupy, playbooky, onboarding), podpora zdieľania znalostí v time a efektívnejšieho riešenia incidentov	Uchovávanie a zdieľanie dokumentácie, verzovanie stránok,RBAC prístup, predpripravené šablóny, full-text vyhľadávanie, možnosť integrácie s inými nástrojmi	Dokumentácia SOC procesov, incident postupy, SOAR playbooky, reporty	Dokumentácia (runbooky/playbooky), informácie z predchádzajúcich incidentov (lesson learned)	LDAP/OIDC (podľa konfigurácie), API, Git sync (ak využité)	self-hosted (Docker)	Databáza + súbory (Markdown/HTML dokumenty); retencia podľa interných pravidiel	Roly (read/edit/admin), práva na čítanie, zapisovanie	SOC tím (bezpečnostní analytici) + SOC manažér	Udržiavať "single source of truth"; zaviesť proces revízie (napr. kvartálne)

Integračný tok

Oblasť / Funkcia (SOC)	Komponent (produkt)	Tok dát	Komunikačný tok (Zdroj → Cieľ)	Mechanizmus	Formát/payload	Trigger/Frekvencia	Výstup
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)	Tok do SIEM: logy, sieťové dáta, IoC z CTI Tok zo SIEM: alerty → SOAR/incident response (DFIR IRIS), dáta→ Kibana (reporting)	Tok do SIEM: Wazuh agents → Wazuh → ELK / CTI → ELK/ sieťové zariadenia → ELK Tok zo SIEM: ELK→ SOAR	Log forwarding (syslog/Beats), REST API, Elasticsearch index access, webhooky	JSON formát, ECS (Elastic Common Schema), CSV, NetFlow/IPFIX	Realtime	Indexované udalosti, centralizované a korelované logy, alerty + dashboards
SOAR	Shuffle	Tok do SOAR: alerty zo SIEM, alerty z EDR, IoC z CTI, triggers z incident response, nálezy zo skenovania zraniteľností Tok zo SOAR: akcie → EDR/sieťová infraštruktúra, ticket → ticketing, obohatené dáta z CTI → incident response	Tok do SOAR: ELK → Shuffle(SOAR), Wazuh (EDR) → Shuffle, CTI → Shuffle, skener zraniteľností → Shuffle Tok zo SOAR: Shuffle → Wazuh (EDR), Shuffle → sieťová infraštruktúra, Shuffle→ DFIR IRIS (ticketing)	REST API, webhooky, triggers	JSON/HTTP request, YAML	Realtime/event-drive (pri získaní alaertu zo SIEM/EDR)	Automatizované reakcie v rámci celého SOC cyklu
EDR	Wazuh	Tok do EDR: endpoint telemetria z koncových zariadení Tok z EDR: alerty→ SIEM/SOAR, logy→ SIEM, responce akcie → lokálny endpoint/host	Tok do EDR: Shuffle → Wazuh (EDR) Tok z EDR: Wazuh (EDR) → ELK(SIEM)	Agent-based komunikácia, log forwarding, REST API	JSON (alert), syslog	Pri alerte (zachytené pravidlo) - real time monitoring	Endpoint alerty, odozva a automatická reakcia na koncových zariadeniach
Skener zraniteľností	Greenbone Community Edition (GVM)	Tok do SZ: aktíva z asset management systému, CVE/NVT feedy Tok z SZ: reporty zraniteľností → SIEM/ticketing + incident response, nálezy -.SOAR, dáta → Kibana	Tok do SZ: GLPI/Netbox → GVM Tok z SZ: GVM → ELK, GVM → Shuffle	REST API , feed synchronizácia, export, naplánované skeny	STIX-like entity/IOC query, XML, JSON, CSV, CVE/NVT formáty	On-demand v playbooku, plánované skeny	Obohatené dáta do incidentu, zoznam zraniteľností, skóre rizík
CTI	OpenCTI	Tok do CTI: externé threat intel feedy, IoC z iných zdrojov/CTI nástrojov, incident dáta zo SIEM/ incident response Tok z CTI: obohatené dáta → SIEM/SOAR/ incident response, STIX/TAXII feed → externé CTI nástroje	Tok do CTI: MISP/ iné CTI → OpenCTI, externé zdroje → Open CTI, ELK/ DFIR IRIS → OpenCTI Tok z CTI: CTI —> ELK, CTI → Shuffle, CTI → MISP/ iné CTI	REST API, GraphQL API, STIX/TAXII, konektory	JSON, GraphQL, TAXII, STIX	On-demand v playbooku, pri relevantnom alerte	Obohatené dáta do incidentu, reputácia/tagy/IOC kontext
CTI	MISP	Tok do CTI: externé threat intel feedy, IoC z iných zdrojov/CTI nástrojov, incident dáta zo SIEM/ incident response Tok z CTI: obohatené dáta → SIEM/SOAR/ incident response, STIX/TAXII feed → externé CTI nástroje	Tok do CTI: OpenCTI/ iné CTI → MISP, externé zdroje → MISP, SIEM/ DFIR IRIS → MISP Tok z CTI: CTI —> ELK, CTI → Shuffle, CTI → OpenCTI/ iné CTI	REST API, TAXII, feed import/export	JSON, MISP formát, STIX, CSV, OpenIOC	On-demand v playbooku, pri relevantnom alerte	Obohatené dáta do incidentu, reputácia/tagy/IOC kontext
Asset management	GLPI	Tok do AM system: discovery dáta, informácie o používateľoch/ väzbách na aktíva Tok z AM system:informácie o aktívach → SIEM/SOAR/ incident response nástroje	Tok do AM system: sieťové zariadenia/endpointy → GLPI Tok z AM system:GLPI → skener zraniteľností, GLPI → ELK/Shuffle/ / DFIR IRIS	REST API, discovery agents, AD/LDAP integrácie, import/export	JSON, CSV, LDAP/AD objekty	Real-time, synchronizácia, plánované zisťovanie	Zoznam aktív a ich väzieb, CMDB dáta
Asset management / IPAM/DCIM	NetBox	Tok do AM system: aktuálne dáta o stave sieťovej infraštruktúry (sync z nástrojov/ Source of Truth),discovery dáta, informácie o používateľoch/ väzbách na aktíva, informácie o topológiach Tok z AM system: informácie o aktívach → SIEM/SOAR/ skener zraniteľností/incident response nástroje	Tok do AM system: sieťové zariadenia/endpointy → Netbox Tok z AM system:Netbox → skener zraniteľností, Netbox→ ELK/Shuffle/ DFIR IRIS	REST API,webhooky, import/export, automatizované integrácie (Ansible/ Terraform)	JSON, YAML, CSV	Real-time, synchronizácia, plánované zisťovanie	Zoznam aktív a ich väzieb, topológia sieťovej infraštruktúry, IPAM/DCIM kontext
Ticketing	DFIR IRIS	Tok do Ticketingu: alerty zo SIEM, výstupy zo SOAR, obohatené dáta z CTI, dáta z EDR/skenera zraniteľností, manuálne zadané dáta od používateľa Tok z Ticketingu:incidenty/tickety/ úlohy → incident response nástroj, spätná väzba → SIEM	Tok do Ticketingu: ELK → Shuffle→ DFIR IRIS Tok z Ticketingu:DFIR IRIS (interne vrámci systému), DFIR IRIS → SIEM	REST API, webhooky, internal workflow	JSON, HTTP payloady, rôzne druhy príloh (rôzne formáty)	Po prijatí alertu zo SIEM/SOAR, pri manuálno vytvorení ticketu	Založený ticket, prioritizácia jednotlivých ticketov, určenie zodpovednosti za riešenie
Evidencia, správa incidentov	DFIR IRIS	Tok do IR nástroja: alerty zo SIEM, výstupy zo SOAR, obohatené dáta z CTI, dáta z EDR/skenera zraniteľností, trigger z ticketing systému Tok z IR nástroja: reporty → reporting/knowledge portál, aktualizovaný stav prípadu/ ticketu v ticketing systéme, vykonané akcie v sieti automatizované/ vykonané manuálne adminstrátorom po vyhodnotení prípadu SOC analytikom	Tok do IR nástroja: DFIR IRIS (interne vrámci systému) ticketing → incident response Tok z IR nástroja: DFIR IRIS → Kibana, DFIR IRIS -> Wiki.js	REST API, workflow engine, case management system	JSON, PCAP, screenshoty, logy	Pri vzniku ticketu, SOAR trigger	Vyšetrený incident, vzniktuté reporty z priebehu vzniku a vyšetrovania bezpečnostného incidentu
Reporting	Kibana (ELK)	Tok do reporting: dáta zo SIEM/EDR/skenera zraniteľností/ incident response nástroja Tok z reporting: dashboardy/reporty → SOC tím/manažment	Tok do reporting: ELK (Elasticsearch) → ELK (Kibana), Wazuh → Kibana, GVM → Kibana, DFIR IRIS → Kibana Tok z reporting: Kibana → SOC tím/ manažment	Interné v rámci stacku (Elasticsearch queries), REST API, WEB UI	vizualizácie - JSON, Elasticsearch DLS, CSV/PDF exporty	Priebežne v pravidelných intervaloch, počas celej doby prevádzky SOC	Vizualizácie a dashboardy, operatívne reporty, reporty po analyýze incidentu
Knowledge portál	Wiki.js	Tok do KP: playbooky zo SOAR, získané znalosti/ postupy (lesson learned) z incident response Tok z KP: postupy → SOC tím (analytici), znalosti → SOAR/ ticketing+ incident response nástroj	Tok do KP: Shuffle → Wiki.js, DFIR IRIS → Wiki.js Tok z KP: Wiki.js → SOC tím (analytici), Wiki.js → Shuffle → DFIR IRIS	REST API, WEB UI, GIT integrácia	Text/runbook - Markdown jazyk, HTML, JSON	Po uzavretí bezpečnostného incidentu/bezpečnostnej udalosti	Aktualizované postupy pre riešenie incidentov