V15 SW komponenty
KPB5 – Realizácia riešenia; typ – zoznam; mesiac odovzdania – M24

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

Popis nástrojov

Oblasť / Funkcia (SOC)	Komponent (produkt)	Edícia / Verzia	Účel v SOCsaas	Kľúčové 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	ingest pipeline, normalizácia, vyhľadávanie, alerting (ak povolené), dashboards	syslog, Windows eventy, aplik. logy, sieťové prvky, cloud logy, Wazuh alerts	indexy/logy, detekčné pravidlá, alerty, dashboardy, reporty	REST API, Beats/Agent, syslog, webhooky (podľa stacku)	self-hosted (VM/Docker/K8s)	Elasticsearch storage; retencia konfigurovateľná	používateľské roly, práva na indexy/dashboards	SOC platform tím	Nároky na storage/performanciu; treba riešiť životný cyklus indexov a zálohy
SOAR	Shuffle	podľa implementácie	Orchestrácia a automatizácia reakcií (playbooky)	workflow/playbooky, automatizácia krokov, integrácie, schvaľovania (podľa flow)	alerty z ELK/Wazuh, CTI (OpenCTI/MISP), tickety z DFIR IRIS, webhooky	spustené akcie, záznamy o vykonaní, obohatené incidenty/tickety	REST API, webhooky, konektory	self-hosted (Docker/K8s)	lokálna DB/logy o behu; retencia konfigurovateľná	roly pre tvorbu/spúšťanie workflow	SOC automation/engineering	Dôležité ošetriť tajomstvá (secrets), audit a schvaľovanie zásahov
EDR	Wazuh	podľa implementácie	Endpoint monitoring/detekcie a základná reakcia + posielanie udalostí do SIEM	agent na koncových bodoch, FIM, detekcie, policy, alerting, základné response kroky	endpointy (agent), OS logy, integrity events	alerty, incident events, telemetria do SIEM	Wazuh API, integrácia na Elastic/Logstash, syslog	self-hosted (manager + agents)	Wazuh indexy/archív; retencia konfigurovateľná	roly/užívatelia (Wazuh UI/Elastic)	SOC endpoint tím	Pokrytie agentmi a správne policy sú kritické; treba riešiť onboarding/offboarding endpointov
Skener zraniteľností	Greenbone Community Edition (GVM)	Community	Pravidelné skenovanie infra/servisov a reporting zraniteľností	plánované skeny, CVE detekcia, reporty, scoring (CVSS)	IP rozsahy z NetBox, assety z GLPI, manuálne ciele	nálezy zraniteľností, reporty, exporty	GMP API, exporty (CSV/XML), napojenie cez automatizáciu	self-hosted (VM/Docker)	lokálna DB so scan výsledkami; retencia konfigurovateľná	užívatelia/role v GVM	Vulnerability mgmt	Community edícia môže mať limity v aktualizáciách/komforte; treba nastaviť okná skenov a dopad na sieť
CTI	OpenCTI	podľa implementácie	Správa a korelácia threat intelligence, obohacovanie alertov/incidentov	STIX objekty, knowledge graph, konektory, enrichment	CTI feedy, MISP, manuálne vloženie, externé zdroje	TI entity, väzby, obohatené IOCs, exporty	REST/GraphQL API, konektory, STIX/TAXII (podľa modulov)	self-hosted (Docker/K8s)	DB (napr. Elastic/Neo4j podľa setupu); retencia konfigurovateľná	roly/organizácie/práva	CTI tím	Dôležité nastaviť kvalitu zdrojov, deduplikáciu a "confidence"
CTI	MISP	podľa implementácie	Evidencia, zdieľanie a distribúcia IOCs/events, feedy pre detekcie	eventy, atribúty/IOCs, feedy, tagging, sharing	manuálne a automatické feedy, externé komunity, analýza incidentov	IOC feedy pre SIEM/SOAR/EDR, exporty STIX/JSON/CSV	REST API, exporty (STIX), možné TAXII (podľa konfigurácie)	self-hosted (VM/Docker)	DB udalostí/atribútov; retencia podľa politiky	role-based prístup, sharing pravidlá	CTI tím	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	asset registry, životný cyklus, vzťahy, (voliteľne) helpdesk moduly	onboarding aktív, importy, (voliteľne) NetBox, manuálne záznamy	zoznam aktív, vlastníci, atribúty pre skeny/detekcie	REST API, import/export	self-hosted	DB; retencia podľa interných pravidiel	roly (IT/SOC/čítanie)	IT/Asset tím	Kvalita CMDB je kľúčová pre skeny a priorizáciu incidentov
Asset management / IPAM/DCIM	NetBox	podľa implementácie	Zdroj pravdy pre IP rozsahy, zariadenia, lokality, topológiu (podklad pre skeny a monitoring)	IPAM, DCIM, inventár, vzťahy, exporty	manuálne/automatické napĺňanie infra dát	IP rozsahy pre Greenbone, mapovanie infra pre SOC	REST API, webhooks	self-hosted	DB; retencia podľa interných pravidiel	roly/práva	Network/Infra tím	Treba udržiavať aktuálnosť – inak skeny/monitoring míňajú cieľ
Ticketing	DFIR IRIS	podľa implementácie	Správa ticketov a úloh SOC (triage, eskalácie, SLA)	case/ticket workflow, priradenie, komentáre, SLA/tagy	alerty zo SIEM/SOAR, manuálne vytvorenie	tickety, stavovanie, audit trail	API, webhooky (podľa možnosti), integrácia so SOAR	self-hosted	DB prípadov; retencia konfigurovateľná	roly (analyst/lead/admin), prístup podľa case	SOC operations	Dôležité je jednotné pomenovanie a workflow (stavové modely)
Evidencia, správa incidentov	DFIR IRIS	podľa implementácie	Centrálna evidencia incidentov a dôkazov (case management)	evidovanie incidentov, artefakty, prílohy, časová os, chain-of-custody (ak používané)	tickety, dôkazy z vyšetrovania, exporty z ELK/Wazuh/Greenbone	incidentné spisy, evidenčné záznamy, export pre audit	API, import/export	self-hosted	DB + úložisko príloh; retencia podľa politiky	role-based prístup, obmedzenia na citlivé prípady	DFIR/SOC tím	Treba nastaviť pravidlá práce s dôkazmi a citlivými dátami
Reporting	Kibana (ELK)	podľa ELK	Vizualizácie, dashboardy a reporty pre SOC a management	dashboardy, vizualizácie, (voliteľne) report export	indexy v Elasticsearch	reporty, KPI dashboardy, exporty	REST API (Kibana/Elastic), integrácia v rámci ELK	súčasť ELK	dáta v Elasticsearch; retencia podľa SIEM politiky	roly/dashboards permissions	SOC reporting	Pozor na prístup k citlivým indexom; oddeliť view pre rôzne publikum
Knowledge portál	Wiki.js	podľa implementácie	Znalostná báza (runbooky, postupy, playbooky, onboarding)	verzovanie stránok, šablóny, vyhľadávanie, prílohy	dokumentácia SOC procesov, incident postupy	interná dokumentácia, runbooky	LDAP/OIDC (podľa konfigurácie), API, Git sync (ak využité)	self-hosted	DB + súbory; retencia podľa interných pravidiel	roly (read/edit/admin)	SOC knowledge owner	Udržiavať "single source of truth"; zaviesť proces revízie (napr. kvartálne)

Integračný tok

Oblasť / Funkcia (SOC)	Komponent (produkt)	Tok	Zdroj → Cieľ	Mechanizmus	Formát/payload	Trigger/Frekvencia	Výstup
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)	EDR telemetry	Wazuh agents → Wazuh → ELK	natívna integrácia / ingest	alert/event JSON	realtime	indexované udalosti + dashboards
SOAR	Shuffle	Log ingestion	Zdroje logov → ELK	syslog/Beats → Logstash	syslog/JSON	realtime/batch	centralizované logy
EDR	Wazuh	Alert → SOAR	Wazuh/ELK → Shuffle	webhook/HTTP	JSON (alert)	pri alerte	spustený workflow
Skener zraniteľností	Greenbone Community Edition (GVM)	CTI enrichment	Shuffle → OpenCTI	REST/GraphQL	STIX-like entity/IOC query	on-demand v playbooku	enrichment do incidentu
CTI	OpenCTI	IOC lookup	Shuffle → MISP	REST API	attribute/event search	on-demand v playbooku	reputácia/tagy/IOC kontext
CTI	MISP	Case creation	Shuffle → DFIR IRIS	REST API	case/ticket JSON	pri relevantnom alerte	založený ticket/case
Asset management	GLPI	Asset context	Shuffle/IRIS → GLPI	REST API	asset lookup	pri triage	owner/kritickosť/CMDB dáta
Asset management / IPAM/DCIM	NetBox	Network context	Shuffle/IRIS → NetBox	REST API/webhook	IP/device/site lookup	pri triage	IPAM/DCIM kontext
Ticketing	DFIR IRIS	Scan scope	NetBox → Greenbone	export/API	IP range/targets	plánovane	definované ciele skenu
Evidencia, správa incidentov	DFIR IRIS	Vuln findings → ticket	Greenbone → DFIR IRIS/GLPI	export/API/automatizácia	report (JSON/CSV)	po skene	remediation ticket + evidencia
Reporting	Kibana (ELK)	Reporting	ELK → Kibana	interné v rámci stacku	vizualizácie	priebežne	KPI/operatívne reporty
Knowledge portál	Wiki.js	Knowledge	DFIR IRIS → Wiki.js	manuálne alebo API	text/runbook	po uzavretí	aktualizované postupy