V1S SW components
KPI10 – Implementation of the solution; type – list; delivery month – M24

Funded by the European Union NextGenerationEU
RECOVERY AND RESILIENCE
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC
UNIVERSITY OF ŽILINA Faculty of Management Science and Informatics
BRAIN:IT

List of components

Component name	Application	Version	Licence	Location
ELK Stack	SIEM	Release 8.x	MIT License	Kubernetes
Shuffle	SOAR	Release 2.1.0	GNU Affero General Public License	Kubernetes
Wazuh	EDR	Version 4.14	GNU	Kubernetes
Greenbone Community edition	Vulnerability scanner	Version 24.10	Creative Commons Attribution Share Alike 4.0 International	Kubernetes
OpenCTI	CTI	Version 6.9.0	Apache License, Version 2.0	Kubernetes
MISP	CTI	Version: 2.5.28	AGPL-3.0 license	Kubernetes
GLPI	Asset management	Version 10.0.16	GPL-2.0	Kubernetes
NetBox	Asset management / IPAM/DCIM	Version 4.5	Apache 2.0-license	Kubernetes
DFIR IRIS	Ticketing	Version 2.4.20	LGPL-3.0 license	Kubernetes
DFIR IRIS	Incident recording and management	Version 2.4.20	LGPL-3.0 license	Kubernetes
Kibana (ELK)	Reporting	Version 9.2.3	Apache 2.0-license	Kubernetes
Wiki.js	Knowledge database	Version 2.5	AGPL-v3 License	Kubernetes

Description of tools

Area / Function (SOC)	Component (product)	Edition / Version	Purpose in SOC/cases	Key capabilities	Inputs (data sources)	Outputs (artefacts)	Integrations / API	Deployment	Data storage / retention	Access & RBAC	Operation (owner)	Notes / Risks
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)	depending on the implementation	Central aggregation, indexing and correlation of logs + search and analysis	ingest pipeline, normalization, search, alerting (if enabled), dashboards	syslog, Windows events, application logs, network elements, cloud logs, Wazuh alerts	indices/logs, detection rules, alerts, dashboards, reports	REST API, Beats/Agent, syslog, webhooks (depending on the stack)	self-hosted (VM/Docker/K8s)	Elasticsearch storage; configurable retention	user roles, permissions for indices/dashboards	SOC platform team	Storage/performance demands; the index life cycle and backups need to be addressed
SOAR	Shuffle	depending on the implementation	Orchestration and automation of responses (playbooks)	workflows/playbooks, automation of steps, integrations, approvals (depending on the flow)	alerts from ELK/Wazuh, CTI (OpenCTI/MISP), tickets from DFIR IRIS, webhooks	executed actions, execution records, enriched incidents/tickets	REST API, webhooks, connectors	self-hosted (Docker/K8s)	local DB/run logs; configurable retention	roles for creating/running workflows	SOC automation/engineering	It is important to handle secrets, auditing and approval of interventions
EDR	Wazuh	depending on the implementation	Endpoint monitoring/detections and basic response + sending events to the SIEM	endpoint agent, FIM, detections, policy, alerting, basic response steps	endpoints (agent), OS logs, integrity events	alerts, incident events, telemetry to SIEM	Wazuh API, integration with Elastic/Logstash, syslog	self-hosted (manager + agents)	Wazuh indices/archive; configurable retention	roles/users (Wazuh UI/Elastic)	SOC endpoint team	Agent coverage and correct policies are critical; onboarding/offboarding of endpoints needs to be addressed
Vulnerability scanner	Greenbone Community Edition (GVM)	Community	Regular scanning of infrastructure/services and vulnerability reporting	scheduled scans, CVE detection, reports, scoring (CVSS)	IP ranges from NetBox, assets from GLPI, manual targets	vulnerability findings, reports, exports	GMP API, exports (CSV/XML), connection via automation	self-hosted (VM/Docker)	local DB with scan results; configurable retention	users/roles in GVM	Vulnerability mgmt	The Community edition may have limitations in updates/convenience; scan windows and impact on the network need to be set
CTI	OpenCTI	depending on the implementation	Management and correlation of threat intelligence, enrichment of alerts/incidents	STIX objects, knowledge graph, connectors, enrichment	CTI feeds, MISP, manual input, external sources	TI entities, relationships, enriched IOCs, exports	REST/GraphQL API, connectors, STIX/TAXII (depending on modules)	self-hosted (Docker/K8s)	DB (e.g. Elastic/Neo4j depending on the setup); configurable retention	roles/organizations/permissions	CTI team	It is important to set source quality, deduplication and "confidence"
CTI	MISP	depending on the implementation	Recording, sharing and distribution of IOCs/events, feeds for detections	events, attributes/IOCs, feeds, tagging, sharing	manual and automatic feeds, external communities, incident analysis	IOC feeds for SIEM/SOAR/EDR, STIX/JSON/CSV exports	REST API, exports (STIX), possibly TAXII (depending on configuration)	self-hosted (VM/Docker)	event/attribute DB; retention according to policy	role-based access, sharing rules	CTI team	Sensitive to correct sharing settings (what may be shared externally)
Asset management	GLPI	depending on the implementation	Asset records, CMDB/ITSM records, links to owners and services	asset registry, life cycle, relationships, (optionally) helpdesk modules	asset onboarding, imports, (optionally) NetBox, manual records	list of assets, owners, attributes for scans/detections	REST API, import/export	self-hosted	DB; retention according to internal rules	roles (IT/SOC/read)	IT/Asset team	CMDB quality is key for scans and incident prioritization
Asset management / IPAM/DCIM	NetBox	depending on the implementation	Source of truth for IP ranges, devices, sites, topology (basis for scans and monitoring)	IPAM, DCIM, inventory, relationships, exports	manual/automatic population of infrastructure data	IP ranges for Greenbone, infrastructure mapping for the SOC	REST API, webhooks	self-hosted	DB; retention according to internal rules	roles/permissions	Network/Infra team	Must be kept up to date – otherwise scans/monitoring miss their target
Ticketing	DFIR IRIS	depending on the implementation	Management of SOC tickets and tasks (triage, escalations, SLA)	case/ticket workflow, assignment, comments, SLA/tags	alerts from SIEM/SOAR, manual creation	tickets, status tracking, audit trail	API, webhooks (where possible), integration with SOAR	self-hosted	case DB; configurable retention	roles (analyst/lead/admin), access per case	SOC operations	Uniform naming and workflow (state models) are important
Incident recording and management	DFIR IRIS	depending on the implementation	Central recording of incidents and evidence (case management)	recording of incidents, artefacts, attachments, timeline, chain-of-custody (if used)	tickets, evidence from investigations, exports from ELK/Wazuh/Greenbone	incident files, records, export for audit	API, import/export	self-hosted	DB + attachment storage; retention according to policy	role-based access, restrictions on sensitive cases	DFIR/SOC team	Rules for handling evidence and sensitive data need to be set
Reporting	Kibana (ELK)	as per ELK	Visualizations, dashboards and reports for the SOC and management	dashboards, visualizations, (optionally) report export	indices in Elasticsearch	reports, KPI dashboards, exports	REST API (Kibana/Elastic), integration within ELK	part of ELK	data in Elasticsearch; retention according to SIEM policy	roles/dashboards permissions	SOC reporting	Beware of access to sensitive indices; separate views for different audiences
Knowledge portal	Wiki.js	depending on the implementation	Knowledge base (runbooks, procedures, playbooks, onboarding)	page versioning, templates, search, attachments	documentation of SOC processes, incident procedures	internal documentation, runbooks	LDAP/OIDC (depending on configuration), API, Git sync (if used)	self-hosted	DB + files; retention according to internal rules	roles (read/edit/admin)	SOC knowledge owner	Maintain a "single source of truth"; introduce a review process (e.g. quarterly)

Integration flow

Area / Function (SOC)	Component (product)	Flow	Source + Target	Mechanism	Format/payload	Trigger/Frequency	Output
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)	EDR telemetry	Wazuh agents + Wazuh + ELK	native integration / ingest	alert/event JSON	real time	indexed events + dashboards
SOAR	Shuffle	Log ingestion	Log sources + ELK	syslog/Beats + Logstash	syslog/JSON	real time/batch	centralized logs
EDR	Wazuh	Alert + SOAR	Wazuh/ELK + Shuffle	webhook/HTTP	JSON (alert)	on alert	triggered workflow
Vulnerability scanner	Greenbone Community Edition (GVM)	CTI enrichment	Shuffle + OpenCTI	REST/GraphQL	STIX-like entity/IOC query	on demand in the playbook	enrichment into the incident
CTI	OpenCTI	IOC lookup	Shuffle + MISP	REST API	attribute/event search	on demand in the playbook	reputation/hits/IOC context
CTI	MISP	Case creation	Shuffle + DFIR IRIS	REST API	case/ticket JSON	on a relevant alert	created ticket/case
Asset management	GLPI	Asset context	Shuffle/IRIS + GLPI	REST API	asset lookup	during triage	owner/criticality/CMDB data
Asset management / IPAM/DCIM	NetBox	Network context	Shuffle/IRIS + NetBox	REST API/webhook	IP/device/site lookup	during triage	IPAM/DCIM context
Ticketing	DFIR IRIS	Scan scope	NetBox → Greenbone	export/API	IP ranges/targets	scheduled	defined scan targets
Incident recording and management	DFIR IRIS	Vuln findings + ticket	Greenbone + DFIR IRIS/GLPI	export/API/automation	report (JSON/CSV)	after the scan	remediation ticket + record
Reporting	Kibana (ELK)	Reporting	ELK + Kibana	internal within the stack	visualizations	continuously	KPI/operational reports
Knowledge portal	Wiki.js	Knowledge	DFIR IRIS + Wiki.js	manually or API	text/runbook	after closure	updated procedures