supporting document for V5
linked to KPB2

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

Category	Subcategory	Requirement	ELK Stack	Wazuh	OpenSearch + OpenSearch Dashboards	Graylog (Open)	SIEMonster (Community Edition)	Prelude OSS	AlienVault OSSIM
Functional requirements	Data collection and processing	Supported log formats (syslog, JSON, CSV, CEF, LEEF...)	Supports a wide range of log formats including syslog, JSON, CSV, CEF and others via Logstash and Beats.	Fully supports all common log formats including syslog, JSON, CSV, CEF, LEEF.	Supports a wide range of formats including syslog, JSON, CSV and CEF. Import is often performed via Logstash or an agent.	Supports a wide range of log formats including syslog, JSON and CEF.	Supports a wide range of log formats including syslog, JSON and CEF.	Primarily IDMEF and syslog, limited support for other formats.	Supports a wide range of log formats including syslog, JSON and CEF.
		Supported types of audit logs (e.g. via Auditbeat)	Full support via Auditbeat for audit logs from Linux and Windows systems.	Supports audit logs via its own agent as well as integration with tools such as Auditbeat.	Supported through integration with Beats (Auditbeat, Filebeat), which collect audit records from systems.	Basic support for audit logs, often via external agents.	Basic support for audit logs, often via external agents.	Limited native support, suitable for manual connection.	Basic support for audit logs, often via external agents.
		Supported types of event logs (e.g. via Auditbeat)	Event logs can be collected via Auditbeat and Winlogbeat, including system events and security records.	Event logs are processed via the agent, and both Windows and Linux sources are supported.	Event logs can be processed from multiple system sources via Beats and enriched in the pipeline.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Supported types of system logs (e.g. journald, syslog, dmesg)	Collection of system logs such as journald, syslog and dmesg is supported via Filebeat or Logstash modules.	Full support for system logs such as journald, syslog, dmesg – collected via the agent.	Collection of data from system logs such as syslog, journald or dmesg using log agents such as Filebeat.	Supports a wide range of log formats including syslog, JSON and CEF.	Supports a wide range of log formats including syslog, JSON and CEF.	Primarily IDMEF and syslog, limited support for other formats.	Supports a wide range of log formats including syslog, JSON and CEF.
		How data can be collected (protocol, API, agent, agentless, webhook...)	Data can be collected via an agent (Beats), an agentless approach, REST API, webhooks, or direct log-forwarding protocols.	Data can be collected via the Wazuh agent, but also via agentless modes, API and webhooks.	Supports data collection via an agent (Beats), agentless via syslog, as well as REST API and webhooks.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Real-time vs. batch processing	Supports both real-time stream processing of logs and batch processing of historical data.	Real-time processing – logs are analysed immediately upon receipt.	OpenSearch supports real-time indexing and data streaming. Batch processing is available via the ingest pipeline.	Supports real-time processing with minimal latency.	Supports real-time processing with minimal latency.	Supports real-time processing with minimal latency.	Supports real-time processing with minimal latency.
		Supported protocols (SNMP, Syslog, NetFlow/IPFlow...)	Protocols such as Syslog and NetFlow are supported via the relevant Logstash plugins and Beats modules.	Supports standard protocols such as SNMP, Syslog, NetFlow and others through integrations.	Logs can be obtained via SNMP, Syslog and NetFlow using external modules or log pipeline tools.	Supports a wide range of log formats including syslog, JSON and CEF.	Supports a wide range of log formats including syslog, JSON and CEF.	Primarily IDMEF and syslog, limited support for other formats.	Supports a wide range of log formats including syslog, JSON and CEF.
	Analysis and detection	Real-time analysis	Elasticsearch enables real-time data processing, including event correlation and instant search.	Yes, it supports continuous real-time analysis of incoming data.	Real-time analysis is a core functionality of OpenSearch. Visualizations and queries are updated instantly.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Event correlation (predefined and custom rules)	Correlation is possible via custom rules (Elastic Detection Engine) or integration with ElastAlert and other tools.	It includes an event correlation engine supporting both custom and predefined rules.	Supports both custom and predefined rules using the Alerting plugin or integration with Sigma rules.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Machine Learning/Behavioural analysis	The ML module (X-Pack) provides behavioural analysis and anomaly detection using ML algorithms.	Basic support for behavioural analysis – not ML, but based on rules and behaviour.	Machine learning is available via the ML Commons plugin, but requires additional configuration. Suitable for anomaly detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.
		Threat Intelligence (CTI) integration	Integration with CTI is possible via the Threat Intel module, which supports, for example, enrichment of IOCs from external sources.	Integrates with CTI such as OTX, VirusTotal and MISP for alert enrichment.	Integration with CTI is possible – OpenCTI, MISP or Threat Intel feeds can be aggregated and visualized.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Anomaly detection	Anomalies are detected using ML Jobs or threshold rules in the Detection engine.	Anomaly detection is possible on the basis of behavioural rules and CTI.	Using the ML Commons plugin and custom rules, behaviour that deviates from the norm can be detected.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Support for MITRE ATT&CK mapping	Elastic Security provides basic mapping of detections to MITRE ATT&CK techniques.	Mapping to MITRE ATT&CK is natively supported in correlation.	Manual option for mapping to MITRE ATT&CK, often implemented via external tools or custom dashboards.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Alerting and response	Custom alerting rules and thresholds	Supports the creation of custom alerts, including complex conditions, thresholds, time windows and filters.	Allows the configuration of custom rules, thresholds and responses to events.	Supports complex custom alerting rules via the Alerting module. Thresholds, logic and filters can be defined.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Escalation workflow	The Elasticsearch stack enables a simple escalation workflow using Alerting Rules.	Support for workflows and escalations via rules and notification systems.	Workflow is possible using triggers and action groups. Although it is not a fully fledged SOAR, it can escalate events.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Automated responses (e.g. IP blocking, SOAR integration)	Responses can be performed through integration with SOAR systems or Elastic Actions (e.g. HTTP hook).	Responses such as blocking an IP, running scripts or integration with SOAR are possible.	Supports integration actions – HTTP requests, webhooks – which allow responses to be triggered based on conditions.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Notifications for various platforms (e-mail, Teams,...)	Notifications can be sent via e-mail, MS Teams, Slack or webhook using Alerting modules.	Notifications via e-mail, Slack, Teams and webhooks are supported.	Notifications can be routed to e-mail, Slack, Teams and other platforms using webhooks.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Sending notifications to e-mail, MS Teams, Jira, The Hive	Full support for sending to MS Teams, Jira, The Hive using webhooks or Elastic Actions.	Yes, with the option to configure targets such as e-mail, Jira, MS Teams, The Hive.	Through an extension or using external orchestrators, alerts can be sent to The Hive, Jira and other systems.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Possibility of detailed alert configuration (description, subject, time window, filters, thresholds, logic, severity, score, tags)	Alerts allow advanced settings – conditions, ranges, metadata and scoring logic.	Very detailed options for defining conditions, time windows, scores, thresholds, etc.	High customizability – the user can set detailed conditions for alerts, including scores and weights.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Default rule set – predefined in the tool	Elastic contains basic rules for detecting the most common attacks and techniques.	Contains its own rule package for various types of events.	OpenSearch does not include preset 'security rules'; the user creates monitors and triggers manually.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Possibility of using secondary rule sources (e.g. Sigma rules)	Community rules such as Sigma can be used and imported into Elastic using conversion tools.	Supports the use of rules from external sources such as Sigma.	OpenSearch supports external rules such as Sigma and others via community plugins or custom imports.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Computational performance demands	Computationally demanding – the Elastic stack requires considerable resources with higher log volumes and complex rules.	Demands are moderate – the system handles large volumes of data, but needs optimization.	Computationally demanding with large datasets. Horizontal scaling is recommended under higher load.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Use of Machine Learning-based rules in anomaly detection	ML detections support rule creation using behaviour analysis algorithms.	Does not use ML directly – analysis is performed on the basis of rules, not learning.	ML Commons allows machine learning models to be used directly in anomaly or behaviour detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.	Does not support advanced ML models for detection.
		Possibility of mapping rules to the MITRE ATT&CK framework	Mapping of detections to MITRE ATT&CK is implemented within Elastic Security rules.	Established mapping of rules to the MITRE ATT&CK model is a direct part of the solution.	Manual mapping of alerts and outputs to MITRE ATT&CK is possible via custom tagging and dashboards.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Reporting and visualization	Predefined vs. custom reports	Enables the creation of custom and predefined reports via Kibana Canvas or the Reporting plugin.	Enables the generation of basic and custom reports through extensions.	Possibility of defining custom reports via Dashboards with output to various formats. Overviews are exportable.	Strong visualization support with interactive dashboards and charts.	Visualization possible via the integrated Elastic or Grafana.	Limited visualization or dependent on external tools.	Limited visualization or dependent on external tools.
		Dashboards (including interactive ones) and their categorization	Dashboards are highly customizable and interactive.	Dashboards are available via its own UI as well as via integration with Kibana.	OpenSearch Dashboards enables the creation of advanced interactive panels for monitoring and analysis.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Exporting to various formats (PDF, CSV)	Export to CSV, PDF or via API – via the Reporting plugin or scripts.	Data export to PDF, CSV and JSON is possible via interfaces and tools.	Exporting to CSV and PDF using plugins. Support is native or via community extensions.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Roles and permissions	Access roles are managed via Kibana Spaces, RBAC support.	Support for role-based access control (RBAC) – different levels of access.	RBAC support – access levels can be defined based on roles directly in the interface.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Possibility of creating templates for dashboards	Possibility of creating visual dashboard templates via Canvas or Lens.	Possibility of creating dashboard templates and reusing visualizations.	The user can create dashboard templates and quickly replicate them across organizations.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
Technical requirements	HW and SW requirements	RAM, CPU, disk, GPU	Recommended minimum of 8–16 GB RAM, 4+ CPU cores; demands increase with data volume.	Recommended configuration: min. 8 GB RAM, 4 vCPU, SSD disk (50+ GB).	A minimum of 16 GB RAM, a multi-core CPU and sufficient disk space (SSD preferred) is recommended.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Supported OS (Linux, Windows)	Linux and Windows servers are fully supported as both host systems and endpoints.	Linux (server), Windows/Linux/macOS (agent) – broad cross-platform support.	Supports most Linux distributions, and Windows and macOS as the client environment for Dashboards.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Virtualization option	The Elastic stack is fully virtualizable (VMware, Proxmox) as well as containerizable (Docker, Kubernetes).	Supports virtualization (VM, Docker) as well as containers in Kubernetes.	It is suitable for containers, VMs and physical servers. Docker and Helm installations exist for Kubernetes.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Integrations	XDR, CTI, SOAR, EDR, IAM, NAC, IDS/IPS, cloud (AWS, Azure, GCP)	Supports a wide range of integrations – AWS, Azure, GCP, EDR, SOAR, CTI, XDR, IAM, IDS/IPS.	Integrates with tools such as AlienVault OTX, Suricata, OSSEC, AWS GuardDuty.	Has a large number of available integrations with third-party tools – including CTI, SIEM, IAM and cloud services.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		API (RESTful, Webhook, gRPC...)	Comprehensive RESTful API for all services (Elasticsearch, Kibana, Logstash). Webhook	Support for REST API and webhooks for both inputs and outputs.	Support for REST API, webhooks, integration with the Elastic API, and community plugins for extending functionality.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Data layer (Database)	Data normalization and enrichment	Data are enriched via the ingest pipeline, the Filebeat module and Logstash filter plugins.	CTI data and logs are enriched and normalized before further processing.	Data are normalized using the ingest pipeline. Enrichment can be handled via Logstash or Beats.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Full-text and fast search	Full-text search is one of the main features of Elasticsearch and is extremely fast.	Elasticsearch enables fast and complex search via the UI or API.	High-performance search and aggregations via the Elasticsearch engine. Support for full-text and fuzzy queries.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Compression, archiving	Elastic supports various data archiving and compression modes, including hot/warm storage tiers.	Supports compression and archiving of old data.	OpenSearch allows data archiving, retention and compression policies to be defined according to log type.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Retention (flexible, by log type)	Data retention is configurable according to the index policy or data type (e.g. 30 days for firewall logs).	Support for defining data retention based on data type.	Flexible log retention – the user defines how long different types of logs will be kept.	Support for log retention according to data type and business rules.	Support for log retention according to data type and business rules.	Support for log retention according to data type and business rules.	Support for log retention according to data type and business rules.
	Security	Encryption (both in transit and at rest)	Encryption is available in transit (TLS) as well as at rest Supported via OS/infra (dm-crypt, cloud BYOK)	Support for TLS/SSL for transmissions and data encryption in Elasticsearch.	Encryption at the TLS level (in transit) and on disk (file-based encryption via the OS or cloud services).	Encryption in transit and in some cases also at rest is available.	Encryption in transit and in some cases also at rest is available.	Encryption in transit and in some cases also at rest is available.	Encryption in transit and in some cases also at rest is available.
		RBAC and multi-factor auth	RBAC system in Kibana and support for SAML/LDAP; MFA, however, is available in the Elastic Cloud service, where it is mandatory for access to Elastic Cloud accounts (e.g. TOTP, e-mail, hardware keys	RBAC and support for multi-factor authentication via external services.	RBAC support in Dashboards, support for external identities (LDAP, SAML, OIDC). MFA can be integrated.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Audit trail and data integrity	An audit trail is available via Audit logging in Elasticsearch and Kibana.	Records every analyst action for auditing and forensic analysis.	All changes and accesses can be audited using custom audit log plugins.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
Operational requirements	Administration	UI/UX (clarity, responsiveness)	Modern interface in Kibana – responsive, modular and supports dark/light modes.	User-friendly web interface with reactive components.	The Dashboards interface is modern, responsive and supports dark/light mode. The UX is of a high standard.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		CLI/API support	CLI and API are available for all main services – Elasticsearch, Kibana, Beats, Logstash.	Full CLI and API support for both administration and integration.	CLI and REST API supported. Scripts can perform all main tasks (query, export, settings).	CLI and API support available for administration and integrations.	CLI and API support available for administration and integrations.	CLI and API support available for administration and integrations.	CLI and API support available for administration and integrations.
		Multitenancy (customer isolation)	Multitenancy is supported via Kibana Spaces and role-based security.	Supports multi-tenant separation of customers through RBAC and the UI.	Multitenancy possible via Dashboards spaces or isolated indices with RBAC access control.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Operability	Installation and configuration	Elastic has detailed installation packages, containers and a Helm chart for K8s.	Installation is possible using scripts, containers or distribution packages.	Installation is more complex, but well documented. Docker, Kubernetes and Helm are supported.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		System health monitoring (healthcheck)	Cluster monitoring is available via Stack Monitoring or external systems (e.g. Prometheus).	Supports automated health checks via both the API and the interface.	System health can be monitored via the API, Grafana or custom visualizations in Dashboards.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Backup & recovery	Backup and recovery possible via the Snapshot & Restore feature of Elasticsearch.	Backup of configurations and databases is fully supported.	Backup and recovery are handled using snapshots in Elasticsearch. They can be scheduled and automated.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
		Support, community and documentation	Large community and extensive official documentation with examples and tutorials.	Very active community, excellent documentation and an open-source model.	The OpenSearch community is active, the documentation is extensive, and there are numerous guides and a forum.	Large and active community, available documentation and forum.	Smaller community, but basic documentation available.	Smaller community, but basic documentation available.	Smaller community, but basic documentation available.
		Updates and versioning	Elastic releases regular updates and supports versioning with minimal downtime.	Regular updates of the system and detection rules.	Index management policies – fully supported via ISM (Index State Management). Scheduled system updates – via rolling/restart upgrade.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Deployment	Bare metal, VM, Docker, Kubernetes	Can be deployed on bare metal, in a VM, in Docker containers or in a Kubernetes environment.	Support for all deployment modes, including Kubernetes and Docker.	Installation packages are available for bare metal, containers and Kubernetes clusters.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Scaling	Load balancing, HA, clustering	Elastic supports both horizontal (more nodes) and vertical (more powerful HW) scaling, as well as clustering.	Possibility of horizontal scaling and HA clustering.	Supports clustering, load balancing and HA architecture for scalable deployment.	Limited scaling options.	Good scaling options, including support for clustering and HA.	Limited scaling options.	Limited scaling options.
	Extensibility	Extensibility through plugins	Logstash, Kibana and Elasticsearch support a plugin architecture for extensibility.	Plugin system for extension with additional functionality.	Possibility of extending functionality via plugins developed both by the community and by Amazon.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Automation	Automation (scripts, playbooks)	Automation via Watcher, Elastic Actions, scripts, or integration with SOAR such as Shuffle.	Supports scripting as well as external playbooks (e.g. Ansible, SOAR).	Automation via API, trigger-based alerting and options for connecting to orchestrators (e.g. StackStorm).	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Regulatory compliance	GDPR, ISO 27001, PCI DSS,...	Support for GDPR, ISO 27001 and others – in combination with logging, retention and audit trail.	Helps in achieving GDPR, ISO and NIST standards through auditing and logging.	OpenSearch can be configured to meet the requirements of GDPR, ISO, SOC2 and other regulatory frameworks.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.	Partial or dependent support; requires additional configuration.
	Licensing	Licence type (open-source, freemium, commercial)	Elastic has its own licence (SSPL) – the core is open-source, some features are in the Basic/Free edition.	Fully open-source solution without a commercial licence.	Open-source licence under Apache 2.0. No restrictions on core functionality.	Fully open-source with no licence fees.	Fully open-source with no licence fees.	Fully open-source with no licence fees.	Fully open-source with no licence fees.
	Costs	TCO, maintenance demands	Infrastructure costs are high (compute resources, storage), but the software is free in the basic version.	Moderately high infrastructure costs, but low licensing costs.	Low licensing costs, but a higher TCO with complex integrations and the need for one's own infrastructure. Open-source solution with low licensing costs. Higher overall maintenance demands for large-scale installations, given the resource requirements and the expertise needed to administer and scale the system.	No licence fees, but higher integration and operational demands.	No licence fees, but higher integration and operational demands.	Higher administration and maintenance demands, some modules outdated.	Higher administration and maintenance demands, some modules outdated.

supporting document for V5
linked to KPB2

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

Category	Subcategory	Requirement	Threat intel module (ELK)	MISP	OpenCTI	IntelMQ	YETI	Vulmatch
Functional requirements	Types of CTI	Support for strategic CTI (reports, impact analyses, attack trends)	Support only for limited strategic analysis – depends on integrations with external tools or third-party plugins.	MISP provides partial support for strategic CTI through manual entry of reports and analytical notes.	OpenCTI provides comprehensive support for strategic CTI, enabling analytical assessments and relationships.	The tool is oriented towards the collection and distribution of technical data, while strategic CTI is not at the centre of its focus.	YETI focuses mainly on operational and tactical CTI; the strategic level is poorly supported.	Focuses mainly on automated matching of IOCs and CVEs; strategic CTI is not supported.
		Support for operational CTI (TTPs, group profiling)	Does not provide direct support for TTPs or group profiling, but logical add-ons and correlation rules can be used.	Support for operational CTI is strong – MISP allows TTPs to be recorded and incidents to be linked to groups.	Very good support for TTPs, organizations, actors and campaigns, including relationships and timelines.	Support for operational CTI is limited; most of the functionality is focused on IOCs and technical enrichment.	Yes, it provides the ability to profile threat actors and TTPs, although not entirely formally according to ATT&CK.	Does not provide advanced functionality for TTPs or attacker profiling.
		Support for tactical CTI (IOCs, IPs, hashes, URLs, domains)	Good basis for IOCs – through custom indexing and dashboards in Kibana, IOCs can be stored and visualized.	MISP is designed to manage IOCs such as IP addresses, hashes, domains and other artefacts.	IOC support is comprehensive – OpenCTI handles IPs, hashes, domains, URLs and other artefacts.	Full support for tactical CTI – IOCs such as IPs, hashes and URLs are the main domain of IntelMQ.	Supports IOCs – IPs, hashes, URLs and domains are the primary entities.	Basic functionality – technical IOC and CVE matching.
	Data collection	Automated collection from open-source, community and internal sources	Limited capability – some data can be pulled via plugins and API, but native processing specialized for CTI is lacking.	Supports a wide range of open-source and community sources. Automation is possible using cron jobs and the API.	Features advanced data collection using connectors that allow multiple types of sources to be connected.	Automated data collection from various open-source sources is the main functionality of IntelMQ.	Collection from community and open-source sources is possible using scrapers and plugins.	Data collection is possible from several sources, but depends on the implementation.
		Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Depends on what the user configures – some of these sources can be integrated via Logstash and external connectors.	MISP has native support for Abuse.ch, Malware Bazaar and others through integrated modules.	Native connectors for Abuse.ch, Malware Bazaar, MISP and OTX ensure a high-quality data supply.	Supports numerous sources via modules, including Abuse.ch, MISP and others.	Has several available connectors for MISP, Abuse.ch, Malware Bazaar and others.	Partial support for sources such as MISP and VulDB.
		Integration with 3rd party services such as VirusTotal, Shodan, DomainTools, URLScan.io	Support depends on plugins such as ElastAlert or custom linking scripts – it is not ready-made functionality.	Supports integration with external services such as VirusTotal, Shodan and others via modules.	Connectors for VirusTotal, Shodan, DomainTools and other external sources are available.	Integration with external services such as VirusTotal is possible via extensions.	Integrations with external APIs are possible, but require custom integrations.	Integration with APIs such as Shodan or VirusTotal is not directly available.
	Normalization	Ability to normalize CTI data into a unified format	The tool is not primarily intended for CTI normalization, but data can be transformed using Logstash and pipelines.	The ability to normalize data into a STIX-like structure is excellent. Records have a standardized format.	Normalization takes place at the level of entities and relationships in accordance with the STIX 2.1 standard.	IntelMQ has a strong ability to normalize technical data into a unified structure (Message format).	Data normalization takes place at the level of entities and tags – moderately advanced functionality.	Data normalization is not fully supported.
	Processing	Possibility of manual CTI analysis	Enables manual analysis via Kibana and Elasticsearch, but is not intended for comprehensive threat analysis.	Enables manual analysis of IOCs and related threats. Analysts can enter their own assessments.	The GUI allows analysts to work with data manually and add comments and assessments.	Enables simple manual analysis via the CLI or external visualization tools.	Analysts can perform manual IOC analysis in the UI.	The tool does not include a visual interface for manual analysis.
		Semi-automated or fully automated processing and unification of data	The Threat Intel module offers only **partially semi-automated data processing** based on configurable pipelines (e.g. ingest pipeline or Logstash rules)	MISP enables semi-automated processing using event-action rules.	Automatic enrichment using connectors is possible, as is the consolidation of data from various sources.	The strength of IntelMQ is automated processing using a pipeline system (bots).	Supports automatic imports of IOCs and entities, semi-automatic enrichment.	Automated processing of CVE/IOC matching is the main functionality.
		Support for automated playbooks (low-code/no-code)	Support for workflows or data processing via playbooks is limited, available only via integrations or custom scripts.	It is possible to set up some tasks as a workflow, but it is not a low-code system.	Playbook support via connectors (e.g. low-code tools such as TheHive or MISP).	Does not support low-code/no-code playbooks, but the workflow is modular.	Does not support playbooks in the true sense – it is rather a database of IOCs and entities.	Does not support playbooks.
		Deduplication of threats and information	Deduplication is possible using Elastic functions, but it is not specifically focused on threats – it requires advanced configuration.	Deduplicates IOCs based on UUID and type – prevents repeated entries.	The system contains mechanisms for deduplicating entities and IOCs based on identifiers.	Partial deduplication using custom data processing logic.	Partially enables deduplication of IOCs based on hashes and identifiers.	Does not include threat deduplication.
	Integration	Integration with SIEM and firewall for use in automated detections	The possibility of connecting to other security systems such as SIEM and firewalls exists, but requires configuration.	Integration with SIEM and firewalls is common, using the REST API and MISP feeds.	Integration with SIEM via export connectors or direct access to the database via the GraphQL API.	Can be integrated with SIEM (e.g. by exporting data via JSON, syslog).	Integration into SIEM and other tools is possible, but often requires manual exports.	Simple integration with SIEM possible by exporting IOCs.
	Sandboxing	Possibility of testing IOCs and files in a sandbox environment	The tool does not have its own sandboxing capabilities – it must be supplemented with other tools.	Does not support sandboxing – file testing must be done via an external system.	Sandboxing is not integrated, but integration with Cuckoo or JoeSandbox is possible.	Does not provide sandboxing – integration with external sandbox tools is required.	Does not support sandboxing.	A sandbox is not part of the tool.
Technical requirements	Visualization	Visualization of threat intelligence data (Kibana, charts, dashboards)	Kibana provides strong visualization, including charts, heatmaps and timelines – advantageous for IOC and temporal analyses.	Supports basic visualization using built-in statistical overviews and charts.	Interactive visualizations – graphs of entities and their relationships, timelines and statistics.	Visualization is not built in – requires integration with Kibana, Grafana or ELK.	Contains its own dashboards and simple visualization components.	Does not provide its own visualizations.
	Frameworks	Mapping to MITRE ATT&CK for TTP analysis and team collaboration	Possibility of partial mapping using dashboards or custom fields, but without a native MITRE framework.	MISP has a module for linking to the MITRE ATT&CK system using Galaxy tags.	Full integration with MITRE ATT&CK – the TTP entity is a fundamental building block.	Does not support the MITRE ATT&CK framework directly.	Does not support MITRE ATT&CK, but allows manual tagging of TTPs.	Does not support the ATT&CK framework.
	Formats and standards	Support for formats such as STIX/TAXII	STIX/TAXII is not supported natively – it needs to be handled through add-ons or another application.	Full support for STIX and TAXII 2.1 – excellent for interoperability with other systems.	STIX/TAXII support is built in – import/export as well as feeding are seamless.	Does not support STIX/TAXII – works with its own data processing format.	STIX/TAXII support is limited.	STIX/TAXII is not supported.
Operational requirements	Sources	Support for the largest number of authoritative CTI sources	Source support is limited to what the administrator configures manually.	Support for many CTI sources such as CIRCL, OTX, MISP community hubs, Anomali, etc.	The highest level of support for CTI sources – thanks to extensible connectors.	Supports numerous open sources thanks to a rich ecosystem of bots.	Supports several sources, but their number is lower than with MISP or OpenCTI.	Sources are limited, but cover several relevant databases.
	Efficiency	Possibility of using AI for automated processing and filtering	Does not provide native AI functionality for processing – it needs to be supplemented using ML add-ons in the Elastic Stack.	MISP does not use ML directly, but there are external integrations that make this possible.	The tool supports ML in the form of enrichment, prioritization and classification of entities (in future versions).	Does not contain an AI module, but data can be passed to other systems for processing.	Does not support AI – works predominantly manually or semi-automatically.	Does not support AI, but algorithmically saves time by linking CVEs and IOCs.
		Reduced need for manual analysis – saving analysts' time	Reducing manual work is not a priority of this module – it requires manual tuning, dashboards and manual correlation.	Automated filtering reduces the workload of analysts using feed filters and a TTL policy.	A high degree of automation and deduplication saves analysts a considerable amount of work.	Reduces the need for manual work through a high degree of automation in the pipeline.	Reduces the workload on analysts in the area of basic IOC enrichment.	Allows some tasks to be automated, thereby saving analysts time.

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

Category	Subcategory	Requirement	Shuffle	TheHive+ Cortex	StackStorm	Fasten Health Tracecat (ex-Kuiper)	FIR (Fast Incident Response)
Functional requirements	Collection and inputs	Receiving alerts and data from various security systems	Supports workflows and collection from various systems	Collection of alerts from SIEM, EDR, CTI	Trigger-based integration	Focused on incidents from healthcare systems	Webhook or REST input
		Data normalization and parsing	Via custom scripts/parsing	Supports parsing of observables	Can process and modify the data format	Parsing depends on the backend	Basic parsing
		Support for STIX/TAXII, JSON, syslog	JSON, STIX supported via plugins	JSON, STIX, syslog supported	STIX/TAXII manually	Partial JSON support	Support for JSON and part of STIX
	Incident Management	Incident categorization and prioritization	Support for priorities and labels	Strong tagging and typing of incidents	Incidents categorized via metadata	Basic categorization by type	Incident categories optional
		Ability to create incident tickets both manually and automatically	Yes, manually and via trigger	Yes, manually and via API	Trigger creates a ticket	Manual input + API	Manually or via API
		Ticket editing and lifecycle management	Not supported	Complete lifecycle workflow	Workflow management available	Recording and editing of incidents	Basic lifecycle (Open, Investigating, Closed)
	Rules and policies	Predefined playbooks	Yes, basic playbooks available	Templates (template cases) predefined	Workflow templates exist	Several predefined types	Templates not native
		Ability to create custom playbooks without the need for programming	Playbook editor for non-programmers	User templates without code	Playbooks can be created from the GUI	Limited no-code creation	Manual entry of incident type
		Workflow engine with branching, conditions and loops	Strong workflow engine with branching	Via rules and workflow templates	Exceptionally strong workflow system	Simple workflow structures	Workflow is not engine-based
	Response automation	Execution of actions based on triggers	Execution via REST, UI and events	Via Cortex actions (analysers/responders)	Trigger + action combination	Trigger + action	Trigger via API
		Support for manual approval or automatic continuation	Possibility of manual intervention	Manual confirmation optional	Possibility of approval steps	Manual approval available	Manual confirmation step
		Automated responses: IP blocking, host isolation, escalation	Basic responses supported	Strong response options (e.g. IP ban)	Action chaining for responses	Basic response possible	Responses limited
	Orchestration	Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR	Integration with SIEM, EDR, etc. via connectors	Broad integration via analysers	Extensive integration (SIEM, firewall...)	API integration, sometimes via FHIR	Partial connection to other tools
		Centralized logging of actions in playbooks	Audit record of actions possible	Logging of actions in history	Logging of step output	Partial logging	Logs incident steps
Integrations	API and connectors	API-first approach (REST, Webhooks)	REST API-first design	REST API	REST API	REST API supported	REST API
		Support for plug-ins and connectors	Plugin support	Extensible via modules	Packs (plugins)	Built on top of plugins	No plugin system
		Possibility of creating custom connectors	Custom connectors via the UI or Python scripts	Responders + analysers	New packs can be created	Custom connectors via the backend	No
	CTI and enrichment	Integration with CTI sources (Shodan, VirusTotal, AbuseIPDB...)	Integrations e.g. with MISP, OTX	Cortex has MISP, VT, AbuseIPDB	Integration with CTI possible manually	CTI only via external API	CTI only if manually imported
User interface	UI	Web UI for managing incidents and playbooks	Modern and simple UI	Web UI is well structured	Web UI exists, less UX-friendly	UI is modern, but specific	Web UI is simple
		Intuitive visual workflow modelling	Workflow editor is visual	Workflow both simple and advanced	Less visual	Not very visual	No visual workflow
		Dashboards for incident status and statistics	Basic dashboards via plug-in	Four basic dashboards Alerts, Cases, Observables, TTPs	Limited dashboards	Statistics limited	No dashboards
Operation and deployment	Deployment	On-prem / cloud / hybrid option	Local, hosted, cloud and Hybrid	Linux server, on-prem recommended, cloud also supported	On-prem recommended	On-prem and SaaS	On-prem the only option
		Support for containerization (Docker, Kubernetes)	Docker/K8s support	Docker is fully supported	Full container support	Docker support	Docker build exists
	Operation	High availability and clustering	Basic HA support	HA can be handled manually	HA supported via RDB cluster	HA not native	HA not native
		Backup & recovery of playbooks and configuration	Export of configs and workflows	Backup via export	Backup via yaml export	Export of yaml configs	Backup via the database
Security	Access and audit	RBAC and audit trail	RBAC present	RBAC defined	RBAC can be added	Basic RBAC	RBAC for roles
		Encryption of data in transit and data at rest	HTTPS, encryption supported	HTTPS, encryption standard, TLS/SSL -> AES-256	SSL support	SSL, encryption	HTTPS
		MFA support	Supports native MFA	TOTP-based MFA natively supported	MFA requires add-ons	MFA unknown	No
Licensing and TCO	Model	Open-source / freemium / commercial model	Open-source	Open-source	Open-source	Open-source (some parts)	Open-source
		Maintenance and infrastructure demands	Low to moderate demands	Moderate maintenance	Higher complexity	Higher complexity	Low demands
	Support	Support, community and documentation	Large community, active issues on GitHub	Good documentation, Git active	Large DevOps community	Small community	Documentation OK
Regulatory frameworks	Compliance	Assistance with automated fulfilment of GDPR, ISO 27001, SOC2	Helps with auditing, GDPR requires add-ons	Manual GDPR compliance possible, not native	GDPR requires configuration	Not clearly focused on compliance	Not native
		Logging of response activities for audit purposes	Partial support – without a clear specification of the audit trail.	Records every action	Logging of workflow outputs	Not directly	Record of activities in the ticket
Extensions	Testing	Playbook debugging & testing	Yes, debugger included	Not directly	Debugger included	Debugger available	No
	Simulation	Incident simulation (purple teaming support)	Not directly	No	Simulation only via test runs	No	No
	Integration	SOAR-SIEM synchronization of incident status	Not natively	Yes, via connection to SIEM	SIEM sync optional	Not native	Partial sync
	Versioning	Integration with a version control system (e.g. Git)	No	JSON export + GIT	Package export	Manual versioning	No
	Operation	Multitenancy – isolation between multiple clients	Supported	Not native	Not native	No	No

supporting document for V5
linked to KPB2

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

Category	Subcategory	Requirement	Elastic Security	Wazuh	OSSEC	OpenEDR	Velociraptor
Functional requirements	Deployment	Deployment options: on-prem, cloud, hybrid	Yes, support for both on-prem and cloud	Yes, on-prem, cloud and hybrid	On-prem only	Both cloud and on-prem	On-premise, cloud-ready
	Protection of environments	Support for cloud, container and server environments	Yes, including Kubernetes and Docker	Yes, support for servers and containers	Limited container support	Yes, the agent covers multiple environments	Primarily focused on endpoints
		Support for various OSs (Windows, Linux, macOS)	Yes, Windows, Linux, macOS	Yes, all major OSs	Windows, Linux, macOS	Yes	Linux, Windows, macOS
	Data collection	Collection of audit data using agents	Yes, using Elastic Agent	Yes, using the Wazuh agent	Yes, OSSEC agent	Yes	Yes
		File Integrity Monitoring (FIM)	Yes, via Auditbeat	Yes, built-in FIM	Yes	Yes	Yes
		Collection of system metrics, processes and behaviour	Yes, Beats + Agent	Yes, detection of system changes	Yes, basic metrics	Yes, including process behaviour	Yes
		Collection of information on vulnerabilities and configurations	Partially – using integrations	Yes, via the SCA module	Limited	Yes	No
		Collection of application and service logs	Yes, via Beats	Yes, via the log collector	Yes	Yes	Yes
		Data collection from cloud and network sources	Yes, via Elastic Integrations	Partially, using integrations	No	No	Limited
	Analysis	Log analysis and correlation with threats	Yes, with advanced analysis and SIEM	Yes, rules and SIEM module	Basic log analysis	Yes, with UI	Yes, with a focus on forensic analysis
	Detection	Malware and intrusion detection	Yes, detection using rules and ML	Yes, IDS and integration rules	Yes, basic IDS	Yes	No direct IDS
		Heuristic and behavioural analysis	Yes, behaviour and rules	Yes, basic behavioural analysis	No	Yes	Yes, behavioural detection
		Support for ML/AI algorithms for threat detection	Yes, Elastic Stack ML module	Not directly, no ML	No	Yes, ML detection	Yes
		Mapping to the MITRE ATT&CK framework	Yes (via Elastic rules tagging)	Yes	No	No	Yes
	Response	Automatic responses (e.g. device isolation, file quarantine)	Yes, supports SOAR and SIEM responses	Yes, basic responses (scripts)	Limited responses via scripts	Yes, actions via UI	No
		Sending incidents to ticketing systems / SOAR	Yes (via webhooks, Jira, ServiceNow)	Yes	No	No	No
Technical requirements	Visualization	Dashboards for visualizing incidents and system status	Yes, Kibana dashboards	Yes, Wazuh dashboard (Kibana)	No native dashboards	Yes, WebUI	Yes, WebUI
	Monitoring	Notifications to the SOC team about events and incidents	Yes, multiple notification options	Yes, E-mail and webhooks	E-mail	Yes	Yes, alerts
	Performance	Low system load of the agent	Moderate system load	Low load	Low	Moderate	Very low
Operational requirements	Scalability	Support for hundreds to thousands of endpoints	Yes, enterprise scaling	Yes, supports large environments	Medium-sized networks	Yes	Yes
	Management	Simple central management of agents	Yes, via Fleet	Yes, centralized management	Manual configurations	Yes	Yes
		Regular updates of signatures and modules	Yes, updates included in Elastic Agent	Yes, regular updates	Manual updates	Yes	Yes

supporting document for V5
linked to KPB2

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

Category	Subcategory	Requirement	Greenbone Community edition	OpenSCAP
Functional requirements	Licensing	Free version, open-source solution with the possibility of extension	Yes, GCE is open-source with the option to upgrade to the enterprise edition	Yes, fully open-source, part of the Red Hat Security stack
	Scanning	Estimated scanning capacity (for example, min. 100 IP/24h)	High scanning capacity – suitable even for hundreds of IPs per day, depending on performance	Primarily oriented towards individual hosts, not extensive network scans
	Vulnerabilities	Vulnerability test updates – community and enterprise feed	Yes, community feed (GVMD Data Feed), a premium enterprise feed exists	Yes, uses OVAL, SCAP and other standards – updates are manual or repository-based
		Support for CPE, CVE identifiers	Yes, outputs are mapped to CVE/CPE via the OpenVAS engine	Yes, a standard part of SCAP
	Management	Acceptable web interface for managing scans and results	Yes, GSA (Greenbone Security Assistant) – modern web UI	Not directly, usually used via the CLI or third-party tools such as SCAP Workbench
	Scanning	No need for agents (agentless)	Yes, by default it works as an agentless tool	Yes, works without agents on the basis of SCAP/OVAL policies
		Support for scheduling tasks and alerts (optional)	Yes, GVM supports scan scheduling and automatic reports	Not natively, rather dependent on an external scheduler such as cron
	Features	Remediation tickets – integration or export	Export to CSV, PDF, XML, API; no native ticketing, but connection possible	Export to ARF/HTML, no direct integration with ticketing systems
	Reports	Configurable report formats (e.g. CSV, XML, PDF)	Yes – support for CSV, XML, PDF, HTML outputs	Yes – mainly ARF, HTML, XML (depending on the add-on used)
Technical requirements	Deployment	Deployment options: on-premise, cloud/SaaS, VM, Docker	On-premise, Docker and VM support (container versions available)	Primarily on-premise, can be configured as a container
	HW requirements	Minimum and recommended technical requirements (RAM, CPU, disk)	Min. 4 GB RAM, 2 vCPU, SSD disk; 8+ GB RAM recommended	Low requirements – runs even on 1 vCPU, 1 GB RAM, depending on scope
		Number of vCPUs	Minimum 2, 4+ recommended for larger networks	1 is sufficient if extensive computations are not used
		Max. number of network adapters	Depends on the host, GVM has no limits of its own	No limitation – works on top of the OS, does not require adapters
	Architecture	Scanning architecture (monolithic or master/sensor)	Supports a master-sensor architecture for large networks	Monolithic architecture, without sensor support
	Protocol support	Mandatory: DNS, DHCP	Yes, it can identify both DNS and DHCP services during a scan	Not primarily intended for network protocols
		Optional: NTP, GMP, HTTPS, SSH, SNMP, Syslog, IPv6, LDAP, RADIUS	Yes – GMP, SSH, SNMP, HTTPS, LDAP, IPv6, RADIUS, optional plugins	Support depends on the policy used – SCAP standards may include protocols
	Integrations	Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	High scanning capacity – suitable even for hundreds of IPs per day, depending on performance	Possible via OpenSCAP outputs and subsequent conversion
	Score	Support for CVSS 4.0	CVSSv3 supported, CVSSv4 in preparation	Supports CVSS via OVAL definitions
		Support for EPSS – vulnerability exploitation prediction	Not natively, but can be extended via external CTI feeds	Not natively, but can be added manually to assessments
Operational requirements	Updates	Possibility of manual updates, or a custom implementation	Yes – manual updates possible via the CLI and GUI	Yes – OpenSCAP updates dependent on the distribution (e.g. Red Hat feeds)
	Operations	Ensuring exceptions in security systems during scanning	Yes, documented – whitelisting the scanner's IPs and ports is recommended	Yes, runs locally, requires only access to the OS
	Compliance	Compliance policies for standards (e.g. GDPR, ISO, CIS, BSI...)	Support for BSI, ISO 27001 and others – standards-oriented reports	Primarily oriented towards CIS, STIG, NIST – a very strong point of the tool

supporting document for V5
linked to KPB2

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

				Ticketing								
	Category	Subcategory	Requirement	TheHive	Zammad	Request Tracker (RT)	osTicket	RTIR	Kibana (ELK)	Grafana	BookStack	Wiki.js
Ticketing	Functional requirements	Basic functions	Creation and editing of records (tickets)	Support for creating and editing tickets with detailed data	Full support for creating and editing tickets via both the GUI and the API	Basic functionality for creating and managing tickets	Simple interface for creating and editing tickets					
			Ability to change ticket statuses (e.g. New, In progress, Closed, Postponed)	Flexible management of incident states	Full workflow support and state changes	Possibility of defining custom ticket states	Both preset and custom workflow states					
			Assignment to a specific handler (L1 analyst, L2/L3 escalation)	Assignment of tasks to analysts according to roles and escalations	Possibility of assigning tickets to individual agents	Fully supported, with the option of setting SLAs	Assignment support also for multiple teams					
		Notifications	E-mail notifications of status changes, comments, deadlines	Fully configurable e-mail alerts as well as webhooks	Customizable notifications based on events	Notifications for all important actions in a ticket	Automatic alerts according to event type					
		Attachments and evidence	Adding attachments (logs, evidence, screenshots, tool outputs)	Support for uploading various file types to a case	Support for attachments, including via drag-and-drop	Possibility of attaching logs and screenshots to tickets	Simple uploading of attachments in a ticket					
		Time data	Ability to record times (creation, update, escalation, closure)	Detailed time records of all actions	SLA tracking as well as custom metrics	Records all important time events	Time trail from creation to closure					
		Prioritization	Setting incident priority and severity	Configurable priority and severity levels	Possibility of setting priority manually or automatically	Configurable criticality levels	Basic support for priorities in the system					
		Templates	Ability to create templates for recurring incident types	Support for predefined case templates	Creation of predefined ticket templates	Support for ticket templates via extensions	Templates available for quick entry					
		Tagging	Ability to add tags for quick search and filtering	Support for tagging observables and cases	Fully configurable tags and their management	Possibility of creating labels and searching by them	Simple tagging system					
	Technical requirements	Integrations	Integration with SIEM, SOAR, CTI, incident recording tools, reporting and asset management tools	Extensive integration options via Cortex, MISP, API	Support for SIEM and ITSM systems	Can be connected using extensions and plugins	Support for some external systems via API					
		API	REST API and Webhook support	Fully documented REST API and webhooks	REST API for integration with systems	Extensive API for ticket management	REST API and webhook integrations					
		Export	Export to PDF, CSV, JSON formats for documentation and reporting	Possibility of export via both the GUI and the API	Export to multiple formats	Support for CSV and JSON export	Possibility of exporting data from both the GUI and the backend					
		UX/UI	Modern, responsive web interface	Intuitive and responsive GUI focused on analysts	Modern design with fast response	Simple but outdated UI	Friendly interface, somewhat outdated					
	Operational requirements	Audit and transparency	Recording of all changes, accesses and comments in a ticket	Detailed audit trail, including changes to observables	All user actions fully logged	Record of all activities in the ticket	Audit logs available in the system					
		Historical records	Possibility of retrospective review and forensic analysis	Historical overview, including observables and responses	Logging including dates and changes	Record history available	Overview of all changes available					
		Multitenancy	Support for multiple organizational units (departments, customers)	Support for organizations and departments with sharing	Multi-level department management	Basic support for departments via extensions	Support for multiple departments via groups					
		SLA monitoring	Measurement of resolution time and SLA compliance at individual levels	Setting and tracking SLAs directly in the ticket	Possibility of configuring SLA rules	Basic SLA functionality	Configurable SLAs according to ticket type					
		Roles and permissions	RBAC support – access levels for different roles	Detailed RBAC system according to roles and functions	Access policy according to groups	RBAC for individual queues and tasks	Simple role-based RBAC					
Incident recording and management	Functional requirements	Case management	Creation and management of cases with tasks and details	Fully fledged case management via a clear GUI with tasks, observables and comments.				RTIR allows cases to be created and managed via modules such as incident, investigation, report.				
			Adding and tracking observables (IPs, domains, URLs, hash values)	Support for various types of observables – IPs, domains, URLs, hashes, which can be linked to CTI sources.				Tracking of observables is limited and requires supplementation via plugins or custom scripts.				
			Linking of cases based on common indicators	Possibility of linking cases using observables and visual display of relationships.				Linking between cases is manual – using IDs or notes, not automated.				
		Categorization	Categorization of incidents using tags	Tags and incident categories can be assigned by users for easier filtering.				User labels and categories can be created via extended ticket properties.				
		Data analysis and enrichment	Automated enrichment of incident information from internal and CTI sources	Integration with MISP, Cortex and other tools enables automatic data enrichment.				Data enrichment is possible only manually or via integration with external CTI systems.				
		Configuration	Ability to modify the system configuration, manage metrics, create case templates and set rules for sharing tasks and observables between organizations	The GUI allows metrics and case templates to be configured and observables to be managed across organizations.				Configuration is available via the CLI or web GUI, but is not as flexible as TheHive.				
	Technical requirements	Roles and access	Support for multiple user roles – at least analyst and administrator	Support for multiple role levels (admin, analyst, observer) and their permissions.				RTIR supports access levels, but less intuitively than modern platforms.				
		Multi-tenancy	Ability to create multiple organizations, sharing rules between them	Full support for a multi-tenant environment with isolation between organizations.				Support for multiple organizations is available, but more demanding to configure.				
		Integrations	Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins	Supports a standard API for integration with other security components such as SIEM, SOAR, CTI.				Existing plugins enable basic integration with external systems (SIEM, CTI).				
		Export and reporting	Export of incidents to CSV, PDF formats, via REST API	Possibility of export to CSV and PDF; the REST API supports comprehensive reporting.				Export possible via extensions or scripts (primarily CSV, limited PDF).				
		Activity record	Logging of analysts' activities during incident handling (audit trail)	Every change or activity in a ticket is recorded in the audit log.				Action tracking is basic – audit logs are part of the core system.				
	Operational requirements	System administration	Simple management of configurations and updates	Configuration options available via the GUI or API, easy management of templates and rules.				Configuration management is carried out via config files and the web GUI; updates are manual.				
		Customizability	Ability to add custom fields or case types according to the needs of the organization	The user can define custom field types, structures and incident types.				Custom fields can be added using extensions (Custom Fields).				
		Visibility and retrospective analysis	Ensuring traceability and retrospective analysis of incidents	Incidents are stored with a change history; retrospective analysis is supported via the dashboard.				Ticket history is saved, but without graphical retrospective visualization.				
		Team interconnection	Sharing of cases between teams and external partners according to permissions	Sharing of cases between organizations possible with defined access rules.				Sharing possible via access groups, but not in real time with linked teams.				
Reporting	Functional requirements	Overview	Creation of a basic overview of the security and incident status						Supports clear visualizations of Elasticsearch data, including incidents.	Dashboards provide a flexible view of metrics and incidents from multiple sources.		
		Distribution	Ability to download a report or send it automatically (e-mail, webhook)						Distribution of reports possible via automatic scheduling (X-Pack); e-mail sending requires a licence.	Automatic distribution available via Grafana Alerting + Reporting plugins.		
		Customization	Ability to select report content – time period, incident types						Supports customization of time, fields and visualization types in reports.	Full control over the time range, variables and data filters.		
		Automation	Scheduling of regular (e.g. daily, weekly) reports						Report scheduling available via the Reporting module; some features tied to the paid version.	Possibility of scheduling exports via the Grafana Reporting plugin (limited in open source).		
		Ad hoc outputs	Ability to generate one-off ad hoc reports						Supports one-off exports via both the GUI and the API.	Simple export from the dashboard for ad hoc purposes.		
		Personalization	Customization of the visual appearance of the report (logo, colours, header)						Limited options for adjusting report appearance in the basic version.	Possibility of customization using custom templates and HTML headers (plugins).		
	Technical requirements	Output formats	Support for export to PDF, CSV, JSON						Export to PDF and CSV (X-Pack), JSON via API.	Support for export to PDF, PNG (via plugins), CSV via panel.		
		Integration	Integration with tools such as SIEM, Ticketing, Incident recording, Asset management, CTI, ...						Strong integration with the Elastic Stack, SIEM, CTI, Beats, Logstash.	Integration with SIEM (Elastic, Loki), Prometheus, InfluxDB, PostgreSQL and others.		
		Visualization	Ability to integrate charts, tables, statistics, heatmaps						Interactive charts, maps, time series, metrics and heatmaps.	Wide range of widgets: charts, tables, histograms, alerts, maps.		
		Data sources	Support for various sources: databases, logs, API outputs						Works natively with Elasticsearch; API integrations are available.	Supports more than 30+ sources, including SQL, APIs and cloud tools.		
		Access	Web/GUI interface for creating and managing reports						Modern browser-based interface for creating dashboards and reports.	Modern GUI, responsive and customizable in terms of panels.		
	Operational requirements	Audit and archiving	Ability to archive generated reports						Possibility of saving and accessing reports via the Reporting module.	Exports can be archived via scripts or plugins (e.g. Grafana Image Renderer).		
		Access rights	Ability to restrict access to reports by role (RBAC)						RBAC support via Elastic Security, depends on the edition.	RBAC available, basic level of permissions even in the free version.		
		Security	Encrypted transmission of reports during automatic distribution						Supports TLS/SSL for secure distribution and access.	HTTPS support and basic security measures for both the API and the GUI.		
SOC knowledge portal	Functional requirements	Content management	Creation, editing and versioning of records (guides, playbooks, FAQ)	KB articles – creation/editing OK, built-in versioning missing (requires an external solution)							Full support for creating, editing and versioning documents and books.	Advanced creation, versioning and approval of articles, including editing via Git.
		Content management	Support for structured documents – categories, sections, tags	Support for observables and case templates with tags, but not for structured documents in KB form.							Support for structured documents with a hierarchy: books, chapters, pages + tags.	Full support for categories, tags, sections and custom fields.
		Search	Full-text search with support for filters and tags	Possibility of searching by names, observables and tags; no full-text search over text as in a wiki.							Powerful full-text search, support for filters and search by tags.	Powerful search with support for ElasticSearch and a MongoDB backend.
		Linking with incidents	Linking KB records to specific incidents or attack types	Linking via observables and cases, but not separate KB items.							Manual cross-linking or insertion of links to incidents possible.	Possibility of manually linking incidents or external systems.
		Links and attachments	Ability to insert images, logs, links and attachments	Logs, images and files can be attached to incidents or cases.							Simple addition of images, code, documents, tables and files.	Insertion of attachments, images, code blocks, diagrams (PlantUML, Mermaid).
	Technical requirements	Access rights	RBAC support – different access levels for reading, editing, approval	Strong RBAC options with granular access for organizations and roles.							RBAC support: reading, editing, deleting, approving according to role and book.	Role-based RBAC, with finely definable permissions per section or article.
		Integrations	Ability to integrate with ticketing, incident management, SIEM	Integration with MISP, Cortex, SIEM via API; ticketing systems indirectly.							Integration possible via API and webhooks; SIEM and ticketing require middleware.	Integration via REST API, Git synchronization, webhooks and 3rd-party plugins.
		Export	Export of documents to PDF, HTML or Markdown format	Export of cases and observables via API or CSV, not fully fledged KB articles.							Native export to PDF, HTML, Markdown, also via CLI and API.	Export to PDF, HTML and Markdown + synchronization with a remote Git repository.
		UI/UX	Simple and intuitive interface for editing and publishing records	Intuitive GUI for case management, but not as a fully fledged documentation editor.							Simple and attractive interface with a WYSIWYG editor and Markdown support.	Responsive, modern interface with support for multiple editors (WYSIWYG, Markdown).
	Operational requirements	History	Preservation of change history with the ability to restore an older version	Case history is captured, but not as versioning of KB documents.							Every version of a document is saved and can be reverted to.	Full versioning of articles with the possibility of reverting, an overview of changes and comparison.
		Audit	Records of who edited a document and when	Recording of analyst activity is part of the system, not specifically for documents.							Edit history including user, time and change visible in the page detail.	Logging of every action, including user history and changes.
		Process compliance	Ability to create approval workflows for new KB articles	There is no approval workflow for the KB – the workflow is tied to cases and alerts.							Support for article approval through extensions and editor access.	Approval workflow for new or modified articles, especially in enterprise mode.

supporting document for V5
linked to KPB2

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

Category	Subcategory	Requirement	LibreNMS	pi.Alert	NetBox	Ralph	GLPI
Functional requirements	Basic management	Creation, editing and deletion of asset records	Yes, mainly network devices	Basic management of IP and MAC addresses	Yes, detailed items	Yes, CMDB support	Yes, as part of the CMDB
		Differentiation of assets by type – hardware, software, virtual, cloud	Limited	Limited	Yes, with support for custom types	Yes	Yes
	Categorization	Ability to assign tags, categories, owners and status (e.g. active, under maintenance, decommissioned)	Partially, via attributes	Basic tags	Yes, categories and tags	Yes, detailed categories	Yes, flexible tags
	Security	Recording of the security status of each asset (e.g. OS versions, last update)	Yes, SNMP monitoring	Basic level	Not directly	Possibility of extension	Partially, via add-ons
	Location and network	Mapping of assets to locations, VLANs, IP ranges, racks	Yes	Basic display by network	Yes, IPAM and DCIM	Yes	Limited
	Relationships	Relationships between assets (e.g. server – service – application)	Limited	No	Yes, relationship model	Yes	Yes
	Integration	Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident recording	Yes, with Nagios/Zabbix	Limited	Yes, plugins and API	Yes	Yes, native integration
	Search	Filtering, full-text search and export capabilities	Yes	Basic	Yes, powerful search	Yes	Yes
Technical requirements	Import/Export	API support (REST, GraphQL) for asset management and integration	REST API	REST API	REST and GraphQL	REST API	REST API
	Extensibility	Ability to create custom fields, attributes, plugins (e.g. NetBox/Django)	Partially	No	Yes, Django plugins	Yes	Yes
	Data collection	Automated discovery of assets in the network (e.g. SNMP, nmap, APIs of other systems)	Yes, SNMP discovery	Yes, periodic scans	Not native	Limited	Yes (e.g. FusionInventory)
	UI	Web interface with editing capabilities and clear management	Yes	Simple	Modern and configurable	Intuitive	Yes
Operational requirements	History and audit	Recording of changes to assets (who changed what and when)	Basic history	Yes\No	Yes	Yes	Yes
	Lifecycle management	Ability to track the asset life cycle (deployment – decommissioning)	Partially	No	Limited	Yes	Yes
	Notifications	Notifications of status changes, expirations, service intervals	Yes	Basic e-mail	Limited	Yes	Yes