

SIEM

Katéria	Podkatéria	Požiadavka	ELK Stack	Wazuh	OpenSearch + OpenSearch Dashboards	Graylog (Open)	SIEMonster (Community edition)	Prelude OSS	AlienVault OSSIM
Zber a spracovanie dát	Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)	Podporuje širokú škálu formátov logov vrátane syslog, JSON, CSV, CEF a ďalších cez Logstash a Beats.	Plne podporuje širokú škálu formátov logov vrátane syslog, JSON, CSV, CEF, LEEF.	Plne podporuje všetky bežné formáty logov vrátane syslog, JSON, CSV, CEF, LEEF.	Podporuje široké spektrum formátov vrátane syslog, JSON, CSV a CEF. Import sa často realizuje cez Logstash alebo agenta.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Primárne IDMEF a syslog, obmedzená podpora iných formátov.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.
	Podporované typy auditných logov (napr. prostredníctvom Auditbeat)	Plná podpora cez Auditbeat pre auditovacie logy z Linux a Windows systémov.	Podporuje auditné logy cez vlastného agenta aj integráciu s nástrojmi ako Auditbeat.	Podporované prostredníctvom integrácie s Beats (Auditbeat, Filebeat), ktoré zbierajú auditné záznamy zo systémov.	Základná podpora auditných logov, často cez externé agenty.	Základná podpora auditných logov, často cez externé agenty.	Základná podpora auditných logov, často cez externé agenty.	Obmedzená natívna podpora, vhodné pre manuálne pripojenie.	Základná podpora auditných logov, často cez externé agenty.
	Podporované typy udalostných logov (napr. prostredníctvom Auditbeat)	Udalostné logy je možné zbierať cez Auditbeat a Winlogbeat, vrátane systémových udalostí a bezpečnostných záznamov.	Udalostné logy je možné zbierať cez Auditbeat a Winlogbeat, vrátane systémových udalostí a bezpečnostných záznamov.	Udalostné logy sú spracovávané cez agenta a podporuje Windows aj Linux zdroje.	Udalostné logy môžu byť spracované z viacerých systémových zdrojov prostredníctvom Beats a obohatené v pipeline.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Podporované typy systémových logov (napr. journald, syslog, dmesg)	Zber systémových logov ako journald, syslog, dmesg je podporovaný cez Filebeat alebo Logstash moduly.	Plná podpora pre systémové logy ako journald, syslog, dmesg – zhromažďované cez agenta.	Plná podpora pre systémové logy ako journald, syslog, dmesg – zhromažďované cez agenta.	Zber dát zo systémových logov ako syslog, journald alebo dmesg pomocou logagentov ako Filebeat.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Primárne IDMEF a syslog, obmedzená podpora iných formátov.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.
	Akým spôsobom môžu byť zbierané dáta (protokol, API, agent, agentless, webhook...)	Dáta je možné zbierať cez agenta (Beats), agentless prístup, REST API, Webhooky, či priame logforwarding protokoly.	Zber dát je možný cez Wazuh agenta, ale aj cez agentless režim, API a webhooks.	Podporuje zber údajov cez agenta (Beats), agentless cez syslog, ako aj REST API a webhooks.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Reálny čas vs. dávkové spracovanie	Podporuje real-time stream spracovanie logov aj dávkové spracovanie historických dát.	Spracovanie v reálnom čase – logy sú analyzované okamžite po prijatí.	Spracovanie v reálnom čase – logy sú analyzované okamžite po prijatí.	OpenSearch podporuje real-time indexáciu a streamovanie dát. Batchové spracovanie je dostupné cez ingest pipeline.	Podporuje spracovanie v reálnom čase s minimálnym oneskorením.	Podporuje spracovanie v reálnom čase s minimálnym oneskorením.	Podporuje spracovanie v reálnom čase s minimálnym oneskorením.	Podporuje spracovanie v reálnom čase s minimálnym oneskorením.
	Podporované protokoly (SNMP, Syslog, NetFlow/IPFlow...)	Protokoly ako Syslog a NetFlow sú podporované cez príslušné Logstash pluginy a Beats moduly.	Podporuje štandardné protokoly ako SNMP, Syslog, NetFlow a ďalšie prostredníctvom integrácií.	Podporuje štandardné protokoly ako SNMP, Syslog, NetFlow a ďalšie prostredníctvom integrácií.	Logy môžu byť získané cez SNMP, Syslog a NetFlow pomocou externých modulov alebo log pipeline nástrojov.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.	Primárne IDMEF a syslog, obmedzená podpora iných formátov.	Podporuje širokú škálu formátov logov vrátane syslog, JSON a CEF.
Analýza a detekcia	Real-time analýza	Elasticsearch umožňuje spracovanie dát v reálnom čase vrátane korelácie udalostí a okamžitého vyhľadávania.	Áno, podporuje nepretržitú analýzu prijímaných údajov v reálnom čase.	Analýza v reálnom čase je základnou funkcionalitou OpenSearch. Vizualizácie a dotazy sú okamžite aktualizované.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Korelácia udalostí (preddefinované a vlastné pravidlá)	Korelácia je možná cez vlastné pravidlá (Elastic Detection Engine) alebo integráciu s ElastAlert a inými nástrojmi.	Súčasťou je engine na koreláciu udalostí s podporou Alerting pluginu alebo integráciou s Sigma pravidlami.	Podporuje vlastné aj preddefinované pravidlá pomocou Alerting pluginu alebo integráciou s Sigma pravidlami.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Machine Learning/Behaviorálna analýza	Modul ML (X-Pack) poskytuje behaviorálnu analýzu a detekciu anomálií pomocou ML algoritmov.	Základná podpora behaviorálnej analýzy – nie ML, ale založené na pravidlách a správani.	Strojové učenie je dostupné cez ML Commons plugin, ale vyžaduje dodatočnú konfiguráciu. Vhodné na detekciu anomálií.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.
	Threat Intelligence (CTI) integrácia	Integrácia s CTI je možná cez Threat Intel modul, podporuje napríklad enrichovanie IOC z externých zdrojov.	Integruje sa s CTI ako OTX, VirusTotal a MISP pre obohatenie alertov.	Integrácia s CTI je možná – OpenCTI, MISP alebo Threat Intel feeds môžu byť agregované a vizualizované.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Detekcia anomálií	Anomálie sú detegované pomocou ML Jobs alebo prahových pravidiel v Detection engine.	Detekcia anomálií je možná na báze pravidiel správania a CTI.	Pomocou ML Commons pluginu a vlastných pravidiel je možné detegovať správanie, ktoré vybočuje zo štandardu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Podpora pre MITRE ATT&CK mapovanie	Elastic Security poskytuje základné mapovanie detekcií na MITRE ATT&CK techniky.	Mapovanie na MITRE ATT&CK je natívne podporované pri korelácii.	Manuálna možnosť mapovania na MITRE ATT&CK, často realizované cez externé nástroje alebo vlastné dashboardy.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Vlastné alertovacie pravidlá a prahy	Podporuje vytváranie vlastných alertov vrátane komplexných podmienok, thresholdov, časových okien a filtrov.	Umožňuje nastavenie vlastných pravidiel, prahov a reakcií na udalosti.	Podporuje komplexné vlastné alertovacie pravidlá cez Alerting modul. Možno definovať prahy, logiku a filtre.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Funkčné požiadavky	Workflow pre eskaláciu	Elasticsearch stack umožňuje jednoduché workflow pre eskaláciu pomocou Alerting Rules.	Podpora pracovných tokov a eskalácií cez pravidlá a notifikačné systémy.	Workflow je možný pomocou triggerov a action group. Hoci nie je plnohodnotný SOAR, dokáže eskalovať udalosti.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)	Reakcie je možné vykonať pomocou integrácie so SOAR systémami alebo Elastic Actions (napr. HTTP hook).	Reakcie ako blokovanie IP, spustenie skriptov alebo integrácia s SOAR je možná.	Podporuje integračné akcie – HTTP requests, webhooks – ktoré umožňujú spúšťať reakcie na základe podmienok.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Notifikácie pre rôzne platformy (e-mail, Teams,...)	Notifikácie je možné poslať cez e-mail, MS Teams, Slack alebo webhook pomocou Alerting modulov.	Notifikácie cez e-mail, Slack, Teams a webhooks sú podporované.	Notifikácie možno smerovať na e-mail, Slack, Teams a ďalšie platformy pomocou webhooks.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Zaslanie notifikácií na e-mail, MS Teams, Jira, The Hive	Plná podpora pre zaslanie do MS Teams, Jira, The Hive pomocou webhookov alebo Elastic Actions.	Áno, s možnosťou konfigurovať ciele ako e-mail, Jira, MS Teams, The Hive.	Rozišrením alebo pomocou externých orchestrátorov je možné zaslať alerty do The Hive, Jira a ďalších systémov.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Možnosť podrobného nastavenia upozornení (popis, predmet, časové okno, filtre, prahy, logika, závažnosť, skóre, tagy)	Alerty umožňujú pokročilé nastavenia – podmienky, rozsahy, metadáta a skórovacie logiky.	Veľmi detailné možnosti definície podmienok, časových okien, skóre, prahov atď.	Vysoká pripodobnosť – používateľ môže nastaviť detailné podmienky pre upozornenia vrátane skóre a vah.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Predvolená sada pravidiel – vopred definovaná v nástroji	Elastic obsahuje základné pravidlá pre detekciu najbežnejších útokov a techník.	Obsahuje vlastný balík pravidiel pre rôzne typy udalostí.	OpenSearch neobsahuje prednastavené 'security rules'; používateľ si vytvára monitory a triggerly manuálne.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Možnosť využitia sekundárnych zdrojov pravidiel (napr. Sigma rules)	Možno využiť komunitné pravidlá ako Sigma a importovať ich do Elastic pomocou konverzných nástrojov.	Podporuje použitie pravidiel z externých zdrojov ako Sigma.	OpenSearch podporuje externé pravidlá ako Sigma a ďalšie cez komunitné pluginy alebo vlastné importy.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Alertovanie a reakcia	Náročnosť na výpočtový výkon	Výpočtovo náročné – Elastic stack vyžaduje značné zdroje pri vyšších objemoch logov a komplexných pravidlách.	Náročnosť je stredná – systém zvláda veľké objemy dát, ale potrebuje optimalizáciu.	Výpočtovo náročné pri veľkých datasetoch. Je odporúčané škálovať horizontálne pri vyššom zaťažení.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Využitie pravidiel založených na Machine Learning pri detekcii anomálií	ML detekcie podporujú tvorbu pravidiel pomocou algoritmov na analýzu správania.	Nepoužíva ML priamo – analýza sa vykonáva na základe pravidiel, nie učenia.	ML Commons umožňuje použiť modely strojového učenia priamo pri detekcii anomálií alebo správania.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.	Nepodporuje pokročilé ML modely na detekciu.
	Mapovanie detekcií na MITRE ATT&CK je implementované v rámci Elastic Security rules.	Mapovanie detekcií na MITRE ATT&CK je implementované v rámci Elastic Security rules.	Zavedené mapovanie pravidiel na MITRE ATT&CK model je priamo súčasťou riešenia.	Možné manuálne mapovanie alertov a výstupov na MITRE ATT&CK cez vlastné tagovanie a dashboardy.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.

Reportovanie a vizualizácia	Predefinované vs. custom reporty	Umožňuje tvorbu vlastných a predefinovaných reportov cez Kibana Canvas alebo Reporting plugin.	Umožňuje generovanie základných a vlastných reportov prostredníctvom rozšírení.	Možnosť definovať vlastné reporty cez Dashboards s výstupom do rôznych formátov. Prehľady sú exportovateľné.	Silná podpora vizualizácie s interaktívnymi dashboardmi a grafmi.	Vizualizácia možná cez integrovaný Elastic alebo Grafana.	Obmedzená vizualizácia alebo závislá od externých nástrojov.	Obmedzená vizualizácia alebo závislá od externých nástrojov.
	Dashboards (vrátane interaktívnych) a ich kategorizácia	Dashboards sú vysoko prispôsobiteľné, interaktívne.	Dashboards sú dostupné cez vlastné UI aj integráciu s Kibana.	OpenSearch Dashboards umožňuje tvorbu pokročilých interaktívnych panelov pre monitoring a analýzu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Exportovanie do rôznych formátov (PDF, CSV)	Export do CSV, PDF alebo prostredníctvom API – cez Reporting plugin alebo skripty.	Export dát do PDF, CSV a JSON je možný cez rozhrania a nástroje.	Exportovanie do CSV a PDF pomocou pluginov. Podpora je natívna alebo cez komunitné rozšírenia.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Roly a oprávnenia	Prístupové role sú spravované cez Kibana Spaces, podpora RBAC.	Podpora prístupu na základe rolí (RBAC) – rôzne úrovne prístupu.	Podpora RBAC – je možné definovať prístupové úrovne na základe rolí priamo v rozhraní.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Možnosť vytvárania šablón (templates) pre dashboard-y	Možnosť vytvárať vizuálne šablóny dashboardov cez Canvas alebo Lens.	Možnosť tvorby dashboard šablón a opakovaného použitia vizualizácií.	Užívateľ si môže vytvoriť šablóny dashboardov a rýchlo ich replikovať naprieč organizáciami.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Technické požiadavky	HW a SW požiadavky	RAM, CPU, disk, GPU	Odporúčané minimum 8-16 GB RAM, 4+ CPU jadrá; náročnosť rastie podľa objemu dát.	Odporúčaná konfigurácia: min. 8 GB RAM, 4 vCPU, SSD disk (50+ GB).	Odporúča sa minimálne 16 GB RAM, viacjadrový CPU a dostatok diskového priestoru (SSD preferované).	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Podporované OS (Linux, Windows)	Linux a Windows servery sú plne podporované ako host systémy aj endpointy.	Linux (server), Windows/Linux/macOS (agent) – široká multiplatformová podpora.	Podporuje väčšinu Linux distribúcií, Windows a macOS ako klientské prostredie pre Dashboards.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Možnosť virtualizácie	Elastic stack je plne virtualizovateľný (VMware, Proxmox) a kontajnerizovateľný (Docker, Kubernetes).	Podporuje virtualizáciu (VM, Docker) aj kontajner y v Kubernetes.	Je vhodný pre kontajner y, VM aj fyzické servery. Existujú Docker a Helm inštalácie pre Kubernetes.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Integrácie	XDR, CTI, SOAR, EDR, IAM, NAC, IDS/IPS, cloud (AWS, Azure, GCP)	Podporuje široké spektrum integrácií – AWS, Azure, GCP, EDR, SOAR, CTI, XDR, IAM, IDS/IPS.	Integruje sa s nástrojmi ako AlienVault OTX, Suricata, OSSEC, AWS GuardDuty.	Má množstvo dostupných integrácií s nástrojmi tretích strán – vrátane CTI, SIEM, IAM a cloud služieb.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		API (RESTful, Webhook, gRPC...)	Komplexné RESTful API pre všetky služby (Elasticsearch, Kibana, Logstash). Webhook.	Podpora REST API a Webhookov pre vstup aj výstup.	Podpora REST API, webhookov, integrácia s Elastic API a komunitné pluginy na rozšírenie funkcionalít.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Dátová vrstva (Databáza)	Normalizácia a enrichovanie dát	Dáta sú enrichované cez ingest pipeline, modul Filebeat a Logstash filter pluginy.	CTI údaje a logy sa obohatujú a normalizujú pred ďalším spracovaním.	Dáta sú normalizované pomocou ingest pipeline. Enrichment možno riešiť cez Logstash alebo Beats.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Fulltextové a rýchle vyhľadávanie	Fulltextové vyhľadávanie je jednou z hlavných funkcií Elasticsearch a je extrémne rýchle.	Elasticsearch umožňuje rýchle a komplexné vyhľadávanie cez UI alebo API.	Vysokovýkonné vyhľadávanie a agregácie cez Elasticsearch engine. Podpora fulltextu a fuzzy query.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Kompresia, archívácia	Elastic podporuje rôzne režimy archívácie a kompresie dát, vrátane hot/warm storage vrstiev.	Podporuje kompresiu a archíváciu starých dát.	OpenSearch umožňuje definovať politiky archívácie, retencie a kompresie dát podľa typu logu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Retencia (flexibilná, podľa typu logu)	Retencia dát je nastaviteľná podľa index politiky alebo typu dát (napr. 30 dní pre firewall logy).	Podpora pre definovanie retencie dát na základe ich typu.	Flexibilná retencia logov – používateľ definuje, ako dlho sa budú uchovávať rôzne typy logov.	Podpora retencie logov podľa typu údajov a business pravidiel.	Podpora retencie logov podľa typu údajov a business pravidiel.	Podpora retencie logov podľa typu údajov a business pravidiel.
	Bezpečnosť	Šifrovanie (pri prenose aj uložení)	Šifrovanie je dostupné v prenose (TLS) aj pri ukladaní. Podporované cez OS/infra (dm-crypt, cloud BYOK)	Podpora TLS/SSL pre prenosi a šifrovanie údajov v Elasticsearch.	Šifrovanie na úrovni TLS (pri prenose) a na disku (file-based encryption cez OS alebo cloud služby).	Šifrovanie pri prenose a niekde aj pri uložení je dostupné.	Šifrovanie pri prenose a niekde aj pri uložení je dostupné.	Šifrovanie pri prenose a niekde aj pri uložení je dostupné.
		RBAC a multi-factor auth	RBAC systém v Kibane a podpora SAML/LDAP; MFA je ale dostupná v Elastic Cloud službe, kde je povinná pre prístup do Elastic Cloud účtov (napr. TOTP, e-mail, hardvérové kľúče)	RBAC a podpora viacfaktorového overovania cez externé služby.	RBAC podpora v Dashboards, podpora externých identít (LDAP, SAML, OIDC). MFA je možné integrovať.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Audit trail a integrita dát	Audit trail je dostupný cez Audit logging v Elasticsearch a Kibana.	Zaznamenáva každú akciu analytika pre audit a forenznú analýzu.	Všetky zmeny a prístupy môžu byť auditované pomocou vlastných auditlog pluginov.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Prevádzkové požiadavky	Administrácia	UI/UX (prehľadnosť, responzivnosť)	Moderné rozhranie v Kibane – responzívne, modulare a podporuje dark/light módy.	Používateľsky priateľné webové rozhranie s reaktívnymi komponentmi.	Rozhranie Dashboards je moderné, responzívne a podporuje dark/light režim. UX je na vysokej úrovni.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		CLI/API podpora	CLI a API sú dostupné pre všetky hlavné služby – Elasticsearch, Kibana, Beats, Logstash.	Plná CLI a API podpora pre správu aj integráciu.	CLI a REST API podporované. Skripty môžu vykonávať všetky hlavné úlohy (query, export, nastavenia).	Dostupná CLI a API podpora pre správu a integrácie.	Dostupná CLI a API podpora pre správu a integrácie.	Dostupná CLI a API podpora pre správu a integrácie.
		Multiitenancy (izolácia zákazníkov)	Multiitenancy je podporovaná cez Kibana Spaces a zabezpečenie rolami.	Podporuje multiitenantné oddelenie zákazníkov prostredníctvom RBAC a UI.	Multiitenancy možná cez Dashboards spaces alebo izolované indexy s RBAC kontrolou prístupu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
	Prevádzkovateľnosť	Inštalácia a konfigurácia	Elastic má detailné inštalčné balíčky, kontajner y aj helm chart pre K8s.	Inštalácia je možná pomocou skriptov, kontajnerov alebo distribučných balíkov.	Inštalácia je komplexnejšia, ale dobre zdokumentovaná. Podporované sú Docker, Kubernetes, Helm.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Monitoring stavu systému (healthcheck)	Monitoring clusteru je dostupný cez Stack Monitoring alebo externé systémy (napr. Prometheus).	Podporuje automatizovaný healthcheck cez API aj rozhranie.	Zdravie systému možno monitorovať cez API, Grafana alebo vlastné vizualizácie v Dashboards.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Backup & recovery	Záloha a obnova možná cez Snapshot & Restore funkciu Elasticsearch.	Zálohovanie konfigurácií a databáz je plne podporované.	Záloha a obnova sa rieši pomocou snapshotov v Elasticsearch. Je možné plánovať a automatizovať.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Podpora, komunita a dokumentácia	Veľká komunita a rozsiahla oficiálna dokumentácia s príkladmi a tutoriálmi.	Veľmi aktívna komunita, výborná dokumentácia a open-source model.	Komunita OpenSearch je aktívna, dokumentácia je rozsiahla a existuje množstvo návodov a fór.	Veľká a aktívna komunita, dostupná základná dokumentácia a fórum.	Menšia komunita, ale dostupná základná dokumentácia.	Menšia komunita, ale dostupná základná dokumentácia.
		Aktualizácie a verzovanie	Elastic vydáva pravidelné aktualizácie a podporuje verzovanie s minimálnym výpadkom.	Pravidelné aktualizácie systému a pravidiel detekcie.	Politiky index managementu – plne podporované cez ISM (Index State Management). Plánované aktualizácie systému – cez rolling/restart upgrade.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
		Nasadenie	Môže byť nasadený na bare-metal, vo VM, Docker kontajneroch alebo v Kubernetes prostredí.	Podpora pre všetky režimy nasadenia vrátane Kubernetes a Docker.	Dostupné sú inštalčné balíky pre bare-metal, kontajner y aj Kubernetes klastre.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.

Škálovanie	Load balancing, HA, clustering	Elastic podporuje škálovanie horizontálne (viac nodov) aj vertikálne (silnejší HW) a clustering.	Možnosť horizontálneho škálovania a HA klastrovania.	Podporuje clustering, load balancing a HA architektúru pre škálovanie nasadenie.	Obmedzené možnosti škálovania.	Dobré možnosti škálovania vrátane podpory clusteringu a HA.	Obmedzené možnosti škálovania.	Obmedzené možnosti škálovania.
Rozšíriteľnosť	Rozšíriteľnosť pomocou pluginov	Logstash, Kibana a Elasticsearch podporujú pluginovú architektúru pre rozšíriteľnosť.	Pluginový systém pre rozšírenie o ďalšie funkcionality.	Možnosť rozšírenia funkcionality cez pluginy, ktoré sú vyvíjané komunitou aj Amazonom.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Automatizácia	Automatizácia (skripty, playbooky)	Automatizácia cez Watcher, Elastic Actions, skripty, alebo integrácia so SQAR alebo Shuffie.	Podporuje skriptovanie aj externé playbooky (napr. Ansible, SQAR).	Automatizácia cez API, trigger-based alerting a možnosti napojenia na orchestrátory (napr. StackStorm).	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Regulačná zhoda	GDPR, ISO 27001, PCI DSS, ...	Podpora GDPR, ISO 27001 a ďalších – v kombinácii s logovaním, retenciou, audit trailom.	Pomáha pri dosahovaní štandardov GDPR, ISO, NIST cez audit a logovanie.	OpenSearch možno nakonfigurovať tak, aby plnil požiadavky GDPR, ISO, SOC2 a iné regulačné rámce.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.	Čiastočná alebo závislá podpora; vyžaduje doplnkovú konfiguráciu.
Licencovanie	Typ licencie (open-source, freemium, komerčná)	Elastic má vlastnú licenciu (SSPL) – základ je open-source, niektoré funkcie sú v Basic/Freemium.	Plne open-source riešenie bez komerčnej licencie.	Open-source licencie pod Apache 2.0. Žiadne obmedzenia v základnej funkcionalite.	Plne open-source bez licenčných poplatkov.	Plne open-source bez licenčných poplatkov.	Plne open-source bez licenčných poplatkov.	Plne open-source bez licenčných poplatkov.
Náklady	TCO, náročnosť údržby	Náklady na infra sú vysoké (výpočtové zdroje, úložisko), ale softvér je bezplatný v basic verzii.	Stredne vysoké náklady na infraštruktúru, ale nízke licenčné náklady.	Nízke licenčné náklady, ale vyššia TCO pri zložitých integráciách a potrebe vlastnej infraštruktúry. Open-source riešenie s nízkymi licenčnými nákladmi. Vyššia celková náročnosť na údržbu pri rozsiahlych inštaláciách, vzhľadom na požiadavky na zdroje a odbornú znalosť pre správu a škálovanie systému.	Bez licenčných poplatkov, ale vyššia náročnosť na integráciu a prevádzku.	Bez licenčných poplatkov, ale vyššia náročnosť na integráciu a prevádzku.	Vyššia náročnosť na správu a údržbu, niektoré moduly zastarané.	Vyššia náročnosť na správu a údržbu, niektoré moduly zastarané.

CTI

Kategória	Podkategória	Požiadavka	Modul Threat Intel (ELK)	MISP	OpenCTI	IntelMQ	YETI	Vulmatch
Funkčné požiadavky	Typy CTI	Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)	Podpora len obmedzenej strategickej analýzy – závisí od integrácií s externými nástrojmi alebo pluginmi tretích strán.	MISP poskytuje čiastočnú podporu strategickému CTI prostredníctvom manuálneho zadávania správ a analytických poznámok.	OpenCTI poskytuje komplexnú podporu pre strategické CTI, umožňuje analytické hodnotenia a prepojenia.	Nástroj je orientovaný na zber a distribúciu technických údajov, pričom strategické CTI nie je v centre jeho zamerania.	YETI sa zameriava hlavne na operatívne a taktické CTI, strategická úroveň je slabopodporená.	Zameriava sa hlavne na automatizované párovanie IOC a CVE, strategické CTI nie je podporované.
		Podpora operatívneho CTI (TTP, profilovanie skupín)	Neposkytuje priamu podporu TTP alebo profilovanie skupín, no je možné použiť logické doplnky a korelačné pravidlá.	Podpora operatívneho CTI je silná – MISP umožňuje zaznamenávať TTP a prepojiť incidenty so skupinami.	Veľmi dobrá podpora pre TTP, organizácie, aktérov a kampane vrátane prepojení a časových línií.	Podpora pre operatívne CTI je obmedzená, väčšina funkcionality je zameraná na IOC a technické obohatcovanie.	Áno, poskytuje možnosť profilovania aktérov hrozieb a TTP, aj keď nie úplne formálne podľa ATT&CK.	Neposkytuje pokročilú funkcionality pre TTP alebo profilovanie útočníkov.
		Podpora taktického CTI (IOC, IP, hash, URL, domény)	Dobrý základ pre IOC – prostredníctvom vlastného indexovania a dashboardov v Kibane možno uchovávať a vizualizovať IOC.	MISP je navrhnutý na správu IOC ako sú IP adresy, hashe, domény a ďalšie artefakty.	Podpora IOC je komplexná – OpenCTI zvláda IP, hashe, domény, URL a ďalšie artefakty.	Plná podpora taktického CTI – IOC ako IP, hash, URL sú hlavnou doménou IntelMQ.	Podporuje IOC – IP, hash, URL, domény sú primárnymi entitami.	Základná funkcionality – technické IOC a CVE párovanie.
	Zber údajov	Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	Obmedzená možnosť – niektoré dáta možno ťahať cez pluginy a API, ale chýba natívne spracovanie špecializované na CTI.	Podporuje široké spektrum open-source a komunitných zdrojov. Automatizácia je možná pomocou cron jobov a API.	Disponuje pokročilým zberom údajov pomocou konektorov, ktoré umožňujú napojenie viacerých typov zdrojov.	Automatizovaný zber údajov z rôznych open-source zdrojov je hlavná funkcionality IntelMQ.	Zber z komunitných a open-source zdrojov je možný pomocou scraperov a pluginov.	Zber údajov je možný z niekoľkých zdrojov, ale závisí od implementácie.
		Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Závisí od toho, čo používateľ nakonfiguruje – cez Logstash a externé konektory možno integrovať niektoré z týchto zdrojov.	MISP má natívnu podporu pre Abuse.ch, Malware Bazaar a iné prostredníctvom integrovaných modulov.	Natívne konektory pre Abuse.ch, Malware Bazaar, MISP a OTX zabezpečujú kvalitný prístup dát.	Podporuje množstvo zdrojov cez moduly vrátane Abuse.ch, MISP a ďalších.	Má niekoľko dostupných konektorov na MISP, Abuse.ch, Malware Bazaar a ďalšie.	Čiastočná podpora pre zdroje ako MISP a VulDB.
		Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io	Podpora závisí od pluginov ako ElastAlert alebo vlastných prepojujúcich skriptov – nie je predpripravená funkcionality.	Podporuje integráciu s externými službami ako VirusTotal, Shodan a ďalšími cez moduly.	K dispozícii sú konektory na VirusTotal, Shodan, DomainTools a ďalšie externé zdroje.	Integrácia s externými službami ako VirusTotal je možná cez rozšírenia.	Integrácie s externými API sú možné, ale vyžadujú custom integrácie.	Integrácia s API ako Shodan alebo VirusTotal nie je priamo dostupná.
	Normalizácia	Schopnosť normalizovať CTI dáta na jednotný formát	Nástroj nie je primárne určený na CTI normalizáciu, no je možné transformovať dáta pomocou Logstash a pipelines.	Schopnosť normalizovať dáta na STIX-like štruktúru je výborná. Záznamy majú štandardizovaný formát.	Normalizácia prebieha na úrovni entít a vzťahov v súlade so STIX 2.1 štandardom.	IntelMQ disponuje silnou schopnosťou normalizovať technické údaje do jednotnej štruktúry (Message format).	Normalizácia údajov prebieha na úrovni entít a tagov – stredne pokročilá funkcionality.	Normalizácia údajov nie je plne podporená.
	Spracovanie	Možnosť manuálnej analýzy CTI	Umožňuje manuálnu analýzu prostredníctvom Kibany a Elastic Search, ale nie je určený na komplexnú analýzu hrozieb.	Umožňuje manuálnu analýzu IOC a prepojených hrozieb. Analytici môžu vkladať vlastné hodnotenia.	GUI umožňuje analytikom manuálnu prácu s údajmi, pridávanie komentárov a hodnotení.	Umožňuje jednoduchú manuálnu analýzu cez CLI alebo externé vizualizačné nástroje.	Analytici môžu vykonávať manuálnu analýzu IOC v UI.	Nástroj neobsahuje vizuálne rozhranie pre manuálnu analýzu.
		Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	Modul Threat Intel ponúka len čiastočne poloautomatizované spracovanie údajov na základe konfigurovateľných pipeline (napr. ingest pipeline alebo Logstash rules)	MISP umožňuje poloautomatizované spracovanie pomocou event-action pravidiel.	Automatické obohatcovanie pomocou konektorov je možné, ako aj zjednocovanie dát z rôznych zdrojov.	Silná stránka IntelMQ je automatizované spracovanie pomocou pipeline systému (botov).	Podporuje automatické importy IOC a entít, poloautomatické obohatcovanie.	Automatizované spracovanie CVE/IOC párovania je hlavná funkcionality.
		Podpora automatizovaných playbookov (low-code/no-code)	Podpora workflowov alebo spracovania dát cez playbooky je obmedzená, dostupná len cez integrácie alebo vlastné skripty.	Existuje možnosť nastaviť niektoré úlohy ako workflow, ale nejedná sa o low-code systém.	Podpora playbookov cez konektory (napr. low-code tooly ako TheHive alebo MISP).	Nepodporuje low-code/no-code playbooky, ale workflow je modulárny.	Nepodporuje playbooky v pravom zmysle – je skôr databázou IOC a entít.	Nepodporuje playbooky.
		Deduplikácia hrozieb a informácií	Deduplikácia je možná pomocou Elastic funkcií, no nie je špecificky zameraná na hrozby – vyžaduje pokročilé nastavenia.	Deduplikuje IOC na základe UUID a typu – bráni opakovaným záznamom.	Systém obsahuje mechanizmy pre deduplikáciu entít a IOC na základe identifikátorov.	Čiastočná deduplikácia pomocou vlastnej logiky spracovania údajov.	Čiastočne umožňuje deduplikáciu IOC na základe hashov a identifikátorov.	Neobsahuje deduplikáciu hrozieb.
	Integrácia	Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Možnosť prepojenia s inými bezpečnostnými systémami ako SIEM a firewall existuje, ale vyžaduje konfiguráciu.	Integrácia so SIEM a firewall je bežná, využívaním REST API a MISP feedov.	Integrácia so SIEM cez exportné konektory alebo priamy prístup k databáze GraphQL API.	Môže byť integrovaný so SIEM (napr. pomocou exportu údajov cez JSON, syslog).	Integrácia do SIEM a ďalších nástrojov je možná, ale často vyžaduje manuálne exporty.	Možná jednoduchá integrácia so SIEM pomocou exportu IOC.
	Sandboxing	Možnosť testovania IOC a súborov v sandbox prostredí	Nástroj nemá vlastné sandboxing schopnosti – je potrebné doplniť inými nástrojmi.	Nepodporuje sandboxing – testovanie súborov je nutné cez externý systém.	Sandboxing nie je integrovaný, ale je možná integrácia s Cuckoo alebo JoeSandbox.	Neposkytuje sandboxing – je potrebná integrácia s externými sandbox nástrojmi.	Nepodporuje sandboxing.	Sandbox nie je súčasťou nástroja.

Technické požiadavky	Vizualizácia	Vizualizácia threat intelligence dát (Kibana, grafy, dashboards)	Kibana poskytuje silnú vizualizáciu vrátane grafov, heatmap, časových línii – vhodné na IOC a časové analýzy.	Podporuje základnú vizualizáciu pomocou vstavaných štatistických prehľadov a grafov.	Interaktívne vizualizácie – grafy entít a ich prepojení, časové osi a štatistiky.	Vizualizácia nie je vstavaná – vyžaduje integráciu s Kibana, Grafana, alebo ELK.	Obsahuje vlastné dashboards a jednoduché vizualizačné komponenty.	Neposkytuje vlastné vizualizácie.
	Frameworky	Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	Možnosť čiastočného mapovania pomocou dashboardov alebo vlastných polí, ale bez natívneho MITRE frameworku.	MISP má modul na prepojenie so systémom MITRE ATT&CK pomocou Galaxy tagov.	Plná integrácia s MITRE ATT&CK – entita TTP je základným stavebným prvkom.	Nepodporuje MITRE ATT&CK framework priamo.	Nepodporuje MITRE ATT&CK, ale umožňuje manuálne tagovanie TTP.	Nepodporuje ATT&CK framework.
	Formáty a štandardy	Podpora formátov ako STIX/TAXII	STIX/TAXII nie je podporované natívne – potreba riešiť prostredníctvom doplnkov alebo ďalšej aplikácie.	Plná podpora STIX a TAXII 2.1 – výborné pre interoperabilitu s inými systémami.	Podpora STIX/TAXII je vstavaná – import/export aj feedovanie je bezproblémové.	Nepodporuje STIX/TAXII – pracuje s vlastným formátom spracovania údajov.	STIX/TAXII podpora je limitovaná.	STIX/TAXII nie je podporovaný.
Prevádzkové požiadavky	Zdroje	Podpora najväčšieho počtu autoritatívnych CTI zdrojov	Zdrojová podpora je obmedzená na to, čo si administrátor nakonfiguruje manuálne.	Podpora mnohých CTI zdrojov ako CIRCL, OTX, MISP komunitné huby, Anomali atď.	Najvyššia úroveň podpory CTI zdrojov – vďaka rozšíriteľným konektorom.	Podporuje množstvo otvorených zdrojov vďaka bohatému ekosystému botov.	Podporuje viacero zdrojov, no ich počet je nižší ako pri MISP alebo OpenCTI.	Zdroje sú obmedzené, ale pokrývajú niekoľko relevantných databáz.
	Efektivita	Možnosť použitia AI na automatizované spracovanie a filtrovanie	Neposkytuje natívnu AI funkcionality pre spracovanie – je potrebné doplniť pomocou ML doplnkov v Elastic Stack.	MISP nevyužíva ML priamo, ale existujú externé integrácie, ktoré to umožňujú.	Nástroj podporuje ML vo forme obohatenia, prioritizácie a klasifikácie entít (v budúcich verziách).	Neobsahuje AI modul, ale dáta môžu byť odovzdané iným systémom na spracovanie.	Nepodporuje AI – pracuje prevažne manuálne alebo poloautomaticky.	Nepodporuje AI, ale algoritmicke šetrí čas spájaním CVE–IOC.
		Zníženie potreby manuálnej analýzy – šetrenie času analytikov	Zníženie manuálnej práce nie je prioritou tohto modulu – vyžaduje manuálne ladenie, dashboards a ručnú koreláciu.	Automatizácia filtrácie znižuje záťaž analytikov pomocou feed filtrov a TTL politiky.	Silná miera automatizácie a deduplikácie šetrí analytikom značné množstvo práce.	Znižuje potrebu manuálnej práce cez vysoký stupeň automatizácie v pipeline.	Znižuje záťaž na analytikov v oblasti základného IOC obohatenia.	Umožňuje automatizovať niektoré úkony, čím šetrí čas analytikom.

SOAR

Kategória	Podkategória	Požiadavka	Shuffle	TheHive+ Cortex	StackStorm	Fasten Health Tracecat (ex-Kuiper)	FIR (Fast Incident Response)
Funkčné požiadavky	Zber a vstupy	Prijímanie upozornení a dát z rôznych bezpečnostných systémov	Podporuje workflow a zber z rôznych systémov	Zber alertov zo SIEM, EDR, CTI	Trigger-based integrácia	Zamerané na incidenty z healthcare systémov	Webhook alebo REST input
		Normalizácia a parsovanie dát	Cez vlastné skripty/parsing	Podporuje parsing observables	Môže spracovať a upraviť formát dát	Parsovanie závisí od backendu	Parsovanie základné
		Podpora STIX/TAXII, JSON, syslog	JSON, STIX podporované cez pluginy	JSON, STIX, syslog podporované	STIX/TAXII manuálne	Čiastočná podpora JSON	Podpora JSON a časti STIX
	Incident Management	Kategorizácia a prioritizácia incidentov	Podpora priorít a štítkov	Silné tagovanie a typovanie incidentov	Incidenty kategorizované cez metadata	Základná kategorizácia podľa typu	Kategórie incidentov voliteľné
		Možnosť manuálneho aj automatického vytvárania incident ticketov	Áno, manuálne aj cez trigger	Áno, manuálne aj cez API	Trigger vytvára ticket	Ručný vstup + API	Ručne alebo cez API
		Úprava ticketov a lifecycle management	Nie je podporované	Kompletné lifecycle workflow	Workflow manažment dostupný	Záznam a editácia incidentov	Základný lifecycle (Open, Investigating, Closed)
	Pravidlá a politiky	Preddefinované playbooks	Áno, basic playbooky dostupné	Vzory (template cases) preddefinované	Vzory workflowov existujú	Niekoľko preddefinovaných typov	Šablóny nie sú natívne
		Možnosť tvorby vlastných playbookov bez potreby programovania	Playbook editor pre ne-programátorov	Užívateľské šablóny bez kódu	Z GUI je možné vytvárať playbooky	Limitovaná tvorba bez kódu	Zápis typu incidentu ručne
		Workflow engine s vetvením, podmienkami a slučkami	Silný workflow engine s vetvením	Cez pravidlá a workflow šablóny	Mimoriadne silný workflow systém	Jednoduché workflow štruktúry	Workflow nie je engine-based
	Automatizácia reakcií	Spúšťanie akcií na základe triggerov	Spúšťanie cez REST, UI aj eventy	Cez Cortex akcie (analýzy/respondery)	Trigger + action kombinácia	Trigger + akcia	Trigger cez API
		Podpora pre manuálne schválenie alebo automatické pokračovanie	Možnosť manuálneho zásahu	Manuálne potvrdenie voliteľné	Možnosť schvaľovacích krokov	Ručné schválenie dostupné	Ručný krok potvrdenia
		Automatizované reakcie: blok IP, izolácia hostu, eskalácia	Základné reakcie podporené	Silné možnosti odpovedí (napr. ban IP)	Action chaining pre reakcie	Základná reakcia možná	Reakcie obmedzené
	Orchestrácia	Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	Integrácia so SIEM, EDR, atď. cez konektory	Široká integrácia cez analýzy	Rozsiahla integrácia (SIEM, firewall...)	Integrácia API, niekedy cez FHIR	Čiastočné napojenie na iné nástroje
		Centrálne logovanie akcií v playbookoch	Auditný záznam akcií možný	Logovanie akcií v histórii	Logovanie výstupu krokov	Logovanie čiastočné	Loguje kroky incidentu
Integrácie	API a konektory	API-first prístup (REST, Webhooks)	REST API first dizajn	REST API	REST API	REST API podporované	REST API
		Podpora pre plug-iny a konektory	Podpora pluginov	Rozšíriteľné cez moduly	Packy (pluginy)	Nadstavba na pluginoch	Bez plugin systému
		Možnosť vytvárať vlastné konektory	Vlastné konektory cez UI alebo Python skripty	Respondery + analýzy	Nové packy sa dajú tvoriť	Vlastné konektory cez backend	Nie
	CTI a enrichment	Integrácia s CTI zdrojmi (Shodan, VirusTotal, AbuseIPDB...)	Integrácie napr. s MISP, OTX	Cortex má MISP, VT, AbuseIPDB	Integrácia s CTI možná manuálne	CTI len cez externé API	CTI len ak manuálne importované
Užívateľské rozhranie	UI	Webové UI pre správu incidentov a playbookov	Moderné a jednoduché UI	Web UI je dobre štruktúrované	Web UI existuje, menej UX-friendly	UI je moderné, ale špecifické	Web UI je jednoduché
		Intuitívne vizuálne modelovanie workflow	Workflow editor je vizuálny	Workflow jednoduchý aj pokročilý	Menej vizuálne	Nie veľmi vizuálne	Bez vizuálneho workflow
		Dashboardy pre stav a štatistiky incidentov	Základné dashboardy cez plug-in	Štyri základné dashboardy Alerts, Cases, Observables, TTPs	Limitované dashboardy	Štatistiky limitované	Dashboardy nie sú
Prevádzka a nasadenie	Nasadenie	On-prem / cloud / hybrid možnosť	Local, hosted, cloud and Hybrid	Linux server, on-prem odporúčaný, cloud podporuje tiež	On-prem odporúčané	On-prem a SaaS	On-prem jediná možnosť
		Podpora kontajnerizácie (Docker, Kubernetes)	Podpora Docker/K8s	Docker je plne podporovaný	Plná kontajnerová podpora	Docker podpora	Docker build existuje
	Prevádzka	High availability a clustering	Základná podpora HA	HA riešiteľné manuálne	HA podporované cez RDB cluster	HA nie natívne	HA nie natívne
		Backup & recovery playbookov a konfigurácie	Export konfigov a workflow	Záloha cez export	Backup cez export yaml	Export yaml konfigov	Backup cez databázu
Bezpečnosť	Prístup a audit	RBAC a audit trail	RBAC prítomné	RBAC definovaný	RBAC doplniteľné	Základný RBAC	RBAC pre role
		Šifrovanie dát v prenose a uložené dáta	HTTPS, šifrovanie podporované	HTTPS, šifrovanie štandard, TLS/SSL -> AES-256	SSL podpora	SSL, šifrovanie	HTTPS
		MFA podpora	Podporuje natívne MFA	TOTP-based MFA natívne podpora	MFA vyžaduje doplnky	MFA neznáme	Nie

Licencovanie a TCO	Model	Open-source / freemium / komerčný model	Open-source	Open-source	Open-source	Open-source (niektoré časti)	Open-source
		Náročnosť údržby a infraštruktúry	Nízka až stredná náročnosť	Stredná údržba	Vyššia zložitosť	Vyššia zložitosť	Nízka náročnosť
Regulačné rámce	Podpora	Podpora, komunita a dokumentácia	Veľká komunita, aktívne issue na GitHub	Dobrá dokumentácia, Git aktívny	Veľká DevOps komunita	Malá komunita	Dokumentácia OK
		Pomoc pri automatizovanom splnení GDPR, ISO 27001, SOC2	Pomáha s auditom, GDPR vyžaduje doplnky	Manuálna zhoda s GDPR možná, nie je natívne	GDPR vyžaduje konfiguráciu	Nie jasne zamerané na compliance	Nie natívne
	Zhoda	Logovanie reakčných činností pre auditné účely	Čiastočná podpora – bez jasnej špecifikácie audit trailu.	Zaznamenáva každú akciu	Logovanie výstupov workflow	Nie priamo	Záznam činností v tickete
Rozšírenia	Testovanie	Playbook debugging & testing	Áno, debugger súčasťou	Nie priamo	Debugger súčasťou	Debugger dostupný	Nie
	Simulácia	Simulácia incidentov (purple teaming podpora)	Nie priamo	Nie	Simulácia len cez testovacie runy	Nie	Nie
	Integrácia	SOAR-SIEM synchronizácia stavu incidentov	Nie natívne	Áno cez prepojenie so SIEM	SIEM sync voliteľný	Nie natívne	Čiastočný sync
	Verzovanie	Integrácia s verzionovacím systémom (napr. Git)	Nie	Export JSON + GIT	Export balíkov	Manuálne verzovanie	Nie
	Prevádzka	Multitenancy – izolácia medzi viacerými klientmi	Podporuje	Nie natívne	Nie natívne	Nie	Nie

EDR

Kategória	Podkategória	Požiadavka	Elastic Security	Wazuh	OSSEC	OpenEDR	Velociraptor
Funkčné požiadavky	Nasadenie	Možnosti nasadenia: on-prem, cloud, hybrid	Áno, podpora on-prem aj cloud	Áno, on-prem, cloud aj hybrid	On-prem only	Cloud aj on-prem	On-premise, cloud-ready
	Ochrana prostredí	Podpora pre cloudové, kontajnerové a serverové prostredia	Áno, vrátane Kubernetes a Docker	Áno, podpora serverov a kontajnerov	Obmedzená podpora kontajnerov	Áno, agent pokrýva viaceré prostredia	Primárne zamerané na endpointy
	Zber dát	Podpora pre rôzne OS (Windows, Linux, macOS)	Áno, Windows, Linux, macOS	Áno, všetky hlavné OS	Windows, Linux, macOS	Áno	Linux, Windows, macOS
		Zber auditovacích dát pomocou agentov	Áno, pomocou Elastic Agent	Áno, pomocou Wazuh agenta	Áno, OSSEC agent	Áno	Áno
		File Integrity Monitoring (FIM)	Áno, prostredníctvom Auditbeat	Áno, vstavané FIM	Áno	Áno	Áno
		Zber systémových metrik, procesov a správania	Áno, Beats + Agent	Áno, detekcia systémových zmien	Áno, základné metriky	Áno, vrátane správania procesov	Áno
		Zber informácií o zraniteľnostiach a konfiguráciách	Čiastočne – pomocou integrácií	Áno, cez SCA modul	Obmedzene	Áno	Nie
		Zber logov aplikácií a služieb	Áno, cez Beats	Áno, cez log collector	Áno	Áno	Áno
		Zber dát z cloudových a sieťových zdrojov	Áno, cez Elastic Integrations	Čiastočne, pomocou integrácií	Nie	Nie	Obmedzené
	Analýza	Analýza logov a korelácia s hrozbami	Áno, s pokročilou analýzou a SIEM	Áno, pravidlá a SIEM modul	Základná analýza logov	Áno, s UI	Áno, s focusom na forenznú analýzu
	Detekcia	Detekcia malvéru a narušení	Áno, detekcia pomocou pravidiel a ML	Áno, IDS a integračné pravidlá	Áno, základné IDS	Áno	Nie priame IDS
		Heuristická a behaviorálna analýza	Áno, správanie a pravidlá	Áno, základná behaviorálna analýza	Nie	Áno	Áno, behaviorálna detekcia
		Podpora ML/AI algoritmov na detekciu hrozieb	Áno, ML modul Elastic Stack	Nie priamo, bez ML	Nie	Áno, ML detekcia	Áno
		Mapovanie na MITRE ATT&CK framework	Áno (cez Elastic rules tagging)	Áno	Nie	Nie	Áno
	Reakcia	Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)	Áno, podporuje SOAR a SIEM reakcie	Áno, základné reakcie (skripty)	Obmedzené reakcie cez skripty	Áno, akcie cez UI	Nie
		Zasielanie incidentov do ticketovacích systémov / SOAR	Áno (cez webhooks, Jira, ServiceNow)	Áno	Nie	Nie	Nie
Technické požiadavky	Vizualizácia	Dashboardy na vizualizáciu incidentov a systémový stav	Áno, Kibana dashboardy	Áno, Wazuh dashboard (Kibana)	Žiadne natívne dashboardy	Áno, WebUI	Áno, WebUI
	Monitoring	Notifikácie SOC tímu o udalostiach a incidentoch	Áno, viaceré možnosti notifikácií	Áno, E-mail a webhooks	E-mail	Áno	Áno, alerty
	Výkon	Nízka systémová záťaž agenta	Stredná systémová záťaž	Nízka záťaž	Nízka	Stredná	Veľmi nízka
Prevádzkové požiadavky	Škálovateľnosť	Podpora pre stovky až tisíce endpointov	Áno, enterprise škálovanie	Áno, podporuje veľké prostredia	Stredne veľké siete	Áno	Áno
	Správa	Jednoduché centrálné riadenie agentov	Áno, prostredníctvom Fleet	Áno, centralizovaná správa	Ručné konfigurácie	Áno	Áno
		Pravidelné aktualizácie signatúr a modulov	Áno, aktualizácie súčasťou Elastic Agent	Áno, aktualizácie pravidelne	Ručné aktualizácie	Áno	Áno

Skener zraniteľností

Kategória	Podkategória	Požiadavka	Greenbone Community edition	OpenSCAP
Funkčné požiadavky	Licencovanie	Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	Áno, GCE je open-source s možnosťou rozšírenia na enterprise edíciu	Áno, úplne open-source, súčasť Red Hat Security stacku
	Skenovanie	Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)	Vysoká kapacita skenovania – vhodná aj pre stovky IP denne, závisí od výkonu	Primárne orientovaný na jednotlivé hosty, nie na rozsiahle sieťové skeny
	Zraniteľnosti	Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	Áno, komunitný feed (GVMD Data Feed), prémiový podnikový feed existuje	Áno, používa OVAL, SCAP a ďalšie štandardy – aktualizácie sú manuálne alebo repozitárové
		Podpora CPE, CVE identifikátorov	Áno, výstupy sú mapované na CVE/CPE cez OpenVAS engine	Áno, štandardná súčasť SCAP
	Správa	Prijateľné webové rozhranie na správu skenovania a výsledkov	Áno, GSA (Greenbone Security Assistant) – moderné webové UI	Nie priamo, zvyčajne sa používa cez CLI alebo tretie nástroje ako SCAP Workbench
	Skenovanie	Bez potreby agentov (agentless)	Áno, štandardne funguje ako agentless nástroj	Áno, funguje bez agentov na báze politiky SCAP/OVAL
		Podpora plánovania úloh a alertov (voliteľné)	Áno, GVM podporuje plánovanie skenov a automatické správy	Nie natívne, skôr závislé od externého plánovača ako cron
	Funkcie	Tikety na nápravu – integrácia alebo export	Export do CSV, PDF, XML, API; nie natívny ticketing, ale možné napojenie	Export do ARF/HTML, nie priama integrácia s ticketing systémami
Technické požiadavky	Reporty	Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)	Áno – podpora CSV, XML, PDF, HTML výstupov	Áno – hlavne ARF, HTML, XML (v závislosti od použitej nadstavby)
	Nasadenie	Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	On-premise, Docker a VM podpora (kontajnerové verzie dostupné)	Primárne on-premise, je možné nakonfigurovať ako kontajner
	HW požiadavky	Minimálne a odporúčané technické požiadavky (RAM, CPU, disk)	Min. 4 GB RAM, 2 vCPU, SSD disk; odporúčaných 8+ GB RAM	Nízke nároky – beží aj na 1 vCPU, 1 GB RAM, podľa rozsahu
		Počet vCPU	Minimálne 2, odporúčané 4+ pre väčšie siete	1 postačuje, ak sa nepoužívajú rozsiahle výpočty
		Max. počet sieťových adaptérov	Závisí od hostiteľa, GVM nemá vlastné limity	Bez obmedzenia – pracuje nad OS, nevyžaduje adaptéry
	Architektúra	Architektúra skenovania (monolitická alebo master/senzor)	Podporuje master-senzor architektúru pre veľké siete	Monolitická architektúra, bez podpory senzora
	Podpora protokolov	Povinné: DNS, DHCP	Áno, dokáže rozpoznať DNS aj DHCP služby počas skenu	Nie primárne určený na sieťové protokoly
		Voliteľné: NTP, GMP, HTTPS, SSH, SNMP, Syslog, IPv6, LDAP, RADIUS	Áno – GMP, SSH, SNMP, HTTPS, LDAP, IPv6, RADIUS, voliteľné pluginy	Podpora závisí od použitej politiky – SCAP štandardy môžu zahŕňať protokoly
Prevádzkové požiadavky	Integrácie	Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	Vysoká kapacita skenovania – vhodná aj pre stovky IP denne, závisí od výkonu	Možné cez OpenSCAP výstupy a následnú konverziu
	Skóre	Podpora pre CVSS 4.0	CVSSv3 podporované, CVSSv4 pripravované	Podporuje CVSS cez OVAL definície
	Aktualizácie	Podpora pre EPSS – predikcia zneužitia zraniteľností	Nie natívne, ale možnosť rozšírenia cez externé CTI feedy	Nie natívne, ale možné doplniť ručne do hodnotení
		Možnosť manuálnych aktualizácií, alebo vlastná implementácia	Áno – cez CLI a GUI je možné aktualizovať manuálne	Áno – OpenSCAP aktualizácie závislé od distribúcie (napr. Red Hat feeds)
		Operatíva	Zabezpečenie výnimky v bezpečnostných systémoch pri skenovaní	Áno, beží lokálne, vyžaduje len prístup k OS
Prevádzkové požiadavky	Zhodnosť	Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)	Podpora BSI, ISO 27001 a ďalších – reporty orientované na štandardy	Primárne orientovaný na CIS, STIG, NIST – veľmi silná stránka nástroja

Incident handling

Ticketing												
Kategória	Podkategória	Požiadavka	TheHive	Zammad	Request Tracker (RT)	osTicket	RTIR	Kibana (ELK)	Grafana	BookStack	Wiki.js	
Ticketing	Funkčné požiadavky	Základné funkcie	Vytvorenie a editácia záznamov (ticketov)	Podpora vytvárania a editácie ticketov s detailnými údajmi	Plná podpora tvorby a úpravy ticketov cez GUI aj API	Základná funkcionálna na vytváranie a správu ticketov	Jednoduché rozhranie na tvorbu a editáciu ticketov					
			Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)	Flexibilná správa stavov incidentov	Plná podpora workflow a zmena stavov	Možnosť definovať vlastné stavy ticketov	Prednastavené aj custom workflow stavy					
			Priradenie na konkrétného riešiteľa (L1 analytik, eskalácia L2/L3)	Priradenie úloh analytikom podľa rolí a eskalácie	Možnosť pridelenia ticketov jednotlivým agentom	Plne podporované, s možnosťou nastavenia SLA	Podpora priradenia aj pre viaceré tímy					
		Notifikácie	Emailové notifikácie o zmenách stavu, komentároch, deadline	Plne konfigurovateľné emailové upozornenia aj webhooks	Prispôsobiteľné notifikácie podľa udalostí	Notifikácie pre všetky dôležité akcie v tickete	Automatické upozornenia podľa typu udalosti					
		Prílohy a dôkazy	Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)	Podpora nahrávania rôznych typov súborov do prípadu	Podpora príloh aj cez drag-and-drop	Možnosť pripojenia logov, screenshotov k ticketom	Jednoduché nahrávanie príloh v tickete					
		Časové údaje	Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)	Detailná časová evidencia všetkých akcií	Sledovanie SLA aj vlastné metriky	Zaznamenáva všetky dôležité časové udalosti	Časová stopa od vytvorenia po uzavretie					
		Prioritizácia	Nastavenie priority a závažnosti incidentu	Nastaviteľné úrovne priority a závažnosti	Možnosť ručne alebo automaticky nastaviť prioritu	Konfigurovateľné úrovne kritickosti	Základná podpora priorít v systéme					
		Šablóny	Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	Podpora preddefinovaných šablón prípadov	Vytváranie preddefinovaných šablón ticketov	Podpora ticketových šablón pomocou rozšírení	Šablóny dostupné pre rýchle zadanie					
		Tagovanie	Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	Podpora tagovania observables a prípadov	Plne konfigurovateľné tagy a ich správa	Možnosť vytvárať štítky a vyhľadávať podľa nich	Jednoduchý tagovací systém					
	Technické požiadavky	Integrácie	Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov, reportovanie a asset management nástrojmi	Rozsiahle možnosti integrácií cez Cortex, MISP, API	Podpora pre SIEM a ITSM systémy	Možné prepojiť pomocou rozšírení a pluginov	Podpora pre niektoré externé systémy cez API					
		API	Podpora REST API a Webhookov	Plne dokumentované REST API a webhooks	REST API pre integráciu so systémami	Rozsiahle API na správu ticketov	REST API a webhook integrácie					
		Export	Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	Možnosť exportu cez GUI aj API	Export do viacerých formátov	Podpora CSV a JSON exportu	Možnosť exportovať dáta z GUI aj backendu					
		UX/UI	Moderné, responzívne webové rozhranie	Intuitívne a responzívne GUI zamerané na analytikov	Moderný dizajn s rýchlou odozvou	Jednoduché, ale zastarané UI	Priateľské rozhranie, mierne zastarané					
	Prevádzkové požiadavky	Audit a transparentnosť	Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	Podrobný audit trail vrátane zmien observables	Plne logované všetky úkony používateľov	Záznam o všetkých aktivitách v tickete	Audit logy dostupné v systéme					
		Historická evidencia	Možnosť spätného prehľadu a forenzej analýzy	Historický prehľad vrátane observables a reakcií	Logovanie vrátane dátumov a zmien	Dostupná história záznamov	Prehľad o všetkých zmenách dostupný					
		Multitenancy	Podpora viacerých organizačných jednotiek (oddelenia, zákazníci)	Podpora organizácií a oddelení so zdieľaním	Viacúrovňová správa oddelení	Základná podpora oddelení cez rozšírenia	Podpora viacerých oddelení cez skupiny					
		SLA monitoring	Meranie času riešenia a dodržiavania SLA na jednotlivých úrovniach	Nastavenie a sledovanie SLA priamo v tickete	Možnosť konfigurácie SLA pravidiel	Základná SLA funkcionálna	Nastaviteľné SLA podľa typu ticketu					
		Role a oprávnenia	Podpora RBAC – prístupové úrovne pre rôzne role	Detailný RBAC systém podľa rolí a funkcií	Prístupová politika podľa skupín	RBAC pre jednotlivé fronty a úlohy	Jednoduchý RBAC podľa rolí					
		Prípádová správa	Tvorba a správa prípadov (cases) s úlohami a detailmi	Plnohodnotná správa prípadov cez prehľadné GUI s úlohami, observables a komentármi.			RTIR umožňuje vytvárať a spravovať prípady cez moduly ako incident, investigation, report.					
			Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)	Podpora pre rôzne typy observables –IP, domény, URL, hash, ktoré možno prepojiť s CTI zdrojmi.			Sledovanie observables je obmedzené a vyžaduje doplnenie cez pluginy alebo vlastné skripty.					

Evidencia a správa incidentov	Funkčné požiadavky		Prepojenie medzi prípadmi na základe spoločných indikátorov	Možnosť prepojenia prípadov pomocou observables a vizuálne zobrazenie väzieb.				Prepojenie medzi prípadmi je manuálne – pomocou ID alebo poznámok, nie automatizované.				
		Kategorizácia	Kategorizácia incidentov pomocou tagov	Používateľom možno prideľovať tagy a kategórie incidentov pre jednoduchšie filtrovanie.				Používateľské štitky a kategórie je možné vytvárať cez rozšírené vlastnosti ticketu.				
		Analýza a obohacovanie dát	Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Integrácia s MISP, Cortex a ďalšími nástrojmi umožňuje automatické obohacovanie údajov.				Obohacovanie dát je možné len manuálne alebo cez integráciu s externými CTI systémami.				
		Konfigurácia	Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	GUI umožňuje konfigurovať metriky, šablóny prípadov a spravovať observables medzi organizáciami.				Konfigurácia je dostupná cez CLI alebo web GUI, ale nie je natoľko flexibilná ako TheHive.				
	Technické požiadavky	Roly a prístup	Podpora viacerých používateľských rolí – minimálne analytik a administrátor	Podpora viacerých úrovní rolí (admin, analyst, observer) a ich oprávnení.				RTIR podporuje prístupové úrovne, ale menej intuitívne ako moderné platformy.				
		Multitenantnosť	Možnosť vytvárať viaceré organizácie, pravidiel zdieľania medzi nimi	Plná podpora multitenantného prostredia s izoláciou medzi organizáciami.				Podpora pre viac organizácií je dostupná, ale náročnejšia na konfiguráciu.				
		Integrácie	Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	Podporuje štandardné API pre integráciu s ďalšími bezpečnostnými komponentmi ako SIEM, SOAR, CTI.				Existujúce pluginy umožňujú základnú integráciu s externými systémami (SIEM, CTI).				
		Export a reporting	Export incidentov do formátov CSV, PDF, cez REST API	Možnosť exportu do CSV a PDF; REST API podporuje komplexné reportovanie.				Export možný cez rozšírenia alebo skripty (primárne CSV, obmedzené PDF).				
		Záznam činnosti	Logovanie činností analytikov počas riešenia incidentu (audit trail)	Každá zmena alebo aktivita v tickete je zaznamenaná do auditného logu.				Sledovanie akcií je základné – auditné logy sú súčasťou core systému.				
	Prevádzkové požiadavky	Správa systému	Jednoduchá správa konfigurácií a aktualizácií	Konfiguračné možnosti dostupné cez GUI alebo API, ľahká správa šablón a pravidiel.				Správa konfigurácie je realizovaná cez konfiguračný web GUI; aktualizácie ručné.				
		Prispôsobiteľnosť	Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	Používateľ si môže definovať vlastné typy polí, štruktúry a typy incidentov.				Vlastné polia je možné doplniť pomocou rozšírení (Custom Fields).				
		Viditeľnosť a spätná analýza	Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	Incidenty sú uchovávané s históriou zmien, podporovaná spätná analýza cez dashboard.				História ticketu sa ukladá, ale bez grafickej spätnej vizualizácie.				
		Prepojenie tímov	Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	Zdieľanie prípadov medzi organizáciami možné s definovaním prístupových pravidiel.				Zdieľanie možné cez prístupové skupiny, ale nie v reálnom čase s prepojenými tímami.				
Funkčné požiadavky		Prehľad	Vytvorenie základného prehľadu stavu bezpečnosti a incidentov					Podporuje prehľadné vizualizácie z Elasticsearch dát, vrátane incidentov.	Dashboards poskytujú flexibilný pohľad na metriky a incidenty z viacerých zdrojov.			
		Distribúcia	Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)					Distribúcia reportov možná cez automatické plánovanie (X-Pack), e-mailové odosielanie vyžaduje licenciu.	Automatická distribúcia dostupná cez Grafana Alerting + Reporting pluginy.			
		Prispôsobenie	Možnosť výberu obsahu reportu – časové obdobie, typy incidentov					Podporuje prispôsobenie času, polí a typov vizualizácií v reportoch.	Plná kontrola nad časovým rozsahom, premennými a dátovými filtrami.			

Reportovanie		Automatizácia	Plánovanie pravidelných (napr. denných, týždenných) reportov						Plánovanie reportov dostupné cez Reporting modul, niektoré funkcie viazané na platenú verziu.	Možnosť plánovania exportov cez Grafana Reporting plugin (v open source limitované).		
		Ad-hoc výstupy	Možnosť generovania jednorazových ad-hoc reportov						Podporuje jednorazové exporty cez GUI aj API.	Jednoduchý export z dashboardu pre ad-hoc účely.		
		Personalizácia	Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)						Obmedzené možnosti úprav vzhľadu reportu v základnej verzii.	Možnosť prispôsobenia pomocou vlastných šablón a HTML hlavičiek (plugins).		
	Technické požiadavky	Formáty výstupu	Podpora exportu do PDF, CSV, JSON						Export do PDF a CSV (X-Pack), JSON cez API.	Podpora exportu do PDF, PNG (cez pluginy), CSV cez panel.		
		Integrácia	Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...						Silná integrácia s Elastic Stack, SIEM, CTI, Beats, Logstash.	Integrácia so SIEM (Elastic, Loki), Prometheus, InfluxDB, PostgreSQL a ďalšie.		
		Vizualizácia	Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy						Interaktívne grafy, mapy, časové rady, metriky a heatmapy.	Široká paleta widgetov: grafy, tabuľky, histograpy, alerty, mapy.		
		Zdroje dát	Podpora rôznych zdrojov: databázy, logy, API výstupy						Natívne pracuje s Elasticsearch, API integrácie sú dostupné.	Podporuje viac ako 30+ zdrojov vrátane SQL, API a cloudových nástrojov.		
		Prístup	Webové/GUI rozhranie pre tvorbu a správu reportov						Moderné rozhranie v prehliadači pre tvorbu dashboardov a reportov.	Moderné GUI, responzívne a prispôsobiteľné z hľadiska panelov.		
	Prevádzkové požiadavky	Audit a archivácia	Možnosť archivácie vygenerovaných reportov						Možnosť uloženia a prístupu k reportom cez Reporting modul.	Exporty môžu byť archivované cez skripty alebo pluginy (napr. Grafana Image Renderer).		
		Prístupové práva	Možnosť obmedziť prístup k reportom podľa rolí (RBAC)						RBAC podpora cez Elastic Security, závisí od edície.	RBAC dostupné, základná úroveň oprávnení aj vo free verzii.		
		Zabezpečenie	Šifrované prenosy reportov pri automatickej distribúcii						Podporuje TLS/SSL pre zabezpečenú distribúciu a prístup.	HTTPS podpora a základné bezpečnostné opatrenia pre API aj GUI.		
SOC knowledge portal	Funkčné požiadavky	Správa obsahu	Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)	KB články – vytváranie/editácia OK, zabudované verzovanie chýba (vyžaduje externé riešenie)							Plná podpora tvorby, úprav a verzovania dokumentov a kníh.	Pokročilá tvorba, verzovanie a schvaľovanie článkov vrátane úprav cez Git.
		Správa obsahu	Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)	Podpora observables a prípadových šablón s tagmi, ale nie štruktúrovaných dokumentov v KB forme.							Podpora štruktúrovaných dokumentov s hierarchiou: kníhy, kapitoly, stránky + tagy.	Plná podpora kategórií, tagov, sekcií a vlastných polí.
		Vyhľadavanie	Fulltextové vyhľadavanie s podporou filtrov a tagov	Možnosť vyhľadávania podľa názvov, observables a tagov; nie fulltext nad textom ako v wiki.							Výkonné fulltextové vyhľadavanie, podpora filtrov a vyhľadavanie podľa značiek.	Výkonné vyhľadavanie s podporou ElasticSearch a MongoDB backendom.
		Prepojenie s incidentmi	Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	Prepojenie cez observables a prípady, ale nie samostatné KB položky.							Možné manuálne prelinkovanie alebo vloženie odkazov na incidenty.	Možnosť manuálneho linkovania incidentov alebo externých systémov.
		Odkazy a prílohy	Možnosť vkladať obrázky, logy, odkazy a prílohy	Možno pripojiť logy, obrázky a súbory k incidentom alebo prípadom.							Jednoduché pridávanie obrázkov, kódov, dokumentov, tabuliek, súborov.	Vkládanie príloh, obrázkov, kódových blokov, diagramov (PlantUML, Mermaid).
		Prístupové práva	Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie	Silné RBAC možnosti s granularitou prístupov pre organizácie a role.							Podpora RBAC: čítanie, úprava, mazanie, schvaľovanie podľa role a kníhy.	RBAC podľa rolí, s jemne definovateľným oprávnením na sekciu alebo článok.

	Technické požiadavky	Integrácie	Možnosť integrácie s ticketingom, incident managementom, SIEM	Integrácia s MISP, Cortex, SIEM cez API, ticketovacie systémy nepriamo.							Možná integrácia cez API a webhooks, pre SIEM a ticketing potreba middleware.	Integrácia cez REST API, Git synchronizácia, webhooks a 3rd party pluginy.
		Export	Export dokumentov do PDF, HTML alebo Markdown formátu	Export prípadov a observables cez API alebo CSV, nie plnohodnotné KB články.							Natívny export do PDF, HTML, Markdown, tiež cez CLI a API.	Export do PDF, HTML a Markdown + synchronizácia so vzdialeným Git repozitárom.
		UI/UX	Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Intuitívne GUI pre prípadovú správu, ale nie ako plnohodnotný editor pre dokumentáciu.							Jednoduché a pekné rozhranie s editorom WYSIWYG a Markdown podporou.	Responzívne, moderné rozhranie s podporou viacerých editorov (WYSIWYG, Markdown).
	Prevádzkové požiadavky	Historickosť	Zachovanie histórie zmien s možnosťou obnovy staršej verzie	História prípadov je zachytená, ale nie ako verzovanie KB dokumentov.							Každá verzia dokumentu je uložená a možno sa k nej vrátiť.	Plná verzionácia článkov s možnosťou návratu, prehľad zmien a porovnávanie.
		Audit	Záznamy o tom, kto a kedy upravoval dokument	Záznam aktivity analytikov je súčasťou systému, nie špecificky pre dokumenty.							História úprav vrátane používateľa, času, zmeny viditeľná v detaile stránky.	Logovanie každého úkonu, vrátane histórie používateľov a zmien.
		Súlad s procesmi	Možnosť tvorby schvaľovacích workflow pre nové KB články	Neexistuje workflow pre schvaľovanie KB – workflow je viazaný na prípady a alerty.							Podpora schvaľovania článkov prostredníctvom rozšírení a editor prístupov.	Workflow schvaľovania nových alebo zmenených článkov, najmä vo firemnom režime.

Asset management

Kategória	Podkategória	Požiadavka	LibreNMS	pi.Alert	NetBox	Ralph	GLPI
Funkčné požiadavky	Základná správa	Vytvorenie, editácia a mazanie záznamov o aktívach	Áno, hlavne zariadenia v sieti	Základná správa IP a MAC adries	Áno, detailné položky	Áno, CMDB podpora	Áno, ako súčasť CMDB
		Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	Obmedzené	Obmedzené	Áno, s podporou custom typov	Áno	Áno
	Kategorizácia	Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)	Čiastočne, cez atribúty	Základné tagy	Áno, kategórie a tagy	Áno, detailné kategórie	Áno, flexibilné značky
	Zabezpečenie	Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	Áno, SNMP monitoring	Základná úroveň	Nie priamo	Možnosť rozšírenia	Čiastočne, cez doplnky
	Lokalita a sieť	Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	Áno	Základné zobrazenie podľa siete	Áno, IPAM a DCIM	Áno	Obmedzene
	Prepojenia	Väzby medzi aktívami (napr. server – služba – aplikácia)	Obmedzené	Nie	Áno, model vzťahov	Áno	Áno
	Integrácia	Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	Áno, s Nagios/Zabbix	Obmedzené	Áno, pluginy a API	Áno	Áno, natívna integrácia
	Vyhľadávanie	Možnosť filtrovania, fulltextového vyhľadávania a exportu	Áno	Základné	Áno, výkonné vyhľadávanie	Áno	Áno
Technické požiadavky	Import/Export	Podpora API (REST, GraphQL) na správu aktív a integráciu	REST API	REST API	REST a GraphQL	REST API	REST API
	Rozšíriteľnosť	Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)	Čiastočne	Nie	Áno, Django pluginy	Áno	Áno
	Zber dát	Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	Áno, SNMP discovery	Áno, periodické skeny	Nie natívne	Obmedzené	Áno (napr. FusionInventory)
	UI	Webové rozhranie s možnosťou úprav a prehľadnou správou	Áno	Jednoduché	Moderné a konfigurovateľné	Intuitívne	Áno
Prevádzkové požiadavky	História a audit	Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	Základná história	Áno\Nie	Áno	Áno	Áno
	Správa životného cyklu	Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	Čiastočne	Nie	Obmedzene	Áno	Áno
	Notifikácie	Upozornenia na zmenu stavu, expirácie, servisné intervaly	Áno	Základné e-mailové	Obmedzene	Áno	Áno