PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

Podklad pre V4

Prehľad SOC komponentov

Previazané s pracovným balíkom KPB2 – Návrh SOCaaS služby

Obsah

1. KATEGÓRIE NÁSTROJOV V SOC CENTRE A ICH PRÍKLADY

1.1. Nástroje na zber logov a dát (Log Collectors / Agents)

Zbierajú logy, metriky a sieťovú prevádzku zo serverov, klientských zariadení a sieťových prvkov.

- **Filebeat** – zber systémových a aplikačných logov
- **Metricbeat** – zber metrických údajov (CPU, pamäť, disk...)
- **Packetbeat** – sledovanie sieťovej komunikácie
- **Syslog-ng** – klasický logový prijímač pre Unix systémy
- **Auditbeat** – sledovanie systémových udalostí (napr. prihlásenie používateľa)

1.2. Nástroje na spracovanie a prenos logov (Log Processors / Forwarders)

Transformujú, filtrujú alebo smerujú logy do cieľového úložiska.

- **Logstash** – centralizovaný spracovateľ logov (parsing, enrichovanie)
- **Fluentd** – alternatíva k Logstashu, ľahký a flexibilný
- **Vector.dev** – moderný vysokovýkonný logový forwarder

1.3. Nástroje na ukladanie a indexáciu logov (Data Storage / Indexing)

Ukladajú logy a umožňujú ich rýchle vyhľadávanie, filtrovanie a analýzu.

- **Elasticsearch** – distribuovaný fulltextový vyhľadávač a databáza logov
- **OpenSearch** – fork Elasticsearchu (AWS), vhodný pre open-source riešenia
- **TimescaleDB / InfluxDB** – pre časové metriky, hlavne pri monitoringoch

1.4. Nástroje na analýzu útokov a detekciu hrozieb (Threat Detection / IDS / SIEM)

Slúžia na detekciu podozrivých alebo škodlivých aktivít.

- **Suricata** – sieťový IDS/IPS (analýza paketov)
- **Snort** – alternatívny IDS nástroj
- **Wazuh** – host-based detekcia incidentov, file integrity monitoring
- **OSSEC** – jednoduchší HIDS nástroj (staršia verzia Wazuhu)
- **Zeek (Bro)** – sieťová analýza na vyššej úrovni (forenzná analýza)

1.5. Nástroje na správu incidentov a odpoveď (Incident Response / Automation)

Umožňujú zaznamenávať incidenty, prideľovať úlohy a reagovať na hrozby.

- **TheHive** – webová platforma na evidenciu a riešenie incidentov
- **Cortex** – nástroj na automatizované reakcie, pripojený k TheHive
- **MISP** – zdieľanie hrozieb a IoC (Indicators of Compromise) s inými tímami

1.6. Nástroje na vizualizáciu a monitoring (Dashboards / Monitoring Tools)

Slúžia na tvorbu prehľadných dashboardov, grafov, alertov.

- **Kibana** – primárny nástroj na vizualizáciu dát z Elasticsearch
- **Grafana** – pokročilý vizualizačný nástroj pre metriky z Promethea, Elasticu atď.
- **Prometheus** – nástroj na zber a uchovanie časových metrík (napr. CPU, RAM, sieť)
- **Loki** – nástroj od Grafany na vizualizáciu logov

1.7. Nástroje na bezpečnostný monitoring kontajnerov a cloudu (Cloud / Container Security)

Detekujú podozrivé aktivity v kontajneroch, cloude alebo CI/CD pipeline.

- **Falco** – runtime bezpečnostný nástroj pre Kubernetes / Docker
- **Trivy** – skener zraniteľností kontajnerov a Docker obrazov
- **Kube-hunter** – detekcia slabých miest v Kubernetes klustri

1.8. Doplnkové a pomocné nástroje (Utility Tools)

Nástroje na sieťovú analýzu, skenovanie a správu.

- **Nmap** – skener portov a sietí (využitie pri analýze)
- **OpenVAS** – nástroj na hľadanie zraniteľností v systémoch
- **Zabbix / LibreNMS** – sledovanie stavu zariadení (ping, dostupnosť)
- **Ansible** – automatizácia nasadzovania a správy nástrojov

2. PODROBNÁ ANALÝZA SOC NÁSTROJOV

2.1. Nástroje na zber logov a dát (Log Collectors / Agents)

2.1.1. Filebeat

Popis:

Filebeat je ľahký agent vyvinutý spoločnosťou Elastic, určený na zbieranie a odosielanie logov z rôznych systémov (napr. systémové logy, aplikačné logy, webserver logy, databázové logy atď.) do spracovateľského nástroja ako Logstash alebo Elasticsearch. Beží na klientskom zariadení ako démon, priebežne číta log súbory (napr. /var/log/syslog) a odosiela ich ďalej.

Výhody:

- Veľmi nízka spotreba systémových zdrojov.
- Jednoduchá inštalácia a konfigurácia.
- Spoľahlivý prenos logov vďaka zabudovanému bufferu.
- Podpora rôznych typov logov cez moduly (napr. Apache, Nginx, MySQL).
- Možnosť priameho napojenia na Elasticsearch.

Nevýhody:

- Obmedzené možnosti spracovania alebo transformácie logov.
- Pri veľkých objemoch logov môže byť menej výkonný ako iné riešenia
- Vyššia úroveň zabezpečenia (TLS, autentifikácia) vyžaduje dodatočnú konfiguráciu

2.1.2. Metricbeat

Popis:

Metricbeat je agent na zber systémových a aplikačných metrík. Zhromažďuje dáta ako využitie CPU, pamäte, diskov, sieťovej prevádzky, ako aj štatistiky z rôznych aplikácií (napr. Docker, MySQL, Apache). Dáta odosiela do Elasticsearch alebo cez Logstash.

Výhody:

- Jednoduchý spôsob monitorovania výkonnosti serverov a služieb.
- Široká podpora modulov pre známe aplikácie a systémy.
- Nízka spotreba systémových zdrojov.
- Vhodný na integráciu s Grafanou alebo Kibana pre vizualizáciu.

Nevýhody:

- Menej flexibilný v porovnaní s nástrojmi ako Prometheus.
- Niektoré metriky môžu chýbať pre špecifické aplikácie.
- Vyžaduje správne nastavenie intervalov, inak môže zahltiť výstup alebo systém.

2.1.3. Packetbeat

Popis:

Packetbeat je nástroj na pasívne sledovanie sieťovej komunikácie. Zachytáva pakety priamo zo sieťového rozhrania a analyzuje ich podľa protokolov (napr. HTTP, DNS, MySQL, PostgreSQL, Redis, atď.). Výstupy odosiela do Elasticsearch.

Výhody:

- Umožňuje detailnú analýzu sieťovej prevádzky bez potreby meniť aplikácie.
- Vhodný na detekciu neštandardného alebo podozrivého sieťového správania.
- Jednoduchá integrácia do Elastic Stack.

Nevýhody:

- Vyššie nároky na sieťové a výpočtové zdroje pri veľkom množstve paketov.
- Obmedzený rozsah podporovaných protokolov.
- Menej vhodný pre šifrovaný prenos (HTTPS, TLS).

2.1.4. Syslog-ng

Popis:

Syslog-ng je pokročilý logovací démon, ktorý prijíma, spracováva a distribuuje logy zo systémov a aplikácií. Funguje ako centrálne logovacie miesto pre Unix/Linux systémy. Vie prijímať logy prostredníctvom protokolov ako UDP, TCP a TLS.

Výhody:

- Vhodný ako centrálna logovacia brána pre celú sieť.
- Vysoká konfigurovateľnosť a podpora filtrovania logov.
- Podpora šifrovaného prenosu logov.
- Môže zapisovať logy do súborov, databáz alebo odosielať ďalej do nástrojov ako Logstash.

Nevýhody:

- Zložitejšia konfigurácia pri komplexných scenároch.
- Neobsahuje vlastné analytické alebo vizualizačné funkcie.
- Vyžaduje doplnkový systém na ďalšie spracovanie alebo uchovanie logov (napr. Elasticsearch).

2.1.5. Auditbeat

Popis:

Auditbeat je agent z Elastic Beats balíka, ktorý zhromažďuje informácie o udalostiach na úrovni operačného systému. Sleduje napríklad pokusy o prihlásenie, spustenie procesov, zmeny v systémových súboroch a môže byť napojený na Linux Audit Framework.

Výhody:

- Umožňuje detekciu bezpečnostných incidentov na úrovni operačného systému.
- Monitoruje kritické systémové aktivity (napr. zmeny v /etc/passwd, spúšťanie binárnych).
- Výborná integrácia s Elastic Stack.

Nevýhody:

- Vyššia náročnosť na správne nastavenie audit pravidiel.
- Pri veľkom počte udalostí môže generovať veľké objemy dát.
- Vyžaduje pokročilé znalosti operačného systému na efektívne využitie.

2.2. Nástroje na spracovanie a prenos logov (Log Processors / Forwarders)

2.2.1. Logstash

Popis:

Logstash je výkonný a rozšírený nástroj od Elasticu na spracovanie, filtrovanie, transformáciu a smerovanie logov a iných typov dát. Funguje ako „pipeline“ – prijíma vstupné dáta, spracúva ich podľa definovaných pravidiel (filtre, regexy, geoIP, parsovanie JSON...) a následne ich odosiela do výstupného systému, najčastejšie do Elasticsearch.

Výhody:

- Silná integrácia s Elastic Stack.
- Veľké množstvo dostupných pluginov (vstupné, výstupné, filter pluginy).
- Schopnosť komplexného spracovania dát.
- Overené riešenie s veľkou komunitou a dokumentáciou.
-

Nevýhody:

- Vyššie nároky na výpočtové zdroje (pamäť, CPU).
- Zložitejšia konfigurácia (napr. v porovnaní s Fluentd).
- Môže mať nižší výkon pri veľkom počte paralelných vstupov bez optimalizácie.

2.2.2. Fluentd

Popis:

Fluentd je open-source dátový kolektor určený na zjednotenie spracovania logov a ich smerovanie do rôznych systémov (Elasticsearch, Kafka, InfluxDB, atď.). Je alternatívou k Logstashu s dôrazom na nízku spotrebu zdrojov a modularitu. Konfigurácia je založená na jednoduchej štruktúre (pravidlá input → filter → output).

Výhody:

- Veľmi ľahký a efektívny (nižšie nároky než Logstash).
- Obrovská komunita a ekosystém pluginov.
- Flexibilný a rozšíriteľný (pluginy v Ruby a C).
- Môže pracovať aj ako agregátor logov medzi viacerými strojmi.

Nevýhody:

- Vyžaduje znalosť štruktúry pre pokročilé nastavenia.
- Pluginy majú rôznu kvalitu (nie všetky sú oficiálne podporované).
- Mierne zložitejšie ladenie pri chybách v konfigurácii.

2.2.3. Vector (Vector.dev)

Popis:

Vector je moderný nástroj na zber, spracovanie a prenos logov alebo metrík, vyvíjaný spoločnosťou Datadog (pôvodne Timber.io). Je navrhnutý na vysoký výkon, nízku latenciu a bezpečné doručovanie dát. Môže fungovať ako agent aj ako centrálny forwarder, podporuje vstupy ako syslog, journald, Prometheus aj výstupy ako Elasticsearch, Kafka, ClickHouse.

Výhody:

- Napísaný v Rust – extrémne výkonný a bezpečný.
- Jednoduchá, čitateľná konfigurácia (TOML alebo JSON).
- Nízka pamäťová záťaž, vhodný pre veľké objemy dát.
- Silná orientácia na observabilitu a spoľahlivosť (vrátane retry logiky, bufferingu).

Nevýhody:

- Menšia komunita v porovnaní s Logstash alebo Fluentd.
- Niektoré integrácie a pluginy ešte nie sú také rozšírené (novší projekt).
- Vyžaduje učenie sa novej syntaxe a konceptov pre tých, čo sú zvyknutí na Logstash.

2.3. Nástroje na ukladanie a indexáciu logov (Data Storage / Indexing)

2.3.1. Elasticsearch

Popis:

Elasticsearch je distribuovaný vyhľadávací a analytický engine, ktorý funguje ako databáza na ukladanie, indexáciu a vyhľadávanie logov, textových dát a metrických údajov. Je základným komponentom Elastic Stack-u. Používa sa na rýchle vyhľadávanie a filtrovanie veľkého množstva dát, napríklad systémových logov, sieťových udalostí alebo incidentov.

Výhody:

- Veľmi rýchle a výkonné vyhľadávanie nad obrovskými objemami dát.
- Podpora fulltextového aj štruktúrovaného vyhľadávania.

- Distribuovaná architektúra – umožňuje škálovanie a vysokú dostupnosť.
- Nativne integrovaný s Logstash, Beats, Kibana (Elastic Stack).
- Silné možnosti agregácie a analytiky nad dátami.

Nevýhody:

- Vyššie nároky na hardvér pri väčších dátových objemoch.
- Pri nesprávnej konfigurácii môže rýchlo spotrebovať pamäť a CPU.
- Od verzie 7.11 prešli základné funkcie pod komerčnú licenciu (Elastic License), čo môže byť obmedzujúce pre niektoré open-source projekty.

2.3.2. OpenSearch

Popis:

OpenSearch je open-source fork Elasticsearchu a Kibany, vyvíjaný pod záštitou Amazon Web Services (AWS). Vznikol ako odpoveď na zmenu licenčných podmienok v Elastic Stack-e. Ponúka podobnú funkcionalitu ako Elasticsearch, vrátane fulltextového vyhľadávania, indexácie logov a dát, analytiky a vizualizácie.

Výhody:

- Zachováva základné vlastnosti Elasticsearchu, no ostáva úplne open-source.
- Pravidelne vyvíjaný komunitou a AWS tímom.
- Kompatibilný s existujúcimi riešeniami postavenými na Elasticsearch 7.x.
- Obsahuje vlastný vizualizačný nástroj – OpenSearch Dashboards.

Nevýhody:

- Nie je 100 % spätne kompatibilný s novšími verziami Elasticsearchu.
- Menšia komunita a dokumentácia v porovnaní s pôvodným Elastic Stack-om.
- Niektoré pokročilé funkcie Elastic Stack-u (napr. Machine Learning) nie sú dostupné alebo sú menej vyspelé.

2.3.3. TimescaleDB

Popis:

TimescaleDB je rozšírenie databázy PostgreSQL, optimalizované pre časové (time-series) dáta. Využíva sa najmä na ukladanie a analýzu metrických údajov z monitorovacích systémov. Má výhody klasickej relačnej databázy, no zároveň výborný výkon pri práci s časom ako dimenziou.

Výhody:

- Postavené na PostgreSQL – výborná znalosť a stabilita.
- Skvelé pre metriky z monitorovacích nástrojov (napr. z Grafany).
- Výborný výkon pri práci s historickými dátami.
- Pokročilé analytické funkcie nad časovými dátami.

Nevýhody:

- Nie je určená na textové logy alebo fulltextové vyhľadávanie.
- Vyššia komplexita pri škálovaní vo veľmi veľkých prostrediach.

- Neobsahuje „elastic-style“ indexáciu a vyhľadávanie.

2.3.4. InfluxDB

Popis:

InfluxDB je špecializovaná databáza na ukladanie časových dát (time-series database). Je široko používaná pri monitorovaní výkonu serverov, sietí, IoT zariadení, a pod. Dáta sú ukladané v časových radoch a veľmi efektívne agregované.

Výhody:

- Extrémne rýchla pri zápise a čítaní časových dát.
- Ideálne riešenie pre systémy ako Telegraf, Grafana, Kapacitor.
- Dobré pre krátkodobú aj dlhodobú analýzu metrických údajov.
- Jednoduchá inštalácia a integrácia s monitoring systémami.

Nevýhody:

- Nie je určená na spracovanie klasických textových logov.
- Niektoré funkcie v InfluxDB 2.x sú dostupné iba vo verzii s licenciou.
- Zložitejšie replikovanie a škálovanie pri veľkých klastroch.

2.4. Nástroje na analýzu útokov a detekciu hrozieb (Threat Detection / IDS / SIEM)

2.4.1. Suricata

Popis:

Suricata je open-source sieťový IDS/IPS a analýzátor paketov, ktorý dokáže analyzovať sieťovú komunikáciu v reálnom čase, vyhľadávať známe útoky pomocou signatúr a generovať alerty. Okrem detekcie hrozieb podporuje aj funkciu prenosu súborov, protokolovú analýzu (HTTP, TLS, DNS...) a výkonové metriky.

Výhody:

- Pokročilá analýza paketov a protokolov v reálnom čase.
- Podpora viacvláknového spracovania – vysoký výkon.
- Možnosť fungovať ako IDS aj ako IPS.
- Rozšíriteľné pomocou pravidiel (kompatibilné so Snort signatúrami).
- Integrovaná s nástrojmi ako Wazuh alebo Elasticsearch.

Nevýhody:

- Vyššia zložitosť konfigurácie pri väčších sieťach.
- Pri veľkej záťaži je potrebné starostlivo dimenzovať hardware.
- Vyžaduje pravidelnú aktualizáciu signatúr (napr. z ET Open).

2.4.2. Snort

Popis:

Snort je open-source nástroj na detekciu prienikov do siete (IDS), ktorý kontroluje sieťovú prevádzku pomocou signatúr a heuristiky. Je jeden z najstarších a najpoužívanejších IDS nástrojov a býva používaný najmä na detekciu známych útokov a podozrivého sieťového správania.

Výhody:

- Veľká databáza signatúr útokov.

- Široká komunita a množstvo dostupných príkladov konfigurácie.
- Vhodný pre malé až stredné siete.
- Možnosť použiť ako IDS aj IPS.

Nevýhody:

- Jednovláknová architektúra – nižší výkon ako Suricata pri veľkej prevádzke.
- Menej rozšírené protokolové analýzy.
- Menej aktívny vývoj v porovnaní so Suricatou.

2.4.3. Wazuh

Popis:

Wazuh je host-based IDS (HIDS), ktorý monitoruje aktivitu priamo na jednotlivých zariadeniach – napr. systémové zmeny, pokusy o prihlásenie, zmeny v súboroch. Je to moderné riešenie postavené na OSSEC a je úzko integrované s Elastic Stack. Podporuje aj agentov pre Windows, Linux a macOS.

Výhody:

- Výborná integrácia s Elasticsearch a Kibana.
- Zaznamenáva zmeny v súboroch, používateľské akcie, loginy, podozrivú aktivitu.
- Pracuje s databázou hrozieb (threat intelligence).
- Agent-based systém – vhodný pre rôzne operačné systémy.
- Zahrnutý aj modul na compliance monitoring (napr. PCI-DSS, GDPR...).

Nevýhody:

- Vyžaduje správu a aktualizáciu agentov na všetkých zariadeniach.
- Môže generovať veľké množstvo dát (logov), ak nie je správne nastavený.
- Vyššia zložitosť pri rozsiahlych nasadeniach bez automatizácie.

2.4.4. OSSEC

Popis:

OSSEC je open-source HIDS (host-based intrusion detection system), ktorý monitoruje súbory, logy, používateľské akcie a integritu systémových súborov. Je to predchodca Wazuh-u, od ktorého sa odštiepili ďalším vývojom. Je jednoduchší a menej integrovaný, no stále účinný v malých prostrediach.

Výhody:

- Nízka systémová náročnosť.
- Jednoduchá inštalácia a konfigurácia.
- Podpora multiplatformových agentov (Windows, Linux, BSD).
- Vhodný pre menšie nasadenia bez potreby komplexného vizuálneho rozhrania.

Nevýhody:

- Neponúka natívne webové rozhranie ani integráciu s Elastic Stack.
- Slabšia komunita a obmedzený vývoj v porovnaní s Wazuh.
- Menej vhodný pre veľké enterprise nasadenia.

2.4.5. Zeek (predtým Bro)

Popis:

Zeek je pokročilý nástroj na sieťovú analýzu, ktorý umožňuje detailné sledovanie sieťovej prevádzky na vyššej vrstve než Suricata alebo Snort. Nepracuje so signatúrami, ale s vlastným skriptovacím jazykom, pomocou ktorého možno definovať detekčné pravidlá a scenáre. Využíva sa najmä na forenznú analýzu.

Výhody:

- Vysoko konfigurovateľný a skriptovateľný (vlastný jazyk).
- Umožňuje komplexnú analýzu správania na sieti (behaviorálne modely).
- Vhodný pre hĺbkovú forenznú analýzu a dlhodobé sledovanie trendov.
- Dokáže exportovať štruktúrované logy pre ďalšie spracovanie.

Nevýhody:

- Vyžaduje skúsenosti so Zeek skriptovaním.
- Nie je určený na signatúrnu detekciu ako Snort alebo Suricata.
- Môže byť náročnejší na výkon pri rozsiahlej sieťovej prevádzke.

2.5. Nástroje na správu incidentov a odpoveď (Incident Response / Automation)

2.5.1. TheHive

Popis:

TheHive je open-source platforma na správu bezpečnostných incidentov (SIRP – Security Incident Response Platform). Slúži na evidenciu incidentov, ich klasifikáciu, rozdelenie úloh v tíme a sledovanie ich riešenia. Každý incident (tzv. case) môže obsahovať viac alertov, artefaktov (napr. IP adresy, hashe), komentárov a reakčných krokov. Platforma má webové rozhranie a REST API, čo umožňuje ľahkú integráciu s inými systémami ako Cortex a MISP.

Výhody:

- Prehľadná evidencia incidentov a workflow.
- Podpora tímovej spolupráce (priraďovanie úloh, komentáre).
- Flexibilné šablóny pre incidenty (automatické vyplňovanie polí).
- Silná integrácia s Cortexom a MISP.
- Open-source s aktívnou komunitou.

Nevýhody:

- Vyžaduje technické znalosti na nasadenie a správu.
- Rozhranie nemusí byť intuitívne pre menej skúsených používateľov.
- Občasná potreba aktualizácií/patchov, ktoré môžu narušiť kompatibilitu doplnkov.
- Niektoré funkcie (napr. reporting) môžu byť limitované bez vlastného doprogramovania.

2.5.2. Cortex

Popis:

Cortex je open-source nástroj na automatizáciu analýzy a reakcií na incidenty. Je navrhnutý ako rozšírenie TheHive, ale môže fungovať aj samostatne. Využíva tzv. analyzéry (napr. WHOIS lookup, VirusTotal scan, geolokácia IP) a respondery (napr. blokovanie IP vo firewalle, deaktivácia používateľského účtu). Tieto moduly sa vykonávajú na základe artefaktov z incidentov a môžu byť spúšťané manuálne alebo automaticky.

Výhody

- Automatizuje rutinné a opakujúce sa činnosti.
- Umožňuje rýchlu reakciu na hrozby (playbooky).
- Modulárna architektúra – ľahko sa pridávajú vlastné analyzéry/respondery.
- Efektívna integrácia s TheHive (v jednom kliknutí).
- Rozširuje analytické možnosti analytikov.

Nevýhody

- Vyžaduje konfiguráciu a nastavenie autentifikácie (API keys, tokens).
- Pri veľkom množstve požiadaviek môžu niektoré analyzéry spôsobovať oneskorenia.
- Nie všetky analyzéry/respondery sú pravidelne aktualizované.
- Niektoré moduly môžu byť závislé od platených služieb

2.5.3. MISP

Popis

MISP je open-source platforma na zdieľanie informácií o hrozbách (Threat Intelligence). Umožňuje vytvárať a spravovať databázu tzv. eventov, ktoré obsahujú IoC (Indicators of Compromise), ako napr. škodlivé IP adresy, hashe súborov, domény, e-maily a ďalšie údaje spojené s hrozbami. MISP podporuje štandardy ako STIX/TAXII a umožňuje automatickú synchronizáciu s inými MISP inštanciami, čím podporuje komunitné zdieľanie informácií.

Výhody

- Podporuje kolaboráciu medzi tímami a organizáciami.
- Možnosť vytvárať vlastné TI databázy.
- Kompatibilita so štandardmi Threat Intelligence (TAXII/STIX).
- Silné API na integráciu s inými nástrojmi (napr. SIEM, TheHive).
- Umožňuje prispôsobenie kategórií a taxonómií.

Nevýhody

- Používateľské rozhranie môže byť zložité pre začiatočníkov.
- Vyžaduje znalosť práce s IoC a taxonómiami.
- Synchronizácia s inými MISP inštanciami môže byť technicky náročná.
- Potreba pravidelnej údržby databázy (čistenie neaktuálnych eventov).

2.6. Nástroje na vizualizáciu a monitoring (Dashboards / Monitoring Tools)

2.6.1. Kibana

Kibana je vizualizačný nástroj vyvíjaný firmou Elastic, slúžiaci primárne na vizualizáciu a analýzu dát uložených v Elasticsearch. Umožňuje vytvárať prehľadné dashboardy, grafy, tabule, časové línie a vyhľadávať logy. Je často súčasťou ELK stacku (Elasticsearch, Logstash, Kibana), ktorý sa používa na spracovanie a vizualizáciu logov.

Výhody

- Silná integrácia s Elasticsearch.
- Interaktívne a flexibilné vizualizácie.
- Rýchle vyhľadávanie v obrovských množstvách dát (logy, IoC, metriky).
- Vhodné na analýzu bezpečnostných aj výkonnostných dát.

Nevýhody

- Vyžaduje Elasticsearch ako backend (nedá sa použiť samostatne).
- Niektoré pokročilé funkcie sú dostupné len v komerčných verziách.
- Zložitejšie nastavenie pri integrácii s viacerými dátovými zdrojmi.
- V porovnaní s Grafanou menej intuitívne pre rýchlu tvorbu dashboardov.

2.6.2. Grafana

Grafana je open-source vizualizačný nástroj, ktorý umožňuje zobrazovať metriky z rôznych zdrojov – najmä z Promethea, ale aj Elasticu, InfluxDB, MySQL a ďalších. Je mimoriadne flexibilná a vhodná na tvorbu prehľadových dashboardov v rámci monitoringu výkonu, infraštruktúry či bezpečnosti.

Výhody

- Podpora mnohých dátových zdrojov (Prometheus, Loki, Elasticsearch...).
- Veľmi moderné a vizuálne atraktívne dashboardy.
- Možnosť nastaviť alerty, panely, zdieľať dashboardy cez linky.
- Silná komunita a množstvo hotových šablón.

Nevýhody

- Vyžaduje pripojenie k externému dátovému zdroju – sama dáta nezbiera.
- Nastavenie alertingu môže byť zložité pre začiatočníkov.
- Viac pokročilých funkcií (napr. reporting, prístupové role) je dostupných v platených edíciách.

2.6.3. Prometheus

Popis

Prometheus je open-source systém na zber, uchovávanie a spracovanie časových metrík. Je navrhnutý najmä na monitoring infraštruktúry a aplikácií. Pravidelne dotazuje (scrape) metriky z rôznych zdrojov (exportérov) a ukladá ich do vlastnej TSDB (time-series databázy). Najčastejšie sa používa v kombinácii s Grafanou.

Výhody

- Silná podpora pre **časové metriky** (CPU, RAM, sieť, aplikácie).
- Vlastný dotazovací jazyk **PromQL** na analýzu dát.

- Veľké množstvo dostupných **exportérov** (napr. pre Linux, Docker, PostgreSQL...).
- Možnosť nastaviť alerty pomocou Alertmanagera.

Nevýhody

- Nezberá logy (iba metriky).
- Systém nie je ideálny pre dlhodobé ukladanie veľkých dát (bez rozšírení).
- Vyžaduje znalosť PromQL, ktorý má strmšiu krivku učenia.
- Menej vhodný na spracovanie neštruktúrovaných údajov.

2.6.4. Loki

Popis

Loki je open-source systém na zber a vyhľadávanie logov, vyvíjaný rovnakým tímom ako Grafana. Je koncipovaný ako „Prometheus pre logy“, teda zachováva rovnakú filozofiu: ľahké nasadenie, nízke nároky, tagovanie namiesto indexovania. Používa sa spolu s Grafanou na vizualizáciu logov a tvorbu prehľadových panelov.

Výhody

- Jednoduchá integrácia s Grafanou.
- Lacnejšie a rýchlejšie ako Elasticsearch pri väčších objemoch logov.
- Neindexuje celé logy – len metadáta (výrazne nižšie nároky na úložisko).
- Možnosť používať rovnaké nástroje a syntax ako Prometheus.

Nevýhody

- Obmedzená vyhľadávacia funkcionalita v porovnaní s Elasticsearch.
- Mladší projekt – menej modulov a integrácií.
- Vyžaduje správne tagovanie pre efektívne vyhľadávanie.
- Horšie pracuje s veľmi neštruktúrovanými logmi.

2.7. Nástroje na bezpečnostný monitoring kontajnerov a cloudu

2.7.1. Falco

Popis

Falco je open-source runtime bezpečnostný nástroj vyvíjaný projektom Sysdig. Je určený na detekciu podozrivého správania v kontajnerových prostrediach (Docker, Kubernetes). Monitoruje systémové volania jadra v reálnom čase a porovnáva ich s vopred definovanými bezpečnostnými pravidlami. Môže detegovať napr. spustenie shellu v kontajneri, zápis do systémových adresárov, zmeny v konfiguráciách, podozrivý sieťový traffic atď.

Výhody

- **Runtime detekcia hrozieb** – okamžité zachytenie neštandardného správania.
- Vhodný pre **Kubernetes aj Docker**.
- Bohatá knižnica pravidiel + možnosť vytvárať vlastné.
- Podporuje výstupy do alertovacích nástrojov (Slack, syslog, Prometheus...).
- Ľahká integrácia do CI/CD pipeline.

Nevýhody

- Možné falošné pozitíva – vyžaduje doladenie pravidiel.
- Vyššia záťaž na výkon, ak je monitorovaných veľa kontajnerov.
- Potrebuje nízkoúrovňové prístupy (k jadru / systémovým volaniam).
- Konfigurácia môže byť zložitejšia pre nováčikov.

2.7.2. Trivy

Popis

Trivy je ľahký a rýchly open-source skener zraniteľností vyvíjaný firmou Aqua Security. Je určený na analýzu kontajnerových obrazov (Docker), Git repozitárov, Kubernetes manifestov a CI/CD pipeline. Zistí známe zraniteľnosti v knižniciach, OS balíkoch alebo závislostiach, ktoré sú súčasťou image.

Výhody

- Jednoduchý na používanie.
- Rýchly sken a detailné výsledky.
- Podporuje aj **Infrastructure as Code** (napr. Terraform, Helm).
- Funguje lokálne, bez potreby komplexnej inštalácie.
- Pravidelné aktualizácie databázy zraniteľností (NVD, Red Hat, Debian...).

Nevýhody

- Neskenuje runtime správanie – len statické obrazy a konfigurácie.
- Vyžaduje pravidelnú aktualizáciu databázy zraniteľností.
- Pri komplexných obrazoch môže generovať veľa nálezov, z ktorých nie všetky sú relevantné (false positives).
- Niektoré funkcie sú v rozšírenej verzii Aqua Enterprise.

2.7.3. Kube-hunter

Popis

Kube-hunter je open-source nástroj na penetračné testovanie Kubernetes klastrov, vyvinutý spoločnosťou Aqua Security. Slúži na detekciu slabých miest v konfigurácii a nasadení K8s, ako sú otvorené porty, prístupné API bez autentifikácie, či chýbajúce obmedzenia na komunikáciu medzi podmi.

Výhody

- Špecializovaný na Kubernetes bezpečnosť.
- Podporuje aktívny aj pasívny mód skenovania.
- Zrozumiteľné výstupy – každý nález má popis, úroveň závažnosti a odporúčanie.
- Vhodný ako bezpečnostná kontrola pred nasadením do produkcie.
- Možné spúšťať ako kontajner alebo CLI nástroj.

Nevýhody

- Zameraný výhradne na **Kubernetes** – nepoužiteľný mimo K8s prostredí.
- Aktívne testy môžu zasahovať do behu aplikácií (neodporúča sa v produkcii).
- Neodstraňuje zraniteľnosti, len ich deteguje.
- Menej vhodný pre komplexné cloudové prostredia mimo K8s.

2.8. Doplnkové a pomocné nástroje (Utility tools)

2.8.1. Nmap

Popis

Nmap (Network Mapper) je open-source sieťový skener, ktorý slúži na mapovanie sietí, detekciu otvorených portov, služieb a operačných systémov na cieľových zariadeniach. Je široko používaný pri penetračných testoch, bezpečnostných auditoch a sieťovej diagnostike.

Výhody

- Veľmi silný a flexibilný nástroj.
- Podporuje skriptovanie cez Nmap Scripting Engine (NSE).
- Rýchle skenovanie veľkých sietí.
- Vhodný pre sieťových adminov aj etických hackerov.

Nevýhody

- Potrebuje znalosti siete – pre začiatočníkov môže byť komplexný.
- Niektoré skenovacie techniky môžu byť vnímané ako „útočné“.
- Neobsahuje priame výstupy o zraniteľnostiach (na to slúži napr. OpenVAS).

2.8.2. OpenVAS

Popis

OpenVAS je open-source nástroj na skenovanie zraniteľností v systémoch, službách a sieťových zariadeniach. Je súčasťou balíka Greenbone Vulnerability Management (GVM). Vykonáva aktívne skenovanie cieľov a porovnáva ich s databázou známych zraniteľností (napr. CVE).

Výhody

- Silná detekcia známych zraniteľností.
- Možnosť pravidelnej automatizovanej kontroly.
- Použiteľné na rôzne typy systémov (Windows, Linux, sieťové zariadenia).
- Grafické rozhranie (GSA) aj CLI.

Nevýhody

- Zložitejšie nasadenie a konfigurácia.
- Vyššia hardvérová náročnosť.
- Skener môže generovať veľa falošných pozitív.
- Dlhší čas potrebný na úplný sken.

2.8.3. Zabbix / Libre NMS

Popis

Zabbix a LibreNMS sú open- source nástroje na monitoring sietí a zariadení. Umožňujú sledovať dostupnosť, latenciu, stav serverov, prepínačov, routerov a iných sieťových prvkov pomocou SNMP, ICMP, HTTP, agentov a ďalších protokolov. Podporujú alertovanie, vizualizáciu metrík a automatickú detekciu zariadení. Zabbix je komplexný systém s veľkou škálovateľnosťou a rozšíriteľnosťou. LibreNMS je viac zameraný na jednoduché SNMP monitoring a rýchlu inštaláciu.

Výhody

- Široká podpora protokolov a zariadení.
- Možnosť nastaviť upozornenia (e-mail, Telegram, Slack...).
- Vhodné pre nepretržité sledovanie siete.
- Open-source riešenia bez licenčných poplatkov.

Nevýhody

- Vyžadujú samostatný server a konfiguráciu.
- Zabbix môže byť komplexnejší pre začiatočníkov.
- LibreNMS má užší rozsah funkcionalít v porovnaní so Zabbixom.
- Vyššia záťaž pri veľkých inštaláciách.

2.8.4. Ansible

Popis

Ansible je open-source nástroj na automatizáciu IT procesov, najmä nasadzovania softvéru, konfigurácie serverov, aktualizácií a orchestrácie. Je agentless – využíva SSH a YAML playbooky na vykonanie úloh nad vzdialenými systémami. Široko používaný v DevOps, ale aj v bezpečnostných tímoch na rýchle nasadenie pravidiel, nástrojov a konfigurácií.

Výhody

- Jednoduchý a zrozumiteľný syntax (YAML).
- Nevyžaduje agenta – funguje cez SSH.
- Vhodný pre malé aj veľké infraštruktúry.
- Podporuje idempotenciu – vykonanie viackrát má rovnaký výsledok.

Nevýhody

- Menej vhodný na komplexné orchestrácie
- Vyžaduje SSH prístup a dobre nastavené prístupové oprávnenia.
- Zložitejšie ladenie pri veľkých playbookoch.

3. WAZUH

Wazuh je open-source bezpečnostná platforma zameraná na monitorovanie integrity systémov, detekciu hrozieb, správu zraniteľností, log management a detekciu incidentov. Vďaka svojej modularite je vhodná pre použitie v menších aj veľkých IT prostrediach.

Wazuh umožňuje:

- Centralizovaný zber a analýzu logov zo serverov a klientov (Linux, Windows)
- Detekciu podozrivého správania na základe pravidiel a korelácie udalostí
- Monitorovanie súborových zmien, firewallov, antivírusov, autentifikačných pokusov a ďalších bezpečnostných prvkov

3.1. Architektúra systému

Wazuh pozostáva z viacerých komponentov:

- **Wazuh server**: Centrálna jednotka, ktorá prijíma dáta z agentov, vyhodnocuje ich podľa pravidiel a generuje alerty.
- **Wazuh agent**: Ľahký softvér bežiaci na monitorovanom systéme (Linux, Windows), ktorý zbiera logy, zisťuje zmeny v systéme a komunikuje so serverom.
- **Wazuh indexer**: Ukladá a spracúva zozbierané dáta (logy, alerty, udalosti).
- **Wazuh dashboard**: Grafické webové rozhranie na správu, vizualizáciu a vyhľadávanie udalostí.

3.2. Požiadavky na inštaláciu

3.2.1. Wazuh Indexer

Wazuh indexer vyžaduje 64-bitový Intel alebo AMD procesor (architektúra x86_64/AMD64) a systém Linux, aby mohol fungovať.

Odporúčaný OS

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Hardvérové požiadavky

	Minimum		Odporúčané	
Komponent	RAM (GB)	CPU (jadrá)	RAM (GB)	CPU (jadrá)
Wazuh indexer	**4**	**2**	**16**	**8**

3.2.2. Wazuh Server

Wazuh server vyžaduje 64-bitový Intel alebo AMD procesor (architektúra x86_64/AMD64) a systém Linux, aby mohol fungovať.

Odporúčaný OS

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Hardvérové požiadavky

	Minimum		Odporúčané	
Komponent	RAM (GB)	CPU (jadrá)	RAM (GB)	CPU (jadrá)
Wazuh Server	**2**	**2**	**4**	**8**

3.2.3. Wazuh Dashboard

Wazuh dashboard vyžaduje 64-bitový Intel alebo AMD procesor (architektúra x86_64/AMD64) a systém Linux, aby mohol fungovať.

Odporúčaný OS

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Hardvérové požiadavky

	Minimum		Odporúčané	
Komponent	RAM (GB)	CPU (jadrá)	RAM (GB)	CPU (jadrá)
Wazuh indexer	**4**	**2**	**8**	**4**

3.3. Podporované systémy a preddefinované dekodéry vo Wazuh

Wazuh obsahuje množstvo preddefinovaných dekodérov a pravidiel, ktoré umožňujú automatické spracovanie logov z rôznych operačných systémov, bezpečnostných riešení, sieťových zariadení, databáz či webových aplikácií. Vďaka tejto podpore nie je potrebné manuálne vytvárať vlastné dekodéry pre bežne používané riešenia. Táto kapitola obsahuje prehľad všetkých systémov, vendorov a služieb, pre ktoré má Wazuh vstavanú podporu.

3.3.1. Operačné systémy a platformy

- Windows (windows_decoders.xml)
- macOS (macos_decoders.xml)
- OpenBSD (openbsd_decoders.xml)

- Solaris (solaris_decoders.xml)
- Unix/Linux všeobecne (unix_decoders.xml)
- AIX (aix-ipsec_decoders.xml)

3.3.2. Bezpečnostné riešenia a antivírusy

- Windows Defender (v windows_decoders.xml)
- ClamAV (clamav_decoders.xml)
- Kaspersky (kaspersky_decoders.xml)
- Sophos (sophos_decoders.xml, sophos_fw_decoders.xml)
- ESET Remote Administrator (eset-remote_decoders.xml)
- McAfee mcafee_decoders.xml)
- Trend Micro (OSCE) (trend-osce_decoders.xml)
- FireEye (fireeye_decoders.xml)
- Panda Security (PAPS) (panda-paps_decoders.xml)
- Symantec (symantec_decoders.xml)
- Cylance (cylance_decoders.xml)

3.3.3. Firewally, IDS/IPS a sieťové zariadenia

- Cisco ASA, IOS, PIX, VPN, estreamer, FTD (cisco-*.xml)
- Fortinet – FortiGate, FortiDDoS, FortiMail, FortiAuth (forti*.xml)
- Palo Alto Networks (paloalto_decoders.xml)
- pfSense (pfsense_decoders.xml)
- Juniper – Junos (junos_decoders.xml)
- Barracuda (barracuda_decoders.xml)
- Huawei USG (huawei-usg_decoders.xml)
- SonicWall (sonicwall_decoders.xml)
- Check Point (checkpoint_decoders.xml, checkpoint-smart1_decoders.xml)
- Imperva (imperva_decoders.xml)
- Arbor Networks (arbor_decoders.xml)
- Suricata / Snort IDS (zahrnuté vo viacerých pravidlách ako snort_decoders.xml)

3.3.4. Autentifikácia a prístupové systémy

- FreeIPA (freeipa_decoders.xml)
- RSA Authentication Manager (rsa-auth-manager_decoders.xml)
- Identity Guard (identity_guard_decoders.xml)
- OpenLDAP (openldap_decoders.xml)
- PAM (Pluggable Authentication Modules) (pam_decoders.xml)
- sudo / su / login príkazy (sudo_decoders.xml, su_decoders.xml)

3.3.5. Emailové servery a služby

- Postfix (postfix_decoders.xml)
- Sendmail (sendmail_decoders.xml)
- Exim (exim_decoders.xml)
- Courier (courier_decoders.xml)
- Dovecot (dovecot_decoders.xml)
- Microsoft Exchange (MSEXchange) (msexchange-log-decoders.xml)
- FortiMail (fortimail_decoders.xml)

3.3.6. Webové servery, aplikácie a CMS

- Apache (apache_decoders.xml)
- Nginx (nginx_decoders.xml)
- WordPress (wordpress_decoders.xml)
- OwnCloud / Nextcloud (owncloud_decoders.xml, nextcloud_decoders.xml)
- GitLab (gitlab_decoders.xml)
- Jenkins (jenkins_decoders.xml)
- Horde Groupware (horde_decoders.xml)

3.3.7. Virtualizácia a kontajnery

- VMware (vmware_decoders.xml)
- Docker (docker_decoders.xml)
- Proxmox VE (proxmox-ve_decoders.xml)
- FreePBS (freepbs_decoders.xml)

3.3.8. Cloud a služby

- Microsoft Azure (azure_decoders.xml)
- AWS EKS Authenticator (aws-eks-authenticator_decoders.xml)
- QualysGuard (qualysguard_decoders.xml)

3.3.9. Databázové systémy

- MySQL / MariaDB (mysql_decoders.xml, mariadb_decoders.xml)
- PostgreSQL (postgresql_decoders.xml)
- OracleDB (oracledb_decoders.xml)
- Redis (redis_decoders.xml)
- MongoDB (mongodb_decoders.xml)
- SQL Server (sqlserver_decoders.xml)
- TimescaleDB (zvyčajne cez PostgreSQL)

3.3.10. Ostatné služby, logy a nástroje

- SSH / Telnet (ssh_decoders.xml, telnet_decoders.xml)
- FTP servery – vsftpd, proftpd, pure-ftpd, ftpd (viacero *_decoders.xml)
- ARPWatch, NTPD, Samba, racoon, dpkg, oscap, ossec, auditd – rôzne systémové služby
- Roundcube, Puppet, Suhosin, vshell, perdition, portsentry – špecializované služby a moduly

ZOZNAM ZDROJOV

Elastic Beats

- Filebeat: https://www.elastic.co/beats/filebeat
- Metricbeat: https://www.elastic.co/beats/metricbeat
- Packetbeat: https://www.elastic.co/beats/packetbeat
- Auditbeat: https://www.elastic.co/beats/auditbeat
- Dokumentácia: https://www.elastic.co/guide/en/beats/filebeat/current/index.html

Syslog-ng

- Dokumentácia: https://www.syslog-ng.com/technical-documents/list/syslog-ng-open-source-edition
- Produktová stránka: https://www.syslog-ng.com/products/open-source-log-management/

Logstash

- Web: https://www.elastic.co/logstash
- Dokumentácia: https://www.elastic.co/guide/en/logstash/current/index.html

Fluentd

- Web: https://www.fluentd.org/
- Dokumentácia: https://docs.fluentd.org/

Vector.dev

- Web: https://vector.dev/
- Dokumentácia: https://vector.dev/docs/

Elasticsearch

- Web: https://www.elastic.co/elasticsearch
- Dokumentácia: https://www.elastic.co/guide/en/elasticsearch/reference/index.html

OpenSearch

- Web: https://opensearch.org/
- Dokumentácia: https://opensearch.org/docs/latest/

TimescaleDB

- Web: https://www.timescale.com/
- Dokumentácia: https://docs.timescale.com/

InfluxDB

- Web: https://www.influxdata.com/
- Dokumentácia: https://docs.influxdata.com/

Suricata

- Web: https://suricata.io/
- Dokumentácia: https://docs.suricata.io/

Snort

- Web: https://www.snort.org/
- Dokumentácia: https://docs.snort.org/

Wazuh

- Web: https://wazuh.com/
- Dokumentácia: https://documentation.wazuh.com/

OSSEC

- Web: https://www.ossec.net/
- Dokumentácia: https://ossec.github.io/docs/

Zeek (Bro)

- Web: https://zeek.org/
- Dokumentácia: https://docs.zeek.org/