31/10/2023

Report PoC del DB e del sistema SIEM/OSINT

D.2.3.1 Fighting Cybercrime with OSINT

M. Gnaldi, L. Grilli, A. Milani, A. Navarra, M.C. Pinotti, F. Santini, C.Taticchi,
UNIVERSITÀ DEGLI STUDI DI PERUGIA

Sommario

Breve introduzione al deliverable

In questo deliverable l'obiettivo è di descrivere brevemente le scelte riguardanti i sistemi / le architetture considerate per il PoC del SIEM – OSINT che è stato scelto per questo progetto. Alla base del SIEM, il primo dei sistemi che sono utilizzati corrisponde al DBMS che memorizza e rende possibile interrogare e analizzare le informazioni contenute.

Nel mondo moderno, il numero delle minacce informatiche è in costante crescita; in particolare, i sistemi SIEM vengono utilizzati per accrescere le possibilità di analisi delle informazioni di sicurezza collezionate e rendere quindi più veloce ed efficace la risposta di un team di *Incident Response*. Per lo sviluppo di un futuro sistema SIEM, si devono prendere in considerazione vari tipi di database moderni. Un database è una raccolta ordinata di dati strutturati archiviati elettronicamente in un sistema informatico. Il database è controllato da un sistema di gestione del database (DBMS). I dati insieme al DBMS, così come le applicazioni ad essi associate, sono chiamati sistema di database o database.

I DBMS più utilizzati dai SIEM

Questa sezione si ispira al lavoro in [1] che contiene una rassegna dei DBMS utilizzati dai SIEM attualmente più conosciuti. I DBMS considerati si possono basare su differenti caratteristiche, riassunte nelle seguenti classi.

- *DBMS di semplice struttura*
  - Simple Data Structures (file di testo e di log)
  - Hierarchical Databases (file systems, DNS, LDAP)
  - Network Databases (IDMS)
- *Database relazionali*
  - SQL Databases (MySQL, MariaDB, PostgreSQL, SQLite, MSSQL)
  - OLTP Databases
- *NoSQL Databases*
  - Key-Value Databases (Redis, Memcached, etcd)
  - Document Database (MongoDB, RethinkDB)
  - Graph Database (Neo4j, JanusGraph, Dgraph)
  - Columnar Databases (Cassandra, HBase)
  - Time Series Databases (OpenTSDB, Prometheus, InfluxDB, TimescaleDB)
- *Combined Databases*
  - NewSQL Databases (MemSQL, VoltDB, Spanner, Calvin, CockroachDB, FaunaDB, YugabyteDB)

    - Multi-Model Databases (ArangoDB, OrientDB, Couchbase)
- *Object-Oriented Databases (OODB)*
- *Cloud Databases*

I SIEM che utilizzano **database relazionali** sono: IBM QRadar, LOGRHYTHM, AlienVault USM, AlienVault OSSIM, Splunk, FortiSIEM, Wazuh, SolarWinds, ManageEngine, RuSIEM, Prelude OSS, Prelude SIEM, Sagan, Maxpatrol, EventTracker, Trustwave SIEM Enterprise, McAfee (ESM). I database relazionali sono il tipo più antico di database di uso generale ancora ampiamente utilizzato. I dati in un database relazionale sono organizzati in tabelle, costituite da colonne e righe. Ogni colonna in una tabella ha un nome e un tipo. Ogni riga rappresenta un record separato o un elemento dati nella tabella, contenente un valore per ciascuna colonna

I SIEM che utilizzano **database NoSQL** sono: AlienVault USM, AlienVault OSSIM, MozDef, Maxpatrol, SearchInform SIEM. NoSQL è un gruppo di tipi di database che offrono approcci diversi dal modello relazionale standard. NoSQL si riferisce a "non SQL" o "non solo SQL" per chiarire che a volte è consentita una query di tipo SQL. Un database NoSQL, o database non relazionale, offre la possibilità di archiviare ed elaborare dati non strutturati o semistrutturati (al contrario di un database relazionale, che definisce la struttura dei dati in esso contenuti). La popolarità dei database NoSQL sta crescendo man mano che le applicazioni web proliferano e diventano più complesse.

I SIEM che utilizzano **database Cloud** sono HPE, ArcSight, Splunk, Ixia ThreatARMOR, Micro Focus ArcSight, Trustwave SIEM Enterprise. Un database cloud è una raccolta di dati strutturati o non strutturati ospitati su una piattaforma di cloud computing privata, pubblica o ibrida. Esistono due tipi di modelli di database cloud: database tradizionale e “DataBase as a Service” (DBaaS). Nel modello DBaaS, le attività amministrative e la manutenzione vengono eseguite dal fornitore cloud. Per completezza, riportiamo i database utilizzati da 23 SIEM, mostrando una Tabella in [1]:

SIEM	DBMS
IBM QRadar	Ariel database, PostgreSQL, SQLite
LOGRHYTHM	Oracle, SQL Server, MySQL
HPE ArcSight	Own development CORR-E
Splunk	DB2 / Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, and Teradata
McAfee (ESM)	MSSQL, Oracle, MySQL, Data Access Server (DAS), DB2 / UDB
AlienVault USM	RedisDB, MySQL
AlienVault OSSIM	RedisDB, MySQL
FortiSIEM	PostgreSQL
Ixia ThreatARMOR	Rap Sheet
MozDef	RabbitMQ, MongoDB, Elasticsearch, Kibana
Wazuh	MySQL, PostgreSQL
Prelude OSS	MySQL, PostgreSQL
Prelude SIEM	MySQL, PostgreSQL
Sagan	MySQL / PostgreSQL
Maxpatrol	ElasticSearch, MongoDB, MS SQL Express
SolarWinds	MSSQL, Oracle, MySQL, MariaDB.
ManageEngine	Oracle, SQL, DB2, & MySQL
EventTracker	Microsoft SQL Server
Micro Focus ArcSight	Own development CORR-E
Trustwave SIEM Enterprise	Microsoft SQL Server, Microsoft SQL Azure, ORACLE, SYBASE, MySQL, IBM, DB2, Hadoop
BlackStratus SIEMStorm	Own development
SearchInform SIEM	MongoDB
RuSIEM	MySQL / Oracle / MS SQL

Tabella 1: I principali SIEM e i loro database [1]

Per selezionare i database durante la creazione di sistemi SIEM, è necessario tenere conto della comodità di archiviazione, della velocità di acquisizione e utilizzo dei dati. È necessario fornire l'integrazione con altri moduli di sistema e API esterne per fornire supporto database per la maggior parte dei sistemi Deep Packet Inspection, o DPI (sia software che hardware).

Una rassegna sui SIEM più importanti, le loro caratteristiche

Questa sezione si basa invece sull'articolo in [2], in cui i principali SIEM sono passati in rassegna e vengono stilate delle tabelle di comparazione delle loro proprietà.

Per la certificazione, tutti i sistemi SIEM devono essere conformi al gruppo internazionale di standard di sicurezza delle informazioni: ISO/IEC 27000, PCI-DSS, HIPAA, NIST 800-171, DoD, RMF, GDPR. Per risolvere i problemi legati alla sicurezza e alla correzione degli eventi di un sistema SIEM, considera le principali funzionalità dei sistemi SIEM:

- *Aggregazione dei dati*: gestione del data log; i dati vengono raccolti da varie fonti.
- *Correlazione*: trovare attributi comuni, collegare eventi a cluster significativi.
- *Alert*: analisi automatizzata degli eventi correlati e generazione di notifiche (allarmi) in merito a problemi attuali (e-mail, gateway GSM, applicazioni sul telefono).
- *Strutture di visualizzazione*: visualizza grafici per aiutare a identificare le anomalie di lavoro utilizzando modelli preparati.
- *Compatibilità*: utilizzando componenti aggiuntivi per automatizzare la raccolta dei dati, creando report da adattare aggregati dati ai processi esistenti di gestione e audit della sicurezza delle informazioni.
- *Archiviazione dei dati*: l'uso dell'archiviazione dei dati a lungo termine in ordine storico per correlare i dati nel tempo e per ulteriori analisi forensi informatiche e indagini sugli incidenti di rete.

Di seguito si riportano due tabelle provenienti dall'articolo [2], in cui si elencano 20 differenti caratteristiche dei SIEM (riportate di seguito) e si incrociano il loro supporto da parte dei SIEM oppure no.

1. Audit e verifica del rispetto degli standard.
2. Sistema completo/sistema di elaborazione dei registri.
3. Valutazione della sicurezza delle risorse del sistema controllato.
4. Verifica della conformità del sistema di gestione con i requisiti e gli standard esistenti.
5. Gestione del rischio per la sicurezza delle informazioni.
6. Raccolta e archiviazione degli eventi di sicurezza in entrata.
7. Elaborazione e analisi degli eventi di sicurezza registrati.
8. Rilevazione di attacchi e violazioni delle politiche di sicurezza in tempo reale.
9. Identificazione e analisi degli incidenti di sicurezza.
10. La capacità di indagare sugli incidenti.
11. Cerca le vulnerabilità.

12. Formazione dei rapporti.
13. Supporto per lavorare con i cloud.
14. Supporto per lavorare con piattaforme Big Data.
15. Possibilità di integrazione con nuovi sistemi.
16. Funzionalità avanzate di ricerca e visualizzazione dei dati.
17. Interfaccia facile da usare.
18. Sistemi operativi supportati.
19. Le principali fonti dei log.
20. Costo del sistema.

System name	Audit and Compliance	Complete System (PS) / Log Processing System (SOL)	Assessment of the security of the resources at the controlled system	Verification of compliance of the IS management system with existing requirements and standards	Information security risk management	Collecting and storing incoming security events	Processing and analysis of registered security events	Detect attacks and security policy violations in real time	Identification and analysis of security incidents	Incident investigation capability
IBM QRadar	+	PS	+	+	+	+	+	+	+	+
LOGRHYTHM	+	PS	+	+	+	+	+	+	+	+
HPEArcSight	+	PS	+	+	+	+	+	+	+	+
Splunk	+	PS	+	+	+	+	+	+	+	+
McAfee (ESM)	+	PS	+	+	+	+	+	+	+	+
AlienVault USM	+	PS	+	+	+	+	+	+	+	+
Alien Vault OS SIM	–	PS	+	+	+	+	+	+	+	±
FoniSIEM	+	PS	+	+	+	+	+	+	+	+
Ixia ThreatARMOR	+	PS	+	+	+	+	+	+	+	+
MozDef	+	PS	–	+	–	+	+	+	+	+
Wazuh	+	PS	not indicated	+	–	+	+	+	+	+
Prelude OSS	+	PS	not indicated	+	+	+	+	+	+	+
Prelude SIEM	+	PS	not indicated	+	+	+	+	+	+	+
Sasan	–	SOL	–	–	–	+	+	+	+	+
Maxpatrol	+	PS	+	+	+	+	+	+	+	+
SolarWinds	+	PS	+	+	+	+	+	+	+	+
ManateEnaine	+	SOL	–	+	–	+	+	+	+	+
EventTracker	+	PS	–	+	–	+	+	+	+	+
Micro Focus ArcSight	+	PS	+	+	+	+	+	+	+	+
Trustwave SIEM Enterprise	+	PS	–	+	+	+	+	–	+	+
BlackStratus SIEMStonn	+	PS	–	+	–	+	+	+	+	+
SearchInfonn SIEM	+	PS	+	+	+	+	+	+	+	+
RuSIEM	+	PS	+	+	+	+	+	+	+	+

Tabella 2: Analisi multicriteria dei SIEM (parte 1) [2]

Sulla base dell'analisi riportata in queste due tabelle, gli autori di [2] dichiarano che il sistema *FortiSIEM* è il più "ottimale". Anche i sistemi *IBM QRadar*, *LOGRHYTHM*, secondo i criteri di selezione, ottengono un gran numero di punti, ma sono costosi e non disponibili per molte aziende. Inoltre, si consiglia agli sviluppatori di prestare la loro attenzione alle soluzioni open source riportate nelle tabelle, che corrispondono ad *Alien Vault OS SIM*, *MozDef*, *Wazuh*, *Prelude OSS*, *Sasan*, *RuSIEM*.

System name	Search for vulnerabilities	Report generation	Cloud support	Support for working with Big Data platforms	Possibilities of integration with new systems tomorrow	Advanced search and data visualization	User friendly interface	Supported operating systems	Main sources of logs	System cost
IBM QRadar	+	+	+	+	+	+	+	linux	Lots of	$ 63000 +
LOGRHYTHM	+	+	+	+	+	+	+	linux/windows	Lots of	$ 28000 +
HPEArcSight	+	+	+	+	+	+	+	linux	Lots of	500 thousand rubles +
Splunk	+	+	+	+	+	+	+	Unix/Windows	Lots of	Free 500 mb S 5.000 for 1 GB day
McAfee (ESM)	+	+	+	+	+	+	+	Windows	Lots of	$ 261000 +
AlienVault USM	+	+	+	+	+	+	+	Linux/Windows	Lots of	$ 1075/mo.
Alien Vault OS SIM	+	+	–	–	–	+	+	Linux/Windows	Lots of	free
FoniSIEM	+	+	+	+	+	+	+	Linux/Windows	Lots of	$ 900 +
Ixia ThreatARMOR	+	+	–	–	+	+	+	Unix/Windows/ other	Lots of	£ 3158/year
MozDef	–	+	+	+	+	+	+	Centos 7	Json	free
Wazuh	+	+	+	+	+	+	+	Linux	Windows/ Linux logs	free
Prelude OSS	+	+	–	–	–	+	+	Linux	Lots of	free
Prelude SIEM	+	+	–	–	–	+	+	Linux	Lots of	9
Sasan	–	+	–	–	–	+	–	Linux	Lots of	free
Maxpatrol	+	+	+	+	+	+	+	–	Lots of	RUB 1,840,000 +
SolarWinds	+	+	+	+	+	+	+	Linux/Windows agents	Lots of	2.055 € +
ManateEnaine	+	+	–	–	–	+	+	Windows	Windows/ Linux logs	$ 1000 +
EventTracker	+	+	+	+	–	+	+	Windows	Windows/ Linux logs	$8995
Micro Focus ArcSight	+	+	+	+	+	+	+	Linux	Lots of	500 thousand rubles +
Trustwave SIEM Enterprise	+	+	+	+	–	+	+	Centos 7	Lots of	$1000/year
BlackStratus SIEMStonn	+	+	–	–	–	+	+	–	not indicated	–
SearchInfonn SIEM	+	+	+	+	+	+	+	Linux/Windows	Lots of	Negotiable
RuSIEM	+	+	–	–	+	+	+	Ubuntu 16	Lots of	Paid/no fee

Tabella 3: Analisi multicriteria dei SIEM (parte 2) [2]

Considerazioni finali

Per i nostri interessi di progetto, la scelta della base per il SIEM si restringe ad uno dei cinque sistemi Open Source riportati alla fine della sezione precedente, oppure, ad un sistema che non sia direttamente un SIEM, ma che possa servire per implementarne uno, come ELK/OpenSearch.

Lo stack ELK (Elasticsearch, Logstash, Kibana) è una popolare piattaforma di analisi e gestione dei log Open Source. La raccolta, l'elaborazione, la normalizzazione, il miglioramento e l'archiviazione dei dati di registro provenienti da varie fonti sono raggruppati sotto il termine "gestione dei log". È un componente necessario in qualsiasi soluzione SIEM, ma di per sé insufficiente. ELK si occupa della raccolta, elaborazione e archiviazione dei registri. Tuttavia, non garantisce direttamente la

correlazione degli eventi, le funzionalità di avviso e la gestione degli incidenti in modo immediato, che quindi devono essere implementate in qualche maniera.

Come già introdotto, nella sua forma grezza, ELK potrebbe essere un elemento costitutivo di un sistema SIEM completo. Riprova è che per esempio EventTracker utilizza Elastic Search come sistema di indicizzazione. La stessa Elasticsearch ha esteso il suo stack ELK come uno strumento di analisi di sicurezza e lo propone come un SIEM.[1] Elastic Security migliora lo stack ELK con funzionalità di sicurezza aggiuntive, come il rilevamento delle minacce, il rilevamento delle anomalie basato sull'apprendimento automatico, la risposta agli incidenti di sicurezza e le integrazioni con varie origini dati di sicurezza. Consente alle organizzazioni di monitorare e rispondere agli eventi di sicurezza in tempo reale, rendendolo una soluzione completa per l'analisi e le operazioni di sicurezza. In sintesi, lo stack ELK è un insieme di strumenti per la gestione dei log e l'analisi dei dati, mentre Elastic Security è una soluzione incentrata sulla sicurezza costruita sullo stack ELK, che fornisce funzionalità aggiuntive specificatamente personalizzate per i casi d'uso della sicurezza.

Elastic search offre funzionalità di rilevamento di anomalie che necessitano di una qualche orma di pagamento. Inoltre, come rilevamento di minacce gratuite esiste il Detection engine[2] che permette la creazione di regole custom di diversa tipologia come “Custom Query” per KQL (Kibana Query Language), “Threshold”, “Event Correlation”, “Indicator Match” e “New Terms”.

In Eleastic Security, i dati vengono spediti dagli host a Elasticsearch nei seguenti modi:

- **Elastic Defend**: integrazione di Elastic Agent che protegge gli host da malware e fornisce questi set di dati:
    - Windows: processi, rete, file, DNS, registro, caricamenti di DLL e driver, rilevamenti di sicurezza malware, API
    - Linux/macOS: processi, rete, file
- **Integrazioni**: le integrazioni rappresentano un modo semplificato per inviare i dati all'Elastic Stack. Sono disponibili integrazioni per servizi e piattaforme popolari, come Nginx, AWS e MongoDB, nonché molti tipi di input generici come i file di registro.
- **Moduli Beat**: i Beat sono trasportatori di dati leggeri. I moduli Beat forniscono un modo per raccogliere e analizzare set di dati specifici da fonti comuni, come eventi, log e metriche del cloud e del sistema operativo. I moduli comuni relativi alla sicurezza sono elencati su una pagina apposita.[3]

L'app Elastic Security in Kibana viene utilizzata per gestire i Detection Engine, i Case e le Timeline, nonché per amministrare gli host che eseguono Elastic Defend (Administration):

- **Detection Engine**: ricerca automaticamente host sospetti e attività di rete tramite quanto segue:
    - *Detection rule*: cerca periodicamente i dati (indici Elasticsearch) inviati dagli host per eventi sospetti. Quando viene scoperto un evento sospetto, viene generato un

[1] https://www.elastic.co/security/siem
[2] https://www.elastic.co/guide/en/security/current/rules-ui-create.html
[3] https://www.elastic.co/guide/en/security/current/ingest-data.html#enable-beat-modules

avviso. Sistemi esterni, come Slack ed e-mail, possono essere utilizzati per inviare notifiche quando vengono generati avvisi. Puoi creare le tue regole e utilizzare quelle predefinite.
    - *Exception*: ridurre il rumore e il numero di falsi positivi. Le eccezioni sono associate alle regole e impediscono gli avvisi quando vengono soddisfatte le condizioni di un'eccezione. Quando Elastic Defend è installato sugli endpoint, si possono aggiungere eccezioni malware direttamente all'endpoint dall'app Sicurezza.
    - *Machine Learning Job*: rilevamento automatico delle anomalie degli eventi host e di rete. I punteggi di anomalia vengono forniti per host e possono essere utilizzati con le regole di rilevamento.
- **Timeline**: è un'area di lavoro per l'analisi di avvisi ed eventi. Le sequenze temporali utilizzano query e filtri per approfondire gli eventi relativi a un incidente specifico. I modelli di sequenza temporale sono collegati alle regole e utilizzano query predefinite quando vengono esaminati gli avvisi. Le sequenze temporali possono essere salvate e condivise con altri, nonché allegate ai casi.
- **Case**: è un sistema interno per l'apertura, il monitoraggio e la condivisione dei problemi di sicurezza direttamente nell'app Sicurezza. I casi possono essere integrati con sistemi di ticketing esterni.
- **Administration**: visualizza e gestisci gli host che eseguono Elastic Defend.

L'Elastic Agent con l'integrazione Elastic Defend, che protegge gli host e invia log, parametri e dati di sicurezza degli endpoint a Elastic Security. L'Elastic Agent con l'integrazione Elastic Defend fornisce questi dati:

- Processo: Linux, macOS, Windows
- Rete: Linux, macOS, Windows
- File: Linux, macOS, Windows
- DNS: Windows
- Registro di sistema: Windows
- Caricamento di DLL e driver: Windows
- Sicurezza: Windows

Come nota finale, possiamo sottolineare come sia possibile l'integrazione di Elastic Stack con Wazuh. L'integrazione di Wazuh ed Elastic Stack arricchisce l'approccio al monitoraggio della sicurezza fornendo la flessibilità necessaria per gestire e visualizzare i dati raccolti e analizzati da Wazuh in Elastic Stack. Su Internet è possibile trovare dei tutorial che dettagliano l'integrazione.[4]

L'integrazione di Elastic Stack e Wazuh crea una soluzione SIEM che combina le funzionalità di gestione e visualizzazione dei log di ELK con le funzionalità di rilevamento delle minacce in tempo reale e risposta agli incidenti di Wazuh. Questa integrazione migliora l'efficacia complessiva del monitoraggio e dell'analisi della sicurezza.

[4] https://documentation.wazuh.com/current/integrations-guide/elastic-stack/index.html

Wazuh ed Elastic Security (precedentemente noto come Elastic SIEM) sono entrambe soluzioni di sicurezza, ma hanno focus e capacità diverse. Ecco alcune differenze chiave tra Wazuh ed Elastic Security:

- **Focus principale**:
  - *Wazuh*: Wazuh si concentra principalmente sul rilevamento delle intrusioni, sul rilevamento delle minacce e sull'analisi dei log. Fornisce una soluzione SIEM (Security Information and Event Management) focalizzata sull'analisi in tempo reale degli eventi di sicurezza, sul rilevamento delle intrusioni e sulla risposta agli incidenti.
  - *Elastic Security*: Elastic Security è una soluzione di sicurezza basata sull'Elastic Stack (stack ELK), con una forte enfasi sulla gestione dei log, sulla visualizzazione dei dati e sull'analisi della sicurezza. Fornisce funzionalità SIEM insieme a funzionalità come la caccia alle minacce, il rilevamento di anomalie e la sicurezza degli endpoint.
- **Casi d'uso**:
  - *Wazuh*: Wazuh è adatto per le organizzazioni che cercano una soluzione SIEM e di rilevamento delle intrusioni mirata. Eccelle nel rilevamento delle minacce in tempo reale, nell'analisi dei registri e nella risposta agli incidenti.
  - *Elastic Security*: Elastic Security è adatta per le organizzazioni che richiedono una soluzione di sicurezza più ampia, che combina gestione dei log, SIEM, individuzione delle minacce e sicurezza degli endpoint. Fornisce una piattaforma più completa per l'analisi e le operazioni di sicurezza.
- **Machine Learning e Anomaly Detection**:
  - *Wazuh*: Wazuh include alcune funzionalità di rilevamento delle anomalie, ma il suo obiettivo principale è il rilevamento basato su regole e la correlazione degli eventi di sicurezza.
  - Elastic Security: Elastic Security include il rilevamento di anomalie basato sull'apprendimento automatico, fornendo funzionalità avanzate per identificare modelli insoliti e potenziali minacce alla sicurezza. La funzionalità di machine learning è disponibile quando si dispone dell'abbonamento appropriato, si utilizza una distribuzione Cloud o si stia testando una prova gratuita (free trial).
- **Licenza**:
  - *Wazuh*: Wazuh è open source e dispone di un'edizione comunitaria disponibile gratuitamente. Offre anche un abbonamento aziendale a pagamento con funzionalità e supporto aggiuntivi.
  - *Elastic Security*: Sebbene molti componenti dello stack ELK siano open source, Elastic Security dispone anche di funzionalità commerciali ed è disponibile tramite piani di abbonamento.

Disclaimer finale: Elastic search non è più considerato ufficialmente Open Source. Il codice sorgente con licenza Apache 2.0 di Elasticsearch e Kibana è stato modificato in modo che disponga di doppia licenza con Elastic License e SSPL 1.0 (Elastic License and Server Side Public License (SSPL)), offrendo agli utenti la scelta di quale licenza applicare. La nuova licenza di Elastic (Elastic License v2 o ELv2) sarà anche semplificata rendendola sostanzialmente più permissiva. La distribuzione di riferimento continuerà a essere soggetta alla licenza Elastic come è stata per quasi gli ultimi tre anni e non saranno più rilasciate distribuzioni con Apache 2.0. Quindi, la licenza SSPL non è stata approvata

dall'OSI, quindi per evitare confusione il codice non è più riferito come Open Source sul sito di Elastic search. La nuova concede il diritto gratuito di utilizzare, modificare, creare opere derivate e ridistribuire, con tre semplici limitazioni:

- Non si può fornire i prodotti ad altri come servizio gestito.
- Non è possibile eludere la funzionalità della chiave di licenza o rimuovere/oscurare funzionalità protette dalle chiavi di licenza.
- Non è possibile rimuovere o oscurare licenze, diritti d'autore o altri avvisi.

Bibliografia

[1] S. Gnatyuk, R. Berdibayev, I. Azarov, N. Baisholan, and I. Lozova, “Modern Types of Databases for SIEM System Development,” CEUR Workshop Proc, vol. 3187, pp. 127–138, 2021.

[2] S. Gnatyuk, R. Berdibayev, A. Fesenko, O. Kyryliuk, and A. Bessalov, “Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare,” CEUR Workshop Proc, vol. 3188, pp. 149–166, 2021.