Seminario 2

SIEM

Definizione. Il **SIEM** (Security Information and Event Management) è una soluzione di sicurezza progettata per consentire alle organizzazioni di rilevare minacce e anomalie prima che compromettano le attività. Si tratta di una piattaforma centralizzata che consente di monitorare, raccogliere e analizzare dati (log) provenienti da diverse fonti, riducendo significativamente i tempi di risposta in caso di eventi sospetti.

In contesti complessi dove sono presenti grandi volumi di dati, come nel caso dell'Università di Parma, il SIEM permette di:

- Raccogliere log da fonti multiple per ottenere una visione completa del sistema.
- Correlare i dati per identificare pattern di minaccia.
- Analizzare eventi in tempo reale per rispondere rapidamente a incidenti di sicurezza.

I **dati raccolti** (Log) possono provenire da più fonti. Nel caso dell'università di Parma possono essere:

- **Fortigate**: Firewall di perimetro che filtra indirizzi IP, previene intrusioni (IPS), funge da VPN e controlla applicazioni.
- **Microsoft Defender**: Strumento di protezione contro phishing, gestione degli endpoint e threat intelligence.
- **Esfiltrazioni DarkWeb**: Monitoraggio delle password compromesse tramite botnet o altre tecniche di controllo.

Il SIEM raccoglie, correla e analizza i log, offrendo una gestione efficace tramite piattaforme come **ElasticSearch** (ad esempio implementato via Docker).

> **Info**
>
> Nel contesto di un SIEM, ElasticSearch viene utilizzato per archiviare e interrogare i log raccolti, consentendo una gestione centralizzata ed efficiente dei dati di sicurezza.

Raccolta Log

I log, rappresentati come coppie **chiave-valore**, vengono raccolti per un’analisi efficiente e uno storage ottimizzato. Questo processo avviene utilizzando strumenti come **Logstash**, che raccoglie, elabora e trasforma i log, oppure tramite script personalizzati o plugin integrati per gestire i dati in modo efficiente.

Gli obiettivi principali includono:

- Filtraggio accurato dei dati per eliminare rumore inutile.
- Analisi rapida delle informazioni critiche.
- Archiviazione efficiente per la consultazione futura.

Visualizzazione dati

Per analizzare e comprendere meglio i dati raccolti, il SIEM offre interfacce grafiche come **Kibana UI**, che permettono di visualizzare:

- Dashboard personalizzate.
- Grafici e report che evidenziano eventi critici o tendenze anomale.

Anomaly detection

La rilevazione delle anomalie è una componente chiave del SIEM, che utilizza tecniche avanzate per individuare comportamenti sospetti. Tra le analisi principali:

- **Population**: Individua comportamenti che si discostano dalla norma all’interno di un insieme di dati (popolazione).
- **Rare**: Rileva eventi rari o insoliti che potrebbero indicare minacce.
- **Categorization**: Classifica i dati in categorie e individua eventi che non rientrano nei modelli previsti.
- Altre metriche: **Single Metric**, **Multi Metric**, **Geo**, ecc., che permettono di analizzare i dati secondo dimensioni multiple per identificare schemi complessi.