

Day 23 - Ticketing System

Ticketing System

Gestione degli Alert tramite un Sistema di Ticketing

Un sistema di ticketing è essenziale per monitorare e gestire gli incidenti di sicurezza, gli alert e le richieste tecniche in modo strutturato.






Efficienza: Evita di perdere di vista i problemi.




Organizzazione: Ogni ticket contiene tutte le informazioni necessarie per troubleshooting, segnalazioni, o reclami.

Cos'è un Sistema di Ticketing?

• Un sistema di ticketing permette la creazione e gestione centralizzata di **ticket** che possono riguardare:

-  **Richieste di troubleshooting** (risoluzione di problemi tecnici)
-  **Alert di sicurezza** (gestione e risposta agli incidenti)
-  **Reclami** (comunicazioni da parte degli utenti)

• **Vantaggi:**

-  **Audit trail:** Fornisce una traccia dettagliata delle attività eseguite, utile per la **accountability** (responsabilità), che supporta il principio di **Accounting** nella triade **CIA** (Confidentiality, Integrity, Availability).
-  **Gestione delle attività in corso:** Aiuta il SOC a mantenere il focus sui problemi critici in tempo reale.

Ticketing System


Esempi di Sistemi di Ticketing per SOC

Esempi di sistemi di ticketing popolari:

- Kira
- ServiceNow
- Zendesk

Focalizzarsi su osTicket



 **osTicket** è una soluzione **open source** per la gestione dei ticket che offre:

- **Campi personalizzati:** Personalizzazione dei dati per adattarsi alle necessità specifiche del SOC.
- **Filtri per ticket:** Creazione di regole per assegnare e trasferire automaticamente i ticket.
-  **SLA** (Service Level Agreement): Possibilità di impostare scadenze e tempi di risposta, simulando le operazioni di un SOC.

Ticketing System

osTicket - Infrastruttura Flessibile

osTicket può essere implementato sia **on-premise** (installato su infrastruttura locale) che in **cloud**.

-  **Cloud**: Facilità di accesso e scalabilità, senza bisogno di gestire l'infrastruttura fisica.
-  **On-premise**: Maggiore controllo sui dati e sulla sicurezza, ideale per ambienti ad alta sicurezza come i SOC.

Con osTicket, puoi facilmente replicare la struttura e i flussi operativi di un **SOC startup**, con strumenti flessibili per la gestione degli incidenti di sicurezza.