SOC Automation & Orchestration

DEMISTO ENTERPRISE

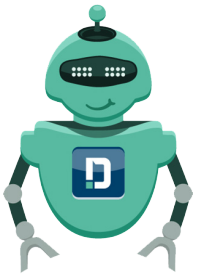
DEMISTO

Automazione e intelligenza artificiale per il SOC

In uno scenario dominato da minacce sempre più sofisticate, coloro che operano nel SOC affrontano sfide molto complesse.

Gli analisti di primo livello sono sommersi da miriadi di allarmi e sono costretti ad effettuare attività lunghe e tediose per eliminare i falsi positivi e per eseguire operazioni molto spesso ripetitive.

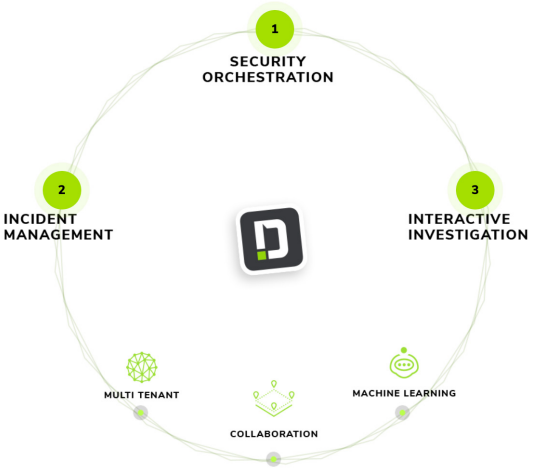
Gli analisti di livello superiore sono invece impegnati nel cercare il cosiddetto “ago nel pagliaio”, ossia le poche informazioni significative all’interno di una massa di informazioni spesso di scarsa rilevanza. Per loro diventa sempre più elevato il rischio di incorrere in un errore umano o in una sottovalutazione di una seria minaccia.



Demisto Enterprise è la soluzione per l’automazione e l’orchestrazione del **Security Operation Center**. Demisto è in grado di mettere in collegamento persone, processi e tecnologie di sicurezza, in un tessuto connettivo in grado di **trasformare le attività del Security Operation Center**, aumentandone l’efficacia e il livello di protezione dell’infrastruttura tecnologica. Demisto Enterprise introduce un livello di automazione tale da garantire la massima efficacia del team di sicurezza, consentendo di raggiungere il massimo livello di protezione dalle minacce Cyber.

Demisto Enterprise integra tutti gli strumenti di sicurezza che vengono gestiti nel **Security Operation Center**, facendoli diventare parte di un unico sistema automatico di gestione degli Incident, grazie alle sue capacità di **orchestrazione, automazione e documentazione**.

Demisto Enterprise, con le sue funzioni di orchestrazione, **genera l’interazione ideale tra persone, processi e strumenti tecnologici**: un portafoglio di procedure pronte (playbook) per automatizzare i processi con oltre 100 integrazioni native e oltre 400 azioni di sicurezza predefinite, strumenti di condivisione e collaborazione come la War Room virtuale, l’utilizzo di tecniche avanzate di Machine Learning per eliminare tutti i processi ripetitivi e valorizzare tutte le attività effettuate.



1) Security Orchestration

Rispondere agli incident di sicurezza con rapidità e scalabilità

L’orchestrazione di Demisto consente ai team di sicurezza di utilizzare le informazioni e gli alert provenienti da tutti gli strumenti di sicurezza e di eseguire playbook automatizzati e standardizzati per fornire una risposta più rapida agli incident di sicurezza.

- **Rende disponibili in modo nativo oltre 100 funzioni di integrazione con strumenti di sicurezza per gestire il processo di analisi**
- **Consente di automatizzare la risposta agli incident mettendo a disposizione oltre 1000 comandi e procedure**
- **Analizza gli Indicatori di Compromissione (IoC) e i più comuni trend cross-incident**

2) Incident Management

Standardizzare i processi attraverso i prodotti e i team

Demisto, snellisce il processo di acquisizione degli avvisi da più fonti e l’attivazione delle procedure automatizzate di risposta. Inoltre, ricostruisce la timeline degli incident per una chiara analisi delle cause che li hanno generati

- **Rende disponibili cinque viste specializzate sul ciclo di vita degli incident**
- **Cattura dati su performance e SLA per garantire “accountability” sulle risposte**
- **Mette a disposizione metriche granulari per valorizzare al massimo i dati all’interno del processo**

3) Interactive Investigation

Migliorare la qualità dell’investigazione con la collaborazione

Demisto supporta l’investigazione in tempo reale, valorizzando le sinergie tra tutti gli specialisti del team di sicurezza e applicando tecniche avanzate di machine learning, così da aumentare l’efficacia della risposta.

- **Mette a disposizione una “War Room” virtuale che attiva il processo collaborativo nelle fasi di analisi e risposta**
- **Processa comandi in tempo reale su diversi strumenti per minimizzare i tempi di passaggio tra console diverse**
- **Utilizza tecniche avanzate di machine learning per rendere più efficienti le operazioni**

PRINCIPALI BENEFICI

Processo consistente, trasparente e documentato

- Investigazioni sugli incident e azioni di risposta guidate da procedure (playbook-driven)
- Documentazione automatica di tutte le indagini e reportistica storica
- Identificazione automatica di investigazioni duplicate
- Ricerca trasversale rispetto a investigazioni, indicatori e prove

Tempo di risoluzione più breve e maggiore efficienza

- Procedure predefinite e personalizzabili per automatizzare azioni ridondanti e ripetibili
- War Room virtuale per condividere investigazioni in tempo reale
- Tracciatura granulare degli incident e delle metriche di analisi

Aumento della produttività degli Analisti e crescita del livello di competenza del Team

- Piattaforma collaborativa che permette agli analisti di condividere informazioni importanti
- Possibilità per gli analistiti di strutturare training basati su indagini di eventi accaduti
- Uso di tecniche di machine learning (ML-powered) per supportare gli analisti nelle investigazioni, utilizzando l'esperienze già vissute

CARATTERISTICHE UNICHE

EDITOR VISUALE DI PLAYBOOK

Playbook facili da sviluppare grazie alle funzioni drag-and-drop e alla disponibilità di centinaia di azioni eseguibili interagendo con un'ampia gamma di prodotti di sicurezza

PIANO DI LAVORO IN TEMPO REALE

Un'interfaccia grafica chiara e intuitiva per rivedere e convalidare le esecuzioni di playbook in tempo reale, con un linguaggio interpretabile sia dall'uomo e sia dalla macchina

PRODUZIONE DI PLAYBOOK CODELESS

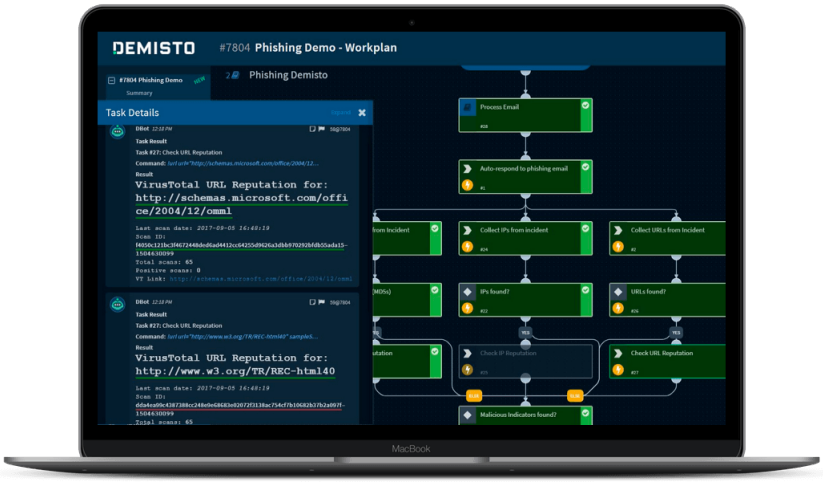
I Playbook sono implementati con "filtri" e "trasformatori" che possono essere manipolati per implementare automazioni complete e sofisticate, senza la necessità di scrivere neanche una riga di codice.

MODULARE E DINAMICO

Tutte le attività possono essere trasformate in Playbook attraverso un processo semplice, veloce, e affidabile in Playbook, grazie alle funzioni di editing visuale, di modifica in tempo reale, di test di condivisione basata su YAML

PIATTAFORMA INTEGRATA ED ESTENSIBILE

Centinaia di integrazioni di prodotti di sicurezza integrate nativamente con funzionalità intuitive e un potente SDK per creare integrazioni personalizzate



ACCELERARE AL MASSIMO LA RISPOSTA AGLI INCIDENT

Nell'attuale scenario, la caratteristica più importante di Demisto Enterprise è quella di garantire un'accelerazione unica al processo di gestione e risposta efficace agli incident di sicurezza, grazie alle funzioni di automazione, orchestrazione, collaborazione e investigazione in tempo reale, tutto concentrato in un'unica console.

gruppo Daman
Passione e Innovazione

Le soluzioni Demisto sono distribuite in Italia dal Gruppo Daman.

Per saperne di più:
www.gruppodaman.it

Per contattarci:
comunicazione@gruppodaman.it
+39.800.741.423