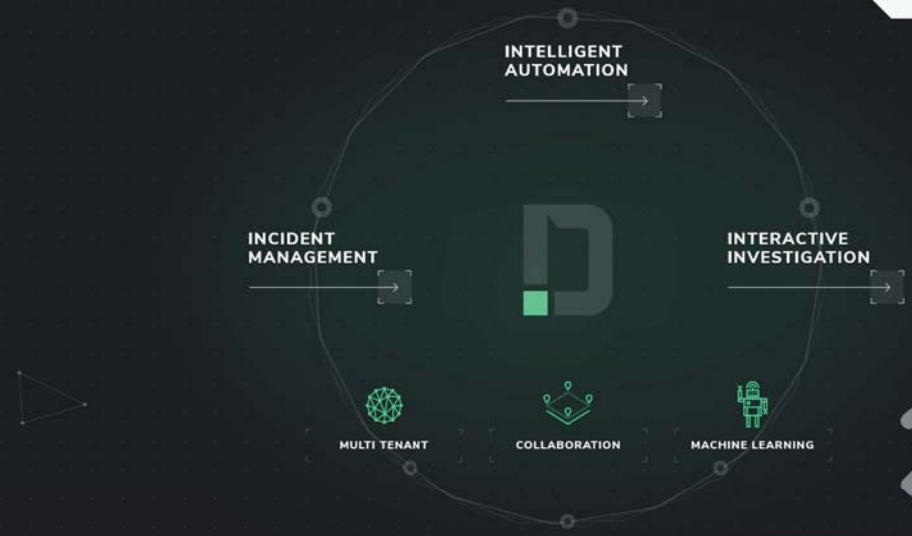
DEMISTO ENTERPRISE

DEMISTO



gruppo Daman

Automazione e intelligenza artificiale: alleati indispensabili per il Security Operation Center

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.

In questo quadro i manager del SOC hanno seri problemi a determinare il ROI degli strumenti di sicurezza, mentre sono sottoposti a **forti pressioni sul mancato rispetto degli SLA**, anche a fronte di metriche di tracciamento incomplete e alla difficoltà di produrre una documentazione esaustiva.

Ma c'è un'ulteriore minaccia che pende sulla loro testa: il rischio che un'analista esperto lasci l'organizzazione, generando una **fatale perdita di competenza** e quindi un arretramento nella capacità del SOC di fare fronte alle proprie sfide.

In questo scenario per i team che operano nei SOC **diventa sempre più difficile agire in modo efficace** e proteggere la propria organizzazione da minacce sempre più avanzate e in grado di superare l'ingente apparato di sicurezza costituito dai numerosi tool implementati negli anni.

Il **tempo necessario per l'identificazione e la risoluzione delle violazioni** è in continuo aumento così come il rischio di subire danni.

E' quindi necessario dotare il SOC di nuove soluzioni in grado di **produrre consistenti benefici** per tutte le figure professionali coinvolte nella gestione del SOC, dall'analista di primo livello fino al manager. Una soluzione in grado di introdurre un **livello di automazione** tale da garantire la massima efficacia del team di sicurezza e quindi il massimo livello di protezione dalle minacce Cyber.

Ed è proprio questo lo scenario nel quale interviene **Demisto Enterprise**, la soluzione in grado di mettere in collegamento persone, processi e tecnologie di sicurezza, aumentando decisamente il livello di protezione dell'infrastruttura tecnologica.

LA SITUAZIONE ATTUALE

Tempi di intervento e risoluzione (MTTR) sempre più lunghi

- Attacchi sempre più sofisticati e sempre piu' numerosi
- Troppi incidenti da gestire in contemporanea
- Poco tempo da dedicare a ogni singolo incident
- Tanti strumenti diversi, non integrati, da dover utilizzare
- Azioni manuali e ripetitive, spesso di "basso contenuto tecnologico"
- Produzione di reportistica relativa ad ogni intervento
- Rischio di commettere errori umani e di sottovalutare serie minacce.

Criticità nel livello di expertise

- Difficoltà a mantenere il livello di reattività allo stesso livello del Cyber Crime
- Molti strumenti scarsamente integrati tra loro
- Best Practice che in caso di incident vengono "trascurate" in favore di approcci "presumibilmente" più efficaci (fattore tempo devastante)
- Mancanza di strumenti collaborativi efficaci, che consentano di condividere le attività in corso e le esperienze già vissute
- Sotto pressione il rischio di commettere errori cresce esponenzialmente

DEMISTO

Demisto Enterprise è il **tessuto connettivo** in grado di trasformare le attività del SOC aumentandone l'efficacia, generando una relazione sinergica tra persone, processi e tecnologie.

Con le sue capacità di **orchestrazione**, Demisto Enterprise valorizza tutte le tecnologie che fanno parte del sistema di sicurezza dell'organizzazione, integrandole nei processi di investigazione relativi agli incident e mettendole al servizio di chi opera all'interno del SOC.

Con le sue capacità di **automatizzare** i processi di investigazione e di intervento, Demisto Enterprise contribuisce ad aumentare l'efficacia del personale del SOC, riducendo al minimo le operazioni ripetitive e tediose, e focalizzando la loro attenzione sulle situazioni effettivamente rilevanti.

Con le sue capacità di **documentare** in modo completo la gestione degli incident e la conformità rispetto agli SLA, Demisto Enterprise permette di evidenziare, attraverso reportistica di dettaglio, tutte le attività di investigazione occorse nel trattamento degli incident, mettendo a disposizione degli auditor aziendali un efficace strumento per rispondere alle esigenze di documentazione dettate dalle più recenti normative in termini di trattamento delle informazioni (es. GDPR). Demisto Enterprise solleva inoltre il personale del SOC da attività che diventano superflue e ridondanti rispetto alla missione principale di una struttura operativa volta a proteggere l'organizzazione da minacce che diventano sempre più sofisticate.

Complete Case Management

Demisto gestisce tutti gli aspetti del ciclo di vita di un incident di sicurezza:

- Piattaforma aperta ed estensibile che **si integra nativamente con più di 100 strumenti** che operano in ambito sicurezza (data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, ...).
- Procedure (playbook) intuitive sviluppate con un approccio drag-and-drop per **automatizzare i processi** e i flussi di lavoro del SOC.
- **Documentazione automatica** di tutti gli incident e delle indagini effettuate per mantenere la tracciatura degli SLA.
- Un **repository centralizzato di tutti gli indicatori** che abilita ricerche sofisticate sugli indicatori e sulle attività di identificazione delle minacce (threat hunting).
- Funzionalità avanzate di ricerca che consentono **l'identificazione automatica degli incident duplicati** e delle relative attività di indagine.
- **Dashboard avanzate e report personalizzabili** per valutare le performance e archiviare i risultati.
- Agenti "dissolvbili" per Windows/Mac/LinuzOS, per **collezionare dati dagli endpoint** nei casi in cui questo possa essere necessario.

Intelligent Automation & Orchestration

Demisto, con le sue funzioni di automazione e 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.
- Flessibilità massima per chi vuole **creare nuove routine** da inserire all'interno delle procedure (playbook).
- **Alta disponibilità delle procedure**, con funzioni di diagnosi in caso di malfunzionamento e possibilità di attivare manualmente anche solo una parte di un'intera procedura.
- **Suggerimenti avanzati riguardo la gestione degli incident** basati sulle capacità di Machine Learnig di Demisto.

Interactive investigation

Le funzioni interattive di indagine di Demisto aiutano gli analisti a collaborare proficuamente e a diventare più efficaci:

- **War Room virtuale** nella quale gli analisti possono collaborare in tempo reale
- Funzioni avanzate che consentono di **mettere in relazione nuovi incident con incident già risolti**, riducendo drasticamente i tempi di indagine.
- **Ambiente dedicato automatizzato** (DBot) che aiuta ad eseguire comandi, suggerisce le assegnazioni agli analisti e le future azioni.
- **Assistente virtuale** che consente il mirroring delle indagini utilizzando la soluzione di collaborative processing Slack.
- Raccolta di prove e sistema di **auto-documentazione** sofisticato.

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 del SOC

- 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 produtttività degli analisti e crescita del livello di competenza del Team

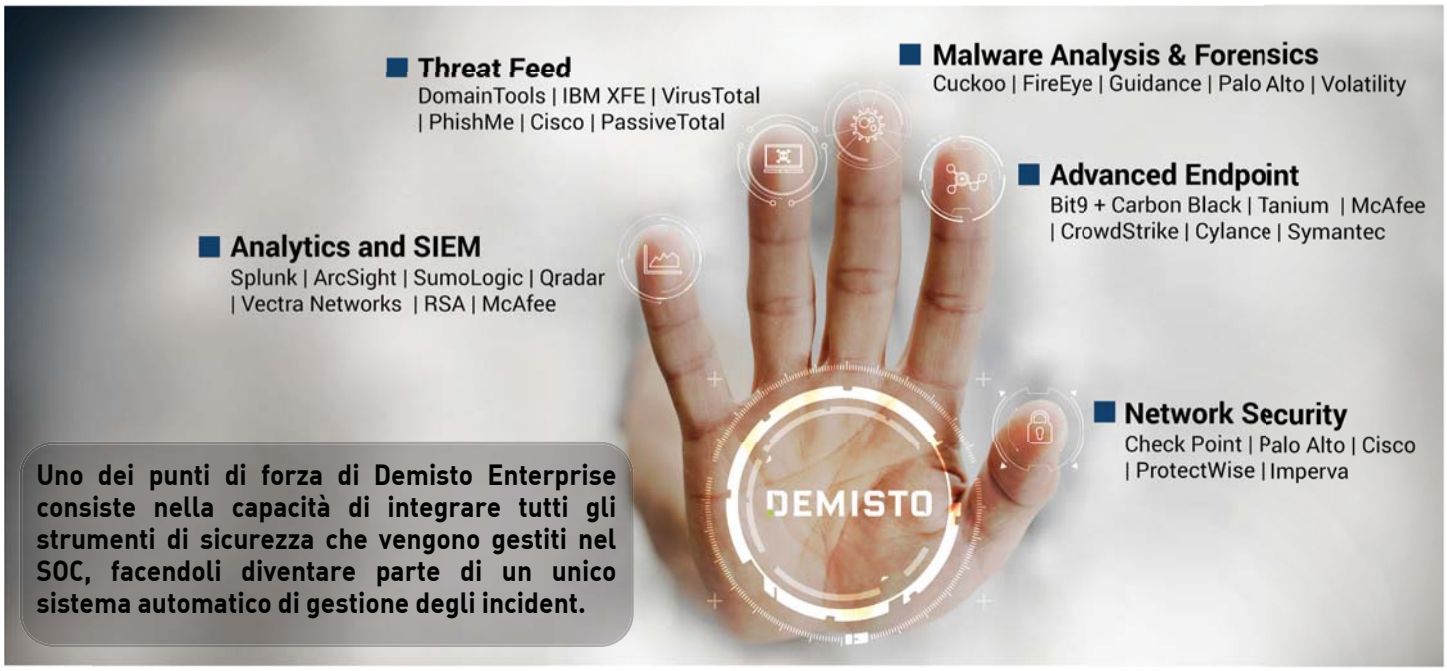
- piattaforma collaborativa che permette agli analisti di condividere informazioni importanti
- possibilità per gli analistiti di strutturare training basati su indagini di eventi accaduti
- uso di tecniche di machine learning (ML-powered) per supportare gli analisti nelle investigazioni, utilizzando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

Machine Learning Powered DBot

Oltre a contribuire alla risoluzione dei problemi correnti e pressanti del SOC, Demisto Enterprise è in grado di **valorizzare la forza del "machine learning"**, e quindi delle capacità di auto-apprendimento dei computer, attraverso una "funzione robotica", chiamata **DBot**.

Questa funzione gli consente di **aumentare nel tempo la sua capacità di automatizzare i processi di gestione degli incident**, fornendo in automatico: suggerimenti e informazioni a supporto dei ticket, processi di analisi, azioni e procedure di risposta, assegnazione di attività agli analisti appropriati, evidenza delle relazioni tra incident diversi. Grazie a questa funzione la gestione di ogni incident si trasforma in un processo di crescita per il DBot e per gli analisti che **riduce il tempo necessario per determinare, contenere e rispondere efficacemente alle minacce**.

INTEGRAZIONE



GESTIONE DEGLI INCIDENT | ORCHESTRAZIONE | AUTOMAZIONE

Automazione Playbook-Driven

Indagini interattive e collaborative

Raccolta e salvataggio delle prove

Risposta e documentazione

Demisto Enterprise

Demisto Enterprise è la **prima e unica piattaforma di Security Operation** che combina: gestione completa degli incident, orchestrazione di tutte le infrastrutture di sicurezza, indagini interattive, funzioni di Machine Learning a partire dalle attività degli analisti. Le funzioni di automazione e orchestrazione contribuiscono ad automatizzare le attività ripetitive e i principali flussi di lavoro del SOC, aumentando l'efficacia degli analisti e riducendo il tempo di risoluzione degli incident (MTTR).