Seminario 5

Nel panorama digitale odierno, la sicurezza informatica è diventata una priorità assoluta per le organizzazioni di qualsiasi dimensione. Le minacce informatiche sono sempre più sofisticate e gli attacchi possono causare danni finanziari, reputazionali e operativi significativi. Per far fronte a questa crescente complessità, i centri di sicurezza informatica si sono evoluti, passando da un approccio reattivo ad uno proattivo. Questo testo illustra l'evoluzione dal **Security Operations Center (SOC)** tradizionale al **Threat Operations Center (TOC)**, un modello più avanzato e completo.

Security Operation Center (SOC)

Un SOC tradizionale si basa su **strumenti di monitoraggio centralizzati** e su un **team di analisti dedicato**. Riceve un flusso enorme di **log ed eventi** provenienti da tutti i dispositivi aziendali: firewall, endpoint (computer, server, dispositivi mobili), sistemi di rete, e altro ancora. Questi dati vengono filtrati attraverso **sistemi automatizzati** che cercano di identificare **attività sospette** o potenzialmente dannose.

Gli analisti del SOC poi entrano in gioco, esaminando gli eventi che vengono **prioritizzati** in base al loro livello di rischio. Il loro compito è **verificare se si tratta di vere minacce** e, in caso affermativo, **intervenire rapidamente** per contenerle e mitigarne i danni. In sostanza, l'obiettivo è **identificare velocemente le minacce e agire per minimizzare l'impatto sull'azienda**.

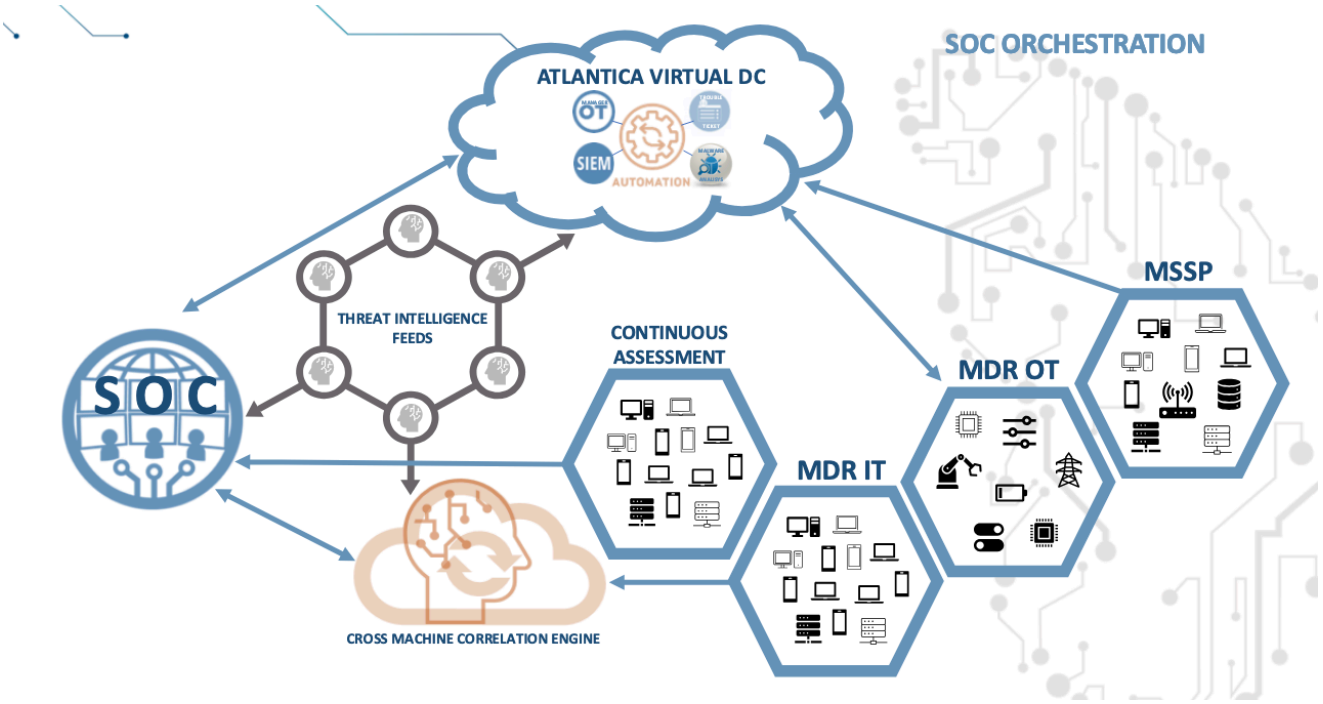
Questo viene considerato un modello di sicurezza **reattivo**.

Next Generation SOC

Per superare i limiti del modello tradizionale, è stato sviluppato il **Next Generation SOC**. Questo si distingue per l'integrazione di tecnologie avanzate, quali l'automazione, l'intelligenza artificiale (IA) e il machine learning. Tali tecnologie permettono un'analisi più intelligente e approfondita dei dati, una migliore capacità di rilevamento delle minacce, anche le più sofisticate, e una significativa riduzione dei tempi di risposta. Inoltre, il Next Generation SOC estende la sua capacità di protezione a infrastrutture complesse e diversificate, includendo ambienti cloud e dispositivi IoT, superando le capacità del SOC tradizionale, tipicamente focalizzato sull'infrastruttura on-premise.

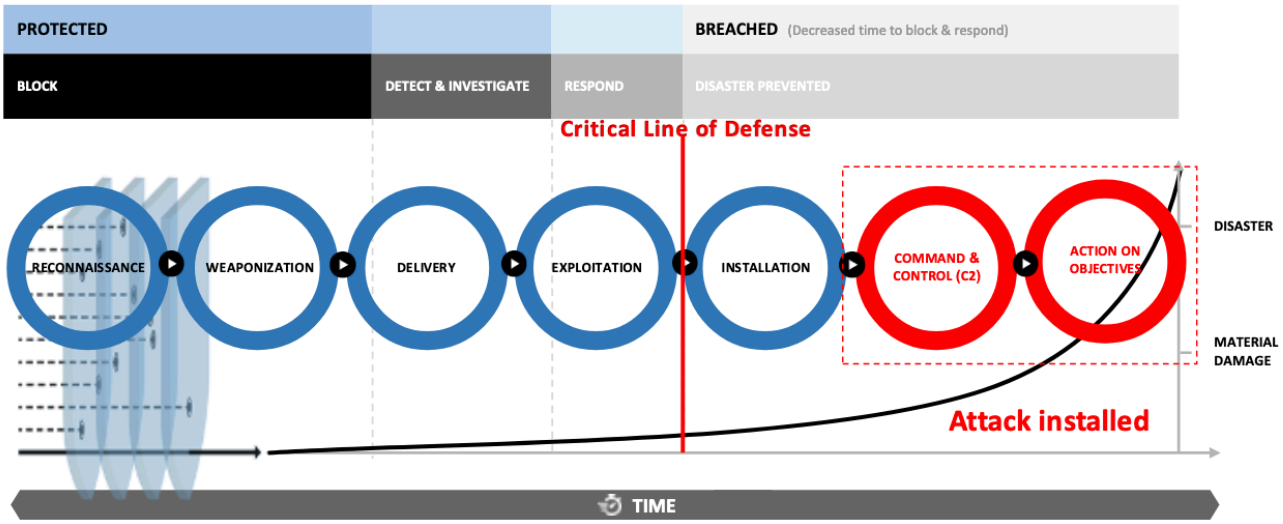
SOC Orchestration

La **SOC Orchestration** rappresenta un elemento chiave per l'efficienza operativa, in particolare in contesti di crescente complessità. Essa si configura come una piattaforma centralizzata che integra e coordina i diversi strumenti e processi di sicurezza. I benefici derivanti dall'orchestrazione includono l'automazione di attività ripetitive, il miglioramento della comunicazione tra i sistemi e una maggiore efficienza complessiva. Questo permette agli analisti di concentrare le proprie risorse sulle minacce più critiche, ottimizzando l'impiego delle competenze specialistiche.



La Intrusion Kill Chain: Un Modello per Comprendere gli Attacchi

La **Intrusion Kill Chain** fornisce un modello strutturato per comprendere le fasi di un attacco informatico. Dalla ricognizione iniziale, alla preparazione degli strumenti di attacco, fino alla consegna, allo sfruttamento delle vulnerabilità, al controllo del sistema compromesso e, infine, al raggiungimento dell'obiettivo finale dell'attaccante, questo modello descrive l'intero ciclo di vita di un attacco. La comprensione di queste fasi è fondamentale per implementare strategie di difesa efficaci, in quanto l'interruzione della catena in una qualsiasi delle sue fasi può prevenire il successo dell'attacco.



Threat Operation Center

Il **Threat Operation Center (TOC)** rappresenta l'evoluzione del SOC verso un modello proattivo di gestione della sicurezza. Il TOC non si limita alla rilevazione e alla risposta agli incidenti, ma adotta una strategia preventiva, basata sulla **threat intelligence**, sull'**analisi comportamentale avanzata** e sulla **correlazione di eventi provenienti da molteplici fonti**. Il TOC si avvale di capacità di **Managed Detection and Response (MDR)** sia per ambienti IT che OT, garantendo una risposta coordinata e tempestiva. L'obiettivo primario del TOC è la riduzione significativa del tempo medio di rilevazione (MTTD) e del tempo medio di risposta (MTTR), migliorando così la resilienza complessiva dell'organizzazione.

Il Paradigma Zero-Trust e la Sua Orchestrazione

Il modello **Zero-Trust** si fonda sul principio della verifica continua e della minima fiducia. Presuppone che nessuna entità, sia essa interna o esterna alla rete aziendale, sia intrinsecamente affidabile. Di conseguenza, ogni richiesta di accesso e ogni transazione devono essere rigorosamente autenticate, autorizzate e monitorate. **L'orchestrazione Zero-Trust** coordina gli strumenti di autenticazione, monitoraggio e verifica per applicare sistematicamente questo principio, rafforzando la sicurezza a tutti i livelli dell'infrastruttura.

Il Modello Operativo: Block, Detect, Investigate, Respond

Il modello operativo **Block, Detect, Investigate, Respond** definisce un ciclo continuo di gestione della sicurezza. Inizia con l'implementazione di controlli preventivi per **bloccare** le

minacce note, prosegue con il monitoraggio continuo per **rilevare** attività anomale, prevede un'analisi approfondita per **indagare** sulle minacce rilevate e si conclude con l'adozione di azioni mirate per **rispondere** e risolvere gli incidenti. Questo processo iterativo garantisce una protezione proattiva e reattiva.

Il Continuous Assessment: Un Processo di Miglioramento Continuo

---

Il **Continuous Assessment** è un processo strutturato per la valutazione continua della postura di sicurezza aziendale. Attraverso la simulazione di attacchi e l'analisi della resilienza del sistema, il Continuous Assessment identifica le vulnerabilità e supporta il miglioramento continuo delle difese. Le fasi principali includono l'identificazione delle vulnerabilità attraverso strumenti di scansione, la simulazione di attacchi tramite penetration testing e la valutazione dei risultati per l'implementazione di azioni correttive.

I Servizi del TOC: Un Supporto Specialistico Avanzato

Il TOC offre una gamma di servizi specialistici per supportare le organizzazioni nella gestione proattiva della sicurezza. Tra questi

- **Early Warning** fornisce informazioni tempestive su minacce emergenti
- **Security Awareness** eroga formazione per il personale
- **Threat Intelligence** offre analisi approfondite sugli attori malevoli e sulle loro campagne
- **Brand Protection** tutela l'immagine aziendale da usi fraudolenti,
- **Malware Analysis** studia il comportamento dei malware
- **Forensics** si occupa della raccolta e conservazione di prove digitali.