La conoscenza è la soluzione alle sfide attuali della Cyber Security

Author : Vincenzo Calabrò

Date : 27 Novembre 2019

Al giorno d'oggi i professionisti della cyber security devono affrontare una quantità di **sfide** senza precedenti e, allo stesso tempo, di **opportunità**. Tra queste ultime devono essere annoverate le informazioni sulle potenziali minacce e vulnerabilità che, all'interno dei sistemi di sicurezza, possono aiutare i professionisti a svolgere il proprio lavoro in maniera più efficace.

Le informazioni di sicurezza, come quelle provenienti dai *Cyber Threat Hunter*, permettono alle organizzazioni di prevenire e di ridurre al minimo i danni derivanti dalle violazioni ai loro sistemi?

Ogni giorno i team di sicurezza (SOC) ricevono un'enorme quantità di avvisi non correlati alle reali minacce a cui sono esposti. Da ciò consegue una serie di **effetti negativi**, quali: l'aumento dei costi di gestione, la perdita di produttività e la riduzione dei livelli di sicurezza.

Alcune recenti soluzioni tecnologiche riescono a fornire un valido supporto alla risoluzione di queste problematiche, perché sfruttano le potenzialità offerte dal *Machine Learning* e dal *Data Analytics.*

Come ci dimostrano le recenti statistiche sui Cyber Security Incident, questo approccio non è ancora pervenuto ai risultati attesi. L'analisi degli eventi avversi ha messo in risalto, in molti casi, una scarsa *compliance* tra gli elementi caratterizzanti l'organizzazione e le soluzioni di sicurezza adottate.

Per risolvere queste problematiche occorre adottare una **strategia operativa**, coerente con l'organizzazione, e un'**infrastruttura tecnologica** che siano in grado di dare un significato a tutti i dati e, di conseguenza, semplificarne l'analisi.

Pertanto i sistemi di *Cyber Threat Intelligence*, su cui si fondano i moderni sistemi di Cyber Security, non devono eseguire le loro analisi basandosi solo sui dati provenienti dai sistemi di apprendimento interni ed esterni - quali gli Alerts, i Behavior o i Security Feed - ma devono comprendere ed esaminare anche gli indicatori che rappresentano il contesto in cui operano.

Apprendere il contesto organizzativo

Il concetto chiave può essere sintetizzato in un solo termine: la **conoscenza** (o *knowledge*).

L’esame approfondito dei Cyber Security Incident ha evidenziato numerose organizzazioni criminali, dotate di un’elevata capacità di attacco, in grado di intraprendere una serie di azioni complesse e sofisticate per il raggiungimento dell’obiettivo, a cui corrispondete una crescente intensità degli effetti negativi.

Le minacce di Cyber Security più nefaste attaccano i target su più fronti e agiscono sfruttando tattiche complesse e strumenti eterogenei. Di conseguenza l’azione di contrasto deve, necessariamente, prevedere una capacità di *Detection* e *Response* che prenda in considerazione tutti i fattori rappresentavi dell’organizzazione stessa.

I principali componenti, che da un lato aiutano a comprendere le criticità di un’organizzazione e, dall’altro, contribuiscono ad alimentare un efficace sistema di Cyber Threat Intelligence, possono essere individuati come segue:

- **le persone**: la classificazione degli attori, la descrizione dei ruoli e delle responsabilità, la consapevolezza del Cyber Risk;
- **i processi**: la descrizione delle attività e delle procedure adottate, i comportamenti degli attori, le interazioni interne ed esterne, la *governance*;
- **la tecnologia**: le caratteristiche e la mappatura delle reti e dei sistemi informatici, degli strumenti di sicurezza e degli altri apparati intelligenti;
- **le informazioni**: il dizionario delle informazioni gestite, la distinzione tra dati sensibili, classificati e non, le informazioni per la gestione della sicurezza;
- **la valutazione dei rischi**: l’analisi dei rischi e delle vulnerabilità, l’accettazione del rischio residuo, il *risk assessment*;
- **i sistemi di controllo**: le policy di sicurezza, i permessi di accesso, i sistemi di autovalutazione e di audit, ecc.

Attuando un processo di *Data Fusion*, le predette informazioni devono essere integrate a quelle pertinenti la Cyber Security (già citate) e produrre una base informativa più coerente, accurata e utile al processo di difesa.

Adottare soluzioni basate sull’Intelligence

Le soluzioni di difesa *Intelligence Driven* aiutano i team ad affrontare efficacemente le nuove sfide. Queste tecnologie, che sfruttano il *Machine Learning* e la capacità di analisi dei Big Data, possono notevolmente favorire e velocizzare il processo di identificazione e analisi dei trend più importanti migliorando così la protezione dalle minacce reali.

Per gestire e risolvere gli attuali problemi di sicurezza le organizzazioni hanno bisogno di nuove tecnologie, come l'apprendimento automatico (ML) e l'intelligenza artificiale (AI), perché i processi di sicurezza convenzionali non possono essere ridimensionati e non sono idonei a

gestire le attuali esigenze di Cyber Security.

Il *Machine Learning* e l'Intelligenza Artificiale facilitano le attività di:

- analisi di tutte le informazioni che arrivano,
- identificazione dei posti giusti in cui cercare le anomalie,
- risposta di cui le organizzazione hanno bisogno per trovare le minacce in pochi minuti o giorni (e non settimane o mesi).

Le capacità computazionali e analitiche di un framework di *Cyber Threat Intelligence* permettono di identificare segnali come gli utenti più rischiosi all'interno di un'organizzazione e le potenziali minacce che questi rappresentano.

Ad esempio, sono in grado di rilevare un attacco completo ad un'organizzazione attraverso la disamina di una combinazione di dati provenienti dall'*Active Directory*, dal Repository degli IP Log, dai Proxy Web e dai dati dai DLP, e, di conseguenza, i team possono rapidamente visualizzare e comprendere lo stato degli utenti, dei repository, degli endpoint e del traffico di rete.

Tutto ciò consente di ottimizzare tempo, risorse e budget spesi per la fase di *detection*; riduce il tempo dedicato alla raccolta dei dati e concede più tempo alla comprensione di un attacco. Il team può valutare, in tempo reale, l'indice di rischio di un'entità come un utente, un file, un dispositivo client, un server, un indirizzo IP o un altro componente IT.

Se tutte queste informazioni potessero essere rappresentate in una *dashboard* intuitiva e interattiva, gli operatori sarebbero messi nelle condizioni di analizzare direttamente i dettagli delle caratteristiche, dei patterns di utilizzo e dei comportamenti di un'entità considerata a rischio più elevato rispetto ad altri. Il sistema d'*Intelligence* offre, inoltre, la possibilità di **apprendere in modo dinamico** i modelli di comportamento e di contesto per ciascuna entità e il modo in cui tali entità interagiscono tra loro. Il *Machine Learning Analytics* è in grado di distinguere facilmente le attività normali da quelle anomale. Ciò comporta una valutazione del rischio di altissima qualità e riduce i falsi positivi caratteristici di altri modelli di valutazione del rischio.

È importante sottolineare che un livello di sicurezza ottimale non dipende solo dalla distribuzione degli strumenti e dalla loro operatività. Gli operatori alla sicurezza devono lavorare a stretto contatto gli altri colleghi, per comprendere i dati e il contesto di riferimento.

Occorre, inoltre, tenere presente che ciò che rende una soluzione così efficace sono i **dati**. Più dati sono disponibili e meglio funziona la logica. Migliore è il funzionamento della logica e più velocemente i team possono rilevare una minaccia reale. E, infine, più velocemente sono in grado di rilevare una minaccia, più velocemente possono rispondere. Pertanto, se si utilizzassero le tecnologie basate sul *Machine Learning*, l'aggiunta di dati da più fonti eterogenee favorirebbe la rilevazione delle minacce.

Conclusioni

I vettori di attacco stanno diventando sempre più celati e variegati, permettendo agli utenti malevoli - come gli hacker o i criminali informatici - di non essere rilevati tramite gli strumenti tradizionali. Per comprendere realmente l'impatto di una minaccia, i team devono adottare un **approccio olistico** che sia in grado di valutare le informazioni da diversi punti di vista.

Gli strumenti di difesa basati su *Machine Learning* e Data Analytics consentono di accedere direttamente a un elenco di segnali di compromissione di ottima qualità, in modo da poter identificare rapidamente le minacce. Poiché nessun addetto alla sicurezza è in grado di superare la velocità computazionale con cui un sistema informatico può elaborare e correlare grandi quantità di dati provenienti da più fonti, questa soluzione offre una capacità di analisi con un livello di efficienza e produttività senza precedenti.

Articolo a cura di **Vincenzo Calabrò**