FORTINET

Utilizza un Security Analystvirtuale basato sull'intelligenza artificiale per modernizzare il SOC

L'intelligenza artificiale (IA) ha la capacità di identificare i modelli in enormi quantità di dati, con la possibilità di rilevare le tendenze e di effettuare classificazioni delle minacce molto più rapidamente rispetto agli esseri umani. Un analista SOC (Security Operations Center) basato sull'intelligenza artificiale che utilizza tecnologie di apprendimento approfondito, ad esempio le reti neurali approfondite, può contribuire a superare il crescente deficit di competenze e a rilevare e rispondere più rapidamente agli incidenti di sicurezza.

Il **74%** dei professionisti della sicurezza afferma che la carenza di competenze in materia di sicurezza informatica ha avuto un impatto sulla loro organizzazione.[1]

Un analista SOC virtuale basato su una rete neurale approfondita contribuisce ad attenuare gli effetti di questa carenza di competenze aiutando a svolgere compiti di basso livello e assistendo gli analisti umani, consentendo loro di operare a un livello superiore.

Un sistema di intelligenza artificiale deve avere determinate caratteristiche per essere considerato valido.

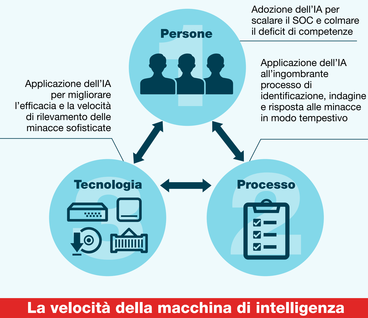
Un Security Analyst zza virtuale basato sull'intelligenza artificiale deve imparare da se stesso

Quando si parla di **algoritmi di machine learning** di uso comune, un securiy analystvirtuale basato su apprendimento approfondito che può operare in modalità non presidiata senza una formazione iniziale in loco è un validissimo aiuto per i team SOC, che si affidano alla sua capacità di adattarsi all'evoluzione del panorama delle minacce informatiche.

Machine learning		Apprendimento approfondito
Presidiato	Modello di addestra-mento	Non presidiato
Dominio controllato dal fornitore	Ospitato su IA	Ovunque, compreso il cliente on-premise
Richiede aggiornamenti basati su cloud	Maturità IA (addestra-mento con-tinuo)	Autoapprendimen-to. Consumo opzio-nale di apprendi-mento globale
Settimane	Addestra-mento on-premise	Preaddestrato per il funzionamento fin dal primo giorno

L'intelligenza artificiale deve collaborare in modo olistico con le persone, i processi e la tecnologia di un'organizzazione

Tale collaborazione migliora la scalabilità dei team, automatizza le attività non qualificate e tiene il passo con la protezione contro le minacce sofisticate.



La velocità della macchina di intelligenza artificiale deve accelerare il rilevamento delle minacce, le indagini e la risposta

Il SOC medio riceve **10.000 avvisi al giorno**, ma ha la manodopera e le risorse per gestirne solo una parte.[2] Due terzi degli analisti della sicurezza indagano su meno di 30 avvisi al giorno,[3] e la metà di questi sono probabilmente falsi positivi.[4]

Un security analyst virtuale basato sull'IA può accelerare il processo di rilevamento e classificazione accurati dei potenziali attacchi, eseguire le fasi investigative necessarie per identificare la fonte della minaccia, i dispositivi interessati e applicare una soluzione adeguata.

In questo modo, si riduce notevolmente il carico sul personale di sicurezza e il costo degli incidenti di sicurezza.

Esempio di ciclo di vita della risposta alle minacce

Prima: l'approccio tradizionale alla risoluzione di WannaCry solo con analisti SecOps

Identificazione (+1 ora)
- Supponiamo 100 su 1.000 avvisi di minacce su un dashboard SOC: la minaccia selezionata può essere ransomware oppure
- L'avviso è stato inviato da un utente interessato

Investigazione (+4 ore)
- Accesso ai prodotti di sicurezza
- Verifica dei registri/avvisi
- Uso di strumenti integrati ed esterni per convalidare il ransomware
- Esecuzione di ricerche esterne
- Accesso ai prodotti di sicurezza per cercare il spostamento laterale di WannaCry
- Creazione del piano di attenuazione

Risposta (+2 ore)
- Messa in quarantena dei dispositivi, segmento di rete
- Formazione dei dispositivi/backup di ripristino
- Applicazione delle patch
- Chiusura del ticket

Dopo: risoluzione di WannaCry con l'analista SecOps potenziato con reti neurali approfondite (IA)

Identificazione (<1 sec)
- IA: ransomware convalidato nel giro di frazioni di secondo
- IA: autoapprendimento delle caratteristiche del nuovo ransomware

Indagine (<5 min)
- IA: fornisce la catena offensiva contro WannaCry con ricerca delle minacce contestuale
- IA: identificazione del paziente zero WannaCry e spostamento laterale
- SecOps: creazione del piano di attenuazione

Risposta (<30 min)
- IA integrata con i controlli di sicurezza:
  - Messa in quarantena dei dispositivi, segmento di rete
- Follow-up SecOps:
  - Correzione dei dispositivi/backup di ripristino
  - Applicazione delle patch
- Chiusura del ticket

[1] Jon Oltsik, "The Life and Times of Cybersecurity Professionals 2019", ESG e ISSA , aprile 2019.
[2] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?", Bricata, 2 ottobre 2019.
[3] "Do SOC overwhelmed by alert overload, struggle with false positives?", Help Net Security, 29 agosto 2019.
[4] Ibid.