Radware AI SOC Xpert

Una svolta per le operazioni SOC di protezione DDoS e delle applicazioni

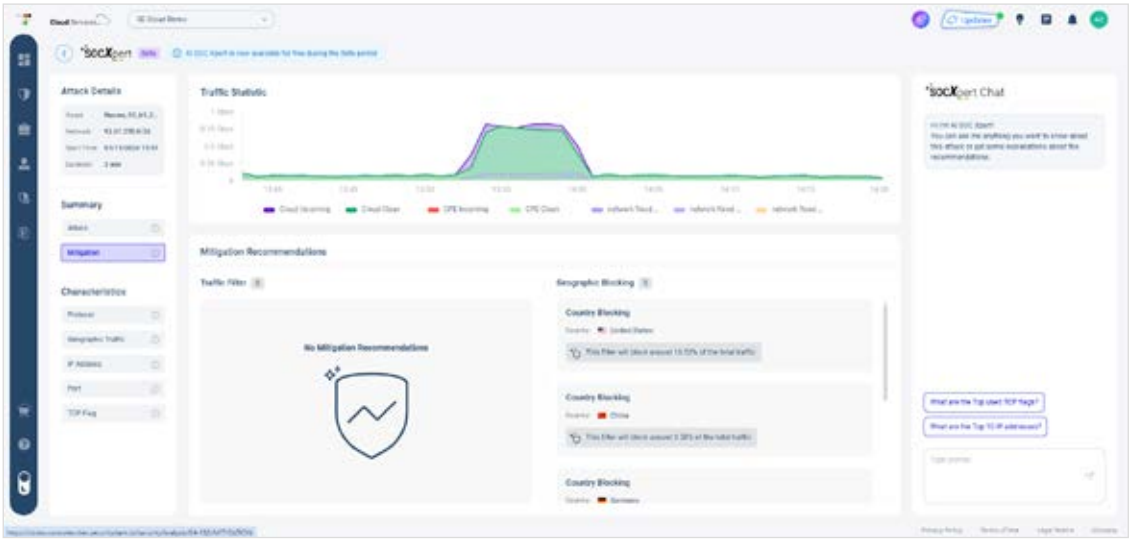
I centri operativi per la sicurezza (SOC) sono fondamentali per la difesa informatica, eppure molti si affidano ancora a sistemi SIEM standard che faticano a gestire gli incidenti di sicurezza DDoS e applicativi. L'intelligenza artificiale generativa (GenAI) ha trasformato i cyberattacchi, permettendo exploit zero-day da parte dei criminali informatici e creando un gap temporale critico per i SOC. La carenza di esperti di sicurezza informatica non fa che peggiorare la situazione per le aziende vulnerabili.
Per contrastare queste sfide, è essenziale utilizzare l'intelligenza artificiale (AI) per potenziare la previsione, il rilevamento e la risposta alle minacce. Le difese proattive basate su AI artificiale consentono una mitigazione più rapida, una riduzione del tempo medio di risoluzione (MTTR) e una maggiore efficienza nella gestione degli incidenti.

Vantaggi principali di AI SOC Xpert

- Analisi e rimedio istantanei con algoritmi AI automatizzati
- Riduzione dell ritardo nell'analisi delle cause principali da giorni a minuti
- Riduzione dei costi e dei ritardi con con tuning e onboarding guidati
- Elevazione delle competenze di tutti gli analisti SOC a livello esperto
- Accesso immediato e intuitivo ai dati forensi tramite assistente AI
- Ricevere strategie di mitigazione basate su attacchi live, tecnologia di deception e crowdsourcing

Figura 1

Il portale cloud unificato di Radware con schermate AI SOC Xpert



All'interno di AI SOC Xpert

Risoluzione automatizzata e istantanea degli incidenti

Gli attacchi rilevati vengono individuati in tempo reale, sfruttando l'analisi basata su AI per generare risoluzioni ottimizzate, adattandosi istantaneamente all'evoluzione degli attacchi. Basandosi sull'ampia esperienza di Radware nella mitigazione degli attacchi reali, le soluzioni raccomandate sono personalizzate per l'incidente specifico e possono essere implementate automaticamente con un semplice clic.

Analisi accelerata delle cause profonde con una riduzione fino a 20 volte del MTTR

AI SOC Xpert acquisisce grandi set di dati sugli eventi di sicurezza ed esegue analisi approfondite per generare automaticamente le RCA e ridurre l'MTTR da giorni a minuti.

Dati e analisi forensi facilmente accessibili tramite un assistente AI intuitivo

Fornisce accesso immediato e piena visibilità a tutte le informazioni richieste, debriefing e l'acquisizione di dati forensi attraverso un assistente intuitivo guidato dall'intelligenza artificiale. Ottieni risposte immediate alle domande, raccomandazioni rapide in tempo reale e un'indagine più approfondita (se necessario) per l'analisi degli incidenti di sicurezza.

Gli agenti SOC sono potenziati per diventare esperti di DDoS e sicurezza delle applicazioni

AI SOC Xpert consente agli esperti del SOC di affrontare efficacemente le minacce significative, siano esse applicative o DDoS, assicurando una risoluzione efficiente e senza soluzione di continuità, accessibile ai membri del SOC di tutti i livelli di esperienza.

Ottimizzazione e onboarding senza soluzione di continuità per un TCO inferiore e un time-to-value più rapido

Il miglioramento della precisione dei criteri di sicurezza attraverso le raccomandazioni per la messa a punto dei criteri elimina la necessità di impostare manualmente le regole e l'intervento umano, riducendo in modo significativo i costi operativi. Inoltre, gli strumenti basati sull'intelligenza artificiale accelerano il processo di onboarding e l'integrazione con le operazioni esistenti, garantendo una rapida implementazione. Questo approccio senza soluzione di continuità ottimizza il valore nel minor tempo possibile, riducendo complessivamente il tempo necessario per ottenere valore.

Strategie di mitigazione basate su dati reali sugli attacchi

Gli utenti ottengono un'ampia visibilità sulle informazioni delle minacce di cyberattacco grazie ai dati derivati da ambienti di produzione in tempo reale. Gli insight si basano sui dati aggregati degli attacchi globali mitigati quotidianamente da Radware. I dati includono informazioni provenienti da attacchi DDoS (Web e rete), WAF, API e bot, oltre che reti di inganno di Radware e crowd sourcing.

Ottimizzare l'efficienza e l'efficacia del SOC

Nell'attuale panorama delle minacce in rapida evoluzione, i team SOC sono sottoposti a un'immensa pressione per rilevare e rispondere rapidamente agli incidenti. AI SOC Xpert potenzia i team SOC, fornendo rilevamento in tempo reale e risposte adattive, riducendo significativamente il tempo e l'impegno necessari per gestire gli incidenti. Questo servizio consente ai team SOC di identificare e risolvere rapidamente i problemi, riducendo al minimo i tempi di inattività e migliorando la postura generale della sicurezza. L'assistente AI intuitivo semplifica l'accesso ai dati e il processo decisionale, permettendo ai team di concentrarsi sulle attività strategiche invece che sui processi manuali. Riducendo i costi operativi e accelerando l'onboarding, garantisce che i team SOC possano operare in modo più efficiente ed efficace, migliorando infine la loro capacità di proteggere l'organizzazione.

RWI 389 | 11.11.2024