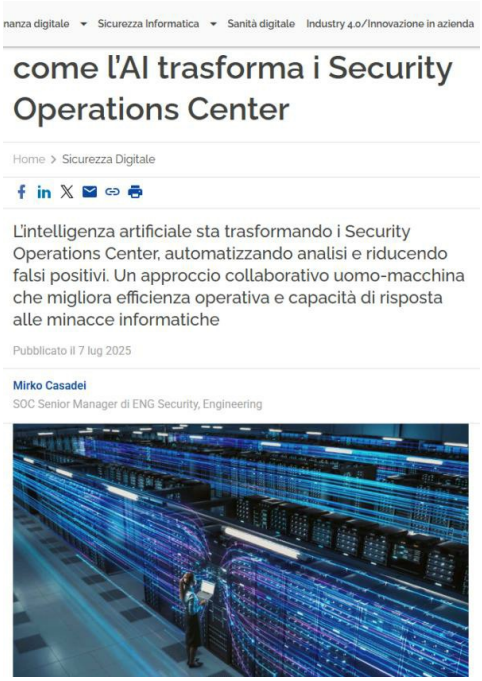
agendadigitale.eu

Gruppo Engineering
b19293b7-7f8c-4a24-92df-74317061122f

Cybersecurity potenziata: come l'AI trasforma i Security Operations Center

Mirko Casadei - SOC Senior Manager di ENG Security, Engineering



gni giorno, i Security Operations Center (SOC), veri e propri centri nevralgici della sicurezza informatica di un'organizzazione, si trovano a gestire un volume estremamente elevato di segnalazioni di sicurezza, molte delle quali si rivelano essere falsi positivi. Questo eccesso di informazioni genera un significativo rumore di fondo che ostacola l'identificazione tempestiva delle minacce reali e rallenta l'attività degli analisti. In un contesto caratterizzato da una crescente pressione normativa e da un aumento degli attacchi informatici, tale inefficienza comporta una perdita di tempo prezioso e può esporre le organizzazioni a rischi considerevoli. Indice degli argomenti AI come alleato strategico nei security operations center Implementazione tecnologica dell'AI nei Security Operations Center Scoring automatico e valutazione delle minacce con l'intelligenza artificiale Reverse engineering e analisi comportamentale con deep learning Reportistica intelligente e gestione incidenti AI-powered Rischi nell'adozione massiva ed incontrollata dell'intelligenza artificiale AI nei SOC, perché è una svolta epocale AI come alleato strategico nei security operations center In questo contesto, l'Intelligenza Artificiale (AI) si sta affermando come un alleato fondamentale: grazie alla sua capacità di analizzare grandi quantità di dati in modo rapido e preciso, può aiutare i SOC a lavorare in modo più efficiente. L'AI può diventare un prezioso alleato nella difesa informatica, quasi come un copilota che affianca gli esperti di sicurezza. È in grado di filtrare e interpretare i segnali, rispondere automaticamente agli attacchi più semplici e lasciare agli specialisti il compito di concentrarsi sulle minacce più pericolose. Non si tratta di sostituire le persone con le macchine, si tratta di un lavoro di squadra tra intelligenza artificiale e intelligenza umana che rappresenta un grande passo avanti nella protezione dei sistemi digitali. Implementazione tecnologica dell'AI nei Security Operations Center L'implementazione dell'AI nei Security Operations Center può avvenire su diversi fronti: tecnologico, di processo e umano. Tra le applicazioni più interessanti e all'avanguardia ci sono quelle che consentono di ottimizzare alcuni task di analisi all'interno del SOC, come ad esempio: Il rilevamento automatico delle informazioni personali identificabili (PII): nel contesto della protezione dei dati personali, il rilevamento automatico delle informazioni personali identificabili (PII) rappresenta una funzione cruciale per garantire la conformità alle normative sulla privacy, come il GDPR. Le PII comprendono dati come nomi, indirizzi, numeri di telefono, indirizzi e-mail, codici fiscali, numeri di carte di credito ovvero informazioni che possono identificare direttamente o indirettamente una persona fisica. Grazie all'AI, è possibile analizzare flussi di dati in tempo reale per identificare automaticamente PII all'interno dei log di sistema o dei file condivisi. Integrata in un DLP (Data Loss Prevention), l'AI permette di bloccare l'invio non autorizzato di documenti contenenti

dati sensibili via e-mail o attraverso servizi cloud. Questa capacità diventa particolarmente essenziale in settori come sanità, legale, servizi finanziari e piattaforme digitali, dove la gestione sicura dei dati personali è una priorità assoluta. Scoring automatico e valutazione delle minacce con l'intelligenza artificiale Nel contesto della sicurezza informatica moderna, la capacità di valutare in modo tempestivo e accurato la gravità delle minacce rappresenta un elemento essenziale per la protezione delle infrastrutture digitali. In tale ambito, l'AI, e in particolare gli algoritmi di machine learning, svolgono un ruolo sempre più centrale, consentendo l'automatizzazione di processi complessi e la riduzione del margine di errore umano. Uno degli strumenti più efficaci introdotti dall'AI è la possibilità di assegnare un punteggio di rischio a ciascun evento di sicurezza. Questo punteggio, noto anche come risk score, viene calcolato tenendo conto di molteplici fattori, tra cui: La frequenza con cui un determinato evento si verifica, che può indicare un attacco persistente o sistematico; La provenienza dell'evento, ad esempio un indirizzo IP noto per attività malevole o proveniente da una regione ad alto rischio; Il comportamento anomalo rispetto ai modelli di attività abituali, rilevato attraverso tecniche di analisi comportamentale. Tali valutazioni non solo permettono di classificare gli eventi in base alla loro pericolosità, ma anche di prioritizzare le risposte da parte degli analisti della sicurezza, ottimizzando l'allocazione delle risorse e riducendo i tempi di reazione. Reverse engineering e analisi comportamentale con deep learning Grazie all'impiego di tecniche avanzate di deep learning, è oggi possibile eseguire analisi comportamentali approfondite su file sospetti, con l'obiettivo di identificare pattern ricorrenti tipici dei malware e suggerire in modo proattivo contromisure efficaci. Un esempio concreto di applicazione di queste tecnologie si può osservare nell'analisi automatica di file eseguibili ricevuti tramite posta elettronica. Un motore basato su AI è in grado di esaminare il contenuto del file, rilevare la presenza di codice offuscato e confrontarlo con modelli noti di ransomware. Qualora vengano riscontrate somiglianze significative, il sistema può generare automaticamente un report tecnico dettagliato, destinato al team di risposta agli incidenti. Questo report include informazioni cruciali per comprendere la natura della minaccia, facilitando una risposta tempestiva e mirata. L'automazione resa possibile dall'AI rappresenta così un'evoluzione strategica per la difesa informatica, migliorando l'efficienza operativa e riducendo significativamente i tempi di reazione. Reportistica intelligente e gestione incidenti AI-powered Nel panorama attuale della cybersecurity, l'intelligenza artificiale si configura come uno strumento essenziale per la gestione e l'analisi dei dati provenienti da una molteplicità di fonti. Aggregando e correlando informazioni eterogenee, dai feed di threat intelligence ai log di sistema, l'AI genera report dettagliati e tempestivi offrendo una visione d'insieme chiara e immediata delle minacce in corso, facilitando il processo decisionale da parte dei responsabili della sicurezza informatica. Ad esempio, in seguito a un attacco di phishing, l'AI può raccogliere rapidamente informazioni sui domini malevoli coinvolti, confrontarli con eventi simili rilevati e, infine, produrre in pochi minuti un report completo per il CISO (Chief Information Security Officer). Questo approccio accelera i tempi di risposta e migliora

la qualità delle informazioni, rendendo più efficace la gestione degli incidenti e la pianificazione strategica. Rischi nell'adozione massiva ed incontrollata dell'intelligenza artificiale L'introduzione dell'AI nella cybersicurezza ha portato a significativi miglioramenti, ma ha anche introdotto nuovi rischi e vulnerabilità. Uno dei rischi principali riguarda la qualità e l'integrità dei dati utilizzati per addestrare i modelli di AI Questi se risultano compromessi, possono portare alla creazione modelli inefficaci o addirittura dannosi. Affidarsi totalmente ai sistemi di AI può portare a una riduzione della vigilanza umana e della capacità di risposta autonoma: gli analisti potrebbero diventare troppo dipendenti dalle decisioni automatizzate, riducendo la loro capacità di intervenire efficacemente in situazioni critiche. Inoltre, i sistemi di AI possono essere vulnerabili a guasti tecnici o attacchi informatici che potrebbero compromettere l'intera infrastruttura di sicurezza. AI nei SOC, perché è una svolta epocale In sintesi, l'introduzione dell'AI nei SOC rappresenta una svolta epocale nella gestione della sicurezza informatica. L'AI non sostituisce gli analisti umani, ma ne amplifica le capacità, automatizzando attività ripetitive e accelerando l'analisi dei dati, così da liberare risorse preziose per affrontare compiti complessi e decisioni critiche. Questo modello collaborativo uomo-macchina non solo migliora l'efficienza operativa, ma rafforza la resilienza complessiva del sistema, ponendo le basi per una difesa proattiva e intelligente contro le minacce sempre più sofisticate del mondo digitale.