Inno 3

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

Pignani e Casadei (Eng Group): SOC difesa strategica


Inno 3

Pignani e Casadei (Eng Group): SOC difesa strategica

12/09/2024 10:45

Minacce AI-driven e sfide normative richiedono alle aziende di rivedere l'approccio cybersecurity. "I SOC di nuova generazione con l'AI e le competenze sono alla base di una proposta concreta per la readiness aziendale". Pignani e Casadei, Gruppo Eng La digitalizzazione delle aziende e di tutte le organizzazioni trasforma gli scenari di cybersecurity. In un contesto dove i dati e le tecnologie digitali sono asset strategici, le minacce informatiche si evolvono in velocità e diventa difficile individuarle, riconoscerle e gestirle. L'intelligenza artificiale, in particolare, rappresenta un elemento chiave di questa trasformazione : da un lato amplifica le capacità difensive delle organizzazioni, dall'altro diventa uno strumento potente nelle mani dei criminali informatici, che la utilizzano per automatizzare e perfezionare attacchi sofisticati e su larga scala. Le aziende sono chiamate a rispondere a queste sfide con strategie innovative e strumenti tecnologici avanzati, integrando allo stesso tempo un approccio collaborativo e tenendo alta l'attenzione sul fattore umano. In questo scenario, il Security Operations Center (SOC) assume un ruolo centrale, non solo come sistema di monitoraggio e risposta, ma anche come fulcro strategico per garantire resilienza e sostenibilità. Tuttavia, adattare il SOC alle specificità di ogni azienda e alle diverse pressioni normative richiede un mix di competenze tecniche, organizzative e strategiche importanti. Sono i temi del confronto con Roberto Pignani, Cybersecurity Executive Director e Mirko Casadei, Cyber Defence Lead, di Cybertech, l'azienda dedicata alla cybersecurity del Gruppo Engineering, che parte proprio dall'analisi dell'evoluzione delle minacce. Davvero l'intelligenza artificiale, in questo contesto, se da un lato rappresenta un'opportunità, dall'altro è un'arma potentissima anche per i criminali informatici. Pignani: "I cyber attaccanti sfruttano l'AI per automatizzare attacchi su larga scala con precisione e adattabilità senza precedenti. Ad esempio, i malware intelligenti sono capaci di auto-apprendere e adattarsi alle difese implementate dalle vittime,

Minacce AI-driven e sfide normative richiedono alle aziende di rivedere l'approccio cybersecurity. "I SOC di nuova generazione con l'AI e le competenze sono alla base di una proposta concreta per la readiness aziendale". Pignani e Casadei, Gruppo Eng La digitalizzazione delle aziende e di tutte le organizzazioni trasforma gli scenari di cybersecurity. In un contesto dove i dati e le tecnologie digitali sono asset strategici, le minacce informatiche si evolvono in velocità e diventa difficile individuarle, riconoscerle e gestirle. L'intelligenza artificiale, in particolare, rappresenta un elemento chiave di questa trasformazione : da un lato amplifica le capacità difensive delle organizzazioni, dall'altro diventa uno strumento potente nelle mani dei criminali informatici, che la utilizzano per automatizzare e perfezionare attacchi sofisticati e su larga scala. Le aziende sono chiamate a rispondere a queste sfide con strategie innovative e strumenti tecnologici avanzati, integrando allo stesso tempo un approccio collaborativo e tenendo alta l'attenzione sul fattore umano. In questo scenario, il Security Operations Center (SOC) assume un ruolo centrale, non solo come sistema di monitoraggio e risposta, ma anche come fulcro strategico per garantire resilienza e sostenibilità. Tuttavia, adattare il SOC alle specificità di ogni azienda e alle diverse pressioni normative richiede un mix di competenze tecniche, organizzative e strategiche importanti. Sono i temi del confronto con Roberto Pignani, Cybersecurity Executive Director e Mirko Casadei, Cyber Defence Lead, di Cybertech, l'azienda dedicata alla cybersecurity del Gruppo Engineering, che parte proprio dall'analisi dell'evoluzione delle minacce. Davvero l'intelligenza artificiale, in questo contesto, se da un lato rappresenta un'opportunità, dall'altro è un'arma potentissima anche per i criminali informatici. Pignani: "I cyber attaccanti sfruttano l'AI per automatizzare attacchi su larga scala con precisione e adattabilità senza precedenti. Ad esempio, i malware intelligenti sono capaci di auto-apprendere e adattarsi alle difese implementate dalle vittime, rendendoli strumenti sempre più difficili da contrastare". Allo stesso tempo, "le tecniche di spear phishing stanno evolvendo grazie alla capacità dell'AI di generare contenuti altamente convincenti e realistici, raccogliendo informazioni su larga scala per personalizzare gli attacchi". L'intelligenza artificiale viene inoltre utilizzata per effettuare scansioni automatizzate, identificando vulnerabilità infrastrutturali in tempi brevissimi. Infine, non mancano le manipolazioni attraverso dispositivi IoT e l'uso dei deepfake, tecnologie che confondono sia gli utenti sia i sistemi di sicurezza, aggravando ulteriormente il quadro delle minacce. "Ci troviamo di fronte a un panorama che richiede quindi contromisure tempestive e che facciano leva a loro volta sulle migliori tecnologie", vuole precisare Pignani. E sì nonostante la crescente sofisticazione degli attacchi, l'AI rappresenta certo un valido alleato per la difesa. Queste tecnologie possono e

devono essere quindi utilizzate dai professionisti della sicurezza "come veri e propri co-piloti digitali, ampliando le capacità operative dei team di sicurezza e migliorando la gestione degli incidenti". Grazie ai sistemi basati su machine learning, è possibile analizzare grandi volumi di dati in tempo reale, identificando comportamenti anomali e distinguendoli dal semplice "rumore di fondo". E l'analisi predittiva consente di prevedere potenziali attacchi, permettendo alle organizzazioni di prepararsi proattivamente. Inoltre, l'AI supporta operazioni complesse come il red teaming, simulando attacchi per testare le difese, e i bisogni di analisi forensi, che ricostruisce eventi e sequenze critiche per comprendere l'origine degli incidenti, oltre che per offrire la documentazione necessaria ai team, anche in relazione alle normative attuali. Ecco perché, spiega Pignani "tutti questi strumenti, integrati nei Security Operations Center, giocano un ruolo fondamentale nel garantire la resilienza delle aziende". L'approccio strategico si basa su due pilastri : "l'adozione di strumenti tecnologici evoluti e la formazione delle persone". Sul fronte tecnologico, "il Gruppo punta su una maggiore visibilità e sul monitoraggio degli asset digitali". Questo obiettivo viene perseguito attraverso "analisi basate su motori avanzati di intelligenza artificiale, capaci di garantire precisione nelle allerte e un'efficace identificazione dei comportamenti anomali". La formazione gioca un ruolo altrettanto cruciale: il capitale umano è costantemente aggiornato per affrontare i cambiamenti tecnologici e gli sviluppi del business digitale e "investire sul capitale umano è essenziale per creare una cultura della sicurezza sia nelle aziende private sia nel mondo della pubblica amministrazione". Le aziende devono poi tenere presente che la cybersecurity oggi rappresenta anche un tema strettamente correlato al business sia in relazione agli sforzi necessari da mettere in campo per la compliance alle normative, sia perché la compliance stessa può rappresentare un elemento di valorizzazione della brand identity. Non solo, la sicurezza stessa "può essere uno stream di business per le aziende, per esempio attraverso la creazione di marketplace e servizi per nuovi modelli di revenues, un altro tema che a livello nazionale, in questo momento, è particolarmente sentito in termini di possibilità di crescita soprattutto per le Pmi". Dal punto di vista tecnologico si tratta di " guadagnare una maggiore visibilità e monitoraggio sugli asset di sicurezza, sugli asset digitali e sugli eventi di sicurezza, anche attraverso un'analisi basata su motori chiaramente evoluti che permettono di avere maggiore precisione nelle allerte e nell'analisi di natura comportamentale". Pignani descrive quindi il SOC come "un centro di raccolta, correlazione e analisi di eventi, dove la tecnologia è essenziale, ma la differenza la fanno gli analisti". Il SOC permette di discriminare tra comportamenti leciti e minacce reali, stabilendo priorità di intervento chiare ed efficaci. "Il supporto decisionale offerto dall' automazione consente quindi agli analisti di concentrarsi su ciò che conta davvero (1), mentre l'integrazione con tecnologie avanzate (2) permette di gestire tempestivamente gli incidenti e di garantire la continuità operativa". Temi entrambi caldi: il primo considerata la carenza di competenze, che Gruppo Eng indirizza oggi con migliaia di ore di formazione per le certificazioni necessarie ad utilizzare con profitto le tecnologie più evolute e di scouting

sul campo alla ricerca di talenti. Il secondo proprio per l'evoluzione negli anni del modello tradizionale di Security Operations Center che oggi deve rispondere alle crescenti esigenze delle organizzazioni e ai cambiamenti del panorama delle minacce. Interviene sul punto Mirko Casadei : " E' tramontato il modello di SOC caratterizzato da un approccio esclusivamente reattivo, basato su un'architettura centralizzata, dove la principale preoccupazione degli analisti era rispondere agli eventi di sicurezza con misure di remediation, utilizzando strumenti basilari come antivirus, sistemi Ips e monitoraggio perimetrale". Un'impostazione questa che, pur efficace in passato, presenterebbe oggi limiti insormontabili con gli analisti a gestire manualmente gli eventi, senza poter contare su strumenti di automazione, il relativo sovraccarico di lavoro e un conseguente ritardo nella risposta alle minacce, ma "soprattutto con un numero limitato di tecnologie disponibili che riduce la capacità di individuare e prevenire attacchi sofisticati". Il passaggio da un approccio puramente reattivo a uno proattivo oggi è invece indispensabile per il cambio di passo. Evidenzia Casadei : "Oggi il SOC moderno si basa su tecnologie avanzate che permettono di anticipare le minacce e di affrontarle in modo tempestivo". E grazie all'utilizzo di strumenti di anomaly detection, basati su tecniche di machine learning, è possibile riconoscere un attacco nelle sue fasi iniziali, riducendo al minimo il margine di errore. Casadei : "L'introduzione di strumenti di intelligenza artificiale generativa rappresenta un supporto fondamentale per gli analisti, in particolare per i professionisti meno esperti. L'intelligenza artificiale aiuta quindi le figure junior a identificare le minacce con maggiore rapidità e precisione, consentendo loro di concentrarsi sugli aspetti più critici della gestione degli incidenti". Un approccio che permette di compensare la crescente domanda di competenze specializzate in un contesto in cui la superficie di attacco è in costante aumento. "L'integrazione tecnologica nel SOC moderno poi non si limita all'utilizzo di strumenti avanzati, ma include anche l'orchestrazione e l'automazione dei processi". Questo garantisce una gestione più efficace degli eventi e una comunicazione tempestiva con i clienti, sempre più preoccupati di ricevere risposte rapide e precise. Ulteriore focus di attenzione è il tema centrale della gestione e della protezione delle identità digitali. Casadei spiega su questo punto che "il monitoraggio non si concentra più esclusivamente sugli indicatori puntuali, ma include anche l'analisi dell'identità digitale. Uno shift guidato dalle pressioni normative, come il GDPR, che impongono controlli rigorosi per proteggere i dati sensibili e garantire la conformità". E prosegue: "Il nostro approccio, quindi, non è solo rispondere a un evento, ma capire effettivamente l'impatto (e il possibile impatto) dell'incidente, considerando il tipo di dati compromessi e il loro utilizzo". Questo approccio proattivo permette di documentare accuratamente gli eventi, offrendo un quadro chiaro ai clienti e alle autorità competenti. La gestione avanzata della threat intelligence (1) e il vulnerability management (2) è evidente rappresentino pilastri fondamentali per un SOC moderno ed efficiente. Come spiega Casadei, "il nostro approccio prevede l'utilizzo della prima in tutti i processi di gestione degli incidenti, arricchendo le informazioni puntuali con fonti molteplici e integrate". E l'aumento esponenziale delle fonti di informazione "ha reso necessario adottare nuove strategie e

strumenti anche per garantire un monitoraggio efficace e proattivo nella gestione delle vulnerabilità ". Entriamo nei dettagli. La Threat Intelligence è passata dall'essere un semplice strumento di "comprensione" a un elemento centrale nella gestione degli incidenti. Secondo Casadei, "il SOC moderno non si limita a utilizzare una o due fonti di Threat Intelligence, ma può arrivare a gestire fino a 15 fonti diverse per un singolo evento. Questa proliferazione di informazioni, pur rappresentando una risorsa preziosa, pone una sfida significativa: distinguere tra dati accurati e fake news". L'AI si rivela quindi fondamentale per discriminare tra le informazioni affidabili e quelle generate in modo illecito, come i deepfake. L'intelligenza artificiale può quindi supportare gli analisti nel filtrare e correlare i dati, evitando di basare l'analisi su fonti inaffidabili. Tuttavia, Casadei sottolinea l'importanza di mantenere il coinvolgimento umano e chiarisce come nonostante l'uso dell'AI sia "fondamentale che il cervello dell'analista rimanga al centro dei processi per garantire decisioni consapevoli". Parallelamente alla Threat Intelligence, il Vulnerability Management si è evoluto per rispondere alle esigenze di un ambiente digitale sempre più complesso. " Il nostro approccio non si limita a identificare le vulnerabilità, ma aiuta le aziende a prioritizzarle in base alle loro necessità di business", spiega Casadei. Con la superficie di attacco in costante espansione, diventa essenziale concentrare gli sforzi sulle vulnerabilità più critiche, garantendo che le risorse vengano allocate in modo efficiente. Ogni giorno emergono nuove vulnerabilità, ed è impossibile per le aziende affrontarle tutte contemporaneamente. Per questo motivo, i servizi di Vulnerability Management del Gruppo Engineering si basano su un modello di prioritizzazione che "considera sia l'impatto delle vulnerabilità sul business sia la loro urgenza in termini di rischio operativo. Questo approccio consente alle organizzazioni di mantenere la continuità operativa senza compromettere la sicurezza". Per garantire un monitoraggio proattivo e l'invio tempestivo di avvisi sulle minacce emergenti, il SOC moderno di Gruppo Eng con Cybertech integra quindi una vasta gamma di strumenti e tecnologie avanzate. Certo i motori di intelligenza artificiale giocano anche in questo caso un ruolo cruciale nell'automatizzare i processi di rilevamento e analisi. E Casadei vuole sottolineare ancora l'importanza dell'automazione, quando afferma che "la gestione orchestrata degli eventi consente di operare in modo preciso e puntuale, riducendo i tempi di risposta e migliorando l'efficacia complessiva del SOC". Un approccio proattivo che non solo migliora la capacità di risposta agli incidenti, ma consente anche di anticipare le minacce, identificando schemi e comportamenti anomali prima che possano trasformarsi in attacchi veri e propri. Casadei : "La chiave per riuscire a fare bene risiede comunque nella capacità di integrare questi strumenti in una strategia unificata, che tenga conto sia delle necessità operative sia delle specificità di ogni organizzazione". Significa progettare il SOC non solo per le grandi aziende, ma anche su misura di piccole e medie imprese che spesso rappresentano l'anello debole della catena di sicurezza. Le Pmi, infatti, possono diventare vettori di attacchi contro aziende più grandi attraverso la supply chain, rendendo necessario un monitoraggio più stringente anche del loro profilo di rischio. Ecco che un esempio pratico di questa personalizzazione è l'analisi del footprint

digitale delle aziende e dei loro fornitori, utilizzata per identificare potenziali vulnerabilità senza violare normative o confini etici. Pignani : "Suggeriamo quindi alle aziende di integrare un sistema di rating che valuti anche i fornitori dal punto di vista della cybersecurity, premiando quelli che adottano comportamenti virtuosi e implementano processi robusti per mitigare i rischi". Anche perché le normative richiedono di ampliare lo spettro di controllo e di promuovere la cultura della sicurezza anche lungo la supply chain: "Elementi che favoriscono una maggiore trasparenza e una migliore gestione del rischio, contribuendo a rafforzare l'intero ecosistema digitale". Tuttavia, come sottolinea Pignani, la chiave per un SOC efficace non è solo la conformità normativa, ma anche la capacità di collaborare: " La sicurezza è proprio un tema di ecosistema. È fondamentale che le aziende, le istituzioni governative e gli operatori privati cooperino attivamente, condividendo informazioni in modo fluido e trasparente per far fronte alle minacce comuni". Questo approccio collaborativo si traduce anche in una comunicazione più fluida e in una maggiore consapevolezza dei rischi. Prosegue Pignani : "La capacità di scalare le attività del SOC in termini dimensionali e orizzontali sarà fondamentale poi per garantire un servizio efficace e flessibile e questa visione integrata consentirà al SOC di adattarsi rapidamente ai cambiamenti del contesto aziendale, mantenendo un equilibrio tra innovazione tecnologica e sostenibilità operativa". Uno degli aspetti più importanti per il futuro del SOC, secondo Pignani, è l 'integrazione del fattore umano nella strategia di sicurezza aziendale. "Il fattore umano resta tra gli elementi più critici della sicurezza", sottolinea. La formazione continua è essenziale per sviluppare competenze adeguate sia sul piano tecnico che comportamentale, al fine di ridurre l'errore umano e costruire una cultura della sicurezza all'interno delle organizzazioni. Si tratta non solo di educare i professionisti del settore, ma anche la popolazione generale, con particolare attenzione ai giovani. "È fondamentale - spiega Pignani - avviare programmi di formazione nazionale per preparare le nuove generazioni a distinguere tra ciò che è reale e ciò che è falso, prevenendo futuri problemi di cybersecurity". E Gruppo Engineering è coinvolto nel progetto Titan, un'iniziativa volta a contrastare la disinformazione utilizzando tecnologie avanzate. Sul fronte tecnologico, invece, il futuro del SOC sarà guidato da un approccio sempre più predittivo. "La resilienza digitale deve essere costruita su filosofie come il modello zero trust, che impone un controllo rigoroso di ogni accesso e transazione all'interno dell'ecosistema digitale", dettaglia Pignani. Questo approccio non solo aumenta la sicurezza, ma garantisce anche un utilizzo più sostenibile delle risorse, ottimizzando gli investimenti in cybersecurity. "Si parla molto di spese in sicurezza, ma è fondamentale che questi investimenti siano mirati e sostenibili, integrati nei processi aziendali senza diventare un collo di bottiglia per il go-to-market", aggiunge. Torna il tema della collaborazione anche tra settore pubblico e privato. Come sottolinea Pignani, "è necessario cooperare a livello nazionale e internazionale, condividendo informazioni e indicatori di compromissione per migliorare la reattività e la proattività di tutto il sistema". Questo approccio collaborativo permette di affrontare le minacce su larga scala, superando i limiti delle singole organizzazioni. Ed è condiviso appieno da Casadei che

specifica come l'utilizzo responsabile dell'intelligenza artificiale debba essere accompagnato da "una maggiore consapevolezza e responsabilità da parte di tutti gli attori coinvolti". Un aspetto più che interessante sulle prospettive future che chiude il confronto è infine il tema della sostenibilità della cybersecurity. Secondo Pignani, " è essenziale che le strategie di sicurezza siano progettate per essere sostenibili non solo dal punto di vista economico, ma anche operativo. Questo richiede un bilanciamento tra tecnologia, processi e risorse umane, integrando la sicurezza nei processi aziendali senza ostacolare la crescita. E la sostenibilità deve essere un obiettivo primario nella cybersecurity, per garantire che le aziende possano proteggersi in modo efficace senza compromettere la loro capacità di innovare e competere". Sintetizza Casadei : "l'evoluzione chiave certo è l'utilizzo responsabile dell'AI, ma non come sostituzione del personale, quanto piuttosto come strumento per potenziarne le capacità, favorendo una maggiore consapevolezza e responsabilità a tutti i livelli". Per saperne di più scarica l'infografica: Potenziare i SOC moderni con le capacità dell'AI Non perdere tutti gli approfondimenti della room Evolve Your Digital Ecosystem © RIPRODUZIONE RISERVATA Condividi l'articolo:.