Dossier

Il Messaggero

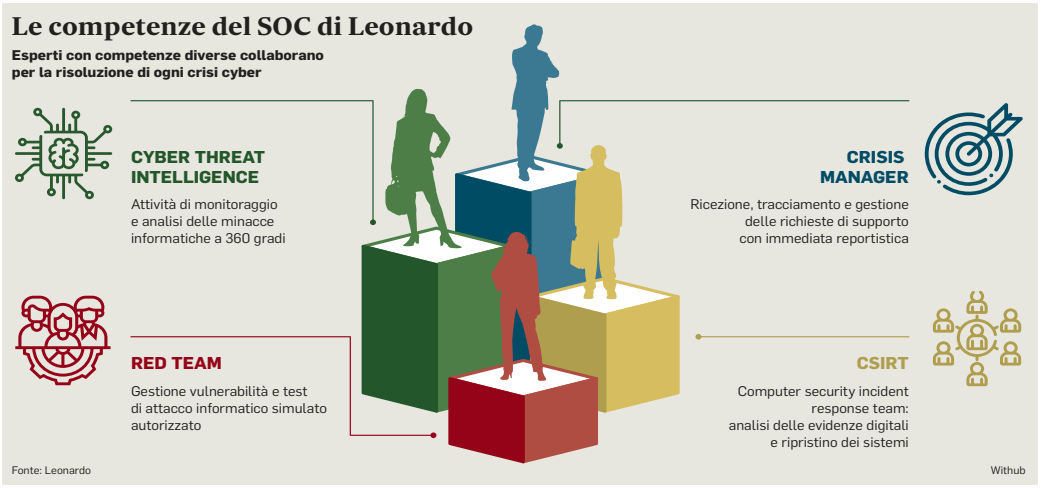
LO STRUMENTO

Digital twin, copia dell'infrastruttura reale da proteggere

Per mettere alla prova la tenuta delle infrastrutture digitali viene utilizzato un poligono virtuale. Un digital twin: la copia digitale è isolata dall'infrastruttura reale, così si può verificare ogni parte del sistema che si vuole proteggere senza causare alcuna compromissione al sistema reale.

OBIETTIVO SICUREZZA

Stephen MacLachlan è nel "Red Team" del Global Security Operation Center di Leonardo: «Fondamentale capire come pensa e agisce il criminale informatico»



Professione hacker etico Lotta ai cyber attacchi

Nella morsa degli hacker, l'Italia nei primi sei mesi del 2023 ha registrato una pericolosa impennata di cyber attacchi: secondo i dati del Clusit, l'Associazione italiana per la sicurezza informatica, il 40% in più rispetto allo stesso periodo del 2022. E quasi quattro volte di più rispetto alla media mondiale che registra una crescita dell'11%. Che cosa è in grado di provocare un cyber attacco? Per capirlo basta immaginare che un gruppo di hacker sfrutti una sola vulnerabilità in un componente software del sistema di controllo di una centrale elettrica di ultima generazione: dopo essere entrati nella rete cercano di alterarne i dati, di interrompere la distribuzione di energia e di causare danni all'infrastruttura. L'obiettivo può essere sia il sabotaggio sia il tentativo di estorcere fondi alla società energetica.

Un attacco del genere, a un servizio essenziale, sarebbe in grado di provocare una crisi sistemica, con gravi ripercussioni sulla vita quotidiana di milioni di persone. Ma non è uno scenario solo ipotetico, gli attacchi cyber sono una realtà nota: gli analisti di Leonardo hanno riscontrato nel 2022 un incremento medio del 180%, rispetto al 2021, delle tecniche offensive più diffuse come ransomware, DDoS, wipers, phishing e campagne di disinformazione. Se le minacce crescono numericamente e si fanno più sofisticate, le istituzioni e le aziende si affidano sempre più agli hacker etici.

IL PROFILO

È il caso di Stephen MacLachlan, 25 anni, che ha trasformato una grande passione per la cyber security, nata sui banchi di scuola a Montopoli di Sabina, una cinquantina di km da Roma, in una carriera di successo nel "Red Team" del Global SOC di Leonardo a Chieti, il centro di eccellenza dell'azienda nel settore, che gestisce ogni anno circa 21.600 incidenti cyber nel mondo. Con le medesime modalità di un hacker, Stephen simula attacchi su infrastrutture di rete e applicazioni per individuarne le vulnerabilità. Il suo scopo però, al contrario di un hacker "cattivo", non è sfruttare le debolezze per compromettere i sistemi ma correggerle e condividere le sue "scoperte" con chi potrebbe essere attaccato e con la comunità dei professionisti della sicurezza.

Fondamentale è saper governare e utilizzare le tecnologie più avanzate, dall'intelligenza artificiale fino a sistemi avanzati di replica digitale, il Digital Twin. «Il primo passo – spiega Stephen MacLachlan – è individuare le criticità dei sistemi informatici. Scansionando la rete è possibile rilevare fino a centinaia di vulnerabilità per ogni sistema che vi risiede». Ecco allora che vengono in aiuto intelligenza artificiale, addestrata con terabyte di dati provenienti da più fonti come web, social media, mezzi di informazione, database, deep e dark web, e supercomputer, vale a dire gli High Performance Computer. «Le infrastrutture HPC di Leonardo – continua MacLachlan – sono in grado di svolgere fino a 5 milioni di miliardi di operazioni al secondo. Algoritmi basati su AI e supercalcolo permettono di prioritizzare le vulnerabilità e proporre soluzioni in grado di risolvere più problematiche allo stesso tempo. Grazie all'utilizzo dell'AI è stato ridotto dell'85% il tempo medio di generazione dei report che permettono di conoscere il livello di rischio delle diverse infrastrutture digitali».

Stephen MacLachlan, 25 anni, al SOC di Leonardo a Chieti

«ALGORITMI BASATI SU AI E SUPERCALCOLO PERMETTONO DI PRIORITIZZARE LE VULNERABILITÀ E PROPORRE SOLUZIONI»

IL POLIGONO VIRTUALE

E poi entra in gioco il Digital Twin. «Per mettere alla prova la tenuta, in gergo si chiama cyber-resilienza, delle infrastrutture digitali delle organizzazioni che si affidano al nostro Red Team di ethical hacker – spiega Stephen MacLachlan – utilizziamo un poligono virtuale, il Cyber Range sviluppato da Leonardo. È in grado di creare una copia digitale dell'infrastruttura da testare, in tutto e per tutto identica all'originale, potendo simulare migliaia di nodi e centinaia di reti e replicare i suoi tool di difesa. Viene creato, con il supporto dell'AI, uno scenario basato sulle vulnerabilità riscontrate ed è questo gemello digitale che io vado ad attaccare, per vedere la reazione. La simulazione di difesa può essere fatta da esperti Leonardo o dall'organizzazione stessa perché la piattaforma consente questo tipo di interazione».

La copia digitale è isolata dall'infrastruttura reale: in questo modo si può verificare ogni parte del sistema che si vuole proteggere, come ad esempio quello di un impianto energetico o quello dei trasporti, senza causare alcuna compromissione al sistema reale.

LA SQUADRA

Quello dell'hacker etico non è un lavoro solitario. «Operare al SOC mi permette di condividere le mie conoscenze con i team che si occupano di intelligence sulla minaccia, di monitoraggio real time della sicurezza e di risposta agli incidenti informatici – sottolinea Stephen – È fondamentale per comprendere come un cybercriminale pensa e agisce, per affinare le mie tecniche di attacco, ma anche quelle di difesa». Gli hacker etici, infatti, entrano in gioco anche testando le risposte agli attacchi reali, per verificare l'implementazione degli interventi previsti dopo la fase di recovery. Uno step essenziale per garantire che le vulnerabilità sfruttate dai criminali non possano essere nuovamente utilizzate e, mettendo a fattor comune i dati di tutti i team, è possibile calcolare in modo dinamico i rischi legati al cyberspazio e prevenire molti attacchi.

Lorena Loiacono

I NUMERI

180%
L'aumento medio, nel 2022, delle tecniche offensive più diffuse

137
In migliaia, gli eventi di sicurezza gestiti al secondo dal SOC

5
I milioni di miliardi di operazioni al secondo eseguiti da davinci-1

8500
I report annuali del SOC sugli attacchi alle infrastrutture

Da Chieti al Medio Oriente, l'operatività no-stop del SOC

Un lavoro costante e continuamente in aggiornamento: gli attacchi si sventano anche con l'aiuto dell'intelligenza artificiale. Un'eccellenza in Italia è il SOC di Leonardo, Global Security Operation Center, con sede principale a Chieti e altri centri operativi in Italia, Europa e Medio Oriente: monitora e gestisce 24 ore su 24 e 7 giorni su 7 le vulnerabilità dei sistemi informatici delle organizzazioni e delle infrastrutture critiche in tutto il mondo. La sicurezza cyber in questo modo è garantita in ogni fase: dall'analisi della minaccia, al monitoraggio dell'infrastruttura da proteggere, dalla rilevazione degli attacchi alla risposta da mettere in campo.

Le attività si basano sulle competenze degli analisti di Leonardo, su strutture di supercalcolo dedicate all'analisi della minaccia, threat intelligence, e su data center che abilitano i servizi di monitoraggio e gestione delle IT, le infrastrutture informatiche, e delle OT, le industriali. Con la threat intelligence infatti si monitorano continuamente fonti aperte, deep e dark web, allo scopo di rilevare e analizzare le attività malevole che avvengono nel cyberspazio.

Il Global Security Operation Center di Leonardo a Chieti

IL PROCESSO

Ogni anno il SOC realizza oltre 8.500 report con informazioni su autori, motivazioni, dinamiche e caratteristiche di attacchi cibernetici che hanno colpito le infrastrutture monitorate. Le informazioni derivanti dall'intelligence sono correlate con più di 137.000 eventi di sicurezza al secondo, provenienti dai sistemi di monitoraggio, per rendere ancora più efficiente il processo di prevenzione e gestione degli incidenti. I danni di un cyber attacco posso essere imponenti: due anni fa, nel 2021, un ransomware ha bloccato il più grande oleodotto della costa Est degli Usa, causando l'interruzione del trasporto di oltre 378 milioni di litri di carburante e costringendo 17 Stati a dichiarare l'emergenza. La cifra pagata ai cybercriminali per decriptare i dati e tornare all'operatività è stata di 5 milioni di dollari. Al "riscatto", pagato da molte organizzazioni colpite da ransomware, si aggiunge il costo dei blocchi di operatività dei sistemi e quello in termini di reputazione. Il conto è da brividi: Gartner stima infatti il costo medio del downtime in caso di attacco ransomware in 5.600 dollari al minuto, circa 300mila dollari l'ora. Le conseguenze di un cyber-attack possono poi impattare la sicurezza stessa dei cittadini.

Per questo, soprattutto, la risposta deve essere immediata: nel mondo della cyber security, la rapidità di reazione può fare la differenza tra un incidente di piccola portata e una vera e propria crisi, ovvero un evento anomalo e straordinario che minaccia obiettivi strategici e funzioni vitali dell'organizzazione colpita. E così anche l'automazione, insieme all'intelligenza artificiale, può avere un ruolo molto importante, velocizzando l'individuazione e la risposta agli attacchi e consentendo di liberare risorse e persone per dedicarle a situazioni anomale e diminuire il tempo di recovery in caso di crisi.

L. Loi.