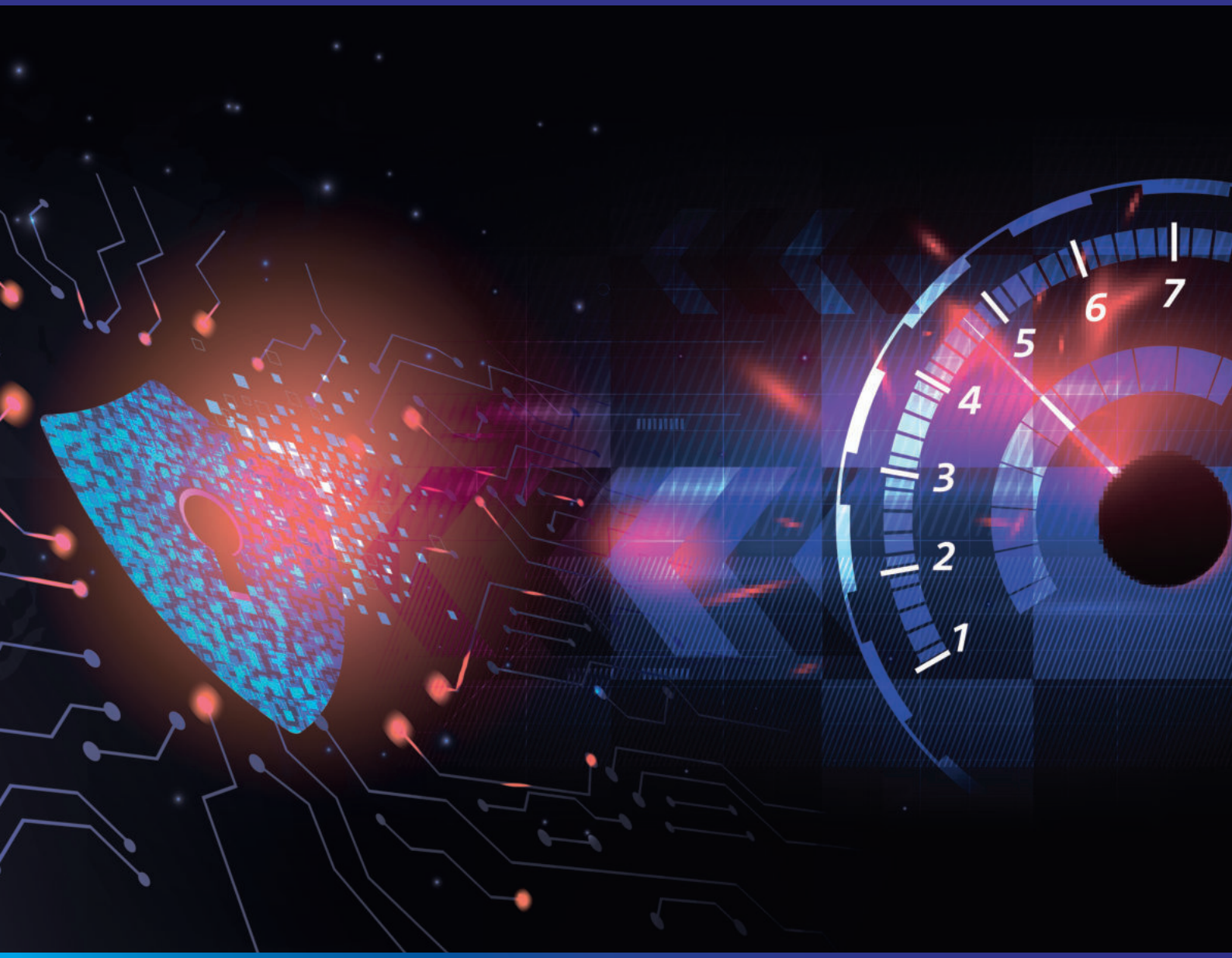
INDIGO COMMUNICATION



IL CONTRASTO AGLI ATTACCHI COMPLESSI PARTE DALLA VELOCITÀ DI REAZIONE

Lo scenario della cybersecurity è in costante evoluzione e le aziende si trovano ad affrontare minacce tanto pericolose quanto difficili da individuare. Le modalità di risposta mescolano in modo variabile competenze interne e appoggio a servizi esterni specializzati per accrescere la capacità di prevenzione e rilevazione rapida.

Non dovrebbe sfuggire più a nessuno quanto si faccia costantemente più complesso lo scenario della cybersecurity. Molti fattori contribuiscono a questa tendenza, dalla regolare scoperta di nuove vulnerabilità in apparati e applicazioni all'affermarsi dell'era della employee mobility, con l'aumento degli accessi remoti e delle applicazioni cloud-based che fanno crescere il numero di dispositivi, dati e flussi da proteggere.

Di per sé, un ideale approccio olistico alla sicurezza aziendale presenterebbe una struttura semplice, che parte dalla valutazione dei rischi, passa per la capacità di rilevare rapidamente le minacce e approda all'ottimizzazione del tempo di risposta, dopo essersi dotati dei corretti strumenti di protezione. Ma nella realtà, la maggior parte delle aziende strutturate e con una certa storia alle spalle deve fare i conti con un'infrastruttura stratificatasi nel tempo, una componente legacy più o meno ingombrante, una consapevolezza dei dipendenti e collaboratori ancora troppo debole, una superficie di esposizione sempre più articolata e i consueti problemi di limitazione dei budget. Non può pertanto essere considerato un caso che la "Cyber Risk Management Survey 2021", realizzata da The Innovation Group (Tig), veda quale principale sfida per i Ciso e security manager delle aziende la capacità di far fronte alla complessità crescente di gestione della cybersecurity, collegata al numero crescente di processi e soluzioni tecnologiche da gestire (49%). Seguono, a breve distanza, la mancanza di risorse qualificate (47%) e una miglior comunicazione al board e top management delle criticità legate a questo tema (42%). Appare naturale rilevare come la presenza di un'infrastruttura It ramificata e stratificata porti con sé il rischio di subire attacchi più insidiosi, per la loro capacità di individuare il punto debole di una catena articolata e poi muoversi in modo spesso elusivo all'interno dei sistemi informativi per raggiungere il proprio scopo. E se phishing e malware sono le tipologie di attacco più comuni rilevate dalle aziende (il primo ha colpito quasi il 90% delle aziende analizzate nella citata ricerca Tig), gli Apt (Advanced Persistent Threat) vengono giudicati fra i più pericolosi in assoluto, preceduti solo dai ransomware e in linea con i Business Email Compromise

Il panorama di riferimento delle aziende italiane

Se la complessità resta un elemento critico, la maggior parte delle tattiche di accesso iniziale all'interno del framework enterprise sono ancora relativamente tradizionali e fanno leva in gran misura sull'elemento umano. La più recente edizione del rapporto Clusit, riferita al primo semestre 2021, attribuisce genericamente al malware un peso del 43% fra le tecniche d'attacco rilevate in Italia (in crescita del 10,5% rispetto al periodo precedente). Tig evidenzia come gli incidenti informatici rilevati in tutto il 2020 abbiano colpito in larga misura gli endpoint, siano essi di proprietà delle aziende (48%) o degli utenti (23%), ma anche l'identità delle persone (45%).

Molti attacchi, dunque, si potrebbero prevenire automatizzando le attività di cybersecurity di routine, concentrando l'attenzione dei team interni sull'analisi orientata alla prevenzione di ciò che potrebbe rendere complesso un incidente. Le cifre esposte dalle ricerche sembrano indicare, anche alla luce degli effetti della pandemia, una situazione ancora di forte vantaggio per gli attaccanti. Il rapporto Clusit, per citare il dato più aggiornato, ha rilevato nella prima metà del 2021 una percentuale di azioni gravi e con effetti molto importanti pari al 74%, contro il 48% dell'anno precedente.

Quali misure sono state messe in campo per contrastare questo stato delle cose? Qual è la reale percezione dei pericoli, il livello di consapevolezza presente a ogni livello e l'insieme delle azioni adottate a protezione del patrimonio di dati e applicazioni? A queste domande ha provato a rispondere un'indagine qualitativa realizzata da Indigo Communication su un campione di realtà di dimensione medio-grande. L'iniziativa ha inteso approfondire il livello di complessità dell'infrastruttura di sicurezza presente nelle aziende, quali misure siano state adottate per contrastare minacce di tipo Apt o correlate ai malware più evoluti oggi in circolazione, in quale misura si stia lavorando su dati pertinenti e in tempo reale, se siano o meno state adottate soluzioni di threat intelligence, come sia stato affrontato il tema della carenza di skill e in quale misura si faccia leva sull'apporto di partner esterni.

La selezione di imprese perlopiù storicamente radicate nei rispettivi settori di appartenenza (finance, costruzioni, manufacturing, retail, telco e servizi) ha confermato, innanzitutto, la presenza di un'infrastruttura di cybersecurity complessa, costruita nel tempo con soluzioni destinate spesso a risolvere problematiche puntuali. Nel 2020, addirittura, si è

> *Molti attacchi si potrebbero prevenire automatizzando le attività di cybersecurity di routine, concentrando l'attenzione dei team interni sull'analisi orientata alla prevenzione di ciò che potrebbe rendere complesso un incidente*

registrata una certa amplificazione dovuta agli effetti provocati dalla pandemia e alle lacune connesse alla particolare congiuntura, con scelte effettuate in tempi brevi per adeguare Vpn e sistemi di endpoint protection, per arrivare nei casi più evoluti alla multifactor authentication e alla cyber threat intelligence. Nelle realtà esaminate, prevale la logica del best-of-breed rispetto a quella della possibile integrazione dal punto di vista del processo o della logica di trasformazione, naturalmente con le dovute eccezioni connesse all'introduzione di una governance sufficientemente strutturata o a scelte consapevolmente diversificate per non legarsi troppo a specifici vendor. Si riconosce, in linea generale, come soprattutto in passato sia stata data una risposta tecnologica anche a problemi che non l'avrebbero richiesta e come ancora pesi la persistenza di una componente legacy non semplice da eliminare o far evolvere per ragioni che spaziano dai budget alla scarsa convinzione da parte del management.

Sono relativamente rari i casi di realtà che abbiano proceduto a un'opera di consolidamento dell'insieme di soluzioni adottate, mentre nessun componente del panel si è spinto verso una logica full (o mostly) cloud.

Come già sottolineato, il mondo degli attacchi informatici è molto ampio e capace di produrre un rumore di fondo generato in larga misura da attacchi tradizionali e ben noti. Per questo, da diverso tempo sono disponibili strumenti che automatizzano l'esecuzione di una serie di azioni studiate per rilevare, investigare e rimediare alle minacce più comuni, sostituendo l'intervento umano. Le aziende analizzate dalla nostra indagine hanno declinato questo concetto nel contesto delle rispettive realtà. L'adozione abbastanza generalizzata (ancorché recente in diversi casi) di soluzioni Edr (Endpoint Detection & Response) da un lato e del Siem (Security Information and Event Management) dall'altro sono misure interpretate in questa logica. Allo stesso modo, è ormai consolidata la scelta di avvalersi di un Soc, in linea di massima in forma ibrida, con la componente di livello 1 e 2 quasi sempre affidata all'esterno. Qui non parliamo tanto di automazione in senso stretto, ma dell'esternalizzazione in forma di servizio di un'attività di prima rilevazione e scrematura che serve a eliminare a monte la necessità di verificare ogni di tipo di alert di sicurezza intercettato dai vari sistemi implementati. La naturale evoluzione, prevista in alcuni dei casi esaminati, porta al Soar (Security Orchestration, Automation and Response), di fatto un insieme di soluzioni software che consente alle aziende di raccogliere e orchestrare dati sulle minacce alla sicurezza da più fonti e rispondere a incidenti di basso livello senza intervento umano. Sostanzialmente in tutte le realtà analizzate, i team di security interni concentrano il proprio lavoro sull'analisi approfondita di ciò che i vari strumenti di primo livello lasciano filtrare, riuscendo meglio a isolare le minacce reali e coordinando le fasi di escalation in caso di vero e proprio incidente.

Strumenti e servizi per raffinare la protezione

Sono diverse le categorie di attacco che preoccupano Le figure It e quelle preposte al presidio della sicurezza informatica. Anche se phishing e malware classici vengono reputati pericolosi solo in parte limitata rispetto alla quantità di tentativi rilevati, l'impossibilità di regimentare oltre una certa soglia il comportamento umano non consente di abbassare la soglia di attenzione. I programmi di formazione e awareness sono costantemente aggiornati un po' ovunque e ci sono anche casi virtuosi di realtà nelle quali gli utenti stessi hanno segnalato mail di phishing mirate che erano sfuggite ai sistemi di intrusion detection & prevention più o meno onnipresenti. Più comune, tuttavia, appare l'individuazione di un'azione non corretta (o perlomeno distratta) da parte di qualche persona e, per quanto possibile, le varie soluzioni fin qui adottate, ormai carrozzate con strumenti di analisi comportamentale, hanno generalmente consentito di intervenire prima che la situazione degenerasse.

Il timore che, per questa via, possa penetrare in azienda soprattutto un ransomware resta molto alto ed è per questo che si preferisce dover analizzare qualche falso positivo in più pur di non attivare meccanismi che potrebbero avere effetti devastanti sull'operatività e sul business. Molti dei soggetti interpellati hanno indicato come elementi di massima preoccupazione anche gli attacchi di tipo Apt, fileless e zero-day exploit. I primi sono particolarmente temuti per la loro capacità di insinuarsi nei sistemi e restare inattivi anche per lunghi periodi di tempo senza essere rilevati, mentre gli ultimi vengono reputati pericolosi by default perché sono basati su vulnerabilità ancora ignote anche agli sviluppatori dei programmi presi di mira. A questi, in qualche caso, si aggiunge la preoccupazione per le azioni di social engineering, con casi concreti di tentativi di frode derivati dalla capacità dell'attaccante di spacciarsi per una figura apicale dell'azienda bersagliata.

Nel campione selezionato per la ricerca, sono presenti sia realtà che presiedono servizi e infrastrutture critiche sia più strettamente private e le prime, soprattutto, hanno mostrato, più delle altre, consapevolezza di poter essere bersaglio di questo genere di attacchi sofisticati. Più o meno in tutti i casi, non sono stati fin qui segnalati incidenti rilevanti. Pur senza ammissioni esplicite, la sensazione che traspare è che le difese contro le minacce più complesse non possano fare più di tanto e ci si affidi alla buona sorte per non essere colpiti.

Uno degli ambiti di sviluppo più recente per aumentare il livello di contrasto riguarda l'adozione della cyber threat intelligence. Molte delle aziende coinvolte se ne stanno servendo, in larga parte come servizio affidato a specialisti esterni, di solito estremamente verticali (e non necessariamente facenti capo ad aziende con base in Italia). Prevale la convinzione che questa opzione consenta di aumentare la visibilità complessiva sulle cyberminacce, anche grazie alla capacità di scandagliare fonti su deep e dark Web. Sull'utilità in sé del servizio non ci sono particolari dubbi e la maggior parte delle aziende mostra anche una complessiva soddisfazione sui risultati ottenuti. Non mancano però situazioni nelle quali la pertinenza delle indicazioni ricevute sia stata giudicata poco efficace, ma la fruizione come servizio garantisce la possibilità di cambiare fornitore con una certa flessibilità. Anche chi non ha ancora effettuato passi in questa direzione prevede di farlo in tempi brevi.

Servizi come la cyber threat intelligence si affiancano all'operato dei Soc, ovvero del team incaricato di garantire la sicurezza delle informazioni all'interno dell'azienda, in associazione con piattaforme come il Siem per la raccolta dei dati, la correlazione di eventi e gli eventuali interventi anche a distanza. Questa componente è quasi sempre costruita in modalità ibrida, con partner esterni, anche qui specializzati o addirittura monoservizio, che svolgono la parte di lavoro più quantitativo e offrono una copertura 24x7, in affiancamento a una struttura interna che si occupa di monitorare la situazione complessiva e lavorare sulle segnalazioni degne di nota.

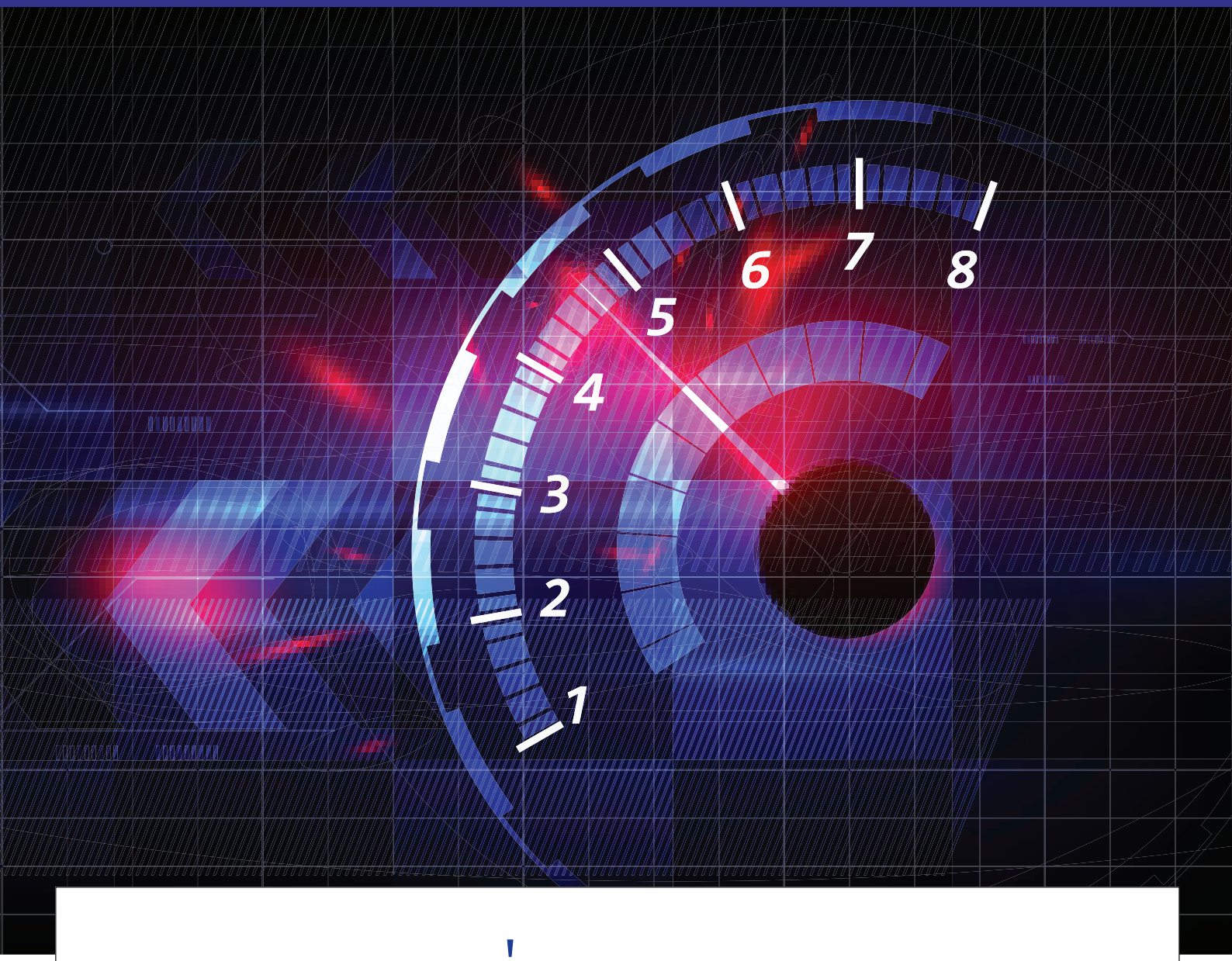
Elementi di complessità da risolvere e prospettive di medio termine

Soprattutto di fronte alle minacce più complesse, appare estremamente critico il tempo di rilevazione e risposta. Molte sono le misurazioni proposte nel tempo e ricavate da casi reali che indicano spesso in mesi la capacità di individuare determinate tipologie di attacco, soprattutto di tipo persistente. La velocità di reazione normalmente si misura nella capacità di esecuzione corretta dei processi essenziali di detection & response, includendo il threat hunting proattivo, l'analisi retrospettiva delle cause, la remediation e la mitigazione.

Il campione esaminato nella nostra indagine rivela un buon livello di preparazione su questo fronte. Alcune delle realtà coinvolte, appartenenti soprattutto al mondo finance o con infrastrutture critiche per il paese, devono rispondere a normative o requisiti che hanno spinto ad adottare misure utili e minimizzare i tempi di rilevazione e risposta, ma in generale, anche a fronte di esperienze sul campo o test effettuati, quasi tutti ritengono di saper intervenire rapidamente in caso di incidente. Ci sono realtà che sono evolute al punto di aver già istituito uno Csirt (Computer Security Incident Response Team) o perlomeno un Cert (Computer Emergency Response Team), ovvero team operativi di sicurezza, che a monte garantiscono in una particolare vigilanza su aspetti come nuovi attacchi e malware, ultime vulnerabilità rilevate e così via, per "conoscere" lo stato della minaccia e valutare le vulnerabilità della propria organizzazione. A valle, invece, essi analizzano e affrontano gli incidenti di sicurezza aiutando a risolverli.

Più che la tecnologia o l'elaborazione di piani di intervento puntuali, a pesare sull'efficacia è soprattutto la carenza di skill, che da tempo, e non solo in Italia, affligge il comparto. Quasi tutte le aziende selezionate hanno confermato la difficoltà nel reperire le competenze necessarie a puntellare la struttura dedicata alla cybersecurity. Qualcuno lavora a stretto contatto con le università per ottenere segnalazioni di profili appetibili, ma le ricerche spesso appaiono

lunghe e controverse. Pertanto, accade con regolarità crescente che si segua la via del potenziamento o della riqualificazione di risorse interne oppure che si scelga di affidarsi a partner esterni per completare l'expertise complessiva dell'azienda.
Numerosi sono i fronti di evoluzione sul breve e medio termine, poiché nel variegato scenario della cybersecurity ogni azienda ha la necessità di coprire qualche aspetto giocoforza lasciato indietro. In alcuni casi, verranno privilegiati gli aspetti di automazione, anche con l'integrazione di tecnologie di intelligenza artificiale e machine learning, mentre in altri si andrà in direzione del potenziamento delle capacità di monitoraggio. Alcune parole-chiave accomunano diverse aziende. Una di queste, già citata, è Soar come concetto dominante dei processi di orchestrazione e automazione di attività ripetitive precedentemente gestite manualmente e aumentare la postura di sicurezza. Un'altra è zero-trust, in linea con la liquefazione del perimetro aziendale che la pandemia ha definitivamente sancito e che porta all'integrazione di framework in grado di chiedere a tutti gli utenti, all'interno o all'esterno della rete dell'organizzazione, di essere autenticati, autorizzati e continuamente validati prima di concedere o mantenere l'accesso ad applicazioni e dati. Un altro tema forte, collegato al progressivo spostamento di applicazioni e carichi di lavoro verso il cloud, riguarda il concetto di Sase (Secure Access Service Edge), che prevede l'implementazione di un framework di sicurezza progettato per far convergere le tecnologie di sicurezza e connettività di rete in un'unica piattaforma per una migrazione ritenuta più rapida e protetta.



Un documento realizzato da

INDIGO COMMUNICATION

Indigo Communications nasce nel 2004 e aggrega una notevole esperienza giornalistica nel segmento hitech. Pubblica il mensile Technopolis e il portale di news e approfondimenti ICT Business, caratterizzati da target e taglio complementari. Accanto all'attività editoriale, ha sviluppato negli ultimi anni competenze e servizi nei settori del content marketing e della lead generation, arricchendo la propria offerta con importanti partnership e progetti su misura per le aziende del comparto ICT.

In collaborazione con

kaspersky

Kaspersky è un'azienda di sicurezza informatica e digital privacy che opera a livello globale fondata nel 1997. La profonda competenza di Kaspersky in materia di threat intelligence e sicurezza si trasforma costantemente in soluzioni e servizi innovativi per proteggere le aziende, le infrastrutture critiche, i governi e gli utenti di tutto il mondo. L'ampio portfolio di soluzioni di sicurezza dell'azienda include la protezione degli Endpoint leader di settore e una serie di soluzioni e servizi specializzati per combattere le minacce digitali sofisticate e in continua evoluzione. Più di 400 milioni di utenti sono protetti dalle tecnologie di Kaspersky e aiutiamo 240.000 clienti aziendali a proteggere ciò che è per loro più importante