Microsoft Security

Operazioni di sicurezza moderne

Procedure consigliate e lezioni apprese in Microsoft Cyber Defense Operations Center

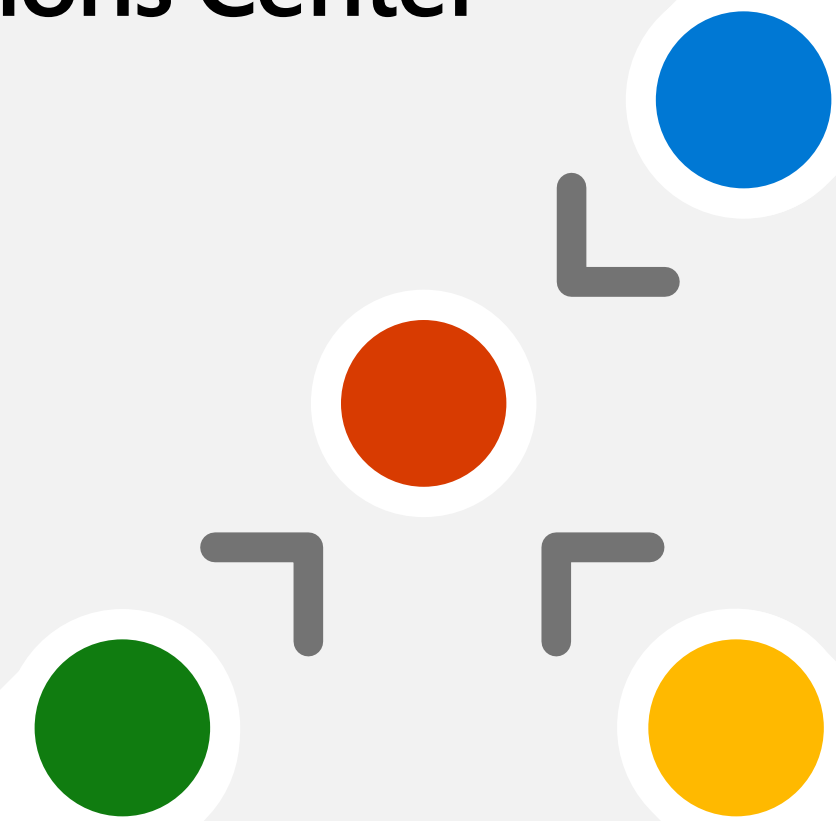


Tabella dei contenuti

1. Overview sulle operazioni di sicurezza 3

Il ruolo delle operazioni di sicurezza

Relazioni aziendali

Funzioni delle tipiche operazioni di sicurezza

2. Modernizzazione delle operazioni di sicurezza 13

Da reattiva a proattiva

Aumento della visibilità

Riduzione della superficie di attacco

Zero Trust e operazioni di sicurezza moderne

Protezione dalle minacce interne

3. Procedure consigliate per le operazioni di sicurezza 27

4. Raccomandazioni finali 38

Overview sulle operazioni di sicurezza

I professionisti della sicurezza sanno che le minacce al proprio ambiente stanno evolvendo e accelerando.

Gli attacchi informatici di oggi sono attività criminali organizzate. I criminali informatici si organizzano e condividono informazioni su ciò che funziona e sulle vulnerabilità. Lavorano per sviluppare le proprie tecniche di pari passo con l'evoluzione della tecnologia. Gli attacchi informatici sono diventati un business industrializzato, sofisticato e remunerativo.

Mentre utenti malintenzionati sviluppano tecniche di attacco moderne, è essenziale che i team di sicurezza lavorino per modernizzare continuamente le proprie operazioni di sicurezza ed essere preparati ad affrontare gli avversari. Questo implica la verifica del proprio stack di tecnologie per assicurarsi di avere protezione e visibilità su tutti i vettori di attacco. Ma implica anche la valutazione dei processi del team addetto alle operazioni di sicurezza: è in grado di proteggere l'azienda dalle minacce reali, di rilevarle e reagire in modo rapido e accurato oppure riceve troppi segnali perdendo tempo prezioso con i falsi positivi?

Abbiamo creato questa guida per aiutarti. I dettagli qui riportati ti aiuteranno a ottimizzare e a mettere a punto le iniziative di modernizzazione delle operazioni di sicurezza e di protezione dell'azienda in un panorama delle minacce in continuo mutamento, che la tua azienda abbia un centro operazioni per la sicurezza (SOC) formalmente istituito o semplicemente un team di professionisti della sicurezza addetto alla difesa dell'azienda.

Lezioni apprese dal SOC Microsoft

Le conoscenze e le procedure consigliate presentate qui derivano dalle conversazioni con i clienti Microsoft e dalla nostra esperienza nello sviluppo e nella maturazione delle procedure delle operazioni di sicurezza in Microsoft.

Anche se per qualcuno può sembrare sorprendente, il Corporate IT SOC di Microsoft protegge un ambiente multipiattaforma con un numero significativo di dispositivi Windows, Linux e Mac che eseguono software Microsoft e non Microsoft. Questo SOC usava un modello SOC tradizionale, simile a quello che vediamo nella maggior parte delle aziende, e Microsoft si è trovata ad affrontare le stesse sfide tipiche di questo modello:

- **Volume di eventi**: il volume elevato e la crescita (attualmente nell'ordine di 20 miliardi di eventi al giorno) superavano la capacità del sistema SIEM locale.
- **Analisti oberati di lavoro**: i set di regole statici generavano quantità eccessive di avvisi con falsi positivi, determinando un sovraccarico.
- **Flussi di lavoro di indagine inefficienti**: l'indagine degli eventi tramite il tradizionale sistema SIEM locale era inefficiente e richiedeva l'uso di query manuali e il passaggio manuale a strumenti diversi.

Il nostro team comprende bene cosa ti trovi ad affrontare, perché ha già sperimentato gli stessi problemi. In questa guida condivideremo le procedure consigliate e le lezioni più importanti che abbiamo appreso nel corso della modernizzazione delle operazioni di sicurezza in Microsoft per l'azienda e i clienti.

Il Corporate IT SOC di Microsoft protegge un ambiente multipiattaforma con un numero significativo di dispositivi Windows, Linux e Mac che eseguono software Microsoft e non Microsoft.

Il ruolo delle operazioni di sicurezza

Le operazioni di sicurezza mantengono e ripristinano le garanzie di sicurezza del sistema mentre è in corso l'attacco. I compiti delle operazioni di sicurezza sono descritti bene dalle funzioni del NIST Cybersecurity Framework:

- **Rilevamento**
- **Risposta**
- **Recupero**

- **Rilevamento**: le operazioni di sicurezza devono rilevare la presenza di avversari nel sistema. Questi, infatti, nella maggior parte dei casi sono incentivati a rimanere nascosti perché così facendo possono raggiungere indisturbati i propri obiettivi. Il rilevamento può avvenire reagendo a un avviso di attività sospetta o rilevando proattivamente eventi anomali nei log delle attività aziendali.

- **Risposta**: al rilevamento di una potenziale azione o campagna ostile, le operazioni di sicurezza devono indagare rapidamente per comprendere se si tratta di un attacco effettivo (vero positivo) o di un falso allarme (falso positivo) e quindi enumerare l'ambito e l'obiettivo dell'operazione.

- **Recupero**: l'obiettivo delle operazioni di sicurezza è preservare o ripristinare le garanzie di sicurezza (riservatezza, integrità, disponibilità) dei servizi aziendali durante e dopo un attacco.

Per un'azienda, le operazioni di sicurezza sono spesso un investimento essenziale per la mitigazione del rischio, poiché sono fondamentali per limitare la quantità di tempo a disposizione di utenti malintenzionati all'interno dell'azienda e il loro livello di accesso. Questo, in ultima analisi, aumenta i costi e diminuisce i vantaggi per l'utente malintenzionato, compromettendone il ritorno sull'investimento (ROI) e le motivazioni che lo spingono ad attaccare l'azienda.

Nelle operazioni di sicurezza, tutto deve essere orientato a limitare il tempo e l'accesso che utenti malintenzionati possono avere alle risorse aziendali durante un attacco, al fine di mitigare il rischio per l'azienda.

Il team delle operazioni di sicurezza si fa spesso promotore anche di un aumento della maturità nell'approccio alla sicurezza aziendale, dal momento che eventuali debolezze possono portare a incidenti che il team dovrà poi gestire.

Relazioni aziendali

Operazioni di sicurezza realmente efficaci non possono permettersi di diventare un'entità separata. Le operazioni di sicurezza devono creare e mantenere relazioni con il lato business dell'azienda. Dal momento che hanno il compito di proteggere l'azienda consentendole di espletare le sue funzioni, è importante che le operazioni di sicurezza conoscano e tengano ben presenti le strategie aziendali. Altrettanto importante è il coinvolgimento dei leader aziendali, in modo da aiutare i decision maker a comprendere le attività delle operazioni di sicurezza e cosa realmente accade durante un attacco.

In Microsoft, abbiamo imparato che le operazioni di sicurezza hanno quattro punti di integrazione funzionale principali con l'azienda:

- **Contesto aziendale (per le operazioni di sicurezza)**
- **Esercitazioni congiunte (con le operazioni di sicurezza)**
- **Aggiornamenti sui principali incidenti (dalle operazioni di sicurezza)**
- **Business intelligence (dalle operazioni di sicurezza)**

- **Contesto aziendale (per le operazioni di sicurezza)**: le operazioni di sicurezza devono essere a conoscenza degli aspetti più importanti per l'azienda, in modo che il team possa applicare tale contesto a situazioni di sicurezza in tempo reale fluide. Cosa produrrebbe l'impatto più negativo per il business? I tempi di inattività dei sistemi critici? La perdita di reputazione e fiducia dei clienti? La divulgazione di dati sensibili? La manomissione di dati o sistemi critici? Abbiamo appreso come sia fondamentale che i principali leader e il personale delle operazioni di sicurezza comprendano questo contesto, mentre si barcamenano tra un flusso continuo di informazioni, valutano incidenti e definiscono le proprie priorità in termini di tempo, attenzione e impegno.

- **Esercitazioni congiunte (con le operazioni di sicurezza)**: i leader aziendali devono periodicamente partecipare, insieme alle operazioni di sicurezza, alle esercitazioni di risposta ai principali incidenti. In questo modo si costruiscono la memoria procedurale e le relazioni fondamentali per un processo decisionale rapido ed efficace nei momenti di forte pressione legati agli incidenti reali, riducendo così il rischio per l'azienda. Questa pratica riduce anche il rischio, evidenziando lacune e supposizioni nel processo che possono essere corrette prima di un incidente reale.

- **Aggiornamenti sui principali incidenti (dalle operazioni di sicurezza)**: le operazioni di sicurezza devono fornire agli stakeholder aziendali aggiornamenti sui principali incidenti mentre questi si verificano. Ciò consente ai leader aziendali di comprendere il rischio e adottare misure proattive e reattive per gestirlo.

- **Business intelligence (dalle operazioni di sicurezza)**: a volte le operazioni di sicurezza rilevano che viene preso di mira un sistema o un set di dati che nessuno si aspetterebbe. Quando le operazioni di sicurezza rilevano gli obiettivi degli attacchi, questi devono essere condivisi con i leader aziendali, poiché questi segnali possono fornire loro informazioni importanti (ad esempio, divulgazione di un'iniziativa aziendale segreta, valore relativo di un set di dati trascurato).

Come lavorano le operazioni di sicurezza con gli altri team dell'azienda, in particolare con il lato business?

La funzione delle operazioni di sicurezza è essenzialmente quella di supportare l'azienda proteggendola. Idealmente, i team addetti alle operazioni di sicurezza dovrebbero essere consapevoli delle priorità aziendali in modo da poter identificare le risorse critiche e stabilire le priorità relative alla sicurezza in base alle priorità aziendali. Ciò consente alle operazioni di sicurezza di concentrarsi sulle risorse più critiche e di proteggerle con i sistemi di difesa, i criteri e le indagini automatiche necessari, in modo da essere allineate al team aziendale.

Quando si verifica un incidente importante, le operazioni di sicurezza devono sapere chi sono i principali stakeholder e informarli immediatamente perché spesso la risposta a un incidente non è solo responsabilità delle operazioni di sicurezza, ma dell'intera azienda:

- **Operazioni di sicurezza**
- **Operazioni**
- **Logistica**
- **Pubbliche relazioni/Comunicazioni**
- **Leadership aziendale**

Per le operazioni di sicurezza, uno dei modi migliori per costruire le necessarie relazioni con l'azienda è costituito dagli esercizi di simulazione per preparare la risposta agli incidenti. Tutti partecipano agli **esercizi di simulazione**, dai team di leadership agli stakeholder coinvolti nella risposta agli incidenti. In questo modo, le operazioni di sicurezza e gli stakeholder aziendali riescono a costruire relazioni. Le due funzioni impareranno a collaborare al meglio e, al momento di un incidente, tutti conosceranno le altre parti, sapranno come interagire e cosa fare per affrontare l'emergenza.

Funzioni delle tipiche operazioni di sicurezza

La componente più comune delle operazioni di sicurezza è l'attività di indagine e reazione agli incidenti ed è qui che la maggior parte dei team delle operazioni di sicurezza inizierà il proprio sviluppo. Le tipiche operazioni di sicurezza vedranno in azione le seguenti funzioni.

- **Indagine e reazione agli incidenti**: analisi degli avvisi provenienti dagli strumenti di sicurezza (ad esempio SIEM, XDR, EDR), indagine e correzione. Nelle aziende più grandi, è probabile che ogni aspetto della risposta agli incidenti venga gestito internamente. Ma nelle piccole aziende o in quelle con funzioni di operazioni di sicurezza meno evolute, talvolta questi compiti sono interamente esternalizzati a un service provider di sicurezza gestita (MSSP). In altri casi, verrà sviluppato un modello ibrido in base al quale la valutazione e la correzione rapida sono esternalizzate al provider MSSP, mentre l'indagine avanzata viene mantenuta internamente.

- **Intelligence tattica sulle minacce**: più frequente nelle grandi aziende, l'intelligence tattica sulle minacce si concentra su aspetti tecnici come indicatori di compromissione, indirizzi IP dannosi, nomi DNS non validi e hash di file. In alcuni casi, l'azienda farà uso di informazioni fornite da un servizio di intelligence sulle minacce per svolgere questa funzione, mentre altre aziende produrranno le proprie informazioni e condurranno le proprie ricerche. L'intelligence tattica sulle minacce è essenzialmente una funzione di supporto della funzione di indagine e reazione e riguarda avvisi e indagini in corso.

- **Gestione di incidenti/crisi**: quando un incidente grave o una crisi di rilevo mette a rischio un'azienda, questa può decidere di avvalersi delle competenze di una figura specializzata, denominata Incident Manager o Crisis Manager. Questo ruolo viene ricoperto da una persona esperta nella gestione della risposta alle situazioni di crisi, nella valutazione degli effetti degli incidenti in termini di normative o adeguamento e nel mantenimento della comunicazione con i leader aziendali durante l'incidente. Nelle grandi aziende ci sarà probabilmente un Incident Manager a tempo pieno, mentre in quelle più piccole questo ruolo verrà ricoperto su base temporanea, a seconda delle esigenze. Questo ruolo richiede un set di competenze specializzato diverso dalle competenze tecniche e investigative di altri analisti.

- **Gestione dedicata dell'infrastruttura SIEM**: le aziende che si affidano a sistemi SIEM locali fortemente basati sull'infrastruttura possono avere un team interno per la gestione dell'infrastruttura. L'infrastruttura di sistemi SIEM locali legacy può diventare molto grande e complessa. In questi casi supportare i team di analisti nelle query avanzate e nella ricerca di utenti malintenzionati può richiedere personale aggiuntivo. Con la migrazione delle aziende a sistemi SIEM basati sul cloud, come Microsoft Sentinel, questa funzione probabilmente non esisterà più o verrà dirottata su altre esigenze dell'infrastruttura, dal momento che i sistemi SIEM basati sul cloud non richiedono la gestione dell'infrastruttura.

L'intelligence tattica sulle minacce è essenzialmente una funzione di supporto della funzione di indagine e reazione e riguarda avvisi e indagini in corso.

Per i team addetti alle operazioni di sicurezza più avanzati:

- **Rilevazione proattiva**: un avversario determinato e di talento talvolta può trovare il modo di aggirare i rilevamenti. Una volta entrato, l'avversario si nasconde nell'ombra mantenendo un basso profilo. Elude i normali processi e può passare inosservato. Il settore sta riconoscendo la necessità di persone che si dedichino alla rilevazione proattiva di avversari per trovare ed eliminare quelli che hanno aggirato le difese primarie. La rilevazione proattiva verrà affrontata più avanti quando verranno illustrate le procedure consigliate per le operazioni di sicurezza.

- **Intelligence strategica sulle minacce**: questa funzione spesso non fa parte delle operazioni di sicurezza, sebbene essa sia strettamente correlata al team delle operazioni di sicurezza. Questa funzione di intelligence sulle minacce è distinta dalla funzione di intelligence tattica sulle minacce descritta in precedenza che offre indicatori di compromissione tecnici. L'intelligence strategica sulle minacce è prospettica e offre indicazioni strategiche, intelligence e ricerca sui tipi di minacce e attacchi di fronte ai quali potrebbe venire a trovarsi l'azienda, nonché considerazioni sui rischi e sulle conseguenze per l'azienda in caso di attacco. Il personale addetto alle attività di intelligence strategica sulle minacce ha il compito di fornire consigli al CISO o ai leader aziendali per far comprendere l'attuale panorama delle minacce e come interpretare le notizie dal punto di vista della sicurezza informatica per poi aggiungerle alla propria pianificazione strategica.

Realisticamente parlando, attualmente si registra una carenza di talenti tra gli analisti della sicurezza. Per le aziende che hanno un team addetto alle operazioni di sicurezza interno, l'obiettivo principale deve essere l'attività di **indagine e reazione agli incidenti**. Quando questa esigenza basilare sarà stata soddisfatta e il team matura e si espande, anche le funzioni delle operazioni di sicurezza potranno essere estese passando alla rilevazione proattiva e all'intelligence strategica sulle minacce. Le aziende che possono contare solo su un piccolo team devono invece concentrarsi sull'identificazione e sulla risposta agli incidenti.

Modernizzazione delle operazioni di sicurezza

La modernizzazione delle operazioni di sicurezza richiede la maturazione di strumenti e processi per supportare un'evoluzione da una posizione reattiva a una posizione proattiva e da un modello basato sul perimetro di rete a un modello di sicurezza che utilizza l'identità come piano di controllo primario per la sicurezza.

Da reattiva a proattiva

Aumento della visibilità

Strumenti e livelli di automazione avanzati offrono agli analisti la possibilità di risparmiare tempo e di avere la visibilità necessaria per passare da risposte puramente reattive alla preparazione proattiva e alla ricerca degli avversari. Questo tipo di strumenti è spesso indicato come XDR (eXtended Detection and Response) e mira

a offrire rilevamenti di alta qualità e altre funzionalità per risorse specifiche come endpoint, identità, account di storage nel cloud e così via.

Molte aziende continuano ad affidarsi a sistemi SIEM locali legacy e a un processo di analisi basato sui log. È importante ricordare, tuttavia, che raccogliere tante informazioni non aiuta necessariamente a rilevare eventuali anomalie. La semplice raccolta di log non sarà infatti di grande aiuto se gli analisti dovranno esaminare quantità troppo elevate di dati. I segnali non verranno colti e aumenteranno le probabilità che gli analisti perdano tempo prezioso dietro ai falsi positivi, mentre le minacce reali non vengono riconosciute. Dall'approccio basato su sistemi SIEM legacy e sui log, le aziende dovrebbero evolvere passando a un modello che usa un sistema SIEM basato sul cloud, come Microsoft Sentinel, e strumenti avanzati, come quelli di rilevamento e risposta per endpoint (EDR) e altri strumenti di rilevamento specializzati. Quando questi strumenti di rilevamento sono integrati con un sistema SIEM basato sul cloud capace di applicare l'apprendimento automatico, l'analisi del comportamento e la tecnologia SOAR (Security Orchestration Automated Response) agli avvisi in arrivo, accadono tre cose:

1. Molti avvisi verranno gestiti tramite l'automazione, senza sottrarre tempo a un analista.

2. La qualità degli avvisi che arrivano alle code degli analisti migliora drasticamente, poiché questi ultimi avranno una precisa visibilità (necessaria per ottenere buoni risultati) su ciò che sta realmente accadendo e dove.

3. Mentre la tecnologia prosegue sulla strada dell'automazione delle funzioni reattive delle operazioni di sicurezza, gli analisti possono concentrarsi maggiormente sull'aspetto della sicurezza legato alla rilevazione proattiva e iniziare a cercare anomalie e avversari nel proprio ambiente.

Questo tipo di evoluzione, da una posizione reattiva a una proattiva e da un sistema SIEM e strumenti locali a un ambiente basato al cloud, non è sempre lineare. Ma è in generale il percorso di maturità che storicamente abbiamo osservato nelle operazioni di sicurezza. Prevediamo che in futuro esso crescerà e lo consigliamo come modello alle aziende interessate a intraprendere passi fruttuosi verso la modernizzazione delle operazioni di sicurezza.

Riduzione della superficie di attacco

Questo è un altro passaggio proattivo che si può intraprendere. La maggior parte degli attacchi contro un'azienda segue la struttura della cosiddetta cyber kill chain. La kill chain ci aiuta a capire come funziona un attacco tipico e quali tecnologie possono aiutare a mitigare le minacce in ogni sezione della chain. Se si comprende il funzionamento della chain, le aziende possono inserire degli "ostacoli" in ogni anello per fermare un attacco o impedirne la diffusione.

Questi sono i passaggi di una tipica kill chain:

1. Ricognizione: i criminali escogitano modi per sfruttare un'azienda o un utente all'interno di un'azienda. Questa attività può includere la ricerca per scoprire informazioni che possono essere usate in una campagna di spear-phishing, un'attività sul dark Web in cui i criminali acquistano informazioni sulle vulnerabilità all'interno di un'azienda oppure la ricognizione per scoprire i punti deboli dell'infrastruttura IT o della base di utenti di un'azienda.

2. Exploit di una vulnerabilità: gli autori di minacce lanciano quindi un attacco. Può trattarsi di una comune campagna di phishing o di una tecnica più sofisticata progettata per introdurre codice dannoso nei sistemi di un'azienda.

3. Spostamento laterale: una volta all'interno, i criminali usano il proprio accesso per spostarsi, spesso inosservati, nei sistemi aziendali per individuare i dati chiave. Possono adottare delle misure per coprire le proprie tracce o aggiungere altri punti di ingresso nel caso venga scoperta la violazione originale.

4. Esfiltrazione dei dati: dopo aver individuato i dati desiderati, ad esempio informazioni personali, finanziarie, proprietà intellettuale o altre informazioni sensibili, i criminali possono rubarli o crittografarli nell'ambito di un attacco ransomware.

La mancanza di orchestrazione tra gli strumenti può tradursi in un ulteriore onere per gli analisti della sicurezza che possono essere costretti a decifrare le minacce manualmente, rallentando le risposte in situazioni in cui il tempo è prezioso.

Una tradizionale strategia di difesa del perimetro non è più sufficiente per mitigare gli attacchi contro un'azienda. Le moderne tecniche di attacco come phishing e password spraying aggirano il perimetro e le sempre più numerose risorse che risiedono nel cloud e nei dispositivi mobili all'esterno della rete aziendale. In risposta, i leader della sicurezza devono allontanarsi dalle protezioni basate sul perimetro, che sono progettate semplicemente per tenere fuori i malintenzionati, per adottare un approccio di protezione/rilevamento/risposta ideato per il mondo contemporaneo basato sulla "supposizione di una violazione".

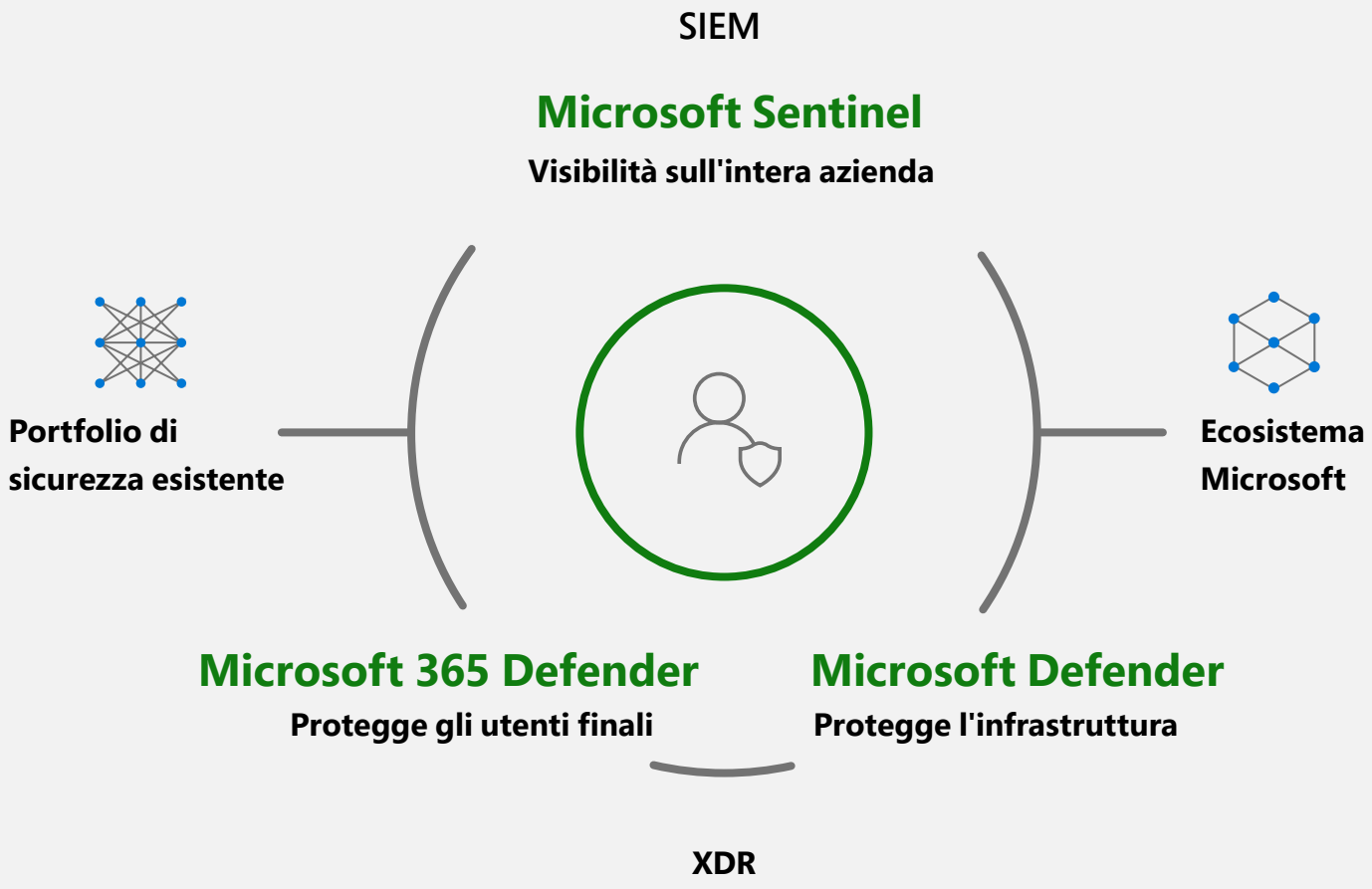
Questo approccio a più livelli, tuttavia, viene spesso implementato con soluzioni mirate distribuite in modo frammentario in sezioni specifiche della kill chain e lascia le aziende in uno stato di vulnerabilità, perché gli strumenti sono spesso isolati e devono essere gestiti separatamente. Questo può comportare la presenza di lacune critiche in termini di visibilità e copertura, falle che gli utenti malintenzionati possono sfruttare.

Un approccio olistico alla mitigazione del rischio per l'odierno panorama delle minacce in continua evoluzione richiede una piattaforma in grado di fornire integrazione e visibilità all'interno dell'azienda ai CISO e ai team addetti alle operazioni di sicurezza. Questo approccio integrato colma le lacune per ridurre la superficie di attacco. Esso è reso possibile dall'integrazione di un **sistema SIEM nativo per il cloud**, che offre una vasta gamma di piattaforme, con soluzioni **XDR (extended Detection and Response)** che forniscono una protezione profonda dalle minacce nei vari domini per aiutare i responsabili della protezione a collegare avvisi apparentemente eterogenei e a contrastare utenti malintenzionati.

Le moderne tecniche di attacco come phishing e password spraying aggirano il perimetro e le sempre più numerose risorse che risiedono nel cloud e nei dispositivi mobili all'esterno della rete aziendale.

L'approccio di Microsoft

Nel SOC Microsoft questa visibilità ampia e approfondita è resa possibile dalle funzionalità SIEM + XDR integrate di Microsoft Sentinel, Microsoft 365 Defender e Microsoft Defender.



- **Microsoft Sentinel,** la nostra soluzione SIEM nativa per il cloud e leader di settore, raccoglie dati ed entità di qualsiasi origine. Sentinel offre analisi di sicurezza intelligenti e intelligence sulle minacce in tutta l'azienda, fornendo rilevamento degli avvisi, visibilità sulle minacce, rilevazione proattiva e una risposta orchestrata alle minacce con tecnologia SOAR integrata.

- **Microsoft 365 Defender** offre funzionalità XDR (eXtended Detection and Response) su identità, endpoint, applicazioni ed e-mail.

- **Microsoft Defender** offre una protezione multicloud completa per IoT, infrastruttura, risorse cloud e workload.

Operazioni di sicurezza

Architettura di riferimento Microsoft

Al centro della nostra visione tecnica per le operazioni di sicurezza ci sono le persone: analisti ed esperti che si dedicano alla rilevazione delle minacce. Per aiutare analisti ed esperti a ottenere buoni risultati, applichiamo le nostre tecnologie di sicurezza SIEM + XDR integrate. Queste tecnologie offrono informazioni approfondite per avvisi di alta qualità che incorporano segnali estremamente approfonditi tramite XDR e segnali estremamente ampi tramite la nostra soluzione SIEM nativa per il cloud, Microsoft Sentinel. La nostra protezione XDR si estende dai prodotti e servizi Microsoft a tutto il resto presente nell'ambiente. Il rilevamento e la risposta coordinati consentono di trovare e rimuovere anche sofisticate catene di attacco per impedire agli avversari di spostarsi all'interno dell'ambiente, nel caso riescano a entrare.

Scopri di più sulla protezione integrata Microsoft dalle minacce con SIEM e XDR

Per aiutare analisti ed esperti a ottenere buoni risultati applichiamo le nostre tecnologie di sicurezza SIEM + XDR integrate. Queste tecnologie offrono informazioni approfondite per avvisi di alta qualità.

Zero Trust e operazioni di sicurezza moderne

La maggior parte delle aziende ha ormai implementato buone difese per gli attacchi basati sulla rete. Gli utenti malintenzionati ne sono consapevoli e hanno quindi trasferito le proprie tattiche sugli attacchi alle identità e alle applicazioni dove le difese sono più deboli. Inoltre, dispositivi e app ora stanno lasciando la rete, eliminando il perimetro come punto di intercettazione in cui le operazioni di sicurezza potrebbero applicare un controllo.

Modernizzare le operazioni di sicurezza significa evolvere le tattiche di difesa in base alle tattiche degli avversari. Ecco perché è consigliabile adottare un **modello di sicurezza Zero Trust**. Il modello Zero Trust è infatti basato sull'identità. Non intendiamo affermare che le reti ora possono essere ignorate, ma che è innanzitutto necessario concentrarsi sulle tecniche di attacco basate sull'identità e il nostro consiglio è quello di fare della creazione di competenze e capacità relative alla sicurezza delle identità una priorità assoluta.

Anziché creare solide difese sulla rete e poi ritenere che tutto ciò che si trova dietro il firewall aziendale sia al sicuro, il modello Zero Trust presuppone la presenza di una violazione e verifica ogni richiesta come se provenisse da una rete non controllata. Nel modello Zero Trust non esistono reti attendibili: tutte le reti sono ostili.

Questi sono i principi guida del modello Zero Trust:

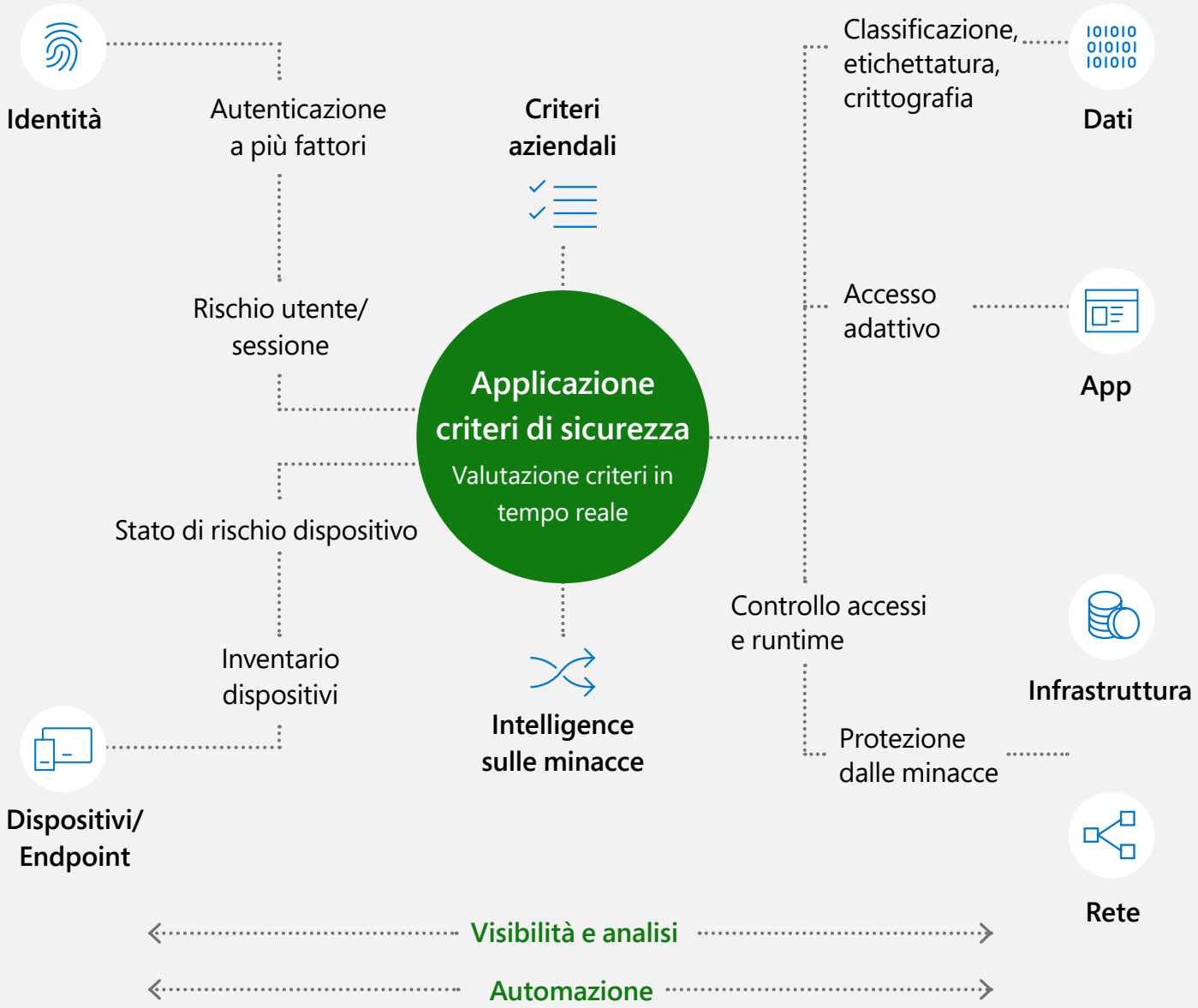
1. Verifica in modo esplicito: esegui sempre l'autenticazione e l'autorizzazione in base a tutti i punti dati disponibili, tra cui l'identità utente, la posizione, lo stato del dispositivo, il servizio o il workload, la classificazione dei dati e le anomalie.

2. Usa l'accesso con privilegi minimi: limita l'accesso degli utenti con le funzionalità JIT (Just-In-Time) e JEA (Just-Enough Access), i criteri adattivi basati sul rischio e la protezione dei dati per salvaguardare
i dati e la produttività.

3. Presupponi la presenza di violazioni: riduci al minimo il raggio di azione delle violazioni e previeni lo spostamento laterale segmentando l'accesso in base alla rete, all'utente, ai dispositivi e al riconoscimento delle applicazioni. Verifica che tutte le sessioni siano crittografate end-to-end. Usa l'analisi per ottenere visibilità, favorire il rilevamento delle minacce e migliorare le difese.

È consigliabile estendere l'approccio Zero Trust all'intero patrimonio digitale e adottarlo come filosofia di sicurezza integrata e strategia end-to-end. Questo è possibile implementando controlli e tecnologie Zero Trust su sei elementi fondamentali: **identità, dispositivi, applicazioni, dati, infrastruttura** e **reti**. Ognuno di questi sei elementi fondamentali è una fonte di segnalazione, un piano di controllo per l'applicazione e una risorsa critica da difendere. Ciò fa di ognuno di essi un'importante area su cui concentrare gli investimenti, a cominciare dall'identità.

Ognuno di questi sei elementi fondamentali è una fonte di segnalazione, un piano di controllo per l'applicazione e una risorsa critica da difendere.


Identità
Autenticazione a più fattori
Criteri aziendali
Classificazione, etichettatura, crittografia
Dati
Rischio utente/ sessione
Accesso adattivo
App
Applicazione criteri di sicurezza
Valutazione criteri in tempo reale
Stato di rischio dispositivo
Controllo accessi e runtime
Infrastruttura
Inventario dispositivi
Intelligence sulle minacce
Protezione dalle minacce
Dispositivi/ Endpoint
Rete
Visibilità e analisi
Automazione

Per aiutarti a pianificare e implementare il passaggio al modello Zero Trust, illustriamo di seguito la nostra roadmap consigliata per perseguire una strategia di modernizzazione Zero Trust.

Allinea la strategia di segmentazione e i team

- Unifica identità, dispositivi, applicazioni, dati, infrastruttura e reti in una singola strategia di segmentazione aziendale. Tutti devono essere sulla stessa lunghezza d'onda, adottando la stessa strategia, con le stesse priorità e parlando la stessa lingua.

Crea un perimetro moderno basato sull'identità

- Stabilisci il tuo **percorso critico** usando le garanzie Utente e Dispositivo.

  Utente: richiedi l'autenticazione senza password o MFA per accedere alle applicazioni moderne.

  Dispositivo: richiedi l'integrità del dispositivo per l'accesso.

È consigliabile implementare prima il percorso critico per gli amministratori IT.

Gli amministratori IT possono fornire un feedback tecnico per aiutarti ad apportare perfezionamenti prima dell'implementazione su vasta scala. Gli amministratori IT sono presi di mira dagli utenti malintenzionati, pertanto una violazione dei loro account può avere un impatto molto significativo. Metti prima al sicuro gli amministratori IT, poi i normali utenti.

Completa la strategia

- Modernizza le app e rinnova le garanzie riguardo alle risorse locali legacy tramite Proxy app.
- Aumenta i livelli di protezione per i dati sensibili (CASB, controllo degli accessi CA, AIP).
- Ritira i protocolli di autenticazione legacy.

Perfeziona la segmentazione e il perimetro di rete

- Segmenta le risorse per business-critical, vita/sicurezza e impatto operativo/fisico.
- Aggiungi la microsegmentazione per ridurre ulteriormente il rischio.
- Ritira e isola le piattaforme legacy, ad esempio quelle con sistemi operativi e applicazioni non supportati.

Introduzione a Zero Trust

Zero Trust è un modello di sicurezza, non una tecnologia specifica, e la sua realizzazione è un percorso, non un passaggio diretto. Nei moderni ambienti di lavoro mobili, remoti e ibridi, le operazioni di sicurezza non possono più basarsi su un perimetro di rete. Il perimetro di rete è di fatto scomparso. Per gettare le basi di un modello Zero Trust, le operazioni di sicurezza devono allinearsi attorno al concetto di protezione basata sull'identità. Gli utenti possono usare molteplici dispositivi e accedere alle risorse aziendali da una varietà di reti e app. Quasi tutte queste risorse richiedono l'autenticazione. Tutte le richieste di accesso hanno quindi come denominatore comune l'identità, indipendentemente dal fatto che provengano da un dispositivo personale in una rete Wi-Fi pubblica o da un dispositivo aziendale che si trova all'interno del perimetro della rete. Usando l'identità come piano di controllo, puoi considerare ogni singola richiesta di accesso come non attendibile fino a quando l'utente, il dispositivo e altri fattori non vengono verificati.

Il primo passo nell'implementazione del modello di sicurezza Zero Trust consiste quindi nel connettere tutte le app a un'unica soluzione di gestione delle identità cloud, ad esempio Microsoft Azure Active Directory. Ciò consente di creare la sicurezza basata sull'identità e di applicare criteri personalizzati all'intero ambiente per controllare l'accesso a ogni app. Dopo aver completato questo passaggio potrai implementare l'autenticazione a più fattori (MFA) per tutte le app. MFA è un criterio di sicurezza coerente ed efficace che può bloccare fino al 99,9% degli attacchi che mirano a compromettere gli account.

Per indicazioni pratiche sull'implementazione di un framework Zero Trust completo nella tua azienda, leggi il piano aziendale Zero Trust.

La soluzione di gestione delle identità consigliata da Microsoft per Zero Trust è Microsoft Azure Active Directory (Azure AD). Per informazioni su come implementare una strategia Zero Trust con Azure AD, leggi la Guida alla distribuzione Zero Trust per Azure Active Directory.

Protezione dalle minacce interne

Con un modello di sicurezza Zero Trust e una suite di sicurezza integrata, le operazioni di sicurezza possono proteggere meglio l'azienda dalle minacce esterne. Ma le operazioni di sicurezza devono anche offrire protezione dalle minacce interne con strumenti e processi che salvaguardano informazioni, utenti e dispositivi.

Da molto tempo, la protezione e la prevenzione della perdita di informazioni sensibili sono una priorità per i team aziendali IT e addetti alle operazioni di sicurezza. I dati ora si estendono ben oltre l'infrastruttura locale in ambienti multicloud e ibridi. I team delle operazioni di sicurezza devono cercare il modo di gestire meglio l'intero ciclo di vita dei dati, dalla loro creazione al ritiro o all'eliminazione.

Per la sicurezza dell'azienda, la consapevolezza dei dati disponibili, chi vi accede e come questi vengono usati sono aspetti che devono essere al centro delle attività del team addetto alle operazioni di sicurezza. Ma, come accade con la semplificazione della sicurezza delle identità, uno degli aspetti chiave di queste iniziative è la riduzione del rischio senza compromettere la produttività degli utenti in questo panorama IT esteso.

Le aziende dispongono di una varietà di tecnologie e strumenti per gestire e proteggere i dati nelle diverse fasi del ciclo di vita. Questi strumenti offrono flessibilità, ma comportano anche notevoli complessità. Un recente studio di IDG ha rilevato che le aziende utilizzano in media quasi cinque sistemi di gestione dei dati diversi per attività come la classificazione, l'e-discovery e la gestione dei record. Le soluzioni di sicurezza integrate possono proteggere anche dalle minacce interne, colmando lacune critiche che causano la perdita di dati e offrendo visibilità end-to-end sull'intero ciclo di vita dei dati.

È consigliabile concentrare le iniziative di protezione end-to-end dalle minacce interne su tre passaggi chiave:

- **Identificazione dei dati**
- **Classificazione dei dati**
- **Distribuzione di strumenti e criteri per salvaguardare i dati**

L'obiettivo deve essere quello di garantire che tutte le informazioni siano protette, comunque e ovunque vengano utilizzate.

Per la sicurezza dell'azienda, la consapevolezza dei dati disponibili, chi vi accede e come questi vengono usati sono aspetti che devono essere al centro delle attività del team addetto alle operazioni di sicurezza.

Differenziazione tra rischio intenzionale e non intenzionale

Le minacce interne sono un aspetto inevitabile di ogni azienda e talvolta i dati sono messi a rischio anche nel normale svolgimento di attività legittime. Basti pensare al numero di persone che accedono alle risorse e al ciclo naturale di avvicendamento di dipendenti nelle aziende. Con i processi, le funzionalità e i controlli giusti, le operazioni di sicurezza possono mantenere la supervisione dei dati e la fiducia degli utenti senza compromettere la produttività.

Una delle funzionalità più importanti da implementare è la differenziazione tra rischio intenzionale e non intenzionale da parte degli utenti. Un utente davvero malintenzionato può cercare di eseguire azioni contrarie ai criteri aziendali, ad esempio disattivando i controlli di sicurezza o installando software dannoso. Spesso lo scopo è quello di divulgare o sottrarre dati per un tornaconto personale o per arrecare danno. Le operazioni di sicurezza devono essere preparate per questi eventi e necessitano di modalità per prevenire, rilevare e contenere questi tipi di minacce.

Ma esistono altre classi di minacce in cui l'utente può anche non essere consapevole di violare i criteri aziendali. Un utente potrebbe ad esempio essere talmente entusiasta di un progetto da condividerne le informazioni al di fuori del proprio gruppo e, così facendo, può divulgarne i dati senza rendersi conto di inviare informazioni sensibili. Le operazioni di sicurezza necessitano di strumenti per fermare la perdita involontaria di dati prima che questa possa avvenire e/o per indagare e vederla in tempo reale, nel contesto, in modo da poterne determinare lo scopo e l'impatto e decidere se si trattava di un singolo atto di disattenzione o parte di un disegno più ampio e potenzialmente dannoso.

Quando individui il rischio, devi assicurarti che l'attenzione resti concentrata sull'attività realmente sospetta, in modo da non causare problemi agli utenti o sovraccaricare gli analisti con avvisi che in realtà sono falsi positivi.

Scopri Gestione dei rischi Insider in Microsoft 365.

Procedure consigliate per le operazioni di sicurezza

Come accennato in precedenza, al centro delle operazioni di sicurezza ci sono le persone, in particolare gli analisti della sicurezza.

Indipendentemente dal livello di maturità delle operazioni di sicurezza, nel corso del loro lavoro, gli analisti avanzeranno in modo formale o informale nel cosiddetto **ciclo OODA**:

- **Osservare**
- **Orientare**
- **Decidere**
- **Agire**

Gli obiettivi devono essere quelli di aiutare le persone a progredire nel ciclo OODA il più rapidamente possibile, con le migliori informazioni possibili, in modo da prendere le decisioni migliori e intraprendere le azioni più efficaci possibili.

Per prendere decisioni migliori più rapidamente, l'attenzione delle operazioni di sicurezza deve essere costantemente posta su come massimizzare la visibilità, ridurre i passaggi manuali e massimizzare l'impatto umano.

Massimizza la visibilità

- **Interno**: riduci al minimo i punti deboli interni garantendo una buona copertura (il più vicino possibile al 100%), così come la copertura dei tipi di risorsa (ad esempio identità, endpoint, e-mail, applicazioni cloud, datacenter locali, datacenter cloud e dati delle applicazioni SaaS e PaaS cloud).

- **Esterno**: assicurati di avere una varietà di feed sulle minacce da origini esterne che offrano informazioni approfondite e contesto dell'ambiente malware esterno, di attacchi tramite e-mail, siti Web di attacco, password/identità compromesse e così via. Massimizza la qualità e l'affidabilità (dettagli rilevanti) delle origini esterne che usi.

Riduci i passaggi manuali (e gli errori)

Automatizza e integra il maggior numero possibile di processi manuali per eliminare le azioni umane non necessarie che causano rallentamenti e potenziali errori umani.

Affinché le operazioni di sicurezza possano distinguere rapidamente il segnale (rilevamenti reali) dai falsi allarmi (falsi positivi) sono necessari investimenti in risorse umane e automazione. Crediamo fermamente nel potere dell'automazione e della tecnologia per ridurre il lavoro dell'uomo. Ma, in ultima analisi, i malintenzionati che ti trovi ad affrontare sono operatori umani, quindi il giudizio umano è fondamentale nel processo di difesa dalle minacce.

L'automazione non usa l'efficienza per eliminare le persone dal processo, ma per supportarle. Rifletti su come automatizzare le attività ripetitive del lavoro dell'analista, in modo che possa concentrarsi su problemi complessi che solo le persone sono in grado di risolvere.

L'automazione consente ai team delle operazioni di sicurezza di fare di più, aumentando la velocità di risposta e acquisendo l'esperienza umana. La fatica a cui è sottoposto il personale è data principalmente da attività ripetitive e queste ultime sono causate da utenti malintenzionati o dal fatto che i responsabili della protezione fanno ripetutamente le stesse cose. Le attività ripetitive sono candidate ideali per l'automazione.

Quando il lavoro ripetitivo e noioso è automatizzato, gli analisti hanno la possibilità di dedicare creatività ed energia alla risoluzione di nuovi problemi posti da utenti malintenzionati e alla rilevazione proattiva di malintenzionati che hanno aggirato le prime linee di difesa.

Massimizza l'impatto umano

Per le aree del processo dove è opportuna l'interazione umana (scelte difficili, nuove decisioni e così via), assicurati che gli analisti abbiano accesso a competenze e informazioni approfondite per prendere decisioni migliori.

Assicurati inoltre che l'apprendimento sia integrato nell'intero processo, inclusa la riflessione sull'opportunità di assistere all'evoluzione di un attacco per comprenderne l'obiettivo (valore a lungo termine) anziché bloccarlo (valore a breve termine).

Prendi decisioni migliori più rapidamente

Massimizza la visibilità

Interno: completezza e diversità della copertura dei sensori

Esterno: diversità e affidabilità dei feed sulle minacce

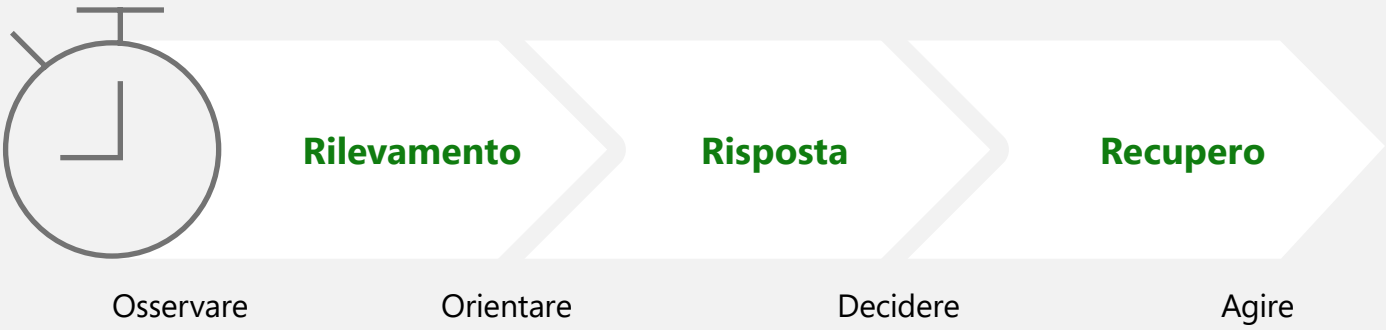
Riduci i passaggi manuali (e gli errori)

Automatizza: attività di rilevamento e risposta

Integra: strumenti di indagine

Massimizza l'impatto umano

Offri agli analisti l'accesso a **competenze approfondite e apprendimento continuo basato sulle informazioni**: osserva gli attacchi e integra quanto appreso nelle difese



Cultura delle operazioni di sicurezza

La cultura delle operazioni di sicurezza è tanto importante quanto le persone che assumi e gli strumenti che usi. La cultura è alla base delle innumerevoli decisioni quotidiane in quanto delinea la risposta che appare più appropriata in situazioni ambigue, che nelle operazioni di sicurezza abbondano.

Concentrando gli elementi culturali sulle persone, sul lavoro in team e sull'apprendimento continuo, il team delle operazioni di sicurezza continua a evolvere per tenere il passo con le minacce dalle quali deve proteggere l'azienda:

- **Uso del talento umano con saggezza**: i nostri dipendenti sono le risorse più preziose che abbiamo nelle operazioni di sicurezza e non possiamo permetterci di sprecarne il tempo in sconsiderate attività ripetitive che possono essere automatizzate. Per contrastare le minacce umane che affrontiamo, abbiamo bisogno di esseri umani esperti e ben preparati in grado di applicare competenza, giudizio e pensiero creativo. Questo fattore umano influisce su quasi ogni aspetto delle operazioni di sicurezza, compreso il ruolo di strumenti e automazione per supportare le persone (anziché sostituirle) e la riduzione del lavoro degli analisti.

- **Lavoro in team**: nel team delle operazioni di sicurezza è consigliabile non tollerare l'atteggiamento di "eroe solitario". Nessuno, da solo, è tanto intelligente quanto l'intero team. Il lavoro in team rende un ambiente di lavoro altamente stressante, come quello delle operazioni di sicurezza, molto più divertente, piacevole e produttivo, quando tutti sanno di far parte dello stesso team e si sostengono a vicenda. Presso il centro operazioni per la sicurezza Microsoft, processi e strumenti vengono progettati suddividendo le attività in specializzazioni e invitando le persone a condividere informazioni, coordinarsi e controllarsi il lavoro a vicenda, imparando costantemente gli uni dagli altri.

- **Atteggiamento shift-left**: per stare al passo con criminali informatici e hacker che aggiornano costantemente le proprie tecniche, i team delle operazioni di sicurezza devono migliorare continuamente e anticipare le proprie attività nella sequenza temporale degli attacchi. L'attenzione alla velocità e all'efficienza aiuta il team a "superare la velocità di attacco", grazie all'analisi di come avrebbe potuto rilevare prima gli attacchi e rispondere più rapidamente. Questo principio è essenzialmente un'applicazione di una mentalità di crescita tramite apprendimento continuo che mantiene il team concentrato sulla riduzione del rischio per l'azienda e i clienti.

Separa gli account con privilegi elevati

Non tutti gli attacchi sono creati allo stesso modo dal punto di vista del danno che possono causare all'azienda, in caso di successo. Gli account di alto profilo, ad esempio membri del consiglio di amministrazione, CEO e CFO, e gli account di amministratore presentano il rischio maggiore, se compromessi. È pertanto necessario prestare prima particolare attenzione alla protezione proattiva di questi account, separandoli in ambienti di elaborazione dedicati tramite l'uso di workstation con accesso con privilegi (PAW) che proteggono questi account importanti da attacchi Internet e altri vettori di minacce.

Metriche: come misurare il successo

Le metriche traducono la cultura in chiari obiettivi misurabili e contribuiscono fortemente a modellare il comportamento delle persone. È fondamentale considerare ciò che misuri e come ti concentri su queste metriche per poi applicarle. In Microsoft, nel centro operazioni per la sicurezza (SOC), misuriamo diversi indicatori di successo, ma teniamo sempre ben presente il fatto che il compito del SOC è gestire variabili significative al di fuori del nostro diretto controllo (attacchi, utenti malintenzionati e così via). Consideriamo le deviazioni principalmente come un'opportunità di apprendimento per il miglioramento di processi o strumenti, piuttosto che come un fallimento da parte del SOC nel raggiungimento di un obiettivo.

Queste sono le metriche che monitoriamo, seguiamo e segnaliamo:

- **Tempo medio di riconoscimento (MTTA)**: la reattività è uno dei pochi elementi su cui il SOC ha il diretto controllo. Misuriamo il tempo che intercorre tra la generazione di un avviso e il momento in cui un analista lo riconosce e avvia l'indagine. Per migliorare la capacità di risposta è necessario che gli analisti non perdano tempo ad analizzare falsi positivi mentre un altro vero positivo rimane in attesa. Raggiungiamo questo obiettivo con un'impietosa definizione delle priorità. Gli avvisi che richiedono la risposta di un analista devono avere un track record di vero positivo del 90%.

- **Tempo medio di risoluzione (MTTR)**: come molti SOC, monitoriamo il tempo necessario per la risoluzione di un incidente per assicurarci di limitare il tempo di accesso di utenti malintenzionati al nostro ambiente, promuovendo efficacia ed efficienza dei processi e degli strumenti del nostro SOC.

- **Incidenti risolti (manualmente o tramite automazione)**: misuriamo quanti incidenti vengono risolti manualmente e quanti tramite automazione. Questo ci assicura livelli di personale appropriati e misura l'efficacia della nostra tecnologia di automazione.

- **Escalation tra ciascun livello**: monitoriamo il numero di incidenti di cui viene eseguita l'escalation tra i livelli di analisti per assicurarci di acquisire accuratamente il workload per ciascun livello. Ad esempio, dobbiamo assicurarci che il lavoro di livello 1 su un incidente di cui è stata eseguita l'escalation non sia totalmente attribuito al livello 2.

Mantieni un'igiene critica

Metodi, difese ed effetti possono diventare complicati, ma il concetto alla base delle attività di utenti malintenzionati è essenzialmente molto semplice: sfruttare le vulnerabilità. E anche ciò che devono fare i professionisti della sicurezza è in sostanza molto semplice da riassumere: eliminare le vulnerabilità.

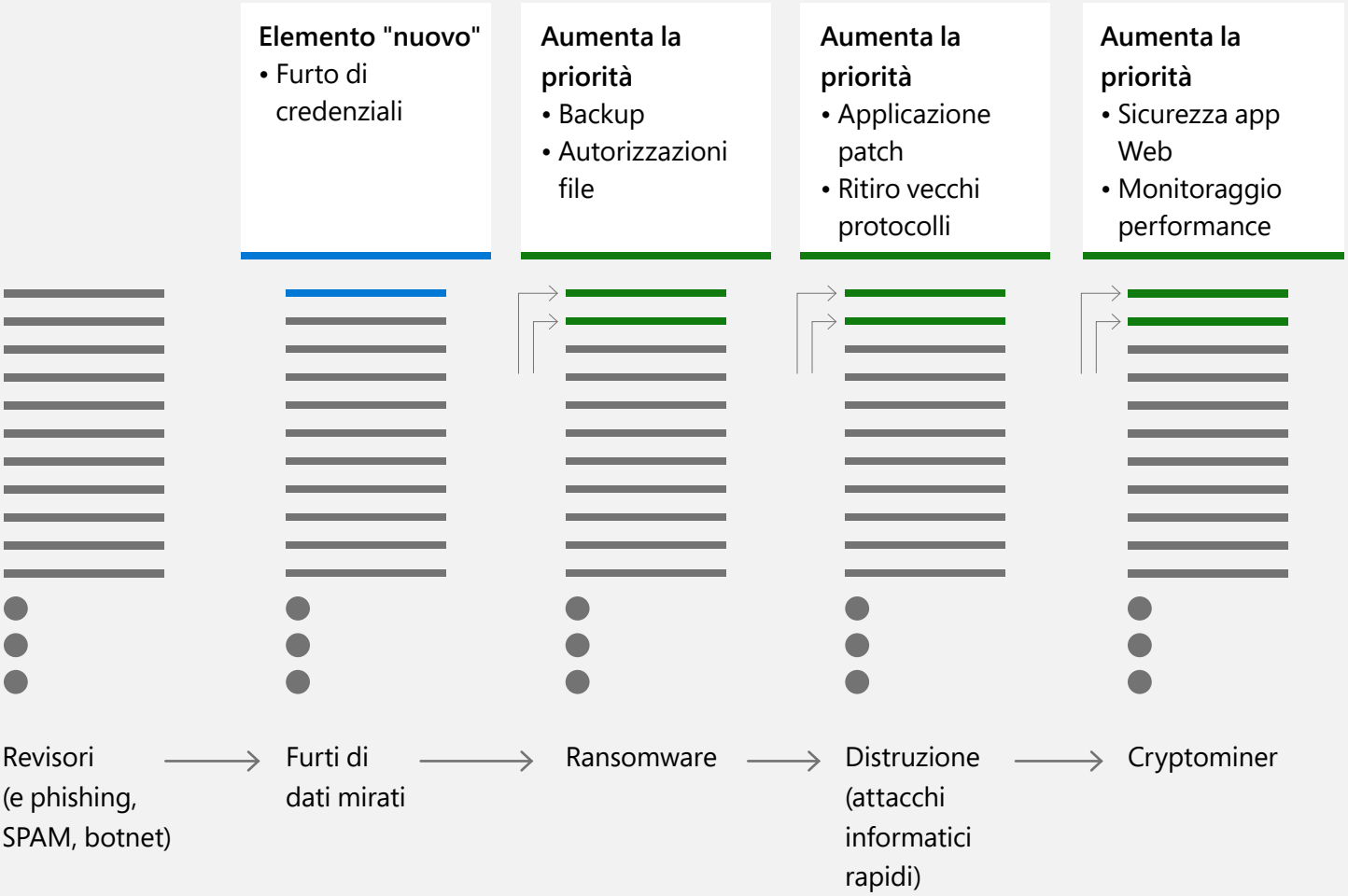
Ogni team delle operazioni di sicurezza è costantemente impegnato ad aggiornare il proprio ambiente. È quel che si chiama "debito tecnico". Il team si occupa di creare i backup o aggiornare le autorizzazioni dei file, ad esempio. Oppure di applicare le patch o ritirare i vecchi protocolli. Si tratta delle stesse procedure consigliate che i team delle operazioni di sicurezza conoscono da molto tempo.

Quando utenti malintenzionati trovano nuovi modi per creare un modello di business o mettono a punto una nuova tecnica di attacco, spesso sfruttano semplicemente le stesse vecchie vulnerabilità, ma in modo nuovo. In alcuni casi, possono sfruttare vulnerabilità che prima non sapevi di avere. Quindi, di fronte all'evoluzione delle tecniche degli utenti malintenzionati, l'imperativo per una buona igiene tecnica rimane lo stesso. Mantenere aggiornato l'ambiente seguendo modalità da tempo note e apprendere altre misure da adottare in base al comportamento dell'utente malintenzionato sono aspetti fondamentali per la protezione dell'azienda, anche dai nuovissimi tipi di attacco.

Quando utenti malintenzionati trovano nuovi modi per creare un modello di business o mettono a punto una nuova tecnica di attacco, spesso sfruttano semplicemente le stesse vecchie vulnerabilità, ma in modo nuovo.

Igiene critica = Debito tecnico da saldare

Il cloud può velocizzarla, ma è comunque necessario un forte impegno



I nuovi modelli di monetizzazione ridefiniscono semplicemente le priorità dello stesso debito di igiene

1. Verifica periodicamente le tue esigenze di igiene critica.

2. Definisci le priorità in base a quanto accade attualmente.

3. Rivedi spesso l'elenco di procedure consigliate e priorità per assicurarti che sia valido per le condizioni attuali.

4. Elimina costantemente il tuo "debito tecnico".

Rilevazione proattiva

La rilevazione delle minacce è un metodo efficace che le operazioni di sicurezza possono usare per ridurre il rischio aziendale. Ma è comunemente rappresentata e percepita come una forma d'arte complessa e misteriosa solo per esperti, che può rivelarsi controproducente. L'espressione "rilevazione delle minacce" indica semplicemente il processo di ricerca proattiva e iterativa, condotto nell'ambiente da analisti esperti, per individuare le operazioni di utenti malintenzionati che hanno eluso altri rilevamenti.

La rilevazione è complementare a processi reattivi, avvisi e rilevamenti e consente di contrastare in modo proattivo utenti malintenzionati. Ciò che distingue la rilevazione dalle attività reattive è la sua natura proattiva, in cui persone esperte dedicano tempo ed energie a riflettere sui problemi, identificare tendenze e modelli e a ottenere una prospettiva più ampia. Tuttavia, un programma di rilevazione di successo non è puramente proattivo, dal momento che richiede di bilanciare costantemente l'attenzione tra iniziative reattive e iniziative proattive. Coloro che si occupano della rilevazione delle minacce dovranno comunque mantenere una connessione con il lato reattivo per avere competenze sempre aggiornate ed essere sintonizzati sulle tendenze nella coda degli avvisi.

In Microsoft, il SOC affronta la rilevazione delle minacce assegnando gli analisti a diversi tipi di attività:

1. Ricerca proattiva di avversari e rilevazione delle minacce. Il personale preposto alla rilevazione delle minacce dedica a questa attività la maggior parte del tempo. Il team esamina una varietà di origini, ad esempio avvisi, indicatori di compromissione esterni e altro. Il team lavora principalmente alla creazione e alla messa a punto di ipotesi strutturate delle possibili azioni da parte di utenti malintenzionati in base a informazioni di intelligence sulle minacce, fenomeni insoliti rilevati nell'ambiente e alla propria esperienza. In pratica, questo tipo di rilevazione delle minacce include:

- **Ricerca proattiva nei dati (query o verifica manuale).**
- **Sviluppo proattivo di ipotesi in base a informazioni di intelligence sulle minacce e altre origini. Vedi la sezione Uso della Knowledge Base MITRE ATT&CK.**

2. Gruppi rossi e viola. Alcuni dei nostri addetti alla rilevazione delle minacce, che lavorano come team blu per la protezione dell'ambiente, si coordinano con i team rossi che simulano gli attacchi e altri che conducono test di penetrazione autorizzati nel nostro ambiente. Questa attività, condotta a rotazione dal personale preposto alla rilevazione delle minacce, solitamente prevede gruppi viola, in cui i team rossi e blu lavorano per svolgere i propri compiti imparando gli uni dagli altri. Ogni attività è seguita da revisioni assolutamente trasparenti che acquisiscono le lezioni apprese condividendole nel SOC, con i team di progettazione dei prodotti e altri team di sicurezza dell'azienda.

3. Incidenti ed escalation. Coloro che si occupano della rilevazione proattiva non lavorano separati dalla sala operativa. Condividono gli stessi spazi in cui si trovano gli analisti che si occupano della parte reattiva, si confrontano spesso, condividono l'oggetto del proprio lavoro, risultati oppure osservazioni interessanti e in genere mantengono la consapevolezza situazionale delle operazioni correnti. Il personale preposto alla rilevazione delle minacce non è necessariamente assegnato a questa attività a tempo pieno, ma può semplicemente restare flessibile e intervenire quando necessario.

Non si tratta di funzioni isolate: i membri di questi team lavorano nella stessa struttura e spesso si confrontano gli uni con gli altri.

Uso della Knowledge Base MITRE ATT&CK

La Knowledge Base MITRE ATT&CK è una vera miniera di informazioni, ma la quantità di queste informazioni può spaventare. La buona notizia è che i prodotti tecnologici possono aiutare a ridurre il lavoro necessario per acquisire valore da MITRE ATT&CK. Oggi molti strumenti, comprese le soluzioni di sicurezza Microsoft, hanno già compiuto un gran lavoro di mappatura alla knowledge base, anche se non in modo completo. Le aziende devono valutare la copertura predefinita offerta dagli strumenti e le eventuali lacune. Laddove esistono queste lacune, è possibile personalizzare la mappatura degli strumenti e della tecnologia esistenti alle aree della Knowledge Base MITRE ATT&CK che si applicano meglio all'azienda per garantire la copertura.

Inoltre, probabilmente non ci sarà bisogno di tutto il contenuto della Knowledge Base MITRE ATT&CK. Considera la knowledge base dal punto di vista di un avversario: non tutti gli avversari del mondo sono interessati a prendere di mira la tua azienda o il tuo business. Riduci il volume di informazioni della knowledge base da monitorare esaminando gli avversari che prendono di mira aziende come la tua e informandoti

sulle tecniche che usano nei loro attacchi. Puoi sviluppare i tuoi rilevamenti in base agli avversari e alle tecniche che, con maggiore probabilità, prenderanno di mira la tua azienda.

In questo modo, la Knowledge Base MITRE ATT&CK diventa uno strumento utile per concettualizzare le possibili azioni di utenti malintenzionati nel caso questi cercassero di condurre un exploit ai danni dell'azienda e per creare rilevamenti in modo proattivo basati su questi modelli di potenziale attacco.

Creazione di relazioni con l'IT

In molte aziende, le operazioni di sicurezza non controllano l'ambiente tecnologico. La scelta degli strumenti in uso nell'ambiente spesso spetta al reparto IT. Le opzioni di risposta e correzione a disposizione delle operazioni di sicurezza spesso dipendono dalle scelte tecnologiche fatte in modo indipendente dal reparto IT. Creare relazioni e una consapevolezza interfunzionale tra IT e operazioni di sicurezza può essere utile. Quando ogni gruppo è consapevole delle attività dell'altro, così come delle sfide e delle limitazioni che deve affrontare nell'adempimento della propria parte dell'obiettivo di proteggere l'azienda, la modernizzazione delle operazioni di sicurezza può risultare più semplice e, di conseguenza, l'azienda sarà più sicura. Inoltre, ci saranno molte occasioni in cui una correzione efficace richiederà l'intervento del personale IT. Buone relazioni e conoscenza dei ruoli del personale IT, delle responsabilità e dei set di competenze dei membri del team IT aiutano le operazioni di sicurezza a contattare la persona giusta più rapidamente in caso di incidente.

Miglioramento continuo

Dopo che un attacco è stato risolto è necessario supporre che gli avversari tenteranno di apprendere da quanto accaduto e che riproveranno con idee e strumenti nuovi. Gli analisti dovranno inoltre apprendere da ogni incidente per migliorare competenze, processi e strumenti. Questo miglioramento continuo è possibile attraverso molti processi informali e formali, dalla revisione formale dei casi alle conversazioni informali in cui gli analisti parlano di storie di incidenti e formulano interessanti osservazioni.

A seconda del carico di lavoro, il team addetto alle indagini può anche rilevare avversari in modo proattivo, restando all'erta e migliorando le proprie competenze. Gli esercizi dei gruppi viola, infine, devono essere pensati con l'obiettivo di un continuo miglioramento. Quando, negli esercizi, i team rossi riescono a eludere il rilevamento effettuato dai responsabili della protezione, è utile accogliere questi momenti come importanti opportunità in cui tutti possono imparare e migliorare.

Raccomandazioni finali

Modernizzare le operazioni di sicurezza è un'impresa impegnativa. Sarà necessario coinvolgere stakeholder dell'intera azienda e non si può pensare di poter fare tutto in una volta. Ma queste sono alcune cose che puoi fare subito per ridurre le vulnerabilità, aumentare la visibilità per le operazioni di sicurezza e migliorare l'efficienza e l'efficacia della difesa dagli attacchi avanzati.

1. Adotta il modello Zero Trust: il modello Zero Trust si basa sulla verifica esplicita, sull'utilizzo del concetto di accesso con privilegi minimi e sul mantenimento di un approccio di "supposizione di violazione". Inizia il tuo percorso Zero Trust trasferendo il piano di controllo per la sicurezza dai perimetri di rete all'identità.

2. Separa gli account con privilegi elevati: identifica gli account aziendali che risulterebbero più allettanti per utenti malintenzionati e separali usando workstation con accesso con privilegi (PAW), proteggendo inoltre gli account di amministratore. Se compromessi, questi account possono causare la maggiore quantità di danni. Perciò inizia da qui le tue iniziative di protezione.

3. Rinforza la supply chain: questo aspetto rientra nella mentalità "shift left" illustrata nella sezione Procedure consigliate di questa guida. L'introduzione di codice o componenti dannosi nei prodotti software che ricevi dai fornitori e che ritieni affidabili è un metodo sempre più comune usato da utenti malintenzionati per eludere le difese. Concentra la tua consapevolezza più in alto nella catena di attacco informandoti su cosa fanno i fornitori per mantenere la sicurezza, acquisisci consapevolezza di cosa usi e dove e continua a investire in una migliore gestione delle risorse.

4. Investi in test di penetrazione: verifica prima che i malintenzionati agiscano. Usa i test di penetrazione per trovare i punti deboli prima di essere attaccato. Usa i risultati dei test di penetrazione non come una pagella, ma come input in un processo di miglioramento continuo.

5. Assicurati di avere funzionalità di indagine complete: assicurati di avere la capacità di indagare nell'intero ambiente. Lavora per ottenere una visibilità completa da diverse prospettive: dall'endpoint all'identità, dai dati all'IoT e tra i cloud. In questo modo potrai effettuare indagini rapide e rilevamenti tempestivi, fondamentali per mantenere la sicurezza.

6. Integra gli strumenti delle operazioni di sicurezza: elimina entità separate e lacune di copertura adottando un approccio integrato. Offri ai tuoi analisti ampiezza e profondità di copertura con un sistema SIEM e XDR integrato nativo per il cloud.

Scopri di più su come le soluzioni di sicurezza integrata Microsoft possono aiutarti a modernizzare le operazioni di sicurezza e a offrire ai tuoi analisti la visibilità necessaria per mantenere l'azienda al sicuro.

Colma le lacune tra soluzioni mirate e ottieni la copertura dell'intero ambiente multipiattaforma e multicloud >

Un approccio integrato per una maggiore efficienza del SOC >

Microsoft

©2022 Microsoft Corporation. Tutti i diritti sono riservati. Questo documento viene fornito "così com'è". Le informazioni fornite e le opinioni espresse in questo documento, inclusi gli URL e altri riferimenti a siti Web Internet, possono variare senza preavviso. Qualsiasi rischio correlato all'uso del documento è a carico dell'utente. Questo documento non garantisce alcun diritto legale sulla proprietà intellettuale di nessun prodotto Microsoft. Il presente documento può essere copiato e utilizzato esclusivamente per uso interno e a scopo di riferimento.