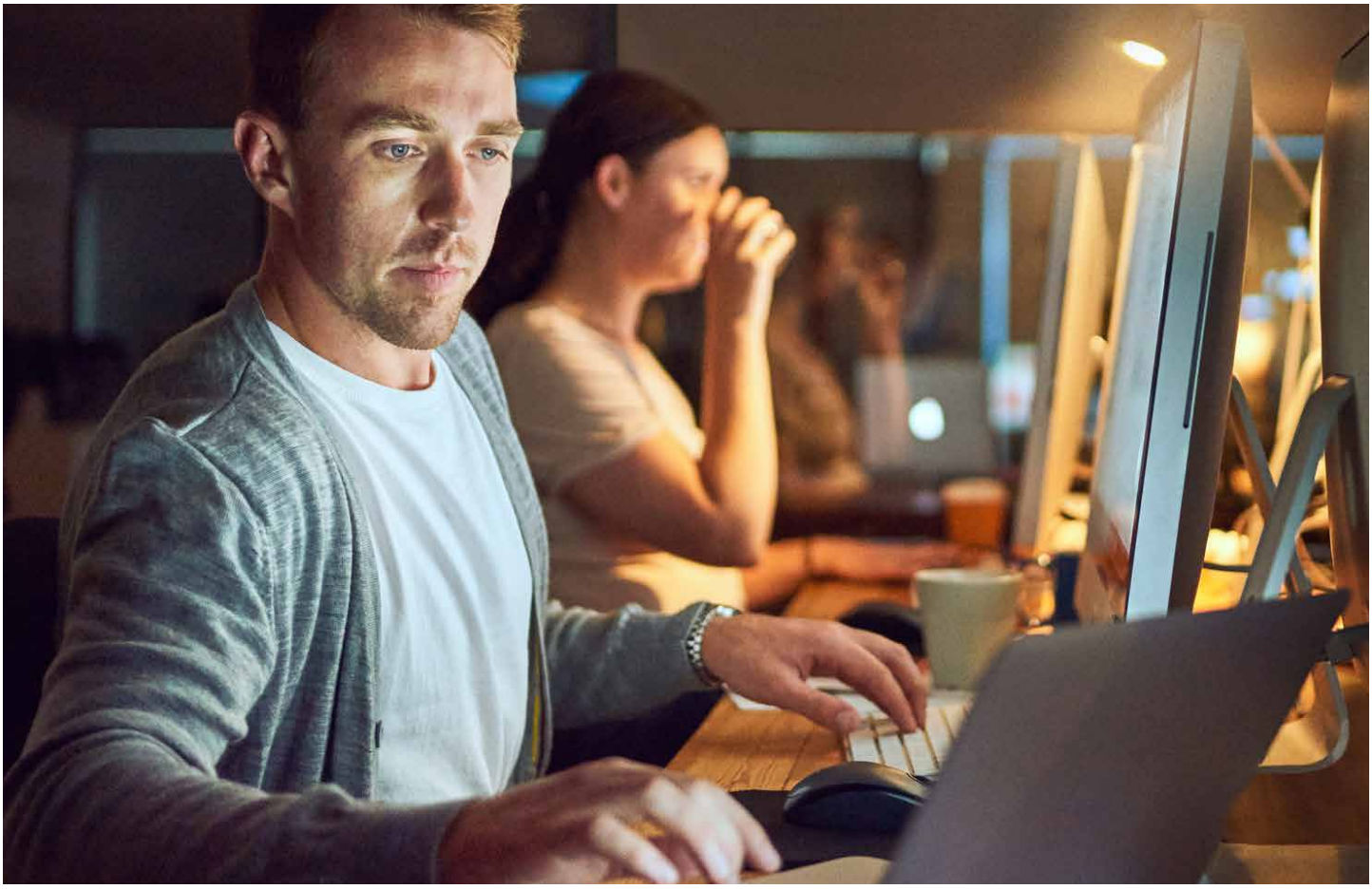
BlackBerry
Intelligent Security. Everywhere.

Guida di valutazione



Guida alla valutazione del livello di sicurezza informatica di BlackBerry

Un quadro di riferimento a quattro livelli per la resilienza contro gli attacchi informatici

Introduzione

I tuoi controlli di sicurezza sono in grado di impedire alle minacce di penetrare le tue difese? Quali investimenti dovresti affrontare per correggere le falle nella tua architettura di sicurezza? È meglio sviluppare internamente gli strumenti e le risorse per la sicurezza o affidarsi a un fornitore di servizi di sicurezza gestita (MSSP) esterno? Riuscirai ad adattarti alle nuove tattiche, tecniche e procedure (TTP) che gli hacker introducono costantemente nei loro arsenali? Ogni azienda risponde in maniera diversa a queste domande, sulla base dei propri obiettivi, del livello di protezione generale e della tolleranza al rischio globale.

La presente guida fornisce un metodo e una procedura che consentono alle aziende di qualsiasi dimensione di valutare e migliorare l'efficienza dei propri programmi di gestione dei rischi informatici. Essa propone un quadro di riferimento a quattro livelli, che comprende piattaforme per la protezione degli endpoint (EPP), soluzioni di Endpoint Detection and Response (EDR), centri operativi per la sicurezza (SOC) e threat hunting, o ricerca delle minacce. Inoltre, tiene conto dei criteri e dei requisiti in termini di risorse necessari a investire in sicurezza in ognuno di questi livelli.

La presente guida fornisce un metodo e una procedura che consentono alle aziende di qualsiasi dimensione di valutare e migliorare l'efficienza dei propri programmi di gestione dei rischi informatici.

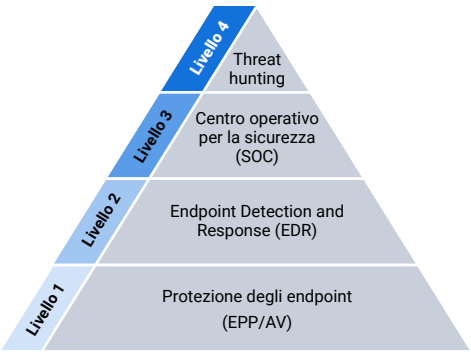
Modello di massima sicurezza

Livello 1: strategia rilevante e a disposizione delle aziende di qualsiasi dimensione

Livello 2: strategia rilevante e a disposizione delle aziende di qualsiasi dimensione, sebbene le imprese più piccole possano affidarne la gestione a un MSSP

Livello 3: più indicato per aziende di grandi dimensioni e multinazionali per via delle risorse di organico e gestionali richieste

Livello 4: indicato soltanto per grandi aziende e multinazionali per via delle competenze specifiche richieste a livello di organico e manutenzione, sebbene alcune aziende possano decidere di affidarsi a un fornitore di soluzioni gestite di rilevamento e risposta (MDR)



LIVELLO 1

Piattaforme per la protezione degli endpoint (EPP)[1]

Al giorno d'oggi, praticamente ogni azienda dispone di una qualche forma di protezione degli endpoint, cosa fondamentale dal momento che oltre il 90% dei malware sono indirizzati agli endpoint tramite tentativi di phishing e spear phishing.[2] Sempre più spesso, però, le aziende scoprono che i prodotti antivirus (AV) legacy nulla possono contro le moderne e sofisticate minacce basate su file o fileless, poiché sfruttano obsolete tecnologie di verifica e riscontro della firma.

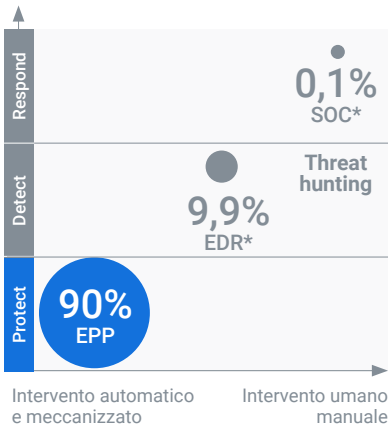
Per firma si intende una stringa di bit univoca che costituisce l'impronta digitale di un file malware. Ogni volta che un prodotto AV tradizionale incontra un nuovo file, ne confronta un byte con quelli presenti nel suo database delle firme. Se trova una corrispondenza, l'antivirus prosegue il confronto dei byte restanti fino a ispezionare l'intero file. Per essere contrassegnato come malware, ogni byte all'interno del file esaminato deve corrispondere esattamente ai byte della firma. Tuttavia, gli strumenti di rilevamento basati su firma sono facili da ingannare se la minaccia offusca o modifica il proprio codice o se il fornitore dell'AV deve ancora ultimare il tedioso processo manuale di creazione e distribuzione degli aggiornamenti delle firme delle oltre 350.000 nuove varianti di malware rilasciate quotidianamente nel mondo.[3]

La procedura di confronto dei singoli byte richiede spesso così tante risorse da rendere gli endpoint poco responsivi o instabili durante le scansioni, intralciando gli utenti e riducendone la produttività. Inoltre, gli antivirus basati su firma implicano lunghi tempi di gestione, poiché i team devono scaricare, installare, distribuire e controllare un flusso costante di aggiornamenti dei file delle firme.

Per fortuna, ora sono disponibili soluzioni per endpoint di nuova generazione che utilizzano tecniche di difesa contro i malware più avanzate, come BlackBerry® Protect, che sfrutta sistemi algoritmici per rilevare i malware e impedirne l'esecuzione. BlackBerry Protect ispeziona ogni singolo file, che sia allegato a un weaponized document o venga copiato dalla flash drive di un dipendente. Sofisticati modelli di machine learning analizzano 2,7 milioni di proprietà dei file[4], scomponendoli nel loro DNA di base per verificare che non costituiscano una minaccia. Quest'analisi dettagliata viene effettuata in pochi millisecondi da un agente agile e leggero, che opera in maniera indipendente su ogni host senza dipendere da database di firme, accesso a Internet o connessione cloud.

Inoltre, BlackBerry Protect offre funzioni di controllo delle applicazioni e degli script, protezione della memoria e implementazione delle politiche sui dispositivi, che prevengono l'esecuzione di attacchi informatici. Questo approccio automatico alla protezione degli endpoint basato sull'intelligenza artificiale è in grado di eliminare il 99,1%[5] delle minacce, consentendo di destinare budget e risorse IT all'implementazione di altre strategie di sicurezza.

Una piattaforma di protezione degli endpoint basata sull'intelligenza artificiale deve contribuire per almeno il 90% alla strategia di sicurezza degli endpoint

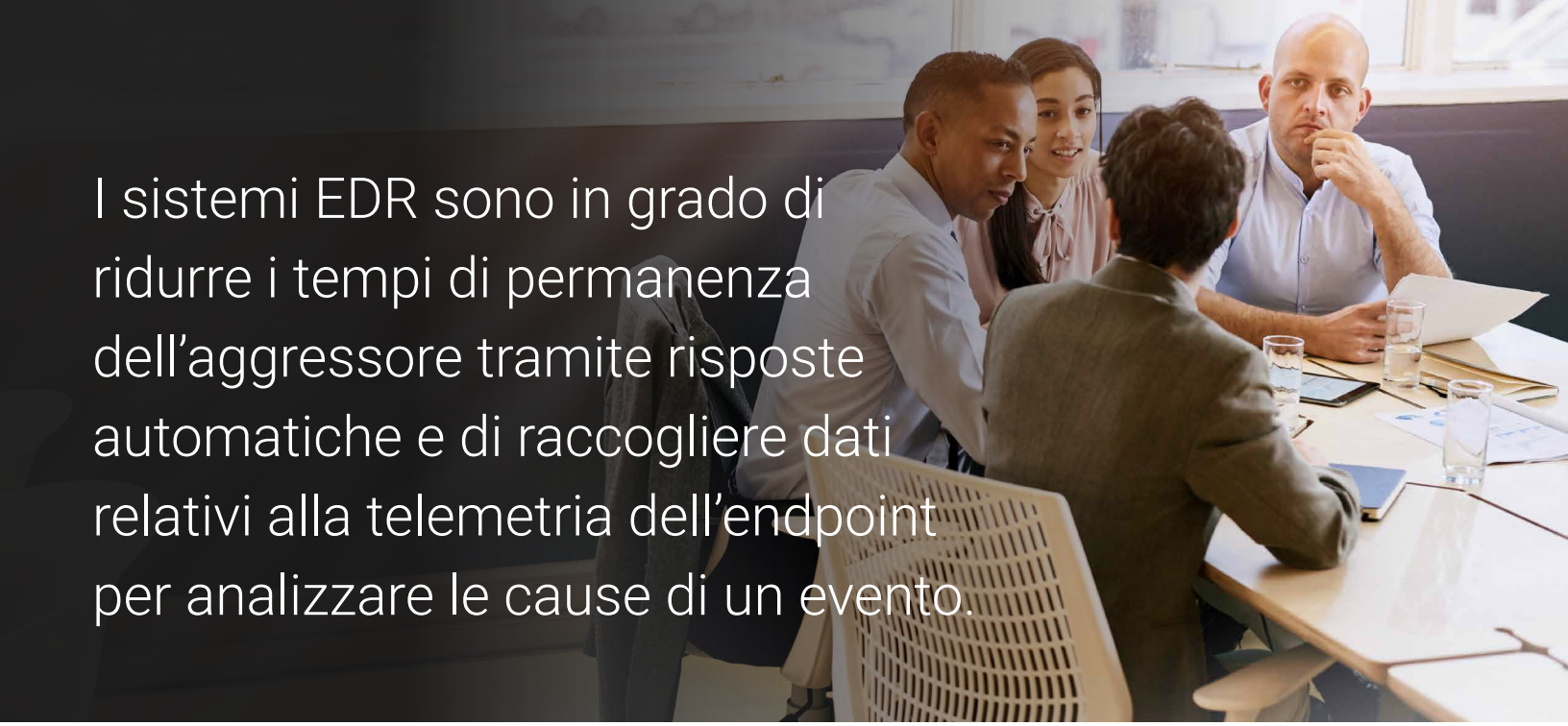


**Percentuale globale di minacce mitigate tramite diversi approcci alla sicurezza*

I vantaggi della prevenzione delle minacce basata sull'intelligenza artificiale

Scarica il nostro white paper, *BlackBerry vs. Traditional Security Approaches* per scoprire i vantaggi offerti dall'intelligenza artificiale nella prevenzione delle minacce e, se non hai ancora abbandonato il tuo antivirus legacy, valuta il passaggio a un sistema di prevenzione delle minacce basato sull'IA.

Sofisticati modelli di machine learning analizzano 2,7 milioni di proprietà dei file, scomponendoli nel loro DNA di base per verificare che non costituiscano una minaccia.



I sistemi EDR sono in grado di ridurre i tempi di permanenza dell'aggressore tramite risposte automatiche e di raccogliere dati relativi alla telemetria dell'endpoint per analizzare le cause di un evento.

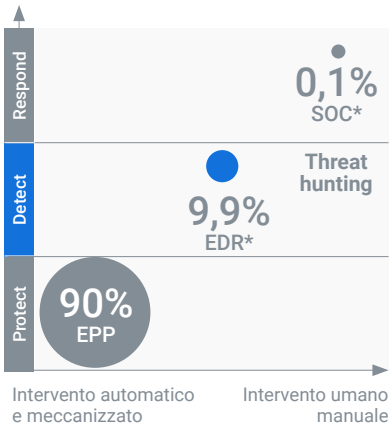
LIVELLO 2

Endpoint detection and response (EDR)

Le soluzioni di Endpoint detection and response (EDR) occupano il livello successivo del nostro quadro di riferimento per la sicurezza. I sistemi EDR sono in grado di ridurre i tempi di permanenza dell'aggressore tramite risposte automatiche e di raccogliere dati relativi alla telemetria dell'endpoint per analizzare le cause di un evento. Tuttavia, è importante considerare alcuni fattori per stabilire se un prodotto EDR è la soluzione giusta per la tua azienda.

- **Rapporto segnale/rumore:** può essere difficile distinguere i segnali di un attacco all'interno del rumoroso flusso di dati EDR. Un data point singolo potrebbe essere significativo soltanto in base al contesto in cui si trova e alla correlazione con altri eventi relativi alla sicurezza.
- **Implementazione a livello dell'endpoint:** molti prodotti EDR tradizionali fanno affidamento su analisi basate su cloud per rilevare le minacce. Tuttavia, le soluzioni EDR più avanzate sono ormai in grado di spostare i processi decisionali di rilevamento e risposta sull'endpoint stesso, eliminando ritardi capaci di trasformare un piccolo problema di sicurezza in un evento incontrollato ben più grave.
- **Infrangere le regole:** gli hacker sviluppano costantemente nuove TTP, progettate per aggirare i tradizionali sistemi EDR basati su regole e renderli altrettanto impotenti e obsoleti che le EPP basate su firma. Le moderne soluzioni EDR incorporano diversi metodi di riconoscimento, incluso il rilevamento delle minacce in base al contesto e la loro identificazione tramite machine learning.
- **Risposte automatiche coerenti:** le procedure di risposta e correzione devono essere avviate in automatico e azionate in maniera uniforme all'interno dell'ambiente.

Una soluzione EDR dovrebbe essere in grado di far fronte a quasi tutti i tipi di minacce che sfuggono a una EPP



**Percentuale globale di minacce mitigate tramite diversi approcci alla sicurezza*

I vantaggi di BlackBerry EDR

Per ulteriori informazioni sui vantaggi di una soluzione EDR basata sull'intelligenza artificiale, visita la nostra pagina dedicata o scarica il white paper intitolato *AI-Based Prevention: The Evolution of Endpoint Prevention and Detection*.

La creazione e il mantenimento di un SOC sono interventi costosi. Perciò, sono molti i fattori da considerare nel valutarne l'implementazione.

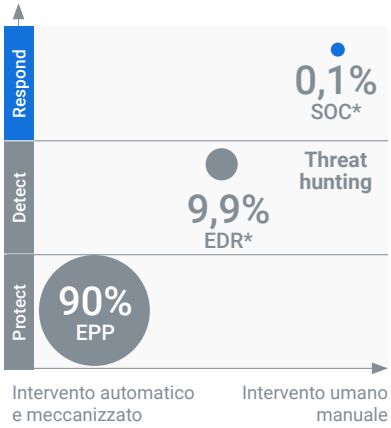
LIVELLO 3

Centro operativo per la sicurezza (SOC)

Il livello di efficienza successivo in materia di protezione è rappresentato dal centro operativo per la sicurezza (SOC), utilizzato principalmente da aziende che investono in maniera significativa in infrastrutture e personale al fine di ridurre il rischio di attacchi informatici e preservare l'agilità aziendale. Gli analisti del SOC selezionano e implementano i controlli di sicurezza, raccolgono e contestualizzano i dati relativi agli eventi, smistano gli allarmi, valutano gli indicatori di compromissione (IOC) e avviano i piani di risposta agli incidenti (IR) per contenere i danni di un attacco andato in porto. La creazione e il mantenimento di un SOC sono interventi costosi. Perciò, è importante che le aziende tengano conto dei seguenti fattori nel valutarne l'implementazione.

- **Disponibilità di personale esperto in materia di sicurezza informatica:** anche le aziende più grandi e floride faticano ad assumere e trattenere team SOC con il giusto mix di competenze ed esperienza in materia di sicurezza degli endpoint e dei perimetri, networking, programmazione e analisi forense. Secondo un recente studio effettuato da Frost and Sullivan[6], i due terzi delle aziende partecipanti hanno dichiarato di non disporre di un numero sufficiente di esperti di sicurezza informatica per coprire le proprie esigenze attuali, sintomo di una carenza di talenti nel campo che non accenna a diminuire. Di conseguenza, molti analisti SOC sono freschi di studi o relativamente poco esperti nell'affrontare sfide complesse legate alla sicurezza. Le problematiche di organico sono ulteriormente aggravate dalla necessità dei SOC delle aziende internazionali di operare 24/24 ogni giorno dell'anno, poiché gli hacker non osservano orari d'ufficio e spesso lanciano attacchi da località oltreoceano. Tenendo conto delle assenze per ferie e malattia, un team SOC completo dovrebbe disporre di almeno 12 o 15 analisti a tempo pieno solo per ottenere la copertura desiderata.
- **Analisti a rischio esaurimento per stress da allarmi frequenti:** gli analisti di un SOC sono esposti a forti livelli di stress e al rischio di esaurimento a causa dell'elevato numero giornaliero di allarmi di sicurezza da smistare. Un'azienda di grandi dimensioni può disporre anche di 50 soluzioni per la sicurezza diverse, che in totale

Un SOC non dovrebbe gestire direttamente in modalità manuale più dello 0,1% delle minacce



**Percentuale globale di minacce mitigate tramite diversi approcci alla sicurezza*

generano decine di migliaia di allarmi[7] ogni giorno. Secondo l'istituto di ricerca Ponemon[8], più della metà sono falsi positivi, che occupano gli analisti per 425 ore alla settimana in indagini inutili. Di conseguenza, il 44% degli allarmi non viene nemmeno analizzato per motivi di stanchezza e solo la metà dei restanti allarmi effettivi viene corretta, come svelato da un'indagine Cisco[9]. I moderni controlli di sicurezza sono in grado di ridurre significativamente il numero degli allarmi e migliorarne l'affidabilità, grazie ad avanzate tecniche di automazione e intelligenza artificiale e all'inclusione delle regole di rilevamento della procedura MITRE ATT&CK®. Tuttavia, per le aziende più piccole e con meno risorse potrebbe essere vantaggioso dal punto di vista economico adottare soluzioni gestite di rilevamento e risposta (MDR) offerte in abbonamento, come BlackBerry® Guard, che non richiede investimenti iniziali in software per la sicurezza e implementazione dei servizi.

- **Investimenti in piattaforme di big data:** gli analisti di un SOC devono poter accedere in qualsiasi momento agli eventi e ai dati sulla sicurezza, per tracciare le attività sospette e identificare gli hacker. A tale scopo, è necessario investire in piattaforme di big data in grado di estrapolare, analizzare, normalizzare e archiviare i dati di registro grezzi provenienti dai prodotti che gestiscono endpoint, server, difese perimetrali e reti aziendali. I costi di archiviazione possono crescere velocemente, sia che l'azienda decida di tenere i dati in loco, sia che scelga di utilizzare un servizio basato su cloud come Amazon Web Services. I dati più significativi possono quindi essere estratti dagli archivi log e inviati a una piattaforma per la gestione di eventi e informazioni sulla sicurezza (SIEM), dove vengono filtrati, contestualizzati, implementati tramite analisi e correlati ai dati provenienti da fonti di informazioni esterne sulle minacce informatiche come VirusTotal. Anche i costi delle soluzioni SIEM possono crescere rapidamente, poiché diversi fornitori formulano i propri prezzi in base al numero potenziale di eventi captati al secondo. I team SOC devono monitorare e gestire tali piattaforme per accertarsi che i dati vengano costantemente aggiornati e validati.
- **L'importanza fondamentale di piani e procedure di risposta agli incidenti:** troppo spesso le aziende investono in infrastrutture e organico per un SOC, ma sottovalutano l'importanza di sviluppare piani e procedure di risposta agli incidenti, una mancanza che equivale a inviare un esercito in battaglia senza piano d'attacco. Infatti, secondo uno studio Telstra del 2018[10], un quarto degli intervistati non aveva o non sapeva se aveva un piano IR. Tale piano deve specificare ogni singola azione da intraprendere in caso di incidente, a partire dalla nomina dei membri di un team IR. Solitamente, questo team include sia i migliori analisti del SOC che il personale di sicurezza di grado più elevato, con esperienza nella raccolta di prove, indagini forensi su endpoint e rete, e analisi di malware; il gruppo è guidato da un manager, che fornisce aggiornamenti sullo stato della sicurezza ai principali stakeholder in ambito commerciale e tecnologico. Le procedure IR devono essere sufficientemente precise da definire le modalità di accesso a dati di rete, memoria e disco rigido, nonché le decisioni da prendere una volta che i sistemi compromessi sono stati individuati. Per esempio, le procedure devono specificare se occorre portare il sistema offline o lasciarlo connesso per conservare l'accesso ai dati di rete. Tutti i criteri alla base di tali procedure e decisioni vanno stabiliti a priori tramite una stretta collaborazione tra la direzione aziendale (inclusi i responsabili della sicurezza informatica), gli specialisti della sicurezza sufficientemente esperti e i proprietari delle applicazioni o dei dati coinvolti. I professionisti del settore della sicurezza hanno il compito di fornire input di natura tecnica, ma i piani di IR devono essere redatti in base agli obiettivi strategici e alla propensione al rischio dell'azienda, piuttosto che fondarsi su best practice teoriche in materia di sicurezza. Infine, è importante che tutte le persone coinvolte, dai dirigenti ai responsabili interni, accettino i rischi e i risultati derivanti dalle decisioni relative all'IR.

Stress da allarmi frequenti

50

soluzioni di sicurezza

×

migliaia di avvisi

425

ore perse

44%

degli allarmi non analizzato a causa dello stress da allarmi frequenti

LIVELLO 4

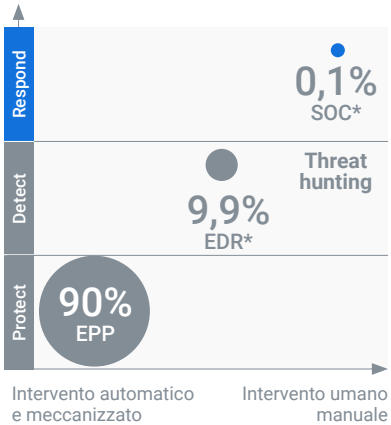
Threat hunting

La ricerca delle minacce rappresenta il quarto e ultimo livello del nostro quadro di riferimento per la sicurezza. A questo stadio di sviluppo, le aziende più mature e di successo raggiungono un approccio alla sicurezza basato sulla prevenzione, che consente di deviare e/o neutralizzare automaticamente oltre il 90% delle minacce. Le politiche di sicurezza vengono implementate tramite efficaci procedure di controllo e le piattaforme di big data raccolgono e contestualizzano i dati per la gestione degli allarmi e l'analisi postincidente. I piani e le procedure di risposta agli incidenti sono ben definiti e garantiscono una correzione rapida ed efficace di violazioni anche gravi.

Tali risorse consentono agli analisti esperti con competenze specifiche di dedicarsi alla ricerca proattiva di prove di attacchi precedentemente non rilevati. I cosiddetti 'threat hunter', i cacciatori di minacce, sfruttano processi basati su informazioni e metodologia per individuare eventi di sicurezza anomali e pattern comportamentali che, combinati tra loro, indicano la possibile presenza di un hacker in uno o più punti della kill-chain. Nonostante qualsiasi azienda possa trarre beneficio da una ricerca attiva delle minacce, è bene tenere conto dei seguenti requisiti prima di investire in questa attività.

- **Obiettivi priorizzati in base al rischio:** la ricerca delle minacce utilizza gli stessi metodi di prova basati su ipotesi iterative delle indagini scientifiche. Per esempio, per sondare l'ipotesi che sia in atto un'esfiltrazione di dati, è possibile ricercare indicatori di compromissione associati a flussi di rete anomali o ad accessi ai dati e comportamenti sospetti da parte degli utenti finali. Gli obiettivi dei threat hunter devono essere definiti in anticipo e priorizzati in base al profilo di rischio e alle strategie aziendali.

La ricerca delle minacce è una procedura ad alto valore aggiunto ma prevalentemente manuale che consente di gestire la piccola percentuale di attività maligne non coperta da soluzioni EDR e EPP



**Percentuale globale di minacce mitigate tramite diversi approcci alla sicurezza*

- **Difficoltà di reclutamento e mantenimento dell'organico:** la scarsa disponibilità di personale specializzato nel campo della sicurezza su scala mondiale è ancora più acuta nel caso degli analisti con il giusto mix di esperienza e competenze richiesto per la ricerca delle minacce. Per le aziende è quasi impossibile reclutare e trattenere theat hunter esperti, attirati dai salari più elevati e dalle migliori condizioni di lavoro offerti talvolta dagli MSSP e dalle aziende di consulenza in materia di sicurezza.
- **Miglioramento delle competenze e addestramento continuo:** così come le aziende sviluppano costantemente il proprio core business per ottimizzare i profitti, anche gli hacker aggiornano di continuo le proprie TTP e i vettori di attacco. Per mantenere lo status quo, le aziende sono obbligate a investire in addestramento continuo, per assicurarsi che i loro threat hunter dispongano delle conoscenze e competenze in campo tecnico e settoriale necessarie ad affrontare i rischi legati all'evoluzione di obiettivi e processi aziendali e delle superfici di attacco.
- **Timore di esposizione dei dati interni:** talvolta, le aziende che non dispongono di personale interno addetto alla ricerca attiva delle minacce diffidano di analoghi servizi offerti da terzi, per paura di esporre i propri dati a rischi sconosciuti e inaccettabili.

Garantire la massima sicurezza è un processo continuo

Speriamo che il nostro sistema di riferimento per la sicurezza a quattro livelli ti abbia aiutato a stimare le esigenze presenti e future della tua azienda. Ciascun livello presenta nuove e importanti possibilità di potenziamento della sicurezza aziendale. Tuttavia, non occorre che tutte le aziende dispongano di soluzioni a tutti e quattro i livelli o che cerchino di sviluppare risorse interne adeguate.

Se la tua azienda è di piccole o medie dimensioni, investire in un SOC per lo smistamento degli allarmi o implementare una piattaforma di big data per facilitare la ricerca delle minacce sarebbe probabilmente poco pratico. Al contrario, potrebbe essere conveniente sfruttare le risorse e le competenze offerte da servizi di MDR e threat hunting come BlackBerry Guard, oltre a stipulare accordi per il mantenimento di rapporti di consulenza per test periodici di penetrazione e valutazioni della risposta agli incidenti. Altre aziende ancora possono trarre vantaggio dall'affidamento di funzioni SOC di routine a un MSSP esterno, in modo che il proprio organico possa concentrarsi sui progetti in materia di sicurezza a supporto degli obiettivi aziendali. Come sempre, a contare è la qualità del lavoro, e non la fonte delle competenze. Ma soprattutto, per garantire alla tua azienda la massima protezione, è necessario attenersi a un programma continuo di auto-miglioramento della sicurezza informatica e di gestione responsabile del rischio.

Ulteriori informazioni

Per ulteriori informazioni sulla soluzione di MRD e threat hunting BlackBerry Guard, visita *la nostra pagina dedicata* o *scarica la scheda dati*.

Ulteriori informazioni

BlackBerry è pronta a diventare tuo partner, grazie a un ampio portfolio di soluzioni e servizi adatti a qualsiasi livello inziale di sicurezza aziendale.

BlackBerry Protect offre una protezione dai malware supportata dall'intelligenza artificiale, associata a controllo delle applicazioni e degli script, protezione della memoria e implementazione delle politiche sui dispositivi, che consente di individuare le minacce e prevenirne l'esecuzione.

BlackBerry® Optics è una soluzione EDR che estende la protezione dalle minacce offerta da BlackBerry Protect tramite un sistema di prevenzione degli incidenti basato sull'intelligenza artificiale, l'analisi delle cause, la ricerca intelligente delle minacce e funzioni di rilevamento e risposta automatiche.

BlackBerry Guard è una soluzione MDR offerta in abbonamento che sfrutta la nostra piattaforma nativa di intelligenza artificiale e il supporto 24/7 del team esperto di prevenzione e risposta agli incidenti di BlackBerry.

Valutazioni della prontezza di risposta agli incidenti: il nostro team ti aiuterà a sviluppare un piano IR e una serie di procedure in linea con i tuoi obiettivi di gestione del rischio, consentendoti anche di dimostrare la conformità alle regolamentazioni in materia.

Contenimento degli incidenti e indagini forensi: in caso di incidente, ti aiuteremo a tracciarlo, contenerlo e porvi subito rimedio, prima che si trasformi in una violazione grave.

Servizi red team: individueremo lacune e vulnerabilità dell'infrastruttura di sicurezza che porrebbero essere sfruttate da aggressori interni o esterni.

1 Per ulteriori informazioni, scarica il nostro eBook dal titolo *Artificial Intelligence: The Smarter Approach To Information Security*.
2 *5 Cybersecurity Statistics Every Small Business Should Know in 2018*. Alert Logic.
3 Signatures Can't Keep Up
4 *The Numbers and Results Don't Lie*
5 *NSS Labs Advanced Endpoint Protection: Cylance Security Value Map,* aprile 2018. La soluzione BlackBerry Protect era precedentemente nota come CylancePROTECT®.
6 *2017 Global Information Security Workforce Study (GISWS)*
7 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence*. L'articolo cita lo studio Ponemon "The Cost of Insecure Endpoints"
8 *Dark Reading. Fighting Alert Fatigue with Actionable Intelligence*. L'articolo cita lo studio Ponemon "The Cost of Insecure Endpoints"
9 *Cisco 2018 Annual Cybersecurity Report* | The defender landscape.
10 *Telstra Security Report 2018.*

Informazioni su BlackBerry

BlackBerry (NYSE: BB; TSX: BB) è un fornitore di servizi e software di sicurezza intelligente a cui si affidano imprese e governi di tutto il mondo. L'azienda gestisce la sicurezza di oltre 500 milioni di endpoint, tra cui 150 milioni di autovetture che percorrono ogni giorno le nostre strade. BlackBerry, che ha sede a Waterloo, in Ontario, sfrutta l'IA e il machine learning per fornire soluzioni innovative nel campo della sicurezza, informatica e fisica, e della protezione dei dati. Inoltre, è leader nei settori della gestione della sicurezza degli endpoint, della crittografia e dei sistemi integrati. La vision di BlackBerry è chiara: garantire un futuro sicuro, connesso e affidabile.

Per maggiori informazioni, visita BlackBerry.com e segui @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MK20-0266 | 200720