Kaspersky Enterprise Cybersecurity

KASPERSKY lab

Guida all'acquisto sull'investimento in Endpoint Detection and Response per le imprese 2017-2018

www.kaspersky.it
#truecybersecurity

Sommario

Introduzione

Uno dei principali obiettivi aziendali di ogni organizzazione è quello di mantenere costante la disponibilità dei dati e dei sistemi che possono essere considerati attendibili ai fini dei processi decisionali. Il panorama in continua evoluzione delle minacce sta portando a una maggiore attenzione, fino a raggiungere il board aziendale, nei confronti della cybersecurity. I team operativi e per la sicurezza IT dovrebbero dimostrare un approccio tanto completo quanto coeso nella sua risposta agli incidenti di sicurezza e alle violazioni dei dati.

La cybersecurity è ora una delle prime 3 priorità riconosciute dal senior managment nella sua ricerca della continuità aziendale per condurre l'agenzia al successo.

Oggi i leader aziendali hanno bisogno di conoscere il panorama delle cyberminacce specifiche per le loro organizzazioni. Le domanda che dovrebbero porsi sono le seguenti:

- La mia azienda comprende quali sono le minacce e i rischi per la sicurezza principali per il nostro settore e per noi stessi?
- Possiamo rilevare e fermare rapidamente i cyberattacchi?
- Come possiamo posizionare la riduzione dei rischi informatici all'interno della nostra strategia generale di sviluppo aziendale?

Gli endpoint in prima linea

Gli endpoint aziendali (i server, le workstation, i telefoni cellulari ecc.) sono dove ha luogo quella sinergia tra i dati, gli utenti e i sistemi delle aziende che generano e implementano i processi aziendali. E questa miriade di singoli dispositivi rimane l'elemento chiave in qualsiasi network, sia da un punto di vista aziendale sia di sicurezza.

Per proteggere questi endpoint, e per evitare che diventino un punto di accesso illecito nell'infrastruttura, i team per la sicurezza delle informazioni dovrebbero adottare processi e tecnologie associati con il rilevamento avanzato, la ricerca delle minacce, la scansione degli IoC, l'analisi del malware, l'analisi forense degli incidenti, l'implementazione della threat intelligence e lo stabilimento di un processo formale di risposta agli incidenti.

Ma da dove iniziare? Passare all'apprendimento automatico avanzato? Migliorare la ricerca delle minacce? Concentrarsi sulla crescita del monitoraggio e del SOC? Meglio forse coprire queste aree, e altre, con una delle nuove soluzioni di Endpoint Detection and Response (EDR). Ma che cosa ci si può aspettare esattamente dall'EDR e qual è il tipo di soluzione che si dovrebbe scegliere?

Questo documento può aiutare a scegliere la soluzione EDR più adatta. Il nostro obiettivo è di evidenziare le differenze essenziali tra i vari tipi di funzionalità di EDR disponibili sul mercato e di aiutare a identificare le tecnologie più valide ad assicurare la continuità aziendale e la sicurezza nell'organizzazione.

Tutto su Endpoint Detection and Response

Un nuovo approccio alla sicurezza degli endpoint

Per prevenire gli attacchi, proteggere il proprio perimetro. È sempre suonato ragionevole: se il perimetro IT è ben difeso, la protezione degli endpoint diventa un livello in più nella strategia complessiva di sicurezza.

Questo approccio, però, non è sufficiente in un mondo in cui, grazie a tecnologie come i dispositivi mobili, i dispositivi connessi (IoT) e il cloud computing, definire e tanto meno difendere il perimetro IT diventa una vera e propria sfida in cui l'evoluzione delle minacce ha reso la difesa basata sui perimetri un approccio obsoleto.

Gli attacchi mirati, il forte aumento delle tecniche di penetrazione complesse, il malware fileless e l'utilizzo di software legittimo, il furto delle credenziali di utenti normali, l'utilizzo di diritti legittimi, lo sfruttamento dei problemi nei criteri di sicurezza e degli errori di configurazione: tutti questi hanno portato le organizzazioni a riconoscere l'importanza delle soluzioni e delle strategie di sicurezza integrate. Questo a sua volta ha portato alla crescita dell'implementazione SIEM e dei SOC (Security Operational Centers). La cybersecurity aziendale è diventata (per necessità) proattiva, poliedrica e altamente specializzata.

Il mondo sta cambiando ed è pronto ad abbracciare un nuovo paradigma di sicurezza degli endpoint. Il focus è ritornato sugli endpoint. Ci sono sempre stati dipartimenti IT lungimiranti che hanno trattato gli endpoint come se ognuno richiedesse il proprio perimetro di sicurezza. E' a causa delle organizzazioni che **non** hanno adottato questo approccio, che gli endpoint non hanno mai smesso di essere il principale obiettivo iniziale dei cybercriminali.

Diventare più proattivi

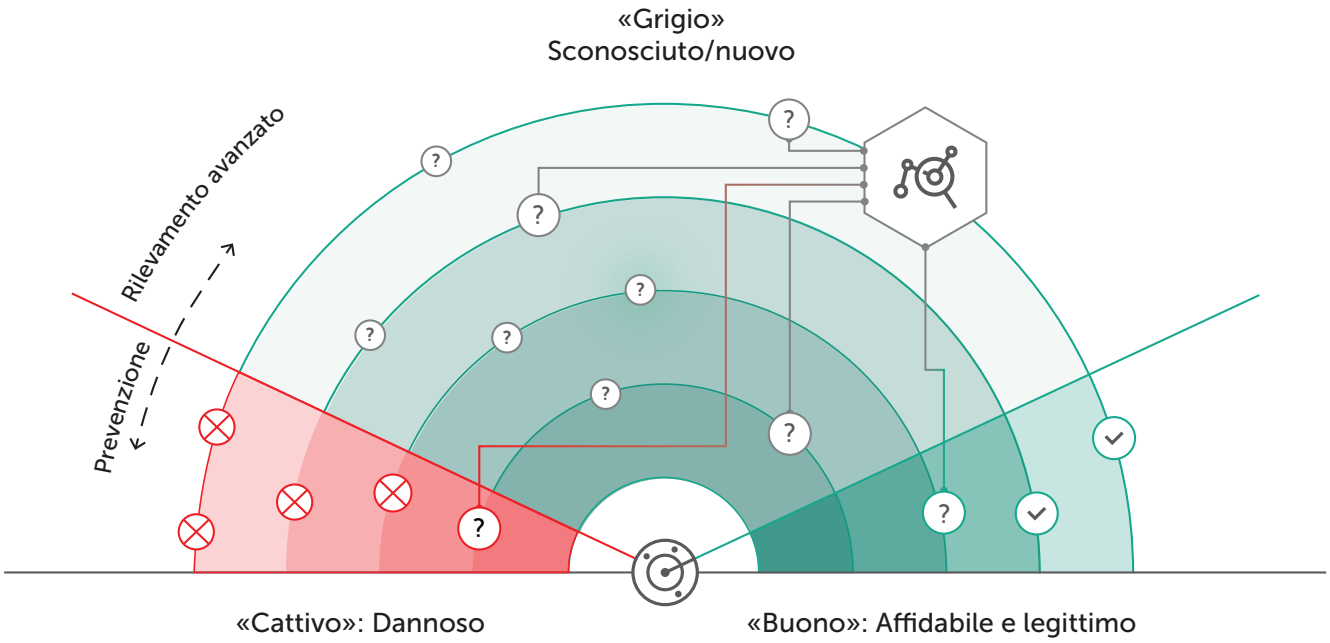
Nel frattempo, le autorità di controllo stanno introducendo nuovi requisiti (GDPR, PCI DSS ecc.) che possono richiedere continuamente il monitoraggio e la registrazione degli incidenti su ogni endpoint della rete. Per la maggior parte delle imprese, il numero di eventi/incidenti registrati dalla loro attuale soluzione di sicurezza continua ad aumentare, tanto che la verifica e l'analisi di ogni evento registrato diventa di per sé un problema. E non è di grande aiuto il fatto che gli esperti di sicurezza che possano gestire queste attività, con le competenze necessarie in campo di reverse engineering, analisi del malware, analisi forense digitale e risposta agli incidenti, non sono molti e sono difficili da trovare.

A questo punto, la maggior parte dei processi di sicurezza che si concentrano sulle minacce avanzate e la maggior parte degli approcci di monitoraggio dei SOC sono essenzialmente reattivi e guidati dagli allarmi. I security officers aspettano la prova di una violazione prima di allertare i security analyst e solo dopo l'incident response team può agire. Nel migliore dei casi, i responder agli incidenti identificano gli artefatti di un attacco nell'ultima fase della catena criminale: nel peggiore dei casi, invece, semplicemente aspettano di contare i danni, a volte mesi dopo che i sistemi sono stati violati. Una situazione del genere è chiaramente insoddisfacente. Per questo motivo le organizzazioni stanno rivedendo i loro processi di sicurezza, in particolare in termini tanto di rilevamento quanto di risposta degli incidenti.

In che modo questo influisce sulle soluzioni per gli endpoint?

La generazione più recente di soluzioni per gli endpoint si concentra sul rilevamento efficace di nuove minacce che colpiscono l'organizzazione, sul pattugliamento e sull'analisi degli eventi in quella "zona grigia" in cui potrebbero essere in agguato minacce sconosciute e indefinite: si tratta della ricerca delle minacce ("threat hunting").

Ricerca delle minacce: aiutare a scoprire le minacce avanzate che si nascondono all'interno dell'organizzazione, utilizzando funzionalità proattive di ricerca delle minacce e incaricando professionisti della sicurezza altamente qualificati ed esperti.



Oltre la protezione degli endpoint

Una ricerca efficace delle minacce è direttamente collegata alle capacità di un SOC maturo. L'aggiornamento delle soluzioni di sicurezza acquistate non è sufficiente. Non si possono semplicemente imporre nuovi requisiti alle tradizionali soluzioni EPP (Endpoint Protection, protezione degli endpoint) in quanto questi non si adatteranno o non funzioneranno in modo efficace.

Si guardi ad alcune questioni chiave risolte in modo efficace dall'EPP tradizionale e alle nuove sfide che la sicurezza degli endpoint affronta ora:

Problemi di controllo e protezione, risolti dalle soluzioni EPP tradizionali:	Nuove sfide avanzate per la sicurezza degli endpoint:
Come proteggersi automaticamente (prevenzione e rollback) dalle minacce esistenti, compresi ransomware e crypto-locker	Come cercare attivamente prove di intrusioni, come gli indicatori di compromissione su tutta la rete in tempo reale
Come gestire centralmente e applicare controlli di sicurezza per il Web, le app e i dispositivi	Come rilevare e correggere un'intrusione prima che l'aggressore abbia la possibilità di arrecare un danno significativo
Come gestire centralmente la valutazione delle vulnerabilità e i processi di gestione delle patch	Come correlare gli avvisi dei controlli di sicurezza della rete per comprendere ciò che sta accadendo nell'endpoint in tempo reale
Come proteggere i dati aziendali e le informazioni sui dispositivi	Come convalidare gli avvisi e i potenziali incidenti rilevati dalle soluzioni di sicurezza
Come distribuire criteri di protezione del Web e delle e-mail a livello di endpoint	Come indagare e gestire centralmente e in modo rapido gli incidenti di gestione su migliaia di endpoint
Come fornire agli utenti degli endpoint set specifici di livelli di sicurezza fatti su misura per le loro esigenze	Come rendere il processo di risposta agli incidenti (lavoro manuale, competenze di livello 3, sovraccarico avvisi ecc.) meno costoso automatizzando le operazioni di routine per il team di sicurezza.

Come si possono affrontare queste nuove sfide?

Strategia di cybersecurity degli endpoint: adattiva, avanzata, predittiva

Più difficili da rilevare e, spesso, più complicati da eliminare, gli attacchi mirati e le minacce avanzate richiedono una strategia di sicurezza adattiva e completa.

Uno dei framework di sicurezza adattivi più efficaci si fonda sull'architettura di sicurezza fattibile descritta da Gartner. Il suo approccio è quello di fornire un ciclo di attività in quattro aree chiave: prevenzione, rilevamento, risposta e previsione.

- **Prevenzione**: sia bloccando le minacce comuni sia rafforzando i sistemi principali per ridurre il rischio di minacce avanzate
- **Rilevamento**: scoprire rapidamente le attività che potrebbero segnalare un attacco mirato o una violazione in corso
- **Risposta**: contenere precisamente la minaccia, condurre indagini e rispondere in modo adeguato agli attacchi
- **Previsione**: sapere dove e in che modo potrebbero manifestarsi nuovi attacchi mirati

Modello di sicurezza adattiva

Essenzialmente, questo presuppone che la prevenzione tradizionale, specialmente per gli endpoint, dovrebbe funzionare in coordinazione con le tecnologie di rilevamento avanzate, le analisi delle minacce, le capacità di risposta e le tecniche predittive di sicurezza. Il risultato che ne scaturirà è un sistema di cybersecurity che si adatta continuamente e risponde alle nuove sfide aziendali.

Le tecnologie multilivello basate sulla prevenzione costituiscono un elemento chiave per questo nuovo approccio proattivo che mira a difendere l'azienda dagli attacchi mirati. Ma se l'autore dell'attacco è altamente motivato o persino ingaggiato da una terza parte per condurre un attacco, una prevenzione basata su un unico approccio non sarà sufficiente. È necessario essere in grado di identificare le minacce, prendere decisioni e prevedere possibili penetrazioni in modo rapido, semplificando allo stesso tempo le operazioni manuali e automatizzando gli strumenti di risposta.

Definizione di EDR

Caratteristiche principali di una soluzione simile all'EDR

Come visto in precedenza, Gartner definisce le soluzioni EDR con le seguenti funzionalità principali:

- rilevare gli incidenti di sicurezza
- contenere l'incidente a livello dell'endpoint, in modo tale che il traffico di rete o l'esecuzione di un processo possano essere controllati in remoto
- indagare sugli incidenti di sicurezza
- ripristinare gli endpoint a uno stato precedente all'infezione

Rilevamento degli incidenti sugli endpoint

È possibile rilevare gli incidenti di sicurezza **monitorando le attività** degli endpoint e gli oggetti, le violazioni dei criteri o convalidando indicatori di compromissione alimentati esternamente (IOC)

Indagini sugli incidenti

È possibile esaminare gli incidenti alla sicurezza. La funzione di indagine dovrebbe includere una sequenza **temporale cronologica** di tutti gli eventi principali degli endpoint per verificare se siano avvenuti cambiamenti tecnici e quali effetti abbiano prodotti.

(inoltro dei privilegi, diffusione, estrazione, geolocalizzazione di C&C e attribuzione dell'avversario se possibile)

Isolamento degli incidenti e risposta

È possibile **isolare** l'incidente all'endpoint e **correggere** gli stessi a uno stato precedente all'infezione.

È possibile rimuovere i file dannosi, eseguire il rollback e correggere altre modifiche oppure creare istruzioni di correzione che possono essere rese disponibili per l'implementazione su altri strumenti

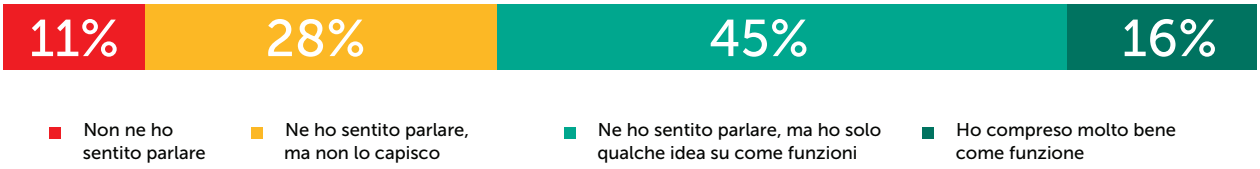
Raccolta di dati forensi

È possibile **raccogliere** set di dati, dati estratti dalla RAM, snapshot del disco rigido per ulteriori analisi

Quanto a fondo comprendono le organizzazioni il funzionamento dell'EDR e come contribuiscono queste tecnologie alla continuità aziendale? Un sondaggio di Kaspersky Lab condotto tra le organizzazioni aziendali lungo il 2016 ha prodotto alcuni risultati preoccupanti.

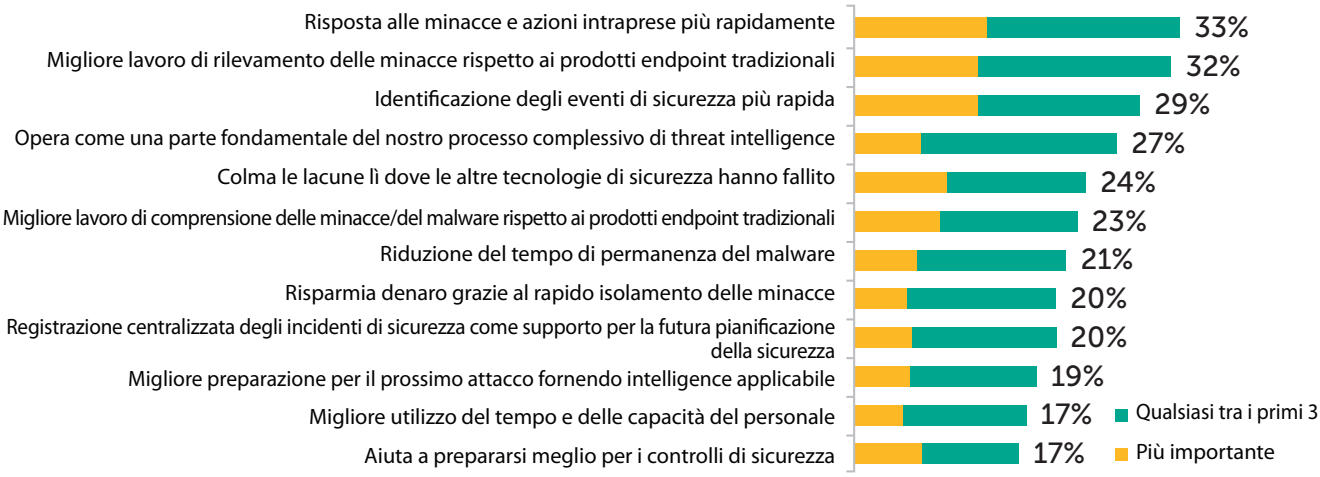
Domanda del sondaggio: "Quanto a fondo conosci la classe di soluzioni EDR?"

Risposta:



Fonte: Esperti IT in aziende con oltre 250 dipendenti

Allo stesso tempo, i rappresentanti aziendali intervistati hanno formulato in modo chiaro le nozioni base sulle loro aspettative e sui risultati che vorrebbero ottenere dall'uso di soluzioni EDR nelle loro organizzazioni:



Questa combinazione tra comprensione limitata e aspettative chiare è preoccupante. I fornitori di soluzioni EDR sono ovviamente interessati a soddisfare queste aspettative, sviluppando "funzionalità letali" che, nella fase pilota, promettono molto e sembrano entusiasmanti, ma che spesso risultano molto meno pratiche e convenienti quando incorporate nel processo del cliente.

Di conseguenza, in alcuni ambienti, l'EDR viene già visto con sospetto.

La salita e il declino delle soluzioni di Endpoint Detection and Response

I primi utenti che hanno adottato soluzioni EDR non sono sempre, purtroppo, i più grandi fan delle tecnologie. Con molte delle prime soluzioni EDR ci sono stati diversi limiti e questo ha portato alla delusione e alla frustrazione di alcuni clienti.

Purtroppo, non vi è ancora un'analisi comparativa stabilita o un report indipendente che esponga tutte le funzionalità chiave e le possibili variazioni delle tecnologie EDR disponibili oggi sul mercato. E molti prodotti "di prima generazione" in questo mercato ancora immaturo inizialmente non sono stati in grado di fornire nella pratica ciò che gli esperti e le organizzazioni si aspettavano.

La maggior parte delle soluzioni hanno iniziato con alcune "funzionalità letali" piuttosto che con caratteristiche complesse. Anziché una soluzione integrata in grado di unificare e automatizzare la threat intelligence per la sicurezza della rete, la ricerca delle minacce, l'anti-malware, la risposta agli incidenti e la capacità di analisi forense, EDR ha dimostrato nella pratica di essere un set di strumenti di analisi e ricerca. E questo toolkit di tecnologie è risultato essere sia costoso per ciò che effettivamente era, sia estremamente difficile da gestire per il professionista della sicurezza medio.

Alcune soluzioni EDR, inoltre, non sono riuscite a mantenere le promesse di efficienza. Quando si risponde a un incidente di malware, una soluzione EDR raccoglierà informazioni dagli endpoint (firme e comportamento del malware) che possono essere utilizzate per identificare infezioni future. Ma se la soluzione non è strettamente integrata con le tecnologie di rilevamento e con i sistemi di sicurezza, vi è un elevato rischio di sovrapposizione e duplicazione, che genera in realtà più processi manuali e ostacola il flusso di lavoro, anziché migliorare l'efficienza e l'efficacia. L'EDR diventa semplicemente un'ulteriore area di archiviazione di dati sulla sicurezza, che non possono di per sé dare informazioni su come l'evento si sia originato o su come impedirne la ricomparsa. Senza una risoluzione dei casi alla radice, integrata nel flusso di lavoro, un'organizzazione non può porre un rimedio una volta per tutte e ridurre il rischio di una reiterazione.

Un'altra carenza è stata che alcune soluzioni inizialmente sul mercato non erano realmente progettate per scoprire o investigare le Advanced Persistent Threat (APT). Per poter fare ciò, i proprietari delle soluzioni EDR hanno ancora bisogno di esternalizzare le attività a esperti (possibilmente appartenenti al fornitore) o di acquistare costosi corsi di formazione supplementari. Se si dovesse ingaggiare un team di risposta agli incidenti esterno ogni volta che viene identificata una violazione, si potrebbe ragionevolmente dubitare della convenienza della soluzione EDR originale.

Una tendenza crescente è stata l'utilizzo di versioni cloud di EDR, con il trasferimento di determinati registri e dati sul cloud del vendor piuttosto che tenerli su agenti installati o in una repository centralizzata. Tuttavia, questo tendeva a portare all'insorgenza di diversi incedenti, con tempi di risposta più lenti (e talvolta senza risposta affatto).

Gran parte di queste situazioni, però, fanno parte del passato e chi sta valutando attualmente il mercato EDR non dovrebbe giudicare i potenziali risultati del loro investimento sulla base delle esperienze dei primi pionieri. Oggi, infatti, il mercato è cresciuto ed è diventato più maturo.

Dunque che cosa si dovrebbe cercare nell'EDR oggi e cosa dovrebbe essere preso in considerazione? Si considerino 5 sfide che è necessario considerare quando si avvia il proprio progetto di EDR.

Le prime 5 sfide che si affrontano quando si avvia un progetto EDR

È inevitabile che ci saranno nuove sfide per le organizzazioni che si affidano a qualsiasi nuova tecnologia o a processi sconosciuti. E poiché le soluzioni EDR sono più costose rispetto alle loro controparti EPP tradizionali, il che giustifica l'investimento nell'EDR in termini di valore aggiunto, confrontarli con i costi di uno strumento SIEM o con strumenti di analisi forense, ad esempio, può essere un'operazione complessa.

La funzione principale di un EDR di livello enterprise è **quella di supportare il team per la sicurezza con indagini basate sulle domande:** i suggerimenti per la ricerca, per ottenere la visibilità, sono interattivi e iniziano con domande o ipotesi. Una domanda o ipotesi iniziale potrebbe essere basata sui passaggi della cyber kill chain e potrebbe essere simile a "è in corso un'estrazione di dati o una comunicazione dannosa?" o "se vi è in corso una connessione sospetta a domini esterni, è più probabile che avvenga attraverso questa parte della rete, ma da quale endpoint e processo?".

Al fine di fornire queste capacità, la soluzione EDR deve avere **funzionalità di indagine-assistenza** nonché di **raccolta di dati** e **funzioni di archiviazione**. E il **rilevamento degli incidenti** dovrebbe incorporare elementi sia automatici sia manuali. Ultimo, ma non per importanza: appena viene rilevato un incidente iniziale, il team per la sicurezza e i responder alle minacce dovrebbero essere attrezzati per **contenere agevolmente** la minacce, **correggere** gli endpoint e **prevenire** che l'attività specifica si verifichi di nuovo.

Si dia uno sguardo a 5 sfide comuni che le organizzazioni dovrebbero prendere in considerazione quando scelgono soluzioni EDR avanzate, o in generale quando vogliono migliorare la propria sicurezza degli endpoint in termini di rilevamento e risposta.

Dati endpoint: troppa visibilità

La protezione degli endpoint in qualsiasi forma inizia con la raccolta di nuovi dati, la loro archiviazione e analisi. Teoricamente, maggiore è la quantità di dati che è possibile raccogliere, maggiore sarà il vantaggio. Lo stesso principio è utilizzato anche per essere applicato ai sistemi SIEM. Ma, per interpretare grandi volumi di dati raccolti, l'operatore EDR ha bisogno anche di contesto rilevante. Per esempio, la scoperta rapida di una connessione dannosa a un dominio non valido è di valore considerevolmente inferiore se non si sa da quale endpoint sia originata, in che modo sia stato avviato il processo, quale sia stata la causa principale e quali risorse possano già essere state colpite.

Le soluzioni EDR immature sul mercato raccolgono alcuni dati ma non forniscono il contesto giusto. Queste possono, ad esempio, consentire ad un operatore di scoprire rapidamente quali macchine archiviano un file con un determinato valore hash, senza fornire informazioni sul modo in cui il file si trovi a essere su queste macchine. Si può fornire un elenco dei processi generati relativi all'oggetto e alle attività, ma senza alcuna visualizzazione. Oppure si possono fornire avvisi complessi su comportamenti atipici o deviazioni, ma senza le scansioni di base e i rapporti.

Alcune soluzioni raccolgono tutti i dati dagli endpoint, poi li presentano direttamente nell'interfaccia, come una finestra diretta nel database. A meno che l'operatore non sia uno scienziato dei dati o un campione dei big data, o un esperto della sicurezza, non sarà in grado di prendere una decisione sulla base di questi dati non elaborati.

Spesso tali sistemi generano migliaia di messaggi e letteralmente milioni di avvisi, che devono tutti essere convalidati da qualcuno. Anche nelle organizzazioni di maggiori dimensioni, è improbabile che il team per il monitoraggio e la risposta sia in grado di gestire più di 50-60 incidenti dalla criticità medio-alta in qualunque momento. Come risultato, abbiamo una soluzione che trova tutto, ma poco o nulla può effettivamente essere fatto su ciò che viene trovato: c'è semplicemente troppo, e non abbastanza, da vedere.

Un compromesso potrebbe essere condividere gli avvisi tra il proprio team per la sicurezza e un MSSP esterno, tuttavia sarà necessario trovare un fornitore con la giusta formazione e competenza. E senza la giusta priorità agli incidenti si potrebbe avere un enorme investimento e spreco di risorse sugli avvisi non critici. Un problema aggiuntivo, come con qualsiasi MSSP, è la questione della fiducia, la riservatezza dei dati e le restrizioni di conformità.

Raccomandazioni:

- Cercare soluzioni che non solo consentano di esporre automaticamente i rischi attraverso gli avvisi, ma che consentano anche una personalizzazione profonda (configurazione di ruoli utente differenti, assegnazione di gruppi VIP, configurazione rapida delle whitelist). Questo permetterà di dare la giusta evidenza alle cose importanti, ridurre ciò che è inutile e verificare che solo le informazioni critiche siano visibili a qualsiasi MSSP esterno.
- Pensare fino a che punto ci si aspetta di condurre le analisi dei dati all'interno dell'organizzazione e quanti dati ci si aspetta di archiviare ed elaborare. Prepararsi alla consegna di terabyte di dati in-house può significare spese non indifferenti per hardware aggiuntivi.

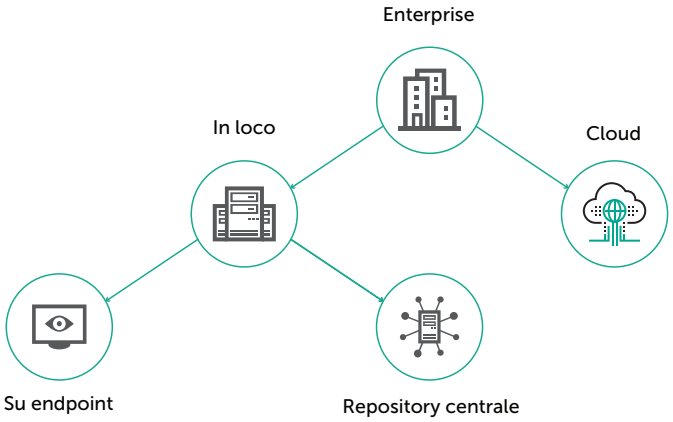
2

Responsabilità per i dati aggregati e archiviati

Un altra importante caratteristica relativa ai dati è il modo in cui sono raccolti e archiviati. Le domande che è necessario chiedere a un EDR sono:

- Quanti dati vengono archiviati e perché?
- Quali dati sono archiviati?
- Dove vengono archiviati?

Ci sono diversi approcci di archiviazione possibili:



Di seguito sono analizzati nello specifico.

Cloud

Molti fornitori offrono soluzioni cloud per memorizzare i dati o persino per gestire gli agenti EDR (i cosiddetti MDR). Si tratta di soluzioni comode ma limitate dalla quantità di dati che possono caricare in qualsiasi momento. Questo include anche avere un canale aperto che trasmette dati al di fuori dell'organizzazione, il che può essere un problema in alcuni ambienti. Quando si prende in considerazione questa opzione, le domande da porsi includono:

- Siamo pronti per inviare dati di sicurezza in un cloud pubblico? Quanto controllo avremo?
- Il fornitore o il provider di cloud che archivierà i miei dati (il quale può essere una terza parte) può essere attendibile? Quanto sono valide le loro dotazioni di cybersecurity?
- L'utilizzo di questo servizio viola la conformità con gli standard di sicurezza interna e/o i requisiti normativi?
- Se vengono inviati al cloud solo piccoli volumi di dati non critici, quando può essere efficace la soluzione?

Sugli agenti

Una cache locale su ciascun dispositivo offre un compromesso tra gli archivi pesanti e il cloud. Questo approccio ha un impatto minore sulla rete e si può supportare simultaneamente un gran numero di agenti. Le informazioni importanti vengono registrate nella cache degli endpoint stessi e tutte le analisi avvengono in tempo reale attraverso le query. Ma un archivio decentralizzato non è sempre il modo più veloce ed efficace per analizzare e rispondere alle informazioni. Se per esempio un sottosegmento della rete non è disponibile, non sarà possibile incorporare nell'analisi globale i dati provenienti dalle macchine coinvolte.

Repository centralizzata in loco

Tutte le informazioni essenziali vengono accumulate e analizzate da un server dedicato con una repository. A fare tutto il lavoro sono un database locale e gli strumenti di analisi (per esempio, una sandbox). Questo approccio locale ha numerosi vantaggi: i dati non vengono memorizzati su dispositivi potenzialmente compromessi (come potrebbe avvenire in teoria con l'archiviazione basata su agenti). Non vi è carico sulle risorse del computer e sarà possibile eseguire query endpoint e ricerche rapide nel database stesso in tempo reale. Le soluzioni in loco come questa sono particolarmente utili nel caso in cui le norme o gli standard di sicurezza richiedono che i dati non vengano trasferiti al di fuori dell'organizzazione.

Raccomandazioni:

- Per l'archiviazione su cloud, valutare il provider di cloud EDR in termini di riservatezza e di controllo dei dati
- Per gli ambienti sensibili, e in cui la conformità alle normative pone possibili restrizioni al trasferimento esterno di dati, la valutazione può includere opzioni di implementazione in loco completamente isolata e l'erogazione privata di threat intelligence.
- Per l'archiviazione di dati basata sugli agenti, verificare che cosa accadrà se un endpoint non è disponibile o è stato compromesso dall'autore dell'attacco (in che modo l'agente stesso, il PC e i dati sono protetti)
- Per le soluzioni in loco, controllare la capacità di archiviazione interna di dati e la quantità di dati inviati da ciascun dispositivo.

Il numero di agenti determinerà i requisiti hardware: se una soluzione EDR richiede solo un piccolo server per supportare centinaia di migliaia di agenti, c'è qualcosa che non va. In media, un endpoint genera circa 10 megabyte di telemetria utile al giorno. Quindi se si hanno 10.000 nodi, si sta usufruendo di 100 gigabyte di dati al giorno (o 3 TB per un database retrospettivo di un mese).

Rilevamento: ricerca manuale vs motori automatizzati

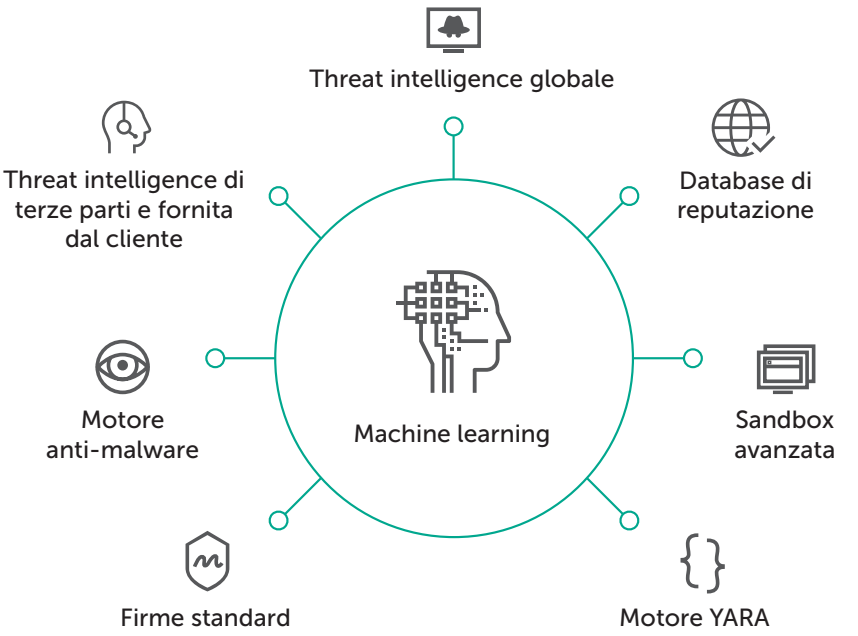
Si è appena discusso di dati e archiviazione. Adesso si passerà a trattare l'analisi dei dati: la ricerca delle minacce e il monitoraggio condotti sai manualmente utilizzando i toolkit, i database e le risorse del fornitore sia automaticamente tramite il sistema EDR stesso. Prima si rileverà un attacco, minori saranno l'impatto finanziario e l'interruzione provocata. La velocità e l'efficacia del rilevamento, dunque, è di primaria importanza (e le tecniche di rilevamento manuali da sole in genere non sono l'approccio più veloce o più efficiente). Molti fornitori offrono le cosiddette "tecniche avanzate di rilevamento" (ad esempio la scansione in tempo reale degli IoC degli endpoint o la ricerca rapida nei database di dati di analisi forense archiviati centralmente), aggiungendo un elemento automatizzato alle funzionalità di rilevamento degli incidenti.

Per sfruttare appieno i dati aggregati, saranno necessarie tecniche di analisi dei dati automatizzate che aiutino gli analisti a individuare i rischi e le minacce che si manifestano sulla rete. Le analisi multilivello e a più dimensioni dovrebbero continuamente fornire non solo informazioni sui nuovi incidenti di sicurezza, ma anche intelligence applicabile, al fine di aiutare il team per la sicurezza a prendere le giuste decisioni ed evitare di spendere tempo inutile sugli eventi non critici.

Tali tecnologie di rilevamento avanzato e di scoperta delle minacce non dovrebbero semplicemente scoprire le comuni attività dannose, ma dovrebbero andare "oltre il malware" per rilevare le violazioni più sofisticate. Non si parla dei livelli di filtraggio delle tecnologie di prevenzione, che costituiscono la base della maggior parte delle soluzioni di EPP, ma di sistemi avanzati di analisi.

Le soluzioni di sicurezza che utilizzano più tecnologie di rilevamento possono aumentare notevolmente le probabilità di individuare più rapidamente gli attacchi e le intrusioni, prima che l'organizzazione subisca gravi danni. Le soluzioni EDR dovrebbero comprendere più motori di rilevamento integrati per offrire da una parte un rilevamento delle minacce avanzato che combini analisi statiche, basate sul comportamento e dinamiche, dall'altra l'accesso in tempo reale alla threat intelligence globale e alle tecnologie di machine learning.

L'obiettivo principale, quindi, è quello di sfruttare più motori di rilevamento diversi possibili per fornire in sede funzionalità da "laboratorio di analisi dei virus", che siano in grado di convalidare le previsioni, avviare nuove indagini o supportare quelle già in corso.



A seconda del fornitore, la tecniche di rilevamento e i motori usati comprenderanno quasi sicuramente un toolkit manuale e sistemi automatizzati in qualche combinazione:

Strumenti di rilevamento manuale

- Caricamento di indicatori di compromissione e ricerca automatizzata/manuale
- Ricerca veloce nei dati retrospettivi
- Sandox (la capacità di inviare un oggetto specifico a una sandbox dedicata o basata su cloud)
- Accesso alle fonti di threat intelligence del fornitore

Rilevamento automatizzato

- Anti-malware
- Norme YARA (personalizzabili dal fornitore e/o il team per la sicurezza)
- Threat Intelligence (fornita automaticamente dal fornitore)
- Servizi basati sulla reputazione (file e/o domini)
- Analisi automatizzata della sandbox di oggetti sospetti
- Machine Learning
    - Apprendimento profondo (nessuna firma: rete neurale)
    - Intelligenza artificiale (analisi comportamentale di base)

Raccomandazioni:

- Chiedere al fornitore EDR quali tecnologie di rilevamento sono disponibili e incorporate
- Scoprire se si stanno utilizzando motori di rilevamento interni, OEM o open-source
- Esplorare la qualità e l'immediatezza della threat intelligence che alimenta questi motori
- Se sono presenti diverse tecnologie di rilevamento, come sono integrate e correlate? (Nessuno vorrebbe finire con incidenti separati che vengono registrati in diversi motori per lo stesso evento)

4

Non basta reagire: è necessario rispondere

Reagire a un incidente è facile: ciò che porta alla risoluzione è una risposta efficace. Il processo di risposta viene attivato non appena viene convalidato un incidente di sicurezza attraverso la classificazione e l'indagine iniziale. Una volta confermato che non si tratta di un "falso positivo", è necessaria una risposta tempestiva e accurata.

Il processo di gestione della risposta agli incidenti dipenderà dalla gravità dell'incidente. La maggior parte degli incidenti avrà un impatto aziendale relativamente piccolo (poiché sono rilevati direttamente all'ingresso). Tuttavia ci saranno quelli che potrebbero portare a situazioni più serie: gravi violazioni di dati, crimini finanziari, spionaggio o ancora peggio. Queste sono le situazioni critiche che richiedono un processo di emergenza di risposta e di indagine.

Una volta che si è scoperto manualmente o si è ricevuto un avviso di sicurezza su una potenziale minaccia, tramite una soluzione di sicurezza di terze parti o il proprio prodotto EDR, cosa succede dopo? Si sono delineati la classificazione, le indagini e i processi di risposta per l'organizzazione? Senza queste configurazioni presenti, in poco tempo il team per la sicurezza può essere inondato dal flusso di lavoro che circonda qualsiasi soluzione EDR.

Rivelare una minaccia attiva è il primo passaggio cruciale per respingere un attacco. Dopo aver individuato la minaccia, è necessario reagire rapidamente potenzialmente su migliaia di endpoint. Una soluzione EDR efficace consentirà la gestione centralizzata degli incidenti su tutti gli endpoint della rete aziendale, con un flusso di lavoro senza interruzioni. Inoltre, una vasta gamma di risposte automatizzate aiuterà le imprese a evitare l'utilizzo di processi di correzione tradizionali, come la cancellazione e la ricreazione d'immagine, che può causare costosi tempi di inattività e perdita di produttività.

La funzionalità di risposta principale dipende dall'approccio del fornitore, ma dovrebbe concentrarsi su queste operazioni comuni:

- Impedire l'avvio di file PE, documenti office e script
- Possibilità di eliminare in remoto il file sulla workstation
- Spostare il file dalla workstation per metterlo in quarantena e ripristinarlo se necessario
- Ottenere il file ed eseguire un'analisi durante l'indagine (ad esempio un'esecuzione forzata della sandbox)
- Forzare l'arresto del processo
- Eseguire il programma o lo script sulla workstation

Alcuni fornitori potrebbero offrire scenari aggiuntivi per favorire risposte più precise. Questi potrebbero includere scenari di isolamento della rete, di isolamento dei processi, di disattivazione degli utenti, di rollback e di correzione.

Raccomandazioni:

Cercare:

- Fornitori con la capacità di mantenere database di threat intelligence potenti e completi e di fornire supporto e consulenza da parte di personale esperto come e quando necessario.
- Soluzioni EDR supportate da corsi di formazione efficaci sulle abilità, che istruiscano i team per la sicurezza in modo che possano stabilire processi efficienti e sfruttare al massimo gli investimenti.
- Un flusso di lavoro senza interruzioni tra processi di rilevamento, ricerca delle minacce, IOC di terze parti e risposta agli eventi, senza la necessità di passare tra diverse console o soluzioni.
- Agenti che siano invisibili per gli utenti finali anche nel corso delle indagini, che non condizioneranno il comportamento degli utenti e che non causeranno tempi di inattività.

5

Prevenzione: EDR o EPP?

Le soluzioni EDR stanno incorporando sempre più elementi di prevenzione nel tentativo di offrire una soluzione "all-in-one". Con la maturazione delle capacità di prevenzione, è possibile che la prevenzione per gli endpoint, la visibilità, il rilevamento e le capacità di risposta convergeranno in un singolo prodotto per gli endpoint.

Ma ancora quel momento non è arrivato. Sebbene si possa essere tentati dal cercare una soluzione che includa la prevenzione al fianco del rilevamento e della risposta, consigliamo, a questo punto, di non prestare molta considerazione a questo aspetto. Scegliere il prodotto desiderato in primo luogo per le sue capacità di visibilità, rilevamento e risposta. Se la soluzione include anche elementi di prevenzione, quello sarà un vantaggio aggiunto. Ma è necessario essere cauti con le soluzioni EDR "di nuova generazione" con capacità di prevenzione immature. Se si tenta di sostituire l'EPP tradizionale con una soluzione EDR, è improbabile riuscire a raggiungere gli stessi livelli di prevenzione.

Tuttavia, molti fornitori di EPP attualmente stanno acquistando o sviluppando il proprio EDR. Se si è soddisfatti dell'EPP attuale e il proprio fornitore EPP offre una soluzione EDR, sarebbe ragionevole valutare sia come interagiscono sia come potrebbero lavorare insieme, soprattutto se questo significa non dover installare un secondo agente per l'EDR.

Raccomandazioni:

- Guardare la roadmap del prodotto EDR e come essa possa evolvere nel tempo per offrire ulteriori funzionalità di prevenzione.
- Se l'idea di protezione degli endpoint, rivelazione e IR integrati è accattivante, guardare l'attuale offerta di EDR del fornitore EPP e vedere quali altre capacità EPP offrono gli altri fornitori EDR.
- Controllare l'architettura EDR e in particolare la possibilità di utilizzare un singolo agente sia per l'EPP sia per l'EDR.

Il futuro dell'Enterprise Endpoint Security

I leader di mercato cercheranno di adottare nuove tecnologie e di sfruttare lo sviluppo interno per aumentare le loro funzionalità EDR.

Per gli esperti di sicurezza, attualmente, il mercato della sicurezza degli endpoint appare eccessivamente saturo di fornitori diversi. È sempre più evidente che ciò non può continuare ad andare avanti. I grandi fornitori alla fine ingloberanno le piccole imprese, utilizzando i loro prodotti per colmare le lacune nel portfolio e migliorare i loro marchi. I leader di mercato cercheranno di adottare nuove tecnologie e di sfruttare lo sviluppo interno per aumentare le loro funzionalità EDR.

Una sicurezza degli endpoint realmente di "nuova generazione", che offra sia metodi di controllo tradizionali sia tecnologie di protezione avanzate, si evolverà attraverso gli sforzi dei principali attori del mercato EPP. La generazione attuale di agenti avanzati di sicurezza degli endpoint, come l'EDR, offre solo elementi con reali funzionalità EPP: non sta puntando infatti ad assumere le vesti di suite di protezione degli endpoint con funzioni complete.

La sicurezza degli endpoint ha cambiato i piani aziendali e continuerà ad attirare sempre più l'attenzione. I futuri clienti adatteranno ed evolveranno le loro strategie di sicurezza, basandosi sulle tecnologie avanzate di protezione degli endpoint combinate con il monitoraggio delle attività degli endpoint.

Dal punto di vista tecnologico, tali soluzioni avanzate formeranno un approccio adattativo all'offerta della protezione, mentre forniranno simultaneamente servizi di rafforzamento dei sistemi, prevenzione delle attività dannose e rilevamento avanzato. Anche la threat intelligence basata su cloud e la machine learning in locale, la ricerca delle minacce, che comprende la risposta attiva e l'indagine rapida, e l'analisi comportamentale profonda e di threat intelligence, faranno la loro parte.

Suggerimenti

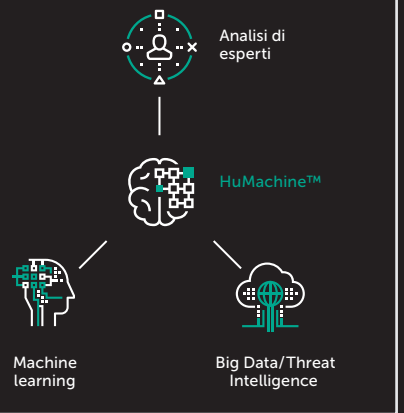
Riconoscendo il crescente bisogno di un'analisi e una protezione degli endpoint più profonda, i professionisti della sicurezza si ritrovano inevitabilmente con un lungo elenco di esigenze ma con dei fondi limitati con cui affrontare tutte queste necessità. Ma anche senza fondi, sembra ragionevole valutare le tecnologie attuali e i possibili sviluppi futuri in termini di come essi corrispondano agli obiettivi aziendali e alle capacità interne. Analizzando e testando a fondo le opzioni, è possibile aiutare sia a concentrare l'attenzione generale dei responsabili delle decisioni aziendali su ciò che le nuove tecnologie possono offrire, sia ad assicurare una pianificazione futura dei fondi per la sicurezza e a sapere che, quando arriva il momento di investire, si sarà pronti a farlo con cognizione.

Azioni da intraprendere subito

1. Valutare le funzionalità di sicurezza complessive. Quanto è veloce e unificato l'attuale processo di risposta agli incidenti? Attualmente sono state implementate le giuste soluzioni, a parte le considerazioni sull'EDR?
2. Comprendere le capacità attuali di rilevamento sugli endpoint. Eseguire analisi e considerare di provare ulteriori fonti di intelligence: ad esempio, guardare all'utilizzo di Feed di dati sulle minacce con il proprio SIEM
3. Pensare a come è possibile iniziare ad aumentare le competenze di IR interne. Valutare le capacità del proprio team e indagare opzioni efficaci di formazione.
4. Iniziare a formulare i requisiti effettivi o la domanda in arrivo e guardare alla selezione di soluzioni EDR in linea con questi aspetti.

Alcuni link utili

1. Linee guida sulla risposta agli incidenti: https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Valutare la propria sicurezza con questo calcolatore di sicurezza IT e scaricare il Report aziendale globale: https://calculator.kaspersky.com/it/



Kaspersky Lab
Enterprise Cybersecurity **www.kaspersky.com/enterprise**
Novità sulle minacce informatiche: **www.securelist.com**
Novità sulla sicurezza IT: **business.kaspersky.com/it**

#truecybersecurity
#HuMachine

www.kaspersky.it