FORTINET

Le 5 principali funzionalità critiche di una piattaforma di rilevamento e risposta

Sommario

Sintesi preliminare

La sofisticazione dei cybercriminali e delle loro campagne rappresenta una problematica e un'opportunità cruciale per i team delle operazioni di sicurezza. Sebbene una difesa informatica di successo richieda la capacità di monitorare molte vie di attacco e vari segnali di attività dannose, il che può essere complicato e richiedere tempo anche per i professionisti della sicurezza più esperti, la distribuzione delle tecnologie giuste svolge un ruolo fondamentale nell'aiutare il team ad avere un quadro generale e a reagire in modo efficace prima che si verifichino danni. Quando si valutano le piattaforme di rilevamento e risposta, è necessario porsi alcune domande cruciali prima di procedere con l'acquisto.

Introduzione

Quando si effettuano investimenti nell'ambito della sicurezza informatica, la maggior parte delle organizzazioni si è storicamente concentrata sulla prevenzione. Tuttavia, come si legge in una nota di ricerca di Gartner, "data la complessità del rilevamento delle minacce, l'era dell'acquisto di un singolo prodotto all'avanguardia per la prevenzione delle minacce è ormai un ricordo del passato. Quello che serve è uno stack di rilevamento in grado di raccogliere una quantità sufficiente di telemetria utilizzando vari metodi, tra cui le API, e di analizzarla correttamente per trovare l'ago dell'attacco nel pagliaio dei dati".[1]

Detto questo, i leader aziendali riconoscono sempre più che la complessità delle infrastrutture di sicurezza e della gestione degli avvisi rappresenta una vera e propria problematica. La buona notizia è che il 75% delle organizzazioni sta perseguendo il consolidamento dei fornitori di sicurezza informatica, preferendo le piattaforme a una serie di prodotti monofunzionali.[2]

Tuttavia, non tutte le piattaforme offrono il giusto livello di copertura: la superficie di attacco e la copertura delle fasi

delle campagne, la tecnologia di rilevamento e il grado di integrazione possono variare notevolmente. Infine, sebbene la tecnologia riceva la massima attenzione, le persone e i processi rimangono essenziali per una difesa efficace. Come riconosce giustamente Gartner, "lo stack migliore è quello che soddisfa in modo più efficace ed efficiente (in termini di costi) gli obiettivi di monitoraggio".[3]

Cinque considerazioni per gli investimenti in rilevamento e risposta alle minacce

Supponiamo che tu stia pensando di adottare un approccio basato su piattaforma al rilevamento e alla risposta o che tu debba modificare il tuo approccio alla gestione dei rischi. In questo caso, ci sono cinque domande cruciali da considerare prima di effettuare nuovi investimenti.

1. Cosa si può ispezionare?

Ci sono molti modi in cui gli autori delle minacce tentano di guadagnare l'accesso a una organizzazione (email, download da Internet, risorse e applicazioni rivolti all'esterno, servizi aziendali e altro), molte destinazioni all'interno di essa (dispositivi degli utenti finali, server applicativi, sistemi IoT e OT e altro), per non parlare di ulteriori obiettivi esterni all'organizzazione (Software-as-a-Service e infrastrutture di cloud pubblico, ad esempio).

Come osservato in una recente sintesi di Gartner, "il numero di POV [punti di vista] di cui dispone uno stack è direttamente correlato alla quantità e al tipo di minacce che è in grado di rilevare e/o alla qualità degli avvisi che produce.

Come minimo, lo stack dovrebbe avere un POV strategico per il tipo di minacce di maggiore interesse".[4] Non è possibile rilevare quello che non si ispeziona, quindi devi assicurarti che tutte le basi (o vettori di attacco e infrastrutture mirate, in questo caso) siano coperte.

2. Tutte le fasi sono coperte?

Oggi molti attacchi attraversano più fasi per aggirare i controlli orientati alla prevenzione, rimanere nascosti per lunghi periodi e aumentare al massimo l'impatto e il ritorno sull'investimento. Il framework MITRE ATT&CK e la catena offensiva informatica di Lockheed Martin riflettono le fasi comuni e le tattiche regolarmente utilizzate, che comprendono la preparazione che precede l'attacco, l'esecuzione dell'attacco e l'attività successiva all'infezione e all'intrusione. Fortunatamente, più fasi vengono eseguite dall'autore delle minacce prima di raggiungere il suo obiettivo finale, più possibilità ha l'organizzazione di rilevare e interrompere l'attacco prima che venga sferrato con successo.

Gartner afferma: "In generale, è meglio trovare uno stack di rilevamento che funzioni nella fase di attacco e che produca gli avvisi di qualità più elevata per gli obiettivi di monitoraggio".[5] A tal fine, una piattaforma per le operazioni di sicurezza deve coprire tutte le vie di attacco e di espansione e tutte le fasi della catena offensiva informatica, tra cui la ricognizione, l'inserimento dell'agente di attacco, il recapito, lo sfruttamento, l'installazione, la comunicazione Command&Control e le ulteriori azioni sull'obiettivo.

3. Quali sono le tecnologie utilizzate per il rilevamento?

Ovviamente, il fatto di ispezionare le attività attraverso i vettori di attacco e lungo la catena di attacco cibernetico non significa automaticamente che si possano rilevare gli attacchi, poiché questi sono sempre più spesso sono progettati per assomigliare o addirittura utilizzare servizi o azioni legittime. Secondo Gartner, "alcuni metodi sono molto semplici al punto da essere deterministici, altri dipendono da una conoscenza approfondita delle minacce, mentre altri ancora potrebbero richiedere un'analisi complessa dei dati. Non esiste un metodo migliore, ma alcuni risultano più efficaci per determinate minacce rispetto ad altri".[6]

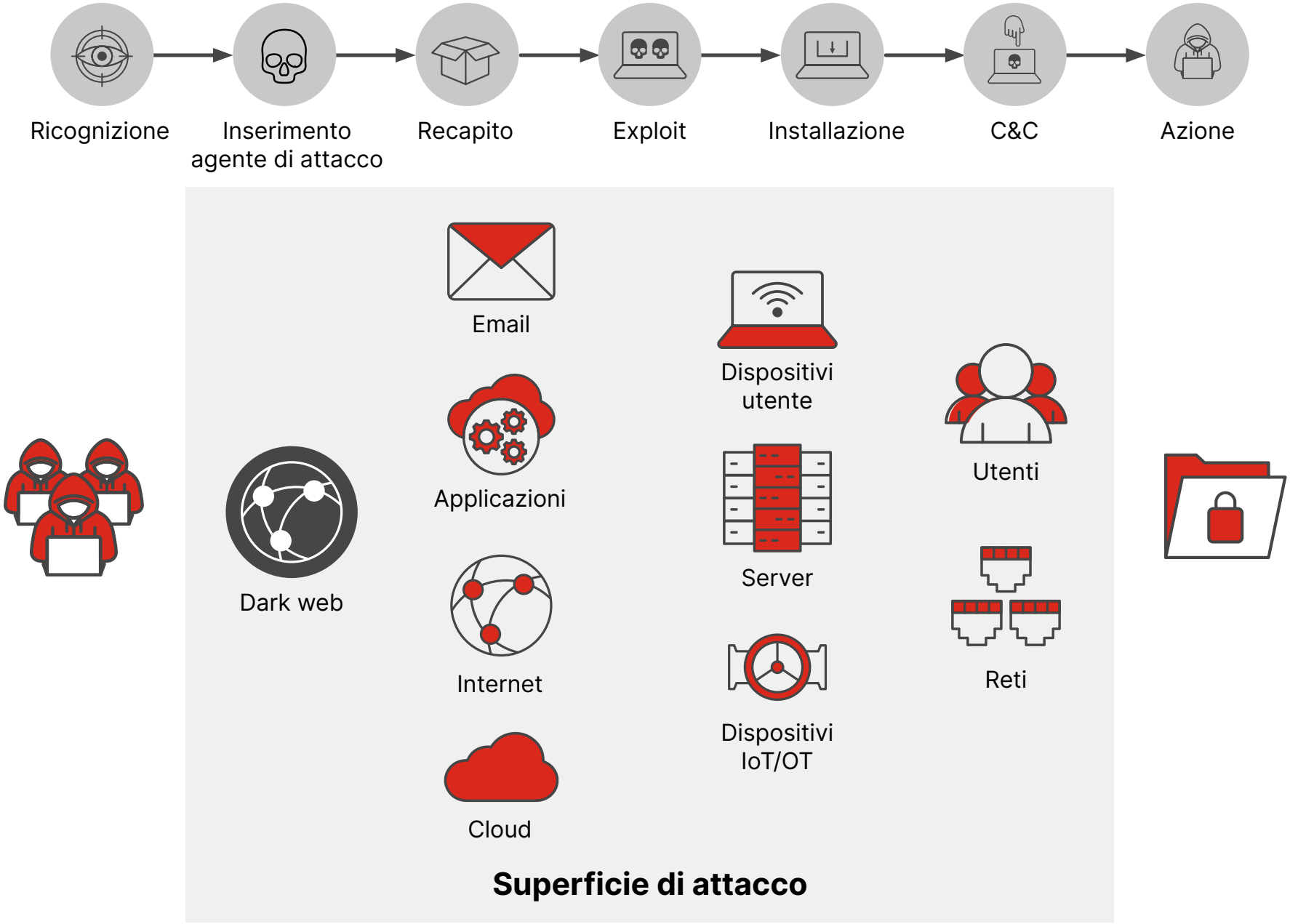

Figura 1: superficie di attacco richiesta e copertura della catena offensiva informatica

La threat intelligence e gli indicatori di compromissione sono molto precisi, ma non molto predittivi. Le regole e l'euristica sono più predittivi, ma spesso producono falsi positivi. I modelli statici di machine learning o deep learning sono molto più predittivi, ma di solito offrono una probabilità che inizialmente può essere difficile da considerare attendibile e da mantenere nel tempo. L'analisi del comportamento offre alcuni dei migliori indicatori, ma solo se questi processi sono in grado di identificare con precisione tattiche, tecniche o procedure note Identificare attività anomale che possono essere non autorizzate o legittime richiede tempo per i team di sicurezza. Considera la giusta combinazione di tecnologie di rilevamento adatte alla tua organizzazione e al tuo team.

4. Chi (o cosa) deve rispondere?

Il rilevamento è solo il primo passo: la convalida e il contenimento degli incidenti sono fondamentali per limitare i rischi e un'indagine completa e un processo di correzione sono necessari per tornare a operazioni sicure.

Tradizionalmente, questa funzione è stata gestita manualmente da professionisti esperti in materia di sicurezza, che rimangono una parte essenziale del processo. Tuttavia, secondo Gartner, "Response SOPs [procedure operative standard]sono sicuramente utili per definire gli obiettivi, i processi e le attività, ma non sono in grado di coprire il livello prescrittivo di quello che deve essere compiuto esattamente su ogni oggetto coinvolto nell'attacco, in base al tipo specifico di attacco appena sferrato".[7]

Le organizzazioni devono decidere quanto affidarsi alle conoscenze istituzionali del team di sicurezza o se costruire tali conoscenze in processi documentati che possono essere orchestrati e automatizzati da una piattaforma. Una solida strategia di operazioni di sicurezza si basa in genere su entrambe questi approcci e le organizzazioni devono determinare il giusto equilibrio da raggiungere.

5. Il tuo team è in grado di eseguirlo?

Ovviamente, anche il sistema più finemente attrezzato, orchestrato e automatizzato non verrà eseguito da solo. Come osserva Gartner: "l'ultima problematica, e spesso la più complessa, è quella correlata alle operazioni... Gran parte del lavoro da svolgere non è legato a guasti e correzioni, ma assume più che altro la forma di riflessioni critiche e indagini a livello di esperti".[8]

Stabilisci se la piattaforma di rilevamento e risposta scelta è in grado di essere gestita dal tuo team o se devi affidarti a esperti esterni. L'outsourcing può essere ad hoc o continuativo e puoi decidere se hai bisogno di supporto per tutte le attività o di una copertura specializzata solo per alcune di queste. In ogni caso, l'outsourcing non esonera l'organizzazione dal rischio informatico, ma semplicemente utilizza le competenze e il personale di altri fornitori, quindi se scegli l'approccio dell'outsourcing, assicurati di scegliere una piattaforma che possa essere supportata da un partner affidabile dotato di tutte le competenze necessarie.

Riepilogo

La sofisticazione degli odierni autori delle minacce e la complessità dei loro attacchi rappresentano una problematica e un'opportunità al tempo stesso. Garantire un sistema di rilevamento efficace che copra l'intera superficie di attacco e la catena offensiva informatica con una tecnologia ad alta fedeltà che consenta una risposta efficiente può ridurre notevolmente i rischi informatici.

[1] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 dicembre 2022.

[2] Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022, Gartner, 13 settembre 2022.

[3] The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations, Gartner, 19 dicembre 2022.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

FORTINET

www.fortinet.com

marzo 24, 2024 1:13 PM

2504903-0-0-EN