SOPHOS
Cybersecurity delivered.

Guida Introduttiva AI Threat Hunting

Indicazioni pratiche su come prepararsi a individuare e neutralizzare le minacce informatiche più elusive

Gli attacchi informatici continuano a evolversi. E i cybercriminali adottano sempre più frequentemente metodi altamente sofisticati ed elusivi per strutturare ed eseguire gli attacchi. Di conseguenza, l'individuazione proattiva e la neutralizzazione delle attività dannose sono diventate cruciali nella lotta contro le minacce avanzate. Ma queste pratiche di sicurezza sono tutt'altro che semplici.

In questo report forniamo indicazioni pratiche per aiutarti a cominciare a svolgere attività di threat hunting, più un compendio degli strumenti e dei framework utilizzati dai team di esperti di sicurezza per tenersi un passo avanti rispetto alle nuove minacce informatiche e rispondere rapidamente ai potenziali attacchi. Infine, delineeremo i cinque passaggi di preparazione per il threat hunting per i professionisti dell'IT.

Whitepaper Sophos. Agosto 2022

Il Quadro Delle Minacce Informatiche Nel 2022

Aumento Del Volume, Della Complessità E Dell'Impatto Degli Attacchi

La cybersecurity è una sfida sempre più ardua per le organizzazioni. L'anno scorso, gli attacchi si sono intensificati: il 57% delle organizzazioni ne ha notato un incremento in termini di volume, il 59% di complessità, e il 53% di impatto. Quasi tre intervistati su quattro (72%) affermano di avere riscontrato un incremento in almeno uno di questi ambiti.

Una tendenza sempre più diffusa è l'aumento degli attacchi alla supply chain, come nel caso dell'incidente che ha coinvolto SolarWinds, che è emerso a marzo 2021. I cybercriminali avevano inserito istruzioni modificate all'interno del codice sorgente della soluzione Orion dell'azienda, che viene utilizzata per gestire reti complesse da remoto. Questa backdoor ha permesso agli hacker di accedere alla rete dei clienti SolarWinds, che include vari enti governativi.

Il Ransomware È Una Minaccia Tangibile Per Tutte Le Organizzazioni

Il 66% delle organizzazioni è stato colpito dal ransomware negli ultimi 12 mesi, una percentuale molto più alta rispetto al 37% del 2020. Si tratta di un aumento del 78% in un anno, il che dimostra che i cybercriminali sono diventati molto più abili a sferrare attacchi su vasta scala.

Utilizzo Più Diffuso Di Strumenti Legittimi Negli Attacchi Informatici

Gli hacker sfruttano sempre più frequentemente copie bootleg o piratate di software commerciali pronti per l'uso e strumenti open source gratuiti. Questi strumenti sono tipicamente realizzati per simulare attacchi informatici, allo scopo di migliorare la sicurezza, ma possono essere utilizzati dai cybercriminali per fare esattamente l'opposto.

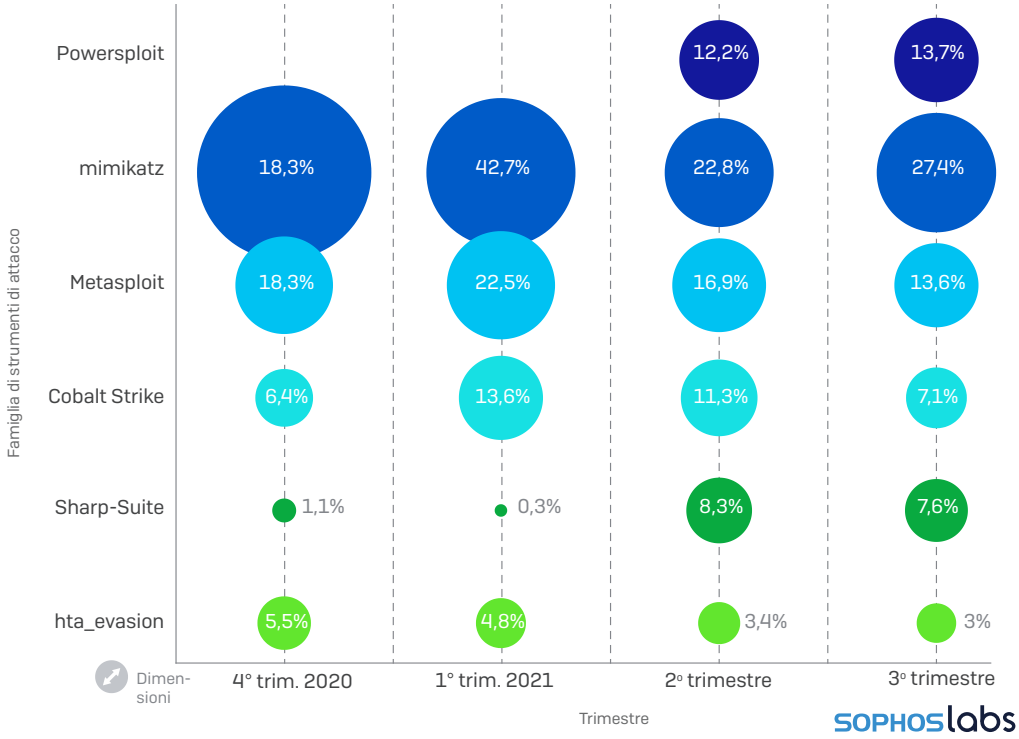
Sebbene non si tratti strettamente di prodotti commerciali, l'uso di strumenti come Mimikatz (utilizzato sia da penetration tester che da autori di malware) è stato osservato in quasi tutti gli attacchi hands-on-keyboard su cui Sophos ha indagato l'anno scorso.

Un altro strumento prominente (grazie alla pubblicazione non autorizzata del suo codice sorgente nel 2020) sono state le copie piratate di Cobalt Strike (un software di simulazione di attacco informatico), che non sono solo state sfruttate per gli attacchi ransomware, ma hanno anche svolto la funzione di payload iniziale per altri malware.

[1]La Vera Storia Del Ransomware 2022 - Sophos
[2]La Vera Storia Del Ransomware 2022 - Sophos

La prevalenza dei principali strumenti di attacco

Gli strumenti di attacco più frequentemente rilevati nel 2020-2021, per singolo computer



Sophos Threat Report 2022

Grazie alla funzionalità "Beacon" di Cobalt Strike, che offre una valida backdoor per i computer Windows, questo software è diventato lo strumento preferito dei cybercriminali. Di conseguenza, la maggior parte dei casi di ransomware che abbiamo osservato negli ultimi 12 mesi includeva l'uso di beacon di Cobalt Strike.

Per informazioni più approfondite sul panorama attuale delle minacce informatiche, dai un'occhiata all'ultimo Sophos Threat Report.

L'Implementazione Di Best Practice Proattive Per La Cybersecurity È Un Must

Attacchi alla supply chain, exploit dei software, strumenti legittimi. Il comune denominatore è la natura di questi approcci: sono coordinati da una mente umana; sono estremamente mirati e calcolati; sono elusivi e impossibili da rilevare con i metodi tradizionali.

Per tenere testa ai criminali, le organizzazioni devono adottare approcci più proattivi alla cybersecurity. La risposta ad avversari umani è appunto un approccio coordinato da menti umane.

E per questo occorre il threat hunting.

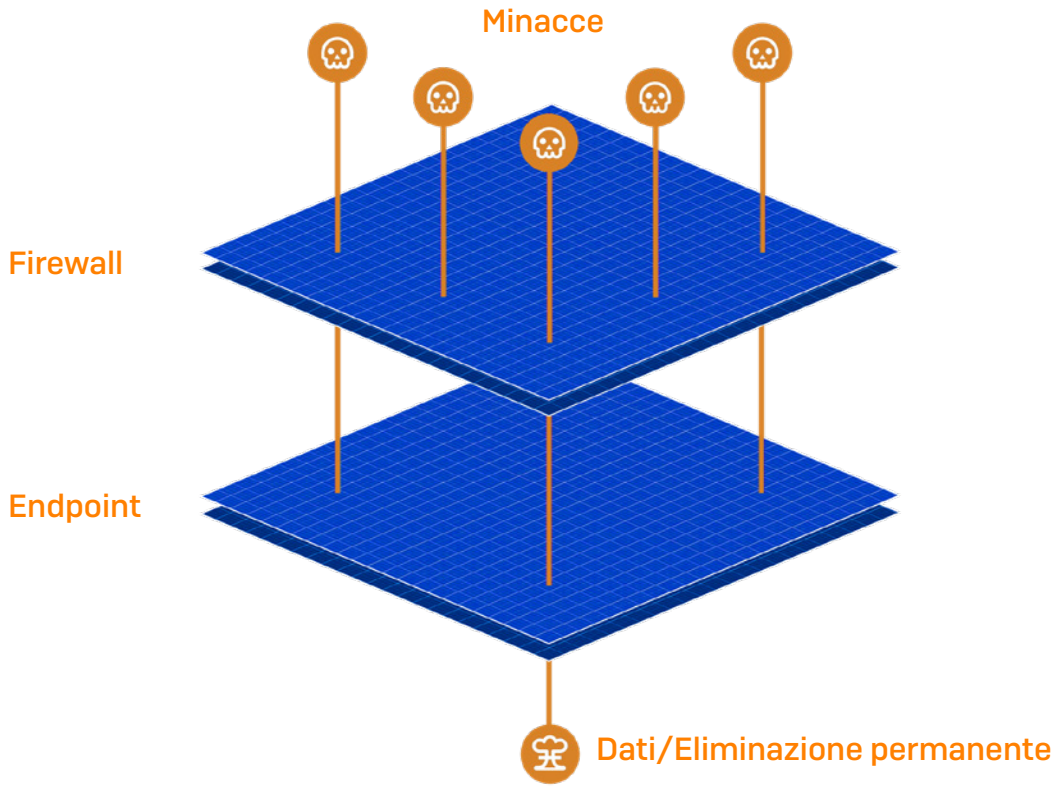
Cos'È Il Threat Hunting?

Il threat hunting è il processo iterativo e proattivo di identificazione delle attività dannose mediante dati di telemetria ottenuti da endpoint e rete, partendo dal presupposto che i cybercriminali siano già riusciti a eludere le difese informatiche. Lo definiamo iterativo, perché è richiesto un adattamento costante, per fare in modo che questo metodo mantenga la sua efficacia nella ricerca e nella neutralizzazione di minacce informatiche in continua evoluzione.

Durante un threat hunting, i team analizzano gli strumenti, le tecniche e le procedure utilizzate dagli hacker per stabilire la fase attuale dell'attacco e ottenere dati di intelligence. Una volta ottenute queste informazioni, viene intrapresa l'azione più appropriata per neutralizzare la minaccia, se richiesto.

Perché Abbiamo Bisogno Del Threat Hunting?

I motivi sono diversi, anche se quello principale è un'unica verità: a differenza di quello che sembrano sostenere in molti, la tecnologia, da sola, non è in grado di bloccare il 100% delle minacce. Anche se si adottano vari livelli di difesa, alcune minacce riescono comunque a infiltrarsi nei sistemi e a compromettere gli ambienti IT.



Come abbiamo già accennato, invece di sferrare attacchi automatici e su vasta scala come in passato, i cybercriminali moderni utilizzano sempre più frequentemente approcci adattivi ed elusivi, caratterizzati da un intervento umano di tipo "hands-on-keyboard".

Questa tendenza si riflette nei risultati delle indagini dei nostri team di risposta alle minacce, che segnalano un notevole aumento nel numero di attacchi controllati e coordinati da hacker umani. Ciò significa che, per tenere testa agli attacchi, i team di sicurezza devono essere in grado di individuare minacce mai osservate prima e pensare come se si fosse già verificata una violazione.

La Mentalità Del Threat Hunting

Spesso gli esperti di threat hunting partono dal presupposto che una potenziale minaccia sia già riuscita a eludere i sistemi di difesa, indipendentemente dal punto della catena di attacco in cui è stata individuata. Adottano questa mentalità perché li induce a raggiungere due obiettivi importanti.

Limitare Il Tempo Di Permanenza Degli Hacker Nei Sistemi

Questo modo di pensare induce i team a limitare il tempo di permanenza dell'autore dell'attacco nei sistemi. Più a lungo un hacker rimane nella rete, più tempo avrà per svolgere attività dannose. Analogamente, meno tempo permettiamo a un cybercriminale di trattenersi all'interno di una rete, meno danni potrà fare. I team di sicurezza non hanno altra scelta se non intercettare le minacce prima che il loro impatto sia evidente, e per farlo devono partire dal presupposto che gli hacker siano già riusciti a eludere i sistemi di difesa.

Ridurre I Tempi Di Rilevamento

Adottare questa mentalità spinge anche i team a ridurre i tempi medi di rilevamento. È possibile che la tua organizzazione abbia livelli di difesa multipli e che la minaccia sia talmente elusiva da attivare il rilevamento in una fase diversa della catena di attacco. Tuttavia, a questo punto potrebbe ormai essere troppo tardi: sono già stati fatti danni e la gravità della minaccia è ormai eccessiva. Cercando di individuare proattivamente la minaccia, potremmo riuscire a identificare eventuali vulnerabilità di sicurezza da risolvere, riducendo anche i tempi necessari per rilevare minacce simili o identiche in futuro.

Chi Svolge Il Threat Hunting?

Il Profilo Di Un Threat Hunter

Prima di addentrarci nell'argomento del threat hunting, è essenziale capire il ruolo di un threat hunter. Il threat hunting è un'operazione estremamente complessa. Chi lavora in questo ambito deve avere una serie di competenze tecniche estremamente specializzate. Sulla base di queste premesse, le caratteristiche tipiche di un threat hunter sono le seguenti:

- **Creatività e curiosità**: l'individuazione delle minacce può essere un po' come cercare un ago in un pagliaio. I threat hunter spesso passano giorni e giorni a individuare le minacce, utilizzando vari metodi per scovarle.
- **Esperienza nell'ambito della cybersecurity**: il threat hunting è una delle operazioni di cybersecurity più avanzate. Di conseguenza, è indispensabile avere competenze di base ed esperienza in questo ambito.
- **Conoscenza del panorama delle minacce**: avere una buona comprensione delle nuove tendenze in tema di minacce è essenziale quando si devono cercare e neutralizzare elementi sconosciuti.
- **Buona intuizione delle intenzioni dei cybercriminali**: la capacità di pensare come un hacker è fondamentale quando si contrastano attacchi coordinati da menti umane.
- **Ottime abilità di scrittura tecnica**: come parte del processo di indagine, i threat hunter devono registrare tutti i risultati delle loro ricerche. Pertanto, la capacità di comunicare informazioni complesse è indispensabile per il successo delle attività di threat hunting.
- **Conoscenza dei sistemi operativi e della rete**: è fondamentale avere conoscenze pratiche avanzate per entrambi.
- **Esperienza di programmazione/scripting**: è richiesta per aiutare i threat hunter a compilare programmi, automatizzare le operazioni, esaminare i log e analizzare i dati necessari per svolgere le indagini.

Purtroppo, trovare questa combinazione di competenze è raro, e il risultato è una scarsità nel settore dell'informatica di personale dotato dei requisiti necessari: il 54% degli amministratori IT ritiene infatti che, anche con tutti gli strumenti a loro disposizione, gli attacchi informatici sono ormai troppo avanzati per essere risolti dal proprio team IT senza un aiuto esterno. Detto questo, nei casi in cui questo tipo di personale è disponibile, si osserva che molto spesso il threat hunting viene svolto da due tipi di team.

Security Operations Center (SOC) Interni

Quando le organizzazioni decidono di svolgere direttamente le proprie attività di threat hunting, i threat hunter lavoreranno all'interno del SOC. Un SOC è una funzione aziendale che si focalizza sul monitoraggio, sul rilevamento, sulle indagini e sulla risposta alle minacce informatiche, migliorando allo stesso tempo il profilo di sicurezza generale dell'organizzazione per cui opera. È il team di riferimento nell'organizzazione per qualsiasi tematica relativa alla cybersecurity.

Fornitori Di SecOps Esterni

Sono sempre più numerose le organizzazioni che affidano le proprie SecOps a fornitori di terze parti. Questo potrebbe essere dovuto a vari motivi: una mancanza di capacità interna (l'anno scorso i team IT hanno notato un aumento pari al 69% del carico di lavoro di cybersecurity), la difficoltà a trovare dipendenti con le giuste competenze, oppure la scelta di affidarsi a esperti esterni impegnati 24/7 in questa attività critica.

Fornitori di Managed Detection And Response (MDR)

L'MDR, fornito come servizio interamente gestito, permette alle organizzazioni di poter contare su un team dedicato di analisti di sicurezza che individuano proattivamente le minacce in agguato a qualsiasi ora del giorno e della notte. Secondo ESG Research, infatti, "il 51% utilizza un fornitore di servizi di rilevamento e risposta alle minacce gestiti (Managed Detection and Response, MDR) per aiutarle a integrare i dati di telemetria per il rilevamento e la risposta alle minacce".

I fornitori di servizi MDR offrono diversi vantaggi rispetto ai programmi di SecOps che si affidano solamente a un team interno. Il vantaggio più importante è spesso l'esperienza.

Il team Sophos MDR vanta migliaia di ore di esperienza, e può dire di avere visto e risolto qualsiasi tipo di problema che i cybercriminali possono causare. È in grado di sfruttare l'esperienza maturata sul campo affrontando gli attacchi di un'organizzazione e di applicarla a tutti i clienti. Un altro vantaggio è la portata delle operazioni: il team Sophos MDR offre supporto 24/7, con tre team internazionali.

Managed Security Service Provider (MSSP)

Le organizzazioni si rivolgono agli MSSP per affidare a loro il compito di gestire parte delle loro IT Ops, permettendo così ai propri team interni di focalizzarsi sulle normali attività di routine quotidiana. Il threat hunting potrebbe essere offerto dagli MSSP come parte di un servizio gestito e potrebbe includere anche opzioni di MDR, come indicato sopra.

Le Tecnologie Essenziali Per Il Threat Hunting

Endpoint Detection And Response (EDR)/Extended Detection And Response (XDR)

Per poter identificare le attività potenzialmente dannose e indagare sull'accaduto, i threat hunter hanno bisogno di dati e strumenti di indagine. Ed è proprio per questo che esistono EDR e XDR: permettono infatti ai threat hunter di visualizzare rapidamente i rilevamenti sospetti e di investigare sulla loro natura.

Come suggerisce il nome stesso, EDR fornisce i dati provenienti dalla soluzione endpoint. XDR, invece, raccoglie i segnali ricevuti dall'intero ambiente informatico, inclusi firewall e soluzioni per dispositivi mobili, e-mail e cloud security. Visto che gli avversari cercano di sfruttare ogni opportunità di attacco, un ambito più ampio per la ricerca degli indicatori di compromissione offrirà maggiori probabilità di intercettarli nelle fasi iniziali della violazione.

Una delle principali sfide pratiche per le soluzioni EDR/XDR sono i dati non pertinenti: i threat hunter ricevano moltissimi segnali e questo potrebbe impedire loro di distinguere tra le informazioni utili e quelle non essenziali. Ed è per questo motivo che è fondamentale utilizzare la propria soluzione EDR/XDR insieme a una protezione endpoint potente e in grado di bloccare subito le minacce: questo permette ai responsabili della protezione di focalizzarsi su un numero ridotto di rilevamenti particolarmente accurati.

L'Anatomia Del Rilevamento E Della Risposta Alle Minacce

Il threat hunting è solo parte di un'operazione più estesa, ovvero quella di rilevamento e risposta alle minacce. Per il threat hunting, Sophos applica un framework di rilevamento e risposta alle minacce, che consiste in cinque componenti principali.

1. Prevenzione

Implementando tecnologie di prevenzione efficaci e configurate correttamente (ad esempio una soluzione di protezione endpoint), puoi impedire agli hacker di infiltrarsi nella tua rete. E soprattutto, in questo modo puoi anche ridurre la quantità di avvisi di sicurezza generati ogni giorno o persino ogni ora. Con meno avvisi da gestire, il team di sicurezza è in grado di riconoscere in maniera più accurata i segnali utili e di focalizzarsi solo sugli indicatori pertinenti, in questo caso gli attacchi elusivi e coordinati dagli hacker in tempo reale.

2. Raccolta di eventi, avvisi e rilevamenti di sicurezza

I dati sono il carburante che alimenta l'individuazione e l'analisi delle minacce. Senza il giusto volume di segnali di buona qualità e di tipo adeguato, identificare in maniera accurata i potenziali indicatori di attacco è difficile per i team SecOps. Eppure i dati senza contesto complicano il processo decisionale degli analisti, quando devono determinare se un elemento costituisce una minaccia. Senza metadati pertinenti per i segnali, gli analisti avranno difficoltà a stabilire se questi segnali sono dannosi o innocui.

3. Assegnazione Di Priorità Ai Segnali Pertinenti

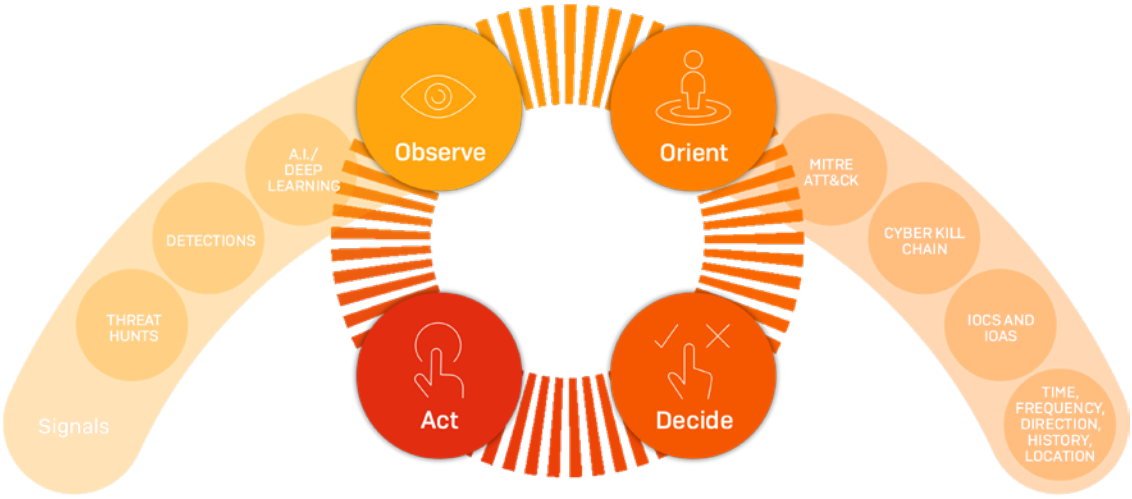
Per prevenire il sovraccarico di dati ed evitare che sfuggano gli elementi che meritano un'indagine più approfondita, bisogna essere in grado di individuare gli avvisi rilevanti. E questo è più difficile di quanto sembri. Più si è in grado di ridurre il tasso di informazioni non pertinenti mediante una combinazione tra automazione, intelligenza artificiale e informazioni contestuali provenienti esclusivamente dall'elemento che ha generato l'evento, maggiore sarà la pertinenza dei risultati. Ma anche con l'automazione, il processo è tutt'altro che semplice.

4. Indagine

Una volta isolati gli indicatori principali, è il momento di aggiungere informazioni approfondite e valutare i risultati delle indagini secondo framework e modelli di settore, per stabilire soglie limite in base alle quali determinare i comportamenti dannosi e quelli innocui.

Framework di indagine OODA

Spesso gli analisti di sicurezza più esperti utilizzano un framework per strutturare le indagini. Il team Sophos MDR adotta, ad esempio, una metodologia investigativa detta "ciclo OODA", che permette di svolgere la sequenza di azioni menzionata prima, per testare e confermare la validità di tutti i risultati ottenuti:



Il ciclo OODA è un concetto militare che permette al nostro team di seguire una progressione logica di ragionamento, che aiuta a capire in maniera completa l'evento e i comportamenti ad esso correlati. Il team può quindi utilizzare queste conoscenze come base per un processo decisionale e intuitivo umano, al fine di stabilire se sono presenti attività dannose all'interno dell'ambiente di un cliente e, in base a questo, decidere come agire.

Quando applicano il framework OODA, spesso gli analisti di sicurezza Sophos procedono seguendo questi passaggi:

- **Osservare**: che cosa si vede in questo rilevamento?
  - Osservazione delle potenziali connessioni esterne e interne, correlate al rilevamento
  - Determinazione di dove sia stato riscontrato il rilevamento e se ci sono utenti implicati
- **Orientare**: che cosa si capisce di questo rilevamento?
  - Raccolta di dati basati sulle prove
  - Comprensione di TTP (tattiche, tecniche, procedure) comuni o specifiche per questo attacco o hacker. Una delle risorse utilizzate per identificare le TTP è il framework MITRE ATT&CK, di cui parleremo in maniera più approfondita nelle prossime pagine di questo report.
  - Raccolta di dati di intelligence sugli indicatori di attacco (IoA) e sugli indicatori di compromissione (IoC)
- **Decidere**: questo rilevamento è dannoso, sospettoso o innocuo? Richiede un'azione?
- **Agire**: in base ai passaggi precedenti, cosa si deve fare?
  - Mitigare, neutralizzare, ricominciare il ciclo, migliorare.

5. Azione

Questa è una fase importantissima. Una volta stabilito che si è alle prese con una minaccia, occorre compiere due azioni, entrambe di fondamentale importanza.

La prima è mitigare il problema più immediato, la seconda è ricordare che molto probabilmente questo risolve solo uno dei sintomi dell'attacco, e che occorre pur sempre individuare e neutralizzare la causa originaria. Inoltre, la prima azione non deve essere svolta a scapito della seconda.

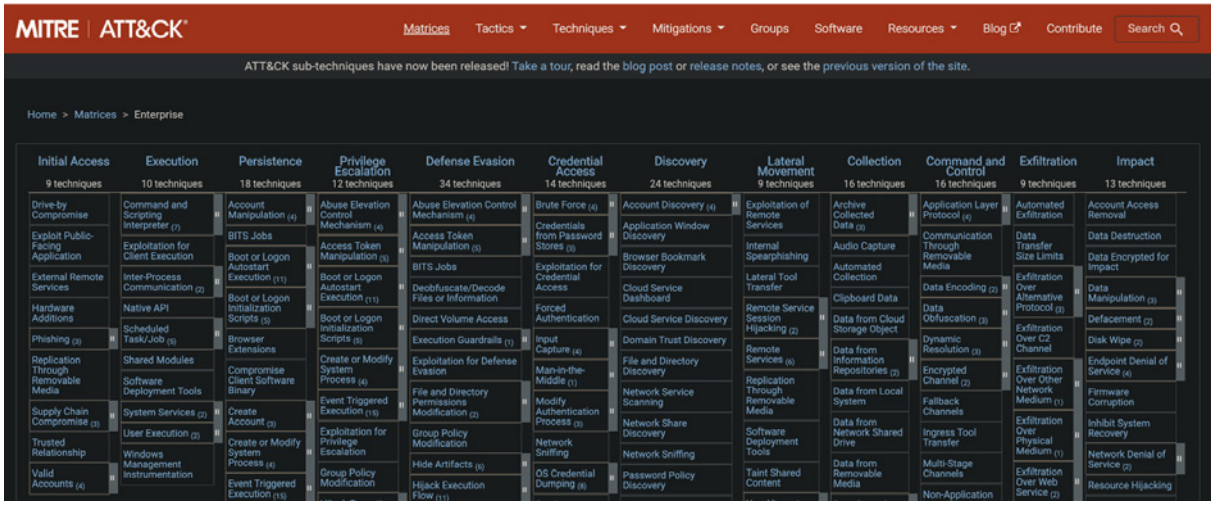
A volte può bastare mettere in quarantena un computer o disconnetterlo dalla rete, mentre altre volte il team di sicurezza dovrà indagare in maniera approfondita sulle rete, per eradicare completamente ogni traccia degli hacker.

Ad esempio, solo perché il malware è stato bloccato e rimosso dai sistemi e l'avviso che lo segnalava non viene più visualizzato, questo non significa che l'hacker sia stato allontanato dall'ambiente.

I threat hunter professionisti, che hanno visto migliaia di attacchi, sanno quando e dove approfondire le indagini. Cercano tracce di attività degli hacker passate, presenti o future che potrebbero avere un impatto sulla rete. Una volta identificate, neutralizzano anche quelle.

Classificazione Delle Minacce: Il Framework MITRE ATT&CK

Una risorsa utilizzata molto frequentemente dai threat hunter è il framework MITRE ATT&CK. Chiunque abbia avuto esperienza nell'ambito della cybersecurity ne avrà sentito parlare. Tra i vari framework, MITRE è una knowledge base accessibile a livello globale, contenente le TTP degli hacker, definite in base a osservazioni effettuate nel mondo reale. Viene utilizzato come fondamento per lo sviluppo di modelli e metodologie specifici per le minacce. Consente ai threat hunter di mappare i comportamenti dei cybercriminali a varie TTP identificate in passato, e questo a sua volta permette di determinare in quale stadio del suo ciclo di vita si trovi un attacco. È fondamentale per la fase "Orientare" del framework OODA.



Puoi ottenere informazioni più dettagliate sul framework MITRE ATT&CK su questa pagina.

Metodi Di Threat Hunting

In questa sezione esamineremo alcuni dei più comuni metodi di threat hunting. Spesso Sophos comincia il threat hunting scegliendo tra due modalità diverse.

Threat Hunting Con L'Utilizzo Di Indizi

Nella nostra organizzazione, ogni rilevamento che richiede un'indagine più approfondita viene verificato da un analista in carne e ossa, che può applicare contesto aziendale e ragionamento umano a qualsiasi situazione. L'analista osserverà i comportamenti e il contesto aziendale precedentemente determinato, formulerà un'ipotesi e successivamente intraprenderà un'azione. L'ipotesi potrebbe prevedere un intervento diretto sul potenziale incidente, oppure la decisione di svolgere ulteriori indagini per aumentare le informazioni disponibili.

Per completare il ciclo, l'analista attenderà e controllerà i risultati dell'ipotesi e dei test. Se occorre indagare ulteriormente, può ripetere il ciclo fino a quando non giunge a una decisione definitiva. Se nel frattempo l'evento si dovesse evolvere al punto di diventare un incidente attivo, l'analista passerà alla modalità di risposta completa per contrastare attivamente la minaccia.

Threat Hunting Senza L'Utilizzo Di Indizi

Mentre il threat hunting con indizi richiede il rilevamento o la generazione da parte di uno dei nostri sensori di un "segnale" potenzialmente pertinente, il threat hunting senza indizi è più strutturato. Anche se continuiamo a utilizzare i nostri algoritmi di intelligenza artificiale per elaborare le elevate quantità di dati da cui attingiamo, il threat hunting senza indizi è quasi sempre coordinato da un analista umano.

Invece di basarci sul segnale sistematico iniziale per decidere che occorre svolgere indagini, eseguiamo proattivamente query sugli ambienti di uno o più clienti. Questo può avvenire per vari motivi, come ad esempio:

- Quando un cliente nello stesso settore verticale è stato attaccato in un modo specifico e pertanto desideriamo svolgere le dovute verifiche per assicurarci che gli stessi cybercriminali non stiano cercando di colpire altri nostri clienti
- Quando i SophosLabs comunicano al team MDR la presenza di un attacco grave che cerca di colpire i clienti che operano nello stesso settore verticale o che presentano caratteristiche simili
- Quando si verifica un evento significativo nel panorama della sicurezza informatica e vogliamo stabilire se ha avuto ripercussioni sui nostri clienti

Case study: La Caccia Al Ransomware Che Ha Portato Alla Luce Un Leggendario Trojan Di Internet Banking

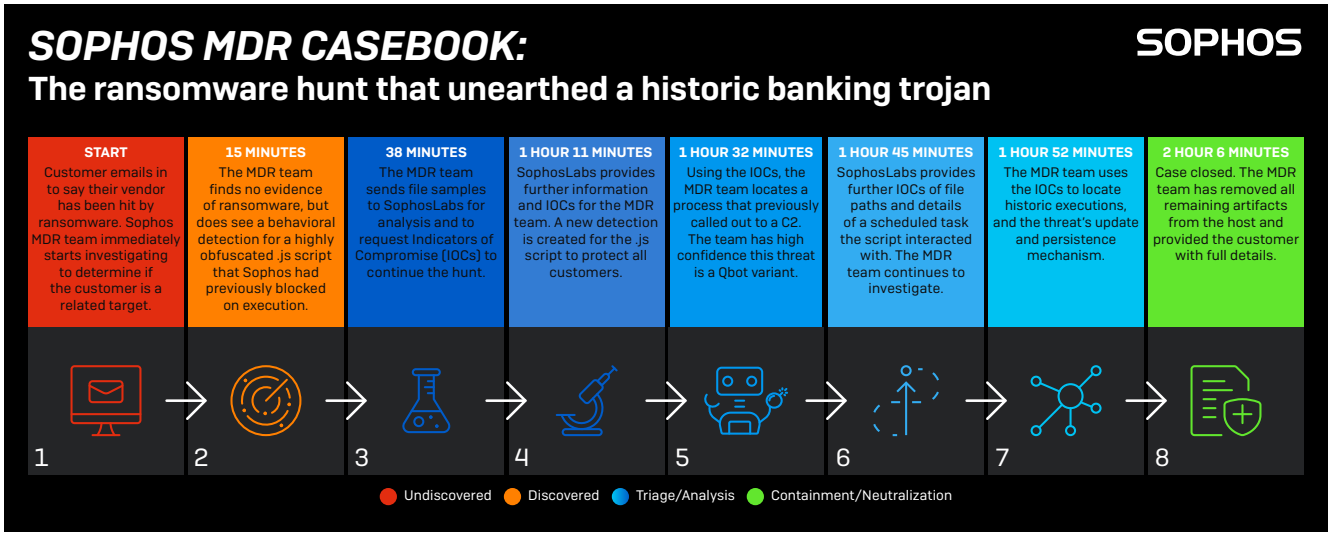
Ora che abbiamo definito le complesse caratteristiche del threat hunting, procediamo ad analizzare un'attività di threat hunting. Questo caso, su cui ha lavorato il team Sophos MDR, è un ottimo esempio di come il threat hunting sia in grado di portare alla luce anche le situazioni più inattese. In questo caso, un cliente ci ha contattati per comunicarci che uno dei vendor con cui aveva collaborato era stato colpito dal ransomware. Di conseguenza, temeva che l'attacco avesse infettato anche la sua organizzazione.

Il team Sophos MDR ha subito avviato le indagini, in collaborazione con i nostri esperti dei SophosLabs. Il team è rapidamente giunto alla conclusione che non c'era alcuna traccia di ransomware. A questo punto alcuni team avrebbero potuto chiudere il caso e passare ad altre attività. Tuttavia, il team Sophos MDR ha proseguito con le indagini, che hanno portato alla luce la presenza di un trojan di internet banking ormai leggendario.

Il cliente ha quindi potuto recuperare la propria tranquillità, nella consapevolezza che la sua azienda non era stata coinvolta in un attacco ransomware, e che un malware di internet banking del passato era stato rimosso: un risultato che non sarebbe stato possibile senza l'intervento di personale esperto.

Come dimostra questo caso, sebbene il ransomware sia spesso la minaccia su cui si tende a focalizzare l'attenzione, è fondamentale essere consci che esistono anche attacchi che cercano di passare inosservati.

In due ore e 6 minuti, l'intero incidente era stato analizzato e risolto.



Per un'analisi approfondita di questo caso, leggi l'articolo su questo link.

Preparazione Per Il Threat Hunting: Cinque Passaggi Per Garantire Ottimi Risultati

Molto probabilmente, a questo punto avrai già una buona comprensione di tutto quello che riguarda il threat hunting. Tuttavia, prima di cominciare, è essenziale verificare che la tua organizzazione sia in grado di svolgerlo in maniera efficace.

1. Capire Il Grado Di Maturità Delle SecOps

Prima di poter iniziare a comprendere i tuoi potenziali avversari informatici, devi conoscere la situazione attuale delle tue SecOps. Mappare i processi a un modello di maturità di cybersecurity (come CMMC) è un ottimo modo per determinare il tuo livello di preparazione (o impreparazione) per il theat hunting. Potrebbe anche essere utile eseguire una valutazione del tuo profilo di sicurezza, per stabilire quanto potresti essere vulnerabile alle minacce.

2. Decidere Come Svolgere Il Threat Hunting

Una volta determinato il tuo livello di maturità informatica, puoi decidere se svolgere il threat hunting internamente, se affidarlo a terzi o se adottare una combinazione di questi due approcci.

3. Identificare Eventuali Lacune Nelle Tecnologie

Valuta gli strumenti che utilizzi al momento e identifica di cos'altro hai bisogno per svolgere il threat hunting in maniera ottimale. Quanto sono efficaci le tue tecnologie di prevenzione? Offrono o supportano funzionalità di threat hunting tramite EDR/XDR?

4. Identificare Eventuali Lacune Nelle Competenze

Il threat hunting è complesso e richiede competenze tecniche specializzate. Se non sono disponibili internamente, puoi esplorare corsi di formazione che aiutano a sviluppare le competenze di cui hai bisogno. Puoi anche collaborare con un fornitore esterno per estendere le potenzialità del tuo team.

5. Sviluppare E Implementare Un Piano Di Incident Response

Prima di cominciare a svolgere il threat hunting, è essenziale che sia stato implementato un piano di incident response funzionale, per fare in modo che ogni risposta venga misurata e controllata. Un piano strategico di risposta ben strutturato e comprensibile, nonché semplice da implementare per tutte le persone coinvolte, riduce drasticamente l'impatto di un attacco sull'organizzazione.

Per essere efficace, un piano di incident response deve definire sia i protocolli di preparazione, rilevamento, reportistica, valutazione, analisi, contenimento e neutralizzazione, sia le attività post-risoluzione. Per consigli su come strutturare un piano efficace per la risposta agli incidenti, consulta la nostra guida alla incident response.

Per ulteriori suggerimenti pratici su come prepararti e come svolgere il threat hunting, dai un'occhiata alla Sophos Threat Hunting Academy.

Come Ti Può Aiutare Sophos

Come abbiamo visto, il threat hunting efficace è un'attività estremamente complessa, che richiede sia l'uso di tecnologie di ultima generazione che l'intervento umano di personale con alti livelli di preparazione ed esperienza. Fortunatamente, Sophos può aiutarti a raggiungere i tuoi obiettivi di threat hunting, indipendentemente dal tuo grado di maturità di cybersecurity.

Prevenzione Degli Incidenti, Per Impedire Alle Minacce Di Infiltrarsi Nella Rete: Sophos Intercept X Endpoint

I threat hunter possono svolgere il proprio lavoro in maniera efficiente solo se non vengono bombardati costantemente da avvisi di sicurezza. Uno dei modi per evitare che succeda è implementare tecnologie di prevenzione di primissima categoria, in modo che i responsabili di sicurezza possano focalizzarsi su un numero minore di rilevamenti accurati, semplificando così il processo di indagine e risposta. Ed è proprio questo che offre Sophos Intercept X Endpoint.

Sophos Intercept X è la soluzione endpoint leader di settore, in grado di ridurre la superficie di attacco e impedire l'esecuzione degli attacchi informatici. Offre la combinazione ottimale tra tecnologie antiexploit e antiransomware, deep learning con intelligenza artificiale e opzioni di controllo, per bloccare le minacce prima che possano compromettere i sistemi. Intercept X adotta un approccio alla protezione endpoint a 360 gradi e basato sulla difesa in profondità, differenziandosi dai sistemi tradizionali che si affidano a una sola tecnica principale.

Le capacità di prevenzione della protezione endpoint di Sophos Intercept X bloccano il 99,98% delle minacce (secondo il punteggio medio delle valutazioni di AV-TEST, condotte tra gennaio e novembre 2021). I responsabili di sicurezza possono così focalizzarsi sugli indicatori sospetti che richiedono un intervento umano.

Qui puoi scoprire di più su Intercept X Endpoint o avviarne una prova gratuita.

Threat Hunting Autonomo: Sophos XDR

Realizzata per gli analisti di sicurezza che lavorano in team SOC dedicati e per gli amministratori IT che svolgono incarichi di sicurezza e si occupano di altre mansioni informatiche, Sophos XDR permette al tuo team di rilevare gli incidenti, svolgere le indagini e rispondere agli attacchi su endpoint, server, firewall, workload del cloud, e-mail, dispositivi mobili e altri sistemi.

Trova immediatamente le informazioni che ti interessano, selezionando la tua configurazione ideale da un catalogo di modelli precompilati e personalizzabili, che includono moltissimi scenari di threat hunting e IT Operations diversi. In alternativa, puoi anche crearne uno tu. Avrai accesso a dati in tempo reale sui dispositivi, a un massimo di 90 giorni di dati su disco, a 30 giorni di dati archiviati sul repository cloud del Sophos Data Lake, nonché a un elenco generato automaticamente di elementi sospetti. In questo modo, saprai sempre da dove cominciare.

Se desideri provare Sophos XDR per svolgere attività di threat hunting in maniera autonoma, Sophos ti offre tutti gli strumenti necessari per condurre attività avanzate di threat hunting e protezione dell'integrità delle SecOps. Puoi attivare una prova gratuita direttamente dal tuo prodotto (se hai un account Sophos Central) oppure avviare una prova di Sophos Intercept X, che include XDR.

Threat Hunting Come Servizio Completamente Gestito O Come Risorsa Per Estendere Le Potenzialità Del Tuo Team: Sophos MDR

Sophos MDR è una soluzione MDR poliedrica, completa e pluripremiata, che applica l'esperienza, le competenze e le molteplici abilità del team di analisti Sophos alla tua rete e ai tuoi ambienti cloud. Sophos diventa a tutti gli effetti un'estensione delle tue SecOps, aggiungendo tutte le sue potenzialità a quelle del tuo team.

Il team Sophos MDR, composto da esperti di threat hunting e risposta alle minacce:

- Intercetta e conferma proattivamente la presenza di potenziali minacce e incidenti
- Utilizza tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce
- Applica il giusto contesto imprenditoriale per le minacce identificate
- Avvia azioni volte a fermare, contenere e neutralizzare le minacce in remoto
- Offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti

Anche se la tua organizzazione ha un Security Operation Center ben rodato, potrebbe esserti utile avere a disposizione una mano in più per monitorare gli ambienti e accertarti che nessuna minaccia possa sfuggire alla tua attenzione. Sophos MDR offre sia threat hunting che protezione endpoint, e garantisce supervisione quotidiana a cura di esperti. La tua rete e le tue risorse cloud sono la priorità principale per gli analisti di rete e i threat hunter Sophos, che svolgono attivamente attività di monitoraggio, correzione e neutralizzazione delle minacce per conto tuo.

Con un adeguato servizio MDR, sia tu che la tua organizzazione potete fare sonni tranquilli, nella certezza di essere nelle mani di un team di esperti altamente qualificati, che monitorano ininterrottamente la tua azienda, individuando proattivamente le minacce, indagando sulle attività sospette e rispondendo ai potenziali incidenti. Con un panorama delle minacce di cybersecurity in costante evoluzione, poter fare affidamento su un team interamente focalizzato sulla cybersecurity favorisce la tranquillità.

Per parlare di come Sophos MDR può assistere la tua organizzazione, rivolgiti al tuo rappresentante Sophos oppure richiedi una richiamata. Nel frattempo, dai un'occhiata alle ultime notizie sulla ricerca e ai casebook di MDR.

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

22-08-08 WP-IT (PC)

SOPHOS