ANOMALI®

Playbook **Gestione di Threat Intelligence**

La tua Guida per la valutazione, la selezione, la gestione e l'ottimizzazione della tua piattaforma di Threat Intelligence (TIP)

Indice

Capitolo 1. Introduzione

Che cos'è una piattaforma di Threat Intelligence?

Gli autori delle minacce sono in continua evoluzione e i loro attacchi sono sempre più sofisticati. Le organizzazioni cercano di contestualizzare questi attacchi sfruttando l'intelligence delle minacce, che sono informazioni processabili riguardanti gli avversari e le loro Tattiche, Tecniche e Procedure (TTP). Una Piattaforma di Threat Intelligence (TIP) è una soluzione che automatizza gran parte del lavoro manuale di ricerca sull'intelligence delle minacce, riduce i tempi di rilevamento e consente agli analisti di indagare sulle minacce informatiche e combatterle in un ambiente consolidato che favorisce la collaborazione con i team all'interno della tua azienda.

L'utilizzo di Threat Intelligence per migliorare il rilevamento delle minacce

Un recente sondaggio condotto tra i professionisti IT dal Ponemon Institute ha indagato sull'uso da parte degli intervistati della Threat Intelligence per il rilevamento delle minacce.

- L'**85%** degli intervistati nel sondaggio Ponemon afferma che la **Threat Intelligence è essenziale** per un approccio di sicurezza efficace, ma solo il **41%** afferma di avere **metodi efficaci per individuare le minacce esterne**.
- Meno della **metà (il 48%)** degli intervistati dal Ponemon dispone di una **piattaforma dedicata di Threat Intelligence**.
- Solo il **33%** degli intervistati dal Ponemon ha dichiarato di **disporre di un budget adeguato per il rilevamento delle minacce**.

Fonte: The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies, Ponemon Institute, 2019

Capitolo 1. Introduzione

In che modo una piattaforma di Threat Intelligence è diversa dalle altre soluzioni di sicurezza:

- ***Aggregazione di informazioni provenienti da più fonti***: la maggior parte delle soluzioni di sicurezza si basa unicamente sulle informazioni interne al proprio ambiente. Una piattaforma di Threat Intelligence avanzata utilizza e mette in correlazione i dati provenienti da fonti esterne e interne, fornendo agli analisti TI informazioni più complete sulle minacce note o sospette.
- ***Cura, normalizzazione, approfondimento e classificazione dei rischi dei dati***: il processo di creazione manuale di report di intelligence sulle minacce, bollettini e profili provenienti da singoli indicatori di compromissione è un'operazione dispendiosa in termini di tempo e denaro. Una piattaforma di Threat Intelligence automatizza gran parte di questo processo, consentendo agli analisti di dedicare meno tempo all'assemblaggio dei dati e più tempo a fornire un'intelligence ad alta fedeltà a supporto di una difesa proattiva.
- ***Integrazione con i sistemi di sicurezza esistenti***: molti fornitori di sicurezza cercano di sostituire gli altri sistemi. Una TIP funziona in combinazione con le soluzioni esistenti, aggiornando l'output di tutte le soluzioni di sicurezza.
- ***Analisi e condivisione della Threat Intelligence***: la creazione della Threat Intelligence non ha senso se non è condivisa con altri analisti. L'effetto ottenuto dalla condivisione della Threat Intelligence in modo sicuro sono output più completi e affidabili che possono essere utilizzati per soluzioni più rapide.

Gli attori della minaccia riutilizzano molti dei propri dispositivi e strategie TTP per colpire organizzazioni e infrastrutture simili. Maggiori saranno le informazioni a tua disposizione sugli attori della minaccia e sulla loro contestualizzazione e più velocemente e più facilmente il tuo team di sicurezza riuscirà a evitare che subiate danni significativi.

Capitolo 1. Introduzione

Panoramica delle fonti dei dati delle minacce

Le piattaforme di Threat Intelligence sono progettate per sfruttare le numerose fonti di dati sulle minacce che possono variare sia come formato che come settore d'interesse. I team addetti alla sicurezza selezionano i feed delle minacce per ricevere informazioni rilevanti per la loro organizzazione.

Le tipiche fonti di dati includono:

- ***Feed Premium di terze parti***: i fornitori di servizi di sicurezza vendono feed altamente specializzati, come ad esempio informazioni su attori di minacce statali o il deep e dark web. Questi feed sono in genere costituiti da informazioni più complete e difficili da acquisire.
- ***Feed open source***: l'intelligence open source è un'informazione gratuita che proviene da ricercatori di sicurezza, blog di fornitori e blacklist o whitelist disponibili pubblicamente.
- ***Gruppi di condivisione delle minacce***: i gruppi di condivisione delle minacce, come gli Information Sharing and Analysis Centers (ISAC), condividono i dati sulle minacce tra membri affidabili dello stesso settore.
- ***Piattaforme di analisi open source***: la MISP è una piattaforma open source per la condivisione delle informazioni sui malware. Anche se non dispone delle funzionalità complete di una piattaforma di Threat Intelligence, la MISP è ideale per coloro che iniziano a raccogliere, condividere, archiviare e correlare gli IOC (Indicator of Compromise).
- ***Knowledge Base della community***: una delle knowledge base attualmente più diffuse per la sicurezza informatica è il framework MITRE ATTACK™. Si tratta di una knowledge base di tattiche e tecniche degli avversari basate su osservazioni del mondo reale accessibile a livello globale. Questo framework viene utilizzato anche come base per lo sviluppo di modelli e metodologie di minacce specifiche nel settore privato, negli enti pubblici e nella community di prodotti e servizi di sicurezza informatica.

La qualità dei dati e delle analisi ricevuti da Anomali ha migliorato la conoscenza del settore della sicurezza informatica dei nostri utenti consentendo loro di identificare in modo più accurato le minacce interne ed esterne all'organizzazione e di migliorare i tempi delle indagini.

Professionista IT | Settore aerospaziale e difesa

Capitolo 2. Quali problemi affrontano le piattaforme di Threat Intelligence?

Automazione dei dati sulle minacce per informazioni più rapide

Il numero e la complessità degli attacchi di cyber security aumentano ogni giorno. Le organizzazioni devono sapere esattamente quali minacce devono affrontare per poter reagire in modo proattivo e stabilire come rispondere agli incidenti in modo più efficace.

Gli analisti cercano le prove di un attacco esaminando gli avvisi di varie soluzioni di sicurezza, in genere del sistema Security Information and Event Management (SIEM). Tuttavia, poiché i SIEM sono stati progettati per elaborare e memorizzare tutti i dati di un'organizzazione, molti avvisi vengono generati senza che ci siano reali minacce, creando falsi positivi. Questi falsi positivi, sebbene non siano effettivamente dannosi, sprecano risorse preziose necessarie per l'analisi dell'avviso.

Con un personale già limitato, ciò può essere penalizzante per l'efficacia di un team addetto alla sicurezza. La Threat Intelligence aiuta gli analisti a filtrare questi avvisi e a convalidarli correlando una intelligence delle minacce accurata con gli indicatori interni all'organizzazione.

La Threat Intelligence può presentare una serie di problemi. Gli IOC possono essere anche milioni e il processo di identificazione di quelli pertinenti richiede molto lavoro. Le piattaforme di Threat Intelligence sono progettate per correlare automaticamente gli input e ottenere informazioni molto più rapide sulle minacce informatiche.

Al momento sono disponibili **350.000** posti di lavoro nella sicurezza informatica e si prevede che entro il 2021 si registrerà una carenza globale di 3,5 milioni di addetti alla cyber security

Fonte: Cyber Security Ventures

Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Utenti frequenti di Threat Intelligence

Le piattaforme di Threat Intelligence sono progettate per restituire agli analisti il tempo che altrimenti servirebbe loro per gestire manualmente le informazioni. I dati grezzi vengono trasformati in informazioni facilmente comprensibili, immediatamente condivisibili e, soprattutto, processabili. Grazie all'intelligence, all'automazione e all'integrazione con gli strumenti di sicurezza esistenti, le organizzazioni sono in grado di comprendere le minacce rilevanti per loro. Gli utenti più frequenti delle piattaforme di Threat Iintelligence includono:

- Analisti di intelligence per le minacce informatiche
- Analisti SOC (Security Operation Center)
- Ricercatori
- Analisti IR (Incident Response)
- CISO (Chief Information Security Officer)

Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Aggregazione e cura dei dati

Le piattaforme di Threat Intelligence raccolgono automaticamente dati sulle minacce, informazioni e intelligence da numerose fonti. Gli analisti della sicurezza devono poter configurare in modo flessibile l'aggregazione di dati e poter acquisire rapidamente informazioni da fornitori o terzi parti affidabili. Questo archivio di informazioni viene quindi incanalato in indagini e altri strumenti di sicurezza.

Molti degli input di una TIP possono essere doppioni, non più dannosi o non essere minacce abbastanza gravi da richiedere un intervento. Le TIP hanno algoritmi di Machine Learning (apprendimento automatico) per classificare le informazioni e riordinare i singoli IOC in base a una moltitudine di fattori rilevanti per le minacce informatiche. Gli indicatori curati vengono presentati in un formato di facile lettura con un punteggio di rischio e le relative informazioni.

> La nostra capacità di acquisire informazioni, arricchire e gestire cluster basati su tag relazionali e tipi di IOC ha notevolmente migliorato i problemi relativi alle minacce per quanto riguarda la parte Intel del nostro SOC. Una volta raggiunto il livello di integrazione dell'automazione, il guadagno è stato esponenziale
>
> ***Supervisore SOC | Società di energia e servizi di pubblica utilità***

Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Indagine

Gli analisti di Threat Intelligence sono responsabili dell'analisi delle minacce e della creazione di nuove informazioni sulle minacce per guidare la strategia di sicurezza. Questo tipo di analisi richiede in genere decine di strumenti e innumerevoli ore di lavoro.

Una TIP consente agli analisti di condurre indagini tramite flussi di lavoro automatizzati e scalabili e di collaborare con team diversi. Gli analisti possono così gestire facilmente IOC noti e focalizzarsi sull'analisi delle minacce invece sconosciute. All'interno della stessa indagine, gli analisti possono associare indicatori ed intelligence, produrre bollettini sulle minacce arricchiti di indicatori, e identificare gli attori di minaccia e i relativi TTP.

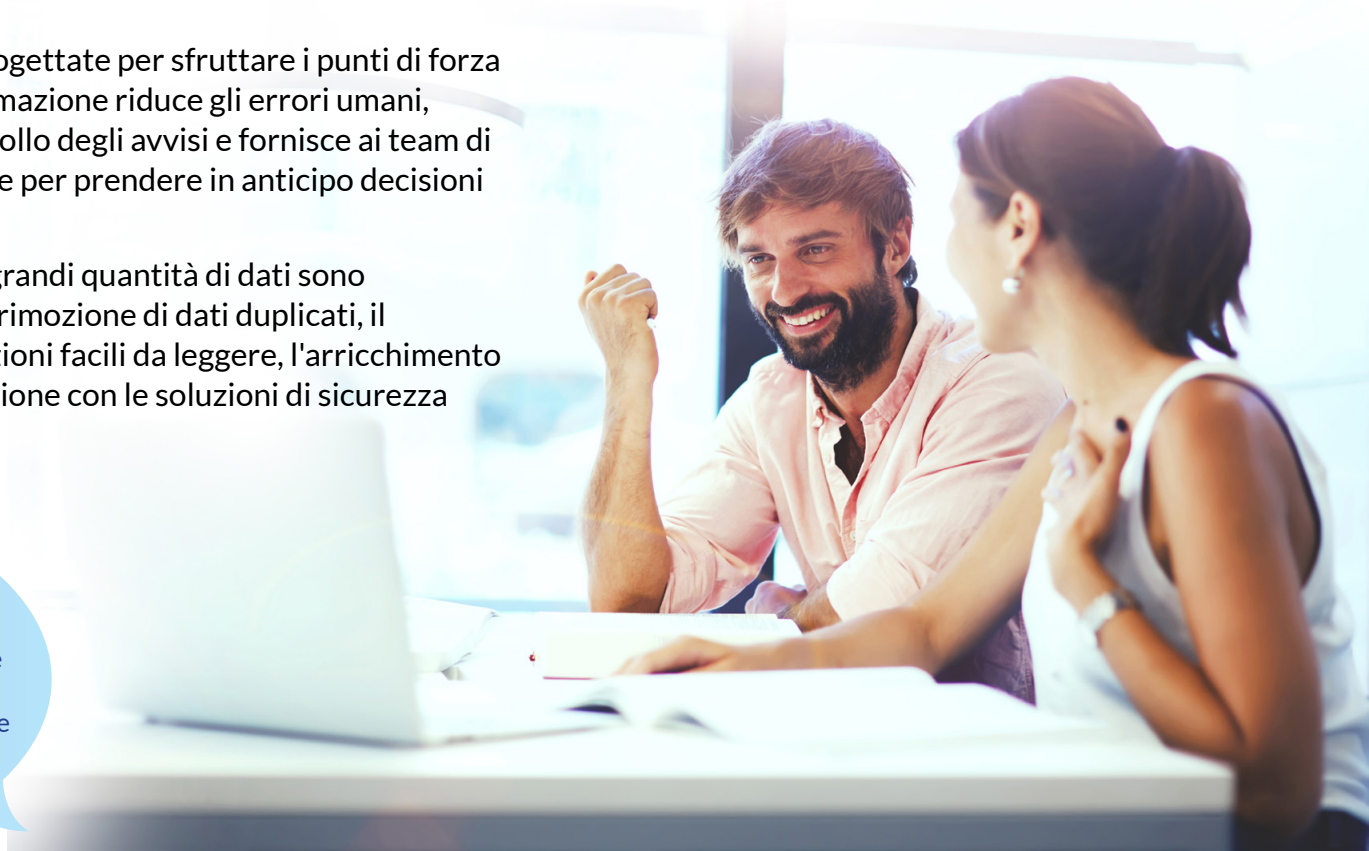
Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Automazione

Le piattaforme di Threat Intelligence sono progettate per sfruttare i punti di forza delle capacità umane e dei macchinari. L'automazione riduce gli errori umani, evita agli analisti il lavoro estenuante di controllo degli avvisi e fornisce ai team di sicurezza il tempo e le informazioni necessarie per prendere in anticipo decisioni sulle minacce informatiche.

I processi laboriosi o ripetitivi che implicano grandi quantità di dati sono completamente automatizzati. Ciò include la rimozione di dati duplicati, il consolidamento di formati diversi in informazioni facili da leggere, l'arricchimento degli indicatori con dati aggiuntivi e l'integrazione con le soluzioni di sicurezza esistenti.

> Anomali ci consente di gestire la grande quantità di dati generati da più risorse Intel e di identificare le minacce rilevanti per la nostra organizzazione. Ora possiamo importare più rapidamente i dati delle minacce, correlare i rischi e quindi esportare solo gli indicatori necessari alla nostra SIEM per una gestione e una mitigazione proattive delle minacce.
>
> ***Analista di Intelligence | FinServ***



Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Integrazione

Le TIP fungono da intermediarie tra le informazioni e le soluzioni di sicurezza esistenti, eliminando la necessità di configurare manualmente una connessione. Gli indicatori vengono inviati ai firewall e ai sistemi di rilevamento delle intrusioni per il blocco attivo, messi in correlazione con le informazioni contenute nelle soluzioni di endpoint e SIEM per assegnare priorità agli avvisi e inviati alle piattaforme di orchestrazione per migliorare i flussi di lavoro.

La flessibilità di queste integrazioni migliora rapidamente la capacità di un team di sicurezza di identificare e contrastare le minacce. Questo vale sia per lo stack di sicurezza di un'organizzazione interamente basato su cloud che per quelli in loco, o in una qualsiasi combinazione delle due situazioni.

Capitolo 3. Cosa cercare in una piattaforma di Threat Intelligence?

Collaborazione e condivisione

Le organizzazioni sono in grado di anticipare le strategie degli autori degli attacchi più efficacemente, identificare le azioni dannose e bloccare gli attacchi con una Threat Intelligence dettagliata e contestualizzata. I team di sicurezza possono migliorare le proprie difese collaborando con altri team per creare questa intelligence e proteggere la community attraverso la condivisione.

Le TIP facilitano la collaborazione sulle indagini e consentono la condivisione istantanea e bidirezionale dell'intelligence. I gruppi di condivisione come gli Information Sharing and Analysis Centers (ISAC) in genere sfrutteranno le piattaforme di Threat Intelligence per allineare aziende in settori simili e aiutare le organizzazioni a trarre vantaggio da risorse e competenze diversificate.

L'automazione di Anomali ci ha consentito di ricercare e condividere informazioni sugli autori di attacchi informatici con i partner del settore in modo rapido e sicuro. Inoltre, l'intelligence che riceviamo da organizzazioni fidate viene automaticamente inserita nei nostri strumenti per la creazione di avvisi.

Professionista IT | Società di energia e servizi di pubblica utilità

Anche se il **59%** degli intervistati afferma che le proprie organizzazioni condividono la Threat Intelligence con altri, il **56%** cita il possibile abuso dei propri dati come motivo della riluttanza a condividere la Threat Intelligence.

Fonte: The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies, Ponemon Institute, 2019

Capitolo 4. Come si inserisce la gestione delle minacce nel ciclo di vita della sicurezza

Stabilire un solido approccio alla sicurezza è un processo iterativo. Tuttavia, può essere difficile tentare di migliorare tutto ciò che entra nel ciclo di vita della sicurezza, ad esempio pianificazione, monitoraggio, rilevamento, analisi, risposta, risoluzione e feedback. La Threat Intelligence supporta ciascuna di queste fasi fornendo un contesto che aiuta a guidare queste azioni in modo che siano più veloci e mirate.

Pianificazione

I team addetti alla sicurezza devono pianificare ogni possibilità. Valutano le minacce che è più probabile che la loro organizzazione si trovi a fronteggiare in base al prodotto o al servizio che produce, in base alla sua geolocalizzazione, alle sue affiliazioni politiche e molto altro ancora. La Threat Intelligence consente a questi team di provare o smentire le proprie teorie. Gli analisti ottengono una maggiore visibilità sulle minacce che possono interessarli e sul modo in cui operano gli autori degli attacchi. Oltre all'analisi di questi dati, informazioni e intelligence, le TIP consentono agli analisti di selezionare e utilizzare gli strumenti più efficaci per la prevenzione e la mitigazione.

Monitoraggio e rilevamento

Esistono diversi modi per rilevare e monitorare comportamenti dannosi, ma l'integrazione della Threat Intelligence è l'unico modo per difendersi in modo proattivo da queste minacce. L'inserimento di un contesto esterno e verificato sugli autori delle minacce e sui loro dispositivi di protezione elimina la necessità per gli analisti della sicurezza di eseguire le ricerche manuali che in precedenza erano necessarie per determinare cos'è dannoso e cosa non lo è. Le organizzazioni possono identificare rapidamente se gli indicatori dannosi sono presenti o meno mettendo in correlazione la Threat Intelligence con i dati provenienti dai sistemi di sicurezza esistenti. Qualsiasi elemento identificato come sospetto può essere inviato automaticamente ai punti di integrazione per il monitoraggio. Ciò consente agli strumenti e al personale di bloccare le minacce ***prima*** che queste entrino nella rete.

Capitolo 4. Come si inserisce la gestione delle minacce nel ciclo di vita della sicurezza

Indagine e analisi

Una volta individuate le entità dannose, gli analisti conducono indagini per determinare l'impatto sulle loro organizzazioni. Le TIP forniscono agli analisti un banco di lavoro per esaminare i dati raccolti e correlare diverse informazioni. Gli analisti partendo dai singoli IOC possono arricchire le informazioni esistenti con dati presi da WHOIS, PassiveDNS e altro ancora per scoprire minacce sconosciute in precedenza.

Risposta e risoluzione

Durante un incidente, una TIP aiuta gli analisti a identificare i modelli e gli attori di minaccia associati per informare più rapidamente gli addetti agli interventi di risoluzione e risposta. Ad esempio, una TIP può informare un analista che un particolare attore è noto per utilizzare uno strumento o una tattica specifici, potenziando un'indagine sugli incidenti più mirata.

Anomali ci consente di automatizzare l'inserimento degli indicatori, offrendo così all'analista più tempo per esaminare e contestualizzare gli incidenti con i dati aggiuntivi forniti in Anomali.

Analista di Intelligence | FinServ

Capitolo 4. Come si inserisce la gestione delle minacce nel ciclo di vita della sicurezza

Feedback

La fase di feedback è fondamentale per migliorare la tua sicurezza attuale. Le piattaforme di Threat Intelligence sono utili per stabilire dove migliorare la tua difesa poiché si collocano tra gli strumenti e le informazioni.

Le aree principali da considerare sono:

- ***La fase di monitoraggio*** per determinare quali fonti di informazioni sono più utili per identificare e bloccare le minacce.
- ***La fase di rilevamento e analisi*** per documentare il tempo necessario per raggiungere una conclusione.
- ***La fase di risposta e risoluzione*** per determinare se sono state acquisite le informazioni corrette e quanto tempo è stato necessario per reagire. Ad esempio, se un attore di minaccia riesce a infettare un sistema, un utente TIP può verificare se le informazioni sulla minaccia erano già disponibili nell'archivio o, in caso contrario, quale altra fonte contenga tali informazioni.

Capitolo 5. Anomali®

Gestione di Threat Intelligence con Anomali

Anomali sfrutta i dati, le informazioni e l'Intelligence per prendere decisioni efficaci in materia di cyber security. Si tratta di una piattaforma che automatizza il rilevamento, l'assegnazione di priorità e l'analisi delle minacce più gravi per la tua organizzazione. Grazie al machine learning, all'automazione e a un esteso ecosistema di partner, Anomali consente agli analisti di sfruttare la Threat Intelligence per ottenere migliori informazioni e migliori risposte agli attacchi informatici.

I tre componenti seguenti fanno parte della piattaforma Anomali.

- **ThreatStream®** è la piattaforma di Threat Intelligence progettata per gli analisti per creare intelligence per le minacce e indagare sugli incidenti di sicurezza. Raccoglie, contestualizza e classifica i complessi e numerosissimi indicatori di rischio con il machine learning per dare priorità agli avvisi urgenti e guidare la strategia di sicurezza.
- **Anomali Match™** è un motore per il rilevamento delle minacce realizzato appositamente per automatizzare e velocizzare il rilevamento delle stesse nel tuo sistema. Anomali Match mette in correlazione dodici mesi di metadati con Threat Intelligence attiva per identificare alla minacce in precedenza sconosciute alla tua organizzazione.
- **Anomali Lens™** consente agli analisti delle minacce e della sicurezza di prendere decisioni più rapide e accurate. Anomali Lens offre accesso immediato all'intelligence strategica e tattica da qualsiasi pagina del browser o del cellulare. Analisti di qualsiasi livello di esperienza possono trarre vantaggio dall'uso di valori in tempo reale e informazioni contestualizzate che accelerano il processo decisionale. I dirigenti possono facilmente accedere all'intelligence comodamente dai loro dispositivi per rimanere informati sulle minacce più recenti che potrebbero colpire la loro azienda.

Vantaggi di Anomali

- Identificazione delle minacce mirate alla tua organizzazione
- Automazione del rilevamento e dell'analisi delle minacce
- Miglioramento della risposta con informazioni sugli attori e i loro comportamenti
- Risparmio di tempo e risorse grazie alla riduzione dell'efficacia degli attacchi
- Possibilità di collaborazione tra gruppi CTI interni ed esterni

> Anomali ci ha consentito di raggiungere un livello superiore in termini di sicurezza informatica, fornendo aggiornamenti sull'intelligence delle minacce arricchiti da tutte le informazioni di cui necessitiamo. In questo modo, possiamo difendere la nostra organizzazione dalle minacce emergenti.
>
> ***Responsabile IT | Società di servizi informatici***

Capitolo 6. Casi studio

Caso studio sulla Colorado Threat Intelligence Sharing (CTIS)

Nel 2017, lo stato del Colorado ha costituito la Colorado Threat Intelligence Sharing Network (CTIS) in collaborazione con Anomali, mettendo in comunicazione governi statali, regionali, provinciali e comunali per consentire ai team di sicurezza di condividere e analizzare le minacce e rispondere in maniera più efficace.

Problematica

Lo Stato del Colorado ha lottato per creare un portale sicuro dove le community locali potessero condividere informazioni fondamentali sulla sicurezza informatica. Il precedente metodo di condivisione delle informazioni tramite e-mail non era sicuro, né collaborativo o sufficientemente utile per le situazioni di emergenza. Senza una condivisione delle minacce sicura e ininterrotta, i dipartimenti statali rischiano di non ricevere informazioni critiche per prevenire e contenere gli attacchi informatici.

Soluzione

Lo Stato del Colorado ha collaborato con Anomali per fornire una piattaforma completa di analisi e condivisione delle minacce, consentendo a tutti i dipartimenti governativi di condividere informazioni riservate in un'unica posizione centrale. Questo portale offre una maggiore visibilità ai governi locali per condividere istantaneamente i dati relativi a potenziali minacce all'interno di una cerchia chiusa di utenti totalmente affidabili.

Vantaggi chiave

- Condivisione sicura e continua delle minacce, accessibile a tutti i dipartimenti locali, tribali, regionali e statali in tutto il Colorado.
- Possibilità di collaborare e condividere informazioni con altri stati tramite l'ISAC multi-stato.
- Potente set di strumenti per l'indagine delle minacce, che consente agli analisti della sicurezza di valutare e comprendere rapidamente gli attacchi.

> "Abbiamo sviluppato la CTIS in tutto lo Stato del Colorado per rispondere a un'esigenza critica di promuovere una più ampia condivisione delle minacce informatiche", ha dichiarato Trevor Timmons, Chief Information Officer dello Stato del Colorado. "Abbiamo assistito a una rapida adozione da parte di tutti gli enti governativi dello Stato del Colorado, con la collaborazione attiva di diversi dipartimenti e contee. Incoraggiamo tutti gli stati a implementare programmi di condivisione delle minacce informatiche per migliorare il proprio approccio alla sicurezza."

Scarica il white paper »

Capitolo 6. Casi studio

Caso studio su Federal System Integrator

L'FSI (Federal Systems Integrator) è un fornitore comprovato di soluzioni informative, ingegneria e analisi per la US Intelligence Community, il Dipartimento della Difesa degli Stati Uniti e altre agenzie federali. Con oltre 40 anni di esperienza, l'FSI progetta, sviluppa e fornisce servizi e soluzioni di importanza critica ad alto impatto per superare i problemi più complessi dei suoi clienti.

Problematica

Lavorando principalmente come integratore di sistemi per clienti in community caratterizzate da intelligence e sicurezza dei dati sensibili, FSI possiede accesso a informazioni importanti e di grande valore. Tale proprietà intellettuale, essenziale per il governo degli Stati Uniti, deve rimanere protetta e sicura.

Soluzione

L'FSI si è rivolto ad Anomali e ha trovato in ThreatStream una soluzione automatizzata di intelligence sulle minacce informatiche. La piattaforma ThreatStream™ contrasta gli avversari unendo l'intelligence processabile con l'infrastruttura di sicurezza esistente.

Vantaggi chiave

- Consolidamento e cura di più fonti di intelligence per le minacce con eliminazione delle ridondanze
- Analisi intervalidata
- Rapida operazionalizzazione dell'intelligence con un'elevata affidabilità

" Lavorare con ThreatStream ci ha aiutato a difenderci in modo molto più efficace dalle minacce, dalle più semplici alle più avanzate, che tentano di compromettere le risorse aziendali quotidianamente." Chief Information Security Officer di Federal Systems Integrator.

Leggi il caso studio completo »

Capitolo 6. Casi studio

Caso studio su UAE Banks Federation (ISAC)

La UAE Banks Federation (UBF) è un'organizzazione no-profit che rappresenta 50 banche membri operanti negli Emirati Arabi Uniti (EAU) e l'associazione leader del settore bancario degli Emirati Arabi Uniti.

Problematica

Gli attacchi informatici sono sempre più frequenti e sofisticati e presentano sfide significative per le organizzazioni e gli interi mercati verticali, che devono proteggere i loro sistemi e dati da avversari capaci. Mentre gli attori e i gruppi di minacce informatiche condividono i loro strumenti, tecniche e procedure (TTP) per attaccare e infiltrarsi nelle organizzazioni, coloro che difendono le reti aziendali e l'infrastruttura critica devono fare lo stesso collaborando con i colleghi in modo affidabile, sicuro ed efficace.

Soluzione

L'iniziativa UBF Tasharuk lanciata nel settembre 2017, basata sul prodotto di punta Anomali ThreatStream. La piattaforma è utilizzata dai membri della Federazione bancaria degli Emirati Arabi Uniti per condividere informazioni pertinenti, tempestive e processabili tra gli istituti finanziari regionali. Un componente con valore aggiunto dell'impegno di Anomali nei centri di analisi e condivisione delle informazioni (ISAC) è il team di ricerca di intelligence noto come "Anomali - Threat Analysis Center (A-TAC)".

Vantaggi chiave

- Miglioramento della consapevolezza situazionale delle minacce informatiche nel settore bancario degli Emirati Arabi Uniti
- Community di professionisti affidabili incentrata sugli obiettivi di sicurezza collettivi
- Approccio alla sicurezza rafforzato e contro gli attacchi informatici per l'intero mercato verticale

" Con il lancio di Tasharuk, siamo stati in grado di semplificare le attività anti-cybercrime delle banche partecipanti e informarle sulle potenziali minacce per migliorarne il sistema di difesa."
HE Abdul Aziz Al Ghurair, Presidente della Federazione delle banche degli Emirati Arabi Uniti.

Visita il blog »

Capitolo 7. Conclusione

Cybercriminali, attori di minaccia a livello delle istituzioni e hacktivist lavorano a tempo pieno per colpire le organizzazioni e sfruttarne i punti deboli. La tua organizzazione può trarre vantaggio dalla comprensione delle vulnerabilità, dalla gestione delle minacce e dalla risoluzione rapida degli eventi.

Tuttavia, anche se la tua organizzazione può aver raccolto grandi quantità di dati da sistemi di sicurezza interni e da feed di minacce esterni, trasferire manualmente tutti questi dati comporta l'uso di enormi risorse umane e tempo, e inevitabilmente si registrerà un gran numero di falsi positivi e falsi negativi. L'analisi di tutti questi incidenti può in breve tempo sovraccaricare un team addetto alla sicurezza già limitato a causa di una crescente carenza di talenti nella cybersicurezza.

Una TIP automatizza il processo di integrazione e analisi dei dati delle minacce interne ed esterne, delle informazioni e dell'intelligence in modo da fornire intelligence sulle minacce processabile, accelerando e semplificando l'intero ciclo di vita della sicurezza. Sia che si tratti di identificare gli IOC pertinenti e di prepararsi ad affrontarli, monitorare, rilevare e analizzare le minacce, rispondere agli eventi o cercare di migliorare le operazioni di sicurezza, una TIP fornisce il contesto necessario per prevenire e affrontare le minacce in modo più rapido ed efficace.

Adottare Anomali equivale ad aggiungere due dipendenti a tempo pieno al tuo team, riducendo allo stesso tempo il tasso di falsi positivi dell'80%.

Direttore IT | Assistenza sanitaria

Lasciati aiutare da Anomali a raggiungere i tuoi obiettivi di gestione e di utilizzo di Threat Intelligence.

PER SAPERNE DI PIÙ

BRIEFING SETTIMANALE SULLE MINACCE DI ANOMALI

STAXX: SOLUZIONE STIX–TAXII GRATUITA

RICHIEDI UNA DEMO

ANOMALI®

Sito Web: www.anomali.com/it

Contattaci: **+1 844-4-THREATS** (847328)
+44 8000 148096 (numero verde internazionale)

Anomali® offre soluzioni di sicurezza informatica basate su intelligence. Le organizzazioni si affidano alla piattaforma Anomali per sfruttare i dati, le informazioni e l'intelligence delle minacce per prendere decisioni efficaci sulla sicurezza informatica che riducono i rischi e rafforzano le difese. Anomali fornisce ai team della sicurezza una piattaforma di Threat Intelligence altamente ottimizzata, potenziata dal Machine Learning, e identifica le minacce nascoste che colpiscono i loro ambienti. La piattaforma Anomali consente alle organizzazioni di collaborare e condividere informazioni sulle minacce tra community affidabili ed è la piattaforma più diffusa per gli ISAC e le principali aziende di tutto il mondo. Per ulteriori informazioni, visita il sito Web www.anomali.com/it e seguici su Twitter @Anomali.

808 Winslow Street, Redwood City, California 94063