proofpoint.

THREAT RESPONSE DI PROOFPOINT

EVITARE CHE INCIDENTI E AVVISI DI SICUREZZA DEGENERINO IN VIOLAZIONI CONCLAMATE

VANTAGGI DI THREAT RESPONSE

- Raccolta automatizzata dei dati delle analisi forensi da sistemi potenzialmente compromessi
- Risparmio di innumerevoli ore per la conferma delle infezioni confrontando i dati del PC del sistema con le analisi forensi della rilevazione
- Riduzione della raccolta di dati manuale da dispositivi esterni, fonti di intelligence ecc.
- Monitoraggio di incidenti e minacce elaborate con un'interfaccia visiva che permette di vedere cosa sta accadendo a colpo d'occhio
- Accelerazione delle decisioni di risposta con visioni integrate dell'attività di minaccia
- Quarantena e contenimento delle minacce automatica o premendo un pulsante per rapida protezione
- Gestione automatica di utenti, e-mail, host, IP e URL su sistemi di esecuzione in tutto il ciclo di vita dell'attacco, al fine di rendere disponibile il personale per altre attività
- Disponibilità di una cronologia verificabile delle azioni di risposta per aumentare il ritorno sull'investimento dell'infrastruttura esistente
- Riduzione della dipendenza dai software personalizzati
- Creazione, monitoraggio e gestione automatica dei rapporti degli incidenti per ridurre l'esigenza di inserimento manuale
- Aggiornamento costante sull'attività dannosa con rapporti aggiornati di utenti, sistemi, gruppi e reparti presi di mira

Threat Response™ di Proofpoint rappresenta un moltiplicatore di forza per le operazioni di sicurezza che predispone e automatizza la risposta all'incidente. La piattaforma associa ricchi dati contestuali agli avvisi di sicurezza per aiutare i team di sicurezza ad assegnare la priorità ed eseguire le azioni di risposta. Raccoglie e analizza il contesto dell'evento di sicurezza relativo a incidenti e indagini e raccoglie le analisi forensi degli endpoint per confermare le infezioni del sistema, al fine di creare profili attivabili degli incidenti. Basandosi sul maggiore contesto, consente azioni di esecuzione e quarantena in modalità automatica oppure premendo un pulsante che sfrutta l'infrastruttura esistente.

LA RISPOSTA MANUALE NON È ADATTA

Presso numerose aziende, la risposta agli incidenti di sicurezza rappresenta un processo lento e impegnativo. Le seguenti attività dispendiose in termini di tempo comportano gravosi colli di bottiglia:

- Identificazione di obiettivi ad alto valore per assegnare la priorità alle minacce
- Identificazione di minacce ad alto valore che possono far parte di campagne o botnet più grandi
- Raccolta e confronto delle analisi forensi degli endpoint per rilevare segnali di infezione
- Gestione di indagini che potrebbero includere più obiettivi e avvisi
- Negoziazione tra sicurezza e infrastruttura con tempi di attuazione dell'esecuzione

Ripetere queste attività per ogni incidente può essere impegnativo per i team di sicurezza i quali, essendo già oberati di lavoro, potrebbero di conseguenza saltare dei passaggi e prendere delle scorciatoie.

La penalità di tempo nell'indagine sull'incidente

L'indagine di risposta all'incidente richiede informazioni da diverse fonti scollegate, nell'ambito delle quali ciascun punto di dati aggiuntivo è come un pezzo di un puzzle. Man mano che ciascun pezzo viene aggiunto, organizzato e analizzato la portata, la gravità e la priorità diventano più chiare.

La conferma che un sistema è stato compromesso in genere richiede una serie di passaggi manuali, dispendiosi in termini di tempo. Durante la fase di

indagine, mentre gli autori dell'attacco si muovono lateralmente nella rete, potrebbero essere trafugati dati importanti dai sistemi infetti. La ricerca dell'indagine completa spesso implica mettere a rischio i dati.

MODERNIZZARE LA RISPOSTA ALL'INCIDENTE CON THREAT RESPONSE

Raccolta e indagine della fonte di avviso della minaccia

La risposta all'incidente presenta quattro principali aree di concentrazione:

- Indagare "chi, cosa e dove" in relazione agli attacchi, inclusi utenti, sistemi e campagne presi di mira
- Verificare le analisi forensi dei sistemi presi di mira rispetto ai rapporti forensi di sandbox
- Arrestare la fuga e la perdita di IP con azioni di contenimento e quarantena
- Monitorare i KPI di risposta all'incidente per assicurare che gli incidenti non sfuggano o vengano dimenticati

Queste aree di concentrazione contribuiscono a identificare quali utenti sono stati infettati, nonché la gravità e urgenza di una minaccia. Contribuiscono inoltre a eliminare i falsi positivi e impedire la diffusione dell'infezione e l'esfiltrazione dei dati.

Chi, cosa e dove con Threat Response

È necessario stabilire subito quali utenti, reparti e gruppi interni sono coinvolti. Conoscere il "chi" implica la possibilità di assegnare la priorità agli obiettivi ad alto valore quali il CFO, il personale dirigente e i sistemi finanziari nell'ambito della mailroom o agli obiettivi di priorità minore.

Oltre a intelligence e contesto interno, i fattori esterni possono offrire indizi su IP o domini sospetti negli avvisi di sicurezza. Questi fattori sono preintegrati in Threat Response con la capacità di importare e sfruttare l'intelligence di terze parti, inclusi feed STIX/TAXII per automatizzare ulteriormente l'analisi.

Questi principali fattori esterni includono:

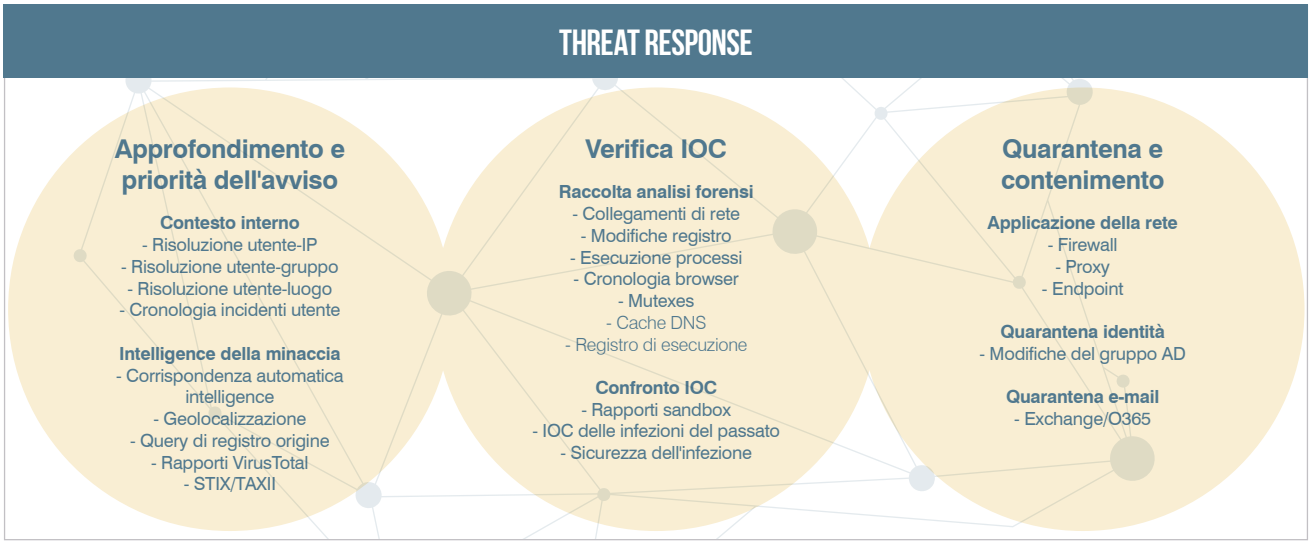
- Quanto è nuovo il dominio/durata della registrazione
- Inserimento del dominio nella blacklist
- Reputazione di IP e URL (categoria e cronologia)
- Geolocalizzazione dell'IP
- Campagne associate
- Settori bersaglio per categorie di clienti

Conferma dell'infezione mediante verifica IOC automatica

Threat Response raccoglie e analizza le analisi forensi degli endpoint dai sistemi bersaglio per fornire una dettagliata istantanea degli indicatori di compromissione (IOC). I dati IOC includono:

- Modifiche registro
- Modifiche file
- Eventi del registro di esecuzione del file recenti
- Mutexes
- Connessioni di rete
- Eventi del registro di eliminazione file
- Processi in esecuzione
- Cronologia del browser
- Cache DNS

Queste informazioni sono confrontate con le modifiche riportate dagli strumenti di analisi malware e altri sistemi per fornire una panoramica dello stato del client. Inoltre gli script di Powershell designati dall'utente possono anche essere endpoint spinti per la raccolta di dati personalizzata o altre attività.



Un'altra capacità principale consiste nel verificare se i sistemi attaccati sono stati infettati in passato. Quando Threat Response esegue una raccolta di endpoint su richiesta, controlla gli IOC non solo dell'attacco presente, ma anche delle infezioni del passato rilevate nel proprio ambiente. Questo approccio aiuta a verificare in modo rapido ed efficace se le infezioni del passato si sono diffuse al sistema attualmente preso di mira.

Integrazione predefinita con intelligence premium e strumenti di terzi

Threat Response verifica automaticamente ogni dominio e IP fornito negli avvisi di sicurezza e rapporti sandbox rispetto ai suoi feed di premium intelligence integrati, inclusa Emerging Threats Intelligence. Questo passaggio elimina ore di noioso lavoro e la ricerca singola manuale tra i servizi di intelligence per trovare IP e host dell'attacco che sfruttano siti dannosi conosciuti.

Threat Response può importare manualmente o automaticamente intelligence delle minacce di terze parti mediante STIX e TAXII. Ciò significa che i team di sicurezza possono importare e confrontare automaticamente i feed di minacce di vari centri di condivisione e analisi delle informazioni (ISAC) predefiniti. Supporta altri set di dati "bring your own intelligence" mediante upload oppure aggiungendo intelligence manualmente.

Utilizzando l'integrazione VirusTotal incorporata, i file possono essere controllati non solo un'unica volta, ma nel corso del tempo. È possibile vedere quanti degli oltre 50 motori anti-virus rilevano proprietà o firme dannose in file rimossi, scaricati o scompattati durante una potenziale infezione. Altre integrazioni predefinite comprendono ricerca WHOIS, geolocalizzazione, connettori Active Directory ecc.

Quarantena e contenimento

Basandosi su contesto e analisi forensi raccolte e analizzate dal sistema, Threat Response dispone di un'ampia visione del contesto della minaccia. Tale visione consente agli analisti di intreprendere azioni di risposta con pressione di pulsante, identificare aree da sottoporre a indagini aggiuntive o attivare risposta automatica come ad esempio ritirare l'e-mail inviata dalla casella e-mail dell'utente, aggiungere utenti a gruppi con autorizzazione ridotta o aggiornare elenchi di blocco di firewall e filtri web.

Gestione degli incidenti

Un rischio nascosto di gestione degli incidenti consiste nella perdita di contesto a causa della quantità di console del sistema e schede del browser utilizzate in combinazione con il copia-incolla di informazioni tra questi sistemi. Oltre alle capacità principali, Threat Response include funzioni chiave di gestione degli incidenti che consentono agli utenti e ai team di indagare gli incidenti senza perdere il contesto durante il passaggio da un sistema all'altro. Oltre alle funzioni base di assegnazione e monitoraggio dell'assegnazione, Threat Response:

- Mantiene la cronologia e la documentazione di ogni incidente e relativa azione intrapresa
- Monitora l'assegnazione dell'incidente a livello di soggetti singoli e team
- Associa gli incidenti alle indagini
- Consente agli utenti o ai membri del team di operare con autorizzazioni diverse

- Attiva le notifiche del flusso di lavoro in base all'avanzamento dell'incidente e al cambiamento dello stato
- Riconosce ruoli e autorizzazioni per le azioni di quarantena, assicurando che esclusivamente le persone giuste possano intraprendere azioni nel momento giusto
- Avvisa utenti o team quando gli incidenti cambiano, ad esempio quando i punteggi di una minaccia superano una soglia o quando è completata un'azione di quarantena

VANTAGGI

Esempi di vantaggi dall'utilizzo di Threat Response e dall'automatizzazione delle azioni di quarantena e contenimento includono:

- Aggiunta di amministratori del database a un'area di penalità limitata, che blocchino l'accesso alle informazioni sensibili durante un incidente
- Eliminazione delle e-mail recapitate affinché non ci sia il rischio che gli utenti facciano di nuovo clic su URL o allegati dannosi
- Blocco della comunicazione da parte di tutti i dipendenti ai siti CNC per rompere la catena di controllo
- Limitazione della capacità delle infezioni malware di diffondersi ad altri sistemi
- Riduzione del lavoro ridondante o doppio dell'analista comprendendo le indagini più ampie delle campagne che colpiscono la propria azienda
- Visualizzazione dei KPI di incidenti lenti o non processati, capacità di gestione dell'incidente e assegnazione dei reparti o dei gruppi autorizzati
- Installazione e configurazione in ore implica migliori risultati di gestione delle risposte e sicurezza, nonché rapido ritorno sull'investimento

RIEPILOGO

Threat Response rappresenta un moltiplicatore di forza per la risposta agli incidenti. Fornisce la predisposizione e l'automatizzazione predefinita della sicurezza acquisendo il contesto, la raccolta di analisi forensi e il confronto di IOC per la verifica delle infezioni, le capacità di quarantena e contenimento e le funzioni di gestione dell'incidente in relazione a incidenti e indagini.

INTEGRAZIONI PREDEFINITE

ORIGINE AVVISO
- Cisco FirePOWER NGIPS
- FireEye serie EX
- FireEye serie NX
- HP ArcSight ESM
- IBM QRadar
- JSON Event Source
- Juniper Secure Analytics
- Palo Alto Networks Wildfire
- Proofpoint TAP
- Splunk Enterprise
- Suricata

RISPOSTA PERSONALIZZATA
- API di risposta personalizzata JSON

EIDR
- Tanium
- Carbon Black

QUARANTENA E-MAIL
- Microsoft Exchange

DISPOSITIVO DI APPLICAZIONE
- Check Point
- Cisco ASA
- Cisco IOS
- Cisco OpenDNS
- CyberArk Enterprise Vault
- Fortinet FortiGate
- Imperva SecureSphere
- Juniper SRX (JUNOS)
- Palo Alto Networks NGFW
- Palo Alto Networks Panorama

MIGLIORAMENTO
- Emerging Threats
- MaxMind
- Microsoft Active Directory
- Proofpoint Threat Graph
- Soltra
- Splunk Enterprise
- Virus Total
- WHOIS

GESTIONE ACCESSO IDENTITÀ
- Centrify
- Microsoft Azure SSO
- Okta
- OneLogin
- Ping Identity

PROXY, ELENCHI BLOCCHI DINAMICI
- Blue Coat ProxySG
- Palo Alto Networks NGFW

BIGLIETTERIA
- BMC Remedy Ticketing System
- JIRA

SOLUZIONI DI AUTENTICAZIONE A DUE FATTORI
- Duo Security
- RSA Securid
- SafeNet
- Symantec 2FA

INFORMAZIONI SU PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), società di sicurezza informatica di nuova generazione, consente alle aziende di proteggere la modalità di lavoro odierna dei propri dipendenti dalle minacce avanzate e dai rischi di conformità. Proofpoint aiuta i professionisti della sicurezza informatica a proteggere i propri utenti dagli attacchi avanzati che li prendono di mira (tramite e-mail, app mobili e social media), a proteggere le informazioni importanti create dai dipendenti e a dotare i team dell'intelligenza e degli strumenti giusti per rispondere rapidamente quando insorgono problemi. Aziende leader di tutte le dimensioni, tra cui oltre il 50 per cento di quelle presenti in Fortune 100, si affidano alle soluzioni di Proofpoint, che sono create per gli ambienti IT odierni mobili e social e sfruttano sia la potenza del cloud sia una piattaforma di analisi basata su big data per combattere le moderne minacce avanzate.