proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Active Exploits Protection

Blocca gli exploit fin dall'inizio—prima che vengano eseguiti

Vantaggi principali

- Assicurati una protezione di prim'ordine contro gli exploit identificando e bloccando l'attività di sfruttamento dannoso all'ingresso della casella email—prima dell'esecuzione del payload o della violazione dell'endpoint.
- Attribuisci le priorità alle vulnerabilità in base agli exploit attivi osservati in ambienti reali.
- Riduci l'esposizione prima dell'implementazione delle patch, proteggendoti dal malware basato su exploit e da attività di comando e controllo.
- Accelera le indagini grazie a dati contestuali sulle minacce attuali e passate e informazioni relative al rilevamento continuamente aggiornate.
- Preparati a flussi di lavoro di sicurezza guidati dall'IA e dagli agenti.

Panoramica

La velocità e la portata degli exploit stanno aumentando. Oltre al fatto che il numero di nuove vulnerabilità divulgate sta raggiungendo livelli record, i criminali informatici le trasformano in armi più rapidamente che mai. Le soluzioni tradizionali di gestione delle vulnerabilità e di gestione dell'esposizione spesso definiscono le priorità in base a punteggi di gravità e ai rischi teorici—ma mancano di visibilità sulle vulnerabilità che i criminali informatici cercano attivamente di sfruttare.

Proofpoint Active Exploits Protection cambia questo modello.

Grazie alla visibilità immediata che offre sulla diffusione degli exploit attraverso email e traffico di rete, Proofpoint aiuta le aziende a identificare le attività dannose prima dell'esecuzione del payload. La soluzione combina informazioni sugli exploit attivi, definizione delle priorità che tiene conto dei criminali informatici e funzionalità di protezione immediata per aiutare i team della sicurezza a concentrarsi su ciò che conta di più e ridurre l'esposizione più rapidamente. Il risultato è un approccio più proattivo alla protezione contro gli exploit, basato sulla prevenzione degli attacchi in una fase più precoce della catena di attacco.

La soluzione: informazioni sugli exploit fin dall'inizio e una protezione immediata

Proofpoint Active Exploits Protection trasforma le informazioni sugli exploit attivi in protezione fruibile e risposta prioritaria. La soluzione combina informazioni sugli exploit che tiene conto dei criminali informatici, rilevamento delle minacce basato su email e rete e integrazioni operative per aiutare le aziende a identificare e bloccare le attività di sfruttamento dannoso prima dell'esecuzione.

Grazie a una visibilità di prim'ordine sugli exploit derivate dalle email, che sono il punto d'inizio di molti attacchi moderni, Proofpoint può identificare i tentativi di distribuzione degli exploit e il comportamento reale dei criminali informatici nella prima fase della catena di attacco, prima dell'esecuzione del payload, della violazione degli endpoint o dello spostamento laterale.

Proofpoint Active Exploits Protection sfrutta queste informazioni uniche sulle vulnerabilità e l'ampia copertura sulle minacce basate su rete e exploit per aiutare le aziende ad assegnare le priorità alle vulnerabilità in base al loro sfruttamento attivo, ridurre la loro esposizione in attesa dell'applicazione delle patch e accelerare le indagini grazie a una threat intelligence fruibile.

Dai priorità agli exploit attivi invece che ai rischi teorici

Concentra gli interventi di correzione sulle vulnerabilità associate a exploit attivi, e non solo sui punteggi CVSS elevati.

Proofpoint Active Exploits Protection collega le informazioni sugli exploit e il comportamento dei criminali informatici osservato attraverso fonti di telemetria mondiali per aiutare le aziende a identificare rapidamente le vulnerabilità che presentano un rischio operativo immediato.

Questo approccio incentrato sui criminali informatici aiuta i team della sicurezza a ridurre il rumore, stabilire meglio le priorità e concentrare le risorse sulle esposizioni con la maggior probabilità di essere sfruttate.

Le principali funzionalità includono:

- Prioritizzazione dell'applicazione delle patch sulla base dei CVE attivamente sfruttati
- Distinzione tra le minacce urgenti e i rischi di minore priorità
- Prioritizzazione delle patch basata su un contesto chiaro e fruibile sulle minacce, inclusi feed in tempo reale di reputazione degli indirizzi IP e dei domini
- Allineamento delle priorità sull'attività reale dei criminali informatici per una miglior efficacia operativa

Ottieni una protezione immediata in attesa dell'applicazione delle patch

L'applicazione delle patch richiede tempo. Proofpoint Active Exploits Protection aiuta le aziende a ridurre l'esposizione durante quel periodo fornendo informazioni continuamente aggiornate sugli exploit e offrendo una protezione immediata delle email e del traffico di rete.

Fornisce una logica di rilevamento tempestiva e affidabile per le minacce avanzate, tra cui:

- Distribuzione del malware
- Comunicazioni di comando e controllo
- Kit di exploit
- Phishing delle credenziali d'accesso
- Diffusione dell'attacco
- Ransomware, botnet
- Anomalie nei protocolli e nelle applicazioni
- Estrazione di criptovalute
- Attacchi di negazione di servizio distribuita (DDoS)
- Attacchi a sistemi di controllo e acquisizione di dati (SCADA)

Le principali funzionalità includono:

- Informazioni sugli exploit continuamente aggiornate e concepite per migliorare la protezione a uno stadio più precoce della catena di attacco
- Regole di rilevamento basate sulla rete per i sistemi IDS, IPS e NGFW e controlli di sicurezza correlati
- Firme affidabili per callback di malware, dropper, comunicazioni di comando e controllo, offuscamento, minacce legate a kit di exploit e sottrazione
- Aggiornamenti quotidiani delle regole per tenere il passo con l'evoluzione del panorama delle minacce
- Copertura delle principali famiglie di malware, campagne di attacco e vettori delle minacce basati sulla rete
- Supporto dei formati IDS e IPS ampiamente utilizzati, incluse implementazioni compatibili con Suricata e Snort

Arricchisci gli strumenti di sicurezza con una threat intelligence mondiale

Proofpoint Active Exploits Protection fornisce informazioni fruibili che si integrano con un'ampia gamma di strumenti di sicurezza, tra cui firewall, soluzioni IDS, IPS, NGFW, UTM e SIEM, sistemi di autenticazione, piattaforme di tracciamento delle minacce, flussi di lavoro di risposta agli incidenti e strumenti di sicurezza personalizzati.

La soluzione fornisce informazioni sulla reputazione e sulle minacce relative a indirizzi IP, domini, malware, firme, campagne sospette e attività di attacco correlate.

Le principali funzionalità includono:

- Threat intelligence attuale e storica per indirizzi IP, domini, hash del malware, firme e contenuto dei messaggi
- Feed di reputazione degli indirizzi IP e dei domini organizzati per categoria delle minacce e punteggio di fiducia
- Aggiornamenti frequenti dei feed con invecchiamento accelerato per riflettere l'attività attuale
- Database mondiale delle minacce consultabile che permette la navigazione, l'approfondimento e le indagini
- Supporto di diversi formati di feed per l'integrazione operativa, tra cui TXT, CSV, JSON, IDS e formati compressi
- Arricchimento basato su API per strumenti SIEM, TIP, risposta agli incidenti e interni

Rafforza la precisione del rilevamento e riduci il rumore

Proofpoint Active Exploits Protection si basa sulle osservazioni di minacce reali, le analisi del malware, i feedback provenienti da sensori in tutto il mondo e ricerche dedicate alle minacce. Questo approccio consente un rilevamento altamente affidabile, riducendo i falsi positivi negli strumenti di sicurezza di rete esistenti.

Le principali funzionalità includono:

- Contenuti dei rilevamenti guidati dalle ricerche e fondati sulle minacce osservate
- Analisi del malware in sandbox per acquisire il comportamento di rete dopo l'esecuzione
- Feedback provenienti da sensori in tutto il mondo per migliorare l'accuratezza del rilevamento
- Descrizioni delle firme, riferimenti e documentazione per supportare i flussi di lavoro degli analisti
- Applicazione delle policy basata su categorie e allineata alle priorità dell'azienda

Scala con flussi di lavoro guidati dall'IA

Proofpoint Active Exploits Protection è concepito per supportare le operazioni di sicurezza moderne incentrate sulla threat intelligence. Le capacità future dovrebbero consentire l'accesso alla threat intelligence attraverso il protocollo MCP e flussi di lavoro basati su agenti, facilitando casi d'uso guidati da API e IA.

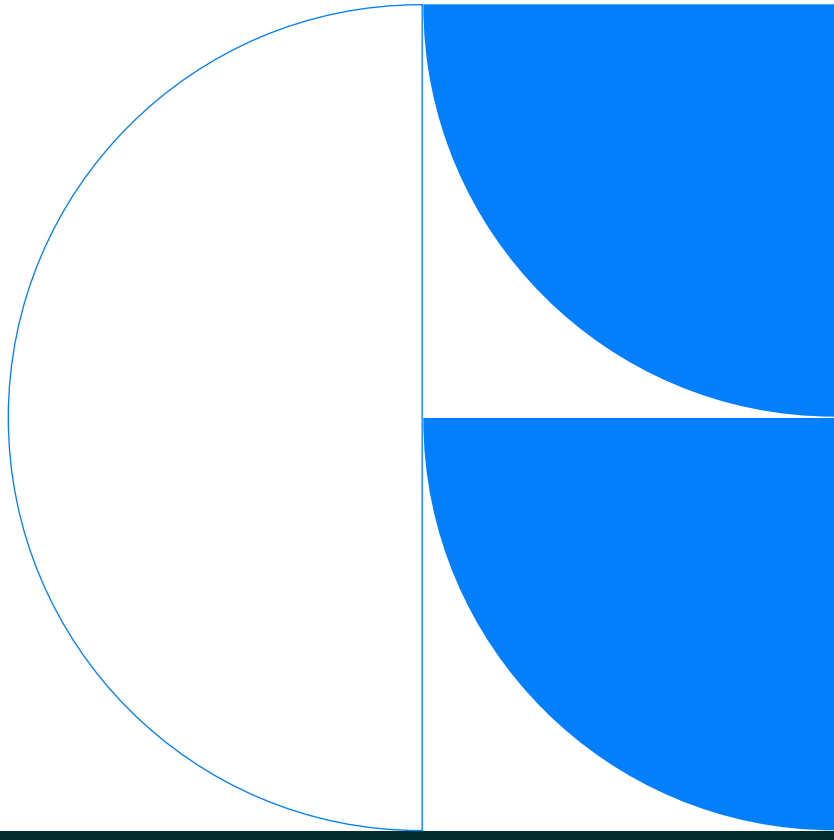
Questi flussi di lavoro sono volti ad aiutare i team a integrare direttamente la threat intelligence prioritaria nelle operazioni di sicurezza automatizzate, accelerare il processo decisionale e ridurre le attività di triage manuale.

Sintesi

Proofpoint Active Exploits Protection aiuta le aziende a prevenire attacchi basati su exploit prima della violazione, combinando visibilità di prim'ordine sugli exploit derivati dalle email, informazioni sugli exploit che tengono conto dei criminali informatici e funzionalità di protezione immediata.

Invece di fare affidamento esclusivamente su punteggi di gravità delle vulnerabilità o modelli di esposizione teorici, Proofpoint Active Exploits Protection consente ai team della sicurezza di stabilire le priorità in base agli obiettivi reali dei criminali informatici.

Unificando definizione delle priorità, protezione e indagine, Proofpoint Active Exploits Protection aiuta i team della sicurezza a concentrarsi su ciò che conta, offrire una protezione immediata e indagare più rapidamente.



proofpoint.