proofpoint

CASO CLIENTE

# Una società di distribuzione dell'energia rafforza le sue difese con Proofpoint

## La sfida

- Aumentare la visibilità sulle minacce contro l'infrastruttura e le risorse strategiche
- Accelerare l'identificazione delle minacce e migliorare la risposta agli incidenti
- Migliorare la raccolta di dati forensi

## La soluzione

Proofpoint Identity Threat Defense

- Proofpoint Shadow

## I risultati

- Nessun falso positivo
- Visualizzazione dell'attività dei criminali informatici in tempo reale
- Riduzione di due terzi dei tempi di indagine
- Disponibilità immediata di dati forensi dettagliati per un processo decisionale basato su prove incontrovertibili
- Sviluppo di una collaborazione reale con Proofpoint per l'intera durata dell'implementazione

## L'azienda

Quest'azienda distribuisce energia e offre servizi correlati a milioni di clienti e partner in tutto il mondo. Questa multinazionale svolge anche operazioni di esplorazione e produzione di energia. Poiché l'energia ha un ruolo strategico per la vita e la sicurezza nazionale, l'azienda si affida all'innovazione tecnologica per sviluppare prodotti, applicazioni e servizi all'avanguardia. Tenendo ben presente la sicurezza, l'azienda si è rivolta a Proofpoint per aggiungere funzionalità uniche che le permettessero di rilevare le attività dannose e godere di informazioni forensi in tempo reale.

## La sfida

Per una società di distribuzione dell'energia, un'importante sfida è la protezione della sua superficie d'attacco complessa. Quest'azienda dispone di un'infrastruttura sia on premise che in cloud, oltre a una rete strategica di controllo e acquisizione dei dati in tempo reale (SCADA) e dispositivi. La presenza di più partner esterni richiede numerose connessioni di rete in ingresso e uscita. La focalizzazione sulle operazioni DevOps richiede anche la protezione degli endpoint per una grande comunità di sviluppatori, nonché di codice applicativo e sistemi di test. Come fornitore di energia, l'azienda ha bisogno di una chiara visibilità sull'infrastruttura di sicurezza e della capacità di acquisire dati di telemetria nel caso di rilevamento di una minaccia per essere conforme con le normative settoriali, il GDPR e altri requisiti di sicurezza.

L'azienda aveva già adottato un approccio di difesa in profondità alla sicurezza e lavora costantemente per implementare e migliorare le best practice. Prima di Proofpoint, in diversi casi, personale interno aveva già fatto scattare allarmi nei sistemi di sicurezza dell'azienda. A ogni allarme, il team SOC doveva recuperare il computer portatile dell'utente e condurre indagini manuali, analizzando i registri di sistema e raccogliendo minuziosamente informazioni forensi sufficienti per ricostruire l'accaduto. Anche recuperando rapidamente il computer portatile, tali indagini possono durare ore. Per migliorare la sua reattività, l'azienda ha lanciato un'iniziativa di sicurezza incentrata sulla protezione di computer portatili e workstation.

## La soluzione

Nella ricerca di una soluzione, l'azienda ha inizialmente preso in considerazione le tecnologie honeypot ma poi è venuta a conoscenza di Proofpoint Identity Threat Defense e della sua tecnologia di esche basata sugli endpoint. La loro scelta è ricaduta su Proofpoint Shadow.

"All'inizio pensavo che Proofpoint Shadow fosse solo un honeypot" spiega il responsabile della sicurezza delle informazioni. "Ma è risultato presto chiaro che l'approccio di Proofpoint era molto più sofisticato".

Le esche senza agent di Proofpoint Shadow, basate sulla threat intelligence e installate su ogni endpoint, sono concepite per imitare dati, credenziali e connessioni reali. Ora, quando un criminale informatico, o un utente interno malintenzionato con un accesso di rete legittimo, cerca di infiltrarsi nei sistemi, si trova di fronte un elevato numero di risorse fasulle molto credibili. Scegliere un percorso sicuro e non individuabile diventa quasi impossibile e il minimo passo falso avvisa il SOC della sua presenza. Una volta attivata l'esca, il sistema inizia a raccogliere numerose informazioni forensi dai sistemi in cui il criminale informatico si è introdotto per fornire dati precisi in tempo reale per una risposta informata e rapida.

> "Proofpoint ha ridotto i tempi di indagine di due terzi. La dashboard grafica ci mostra dove il criminale informatico è entrato in contatto con le risorse strategiche dell'azienda. Possiamo analizzare dettagli specifici, e il sistema ci fornisce automaticamente una cronologia di ciò che è accaduto sull'endpoint. È preziosissimo".
>
> Responsabile della sicurezza delle informazioni, fornitore d'energia

Il fornitore di energia ha implementato Proofpoint Identity Threat Defense a livello globale con l'aiuto del suo MSP e dei Servizi professionali di Proofpoint. La soluzione ha immediatamente identificato delle vie d'accesso ai dati più preziosi e diverse vulnerabilità dovute e errori di configurazione del sistema.

"Proofpoint Identity Threat Defense è incredibilmente utile", afferma il responsabile della sicurezza. "Raccoglie informazioni dagli endpoint e suggerisce le esche più appropriate, facendoci risparmiare tempo e migliorando in modo significativo le nostre difese. Siamo stati anche favorevolmente colpiti dal team Proofpoint. Ascoltano le nostre esigenze, ci aiutano a adattare le difese al nostro ambiente e sono davvero pronti e reattivi".

## I risultati

Una volta implementata, la soluzione Proofpoint ha rilevato immediatamente istanze di tentativi di intrusione di criminali informatici sconosciuti, ingannati da un'esca. Ora, il team SOC può identificare e monitorare l'attività dei criminali informatici in tempo reale. Allo stesso tempo, i dati forensi in tempo reale mettono a disposizione del team SOC informazioni sull'attacco informatico, permettendo loro di analizzare rapidamente in dettaglio informazioni specifiche,

all'insaputa del criminale informatico. Ora il team di risposta agli incidenti può stabilire rapidamente dove concentrare le indagini, sapendo quali sono gli strumenti utilizzati dal criminale informatico. Gli allarmi Proofpoint vengono inviati simultaneamente al sistema ServiceNow dell'azienda, velocizzando l'assegnazione delle attività agli analisti, la prioritizzazione delle risposte e la gestione dei ticket.

"In passato, non avremmo saputo di tale attività", dichiara il responsabile della sicurezza delle informazioni. "Avremmo dovuto aspettate di ricevere avvisi da più livelli di sicurezza per verificare che non si trattasse di un falso positivo, per poi metterlo in quarantena e confiscare il computer portatile prima di poter indagare e raccogliere prove".

### Una vera e propria rivoluzione

"I dati di telemetria si sono rivelati fondamentali" ha aggiunto. "Proofpoint Identity Threat Defense riduce il tempo di indagine di due terzi. La dashboard grafica ci mostra dove il criminale informatico è entrato in contatto con le risorse strategiche dell'azienda. Possiamo analizzare rapidamente le informazioni in dettaglio. La soluzione ci fornisce automaticamente una cronologia di ciò che è accaduto a livello dell'endpoint. È preziosissimo".

I dati di telemetria della soluzione forniscono anche prove incontrovertibili. Se l'attacco informatico è condotto da un utente interno malintenzionato, l'azienda può portare prove innegabili dell'accaduto e agire di conseguenza. In caso di tentativi di attacchi esterni, più frequenti, l'azienda ora dispone di dati dettagliati sugli obiettivi e le tecniche del criminale informatico in modo da rafforzare le difese dove necessario.

### La base per il futuro

Il fornitore d'energia, che deve proteggere i suoi stabilimenti remoti, il suo ambiente SCADA e i suoi dispositivi IoT, prevede di utilizzare Proofpoint Identity Threat Defense per estendere il suo approccio di difesa in profondità a queste risorse.

"Proofpoint Identity Threat Defense è uno strumento fondamentale" ha affermato il responsabile della sicurezza delle informazioni. "Si è rivelato molto efficace. Se, per qualche motivo, dovessimo razionalizzare i nostri strumenti di sicurezza, sarebbe l'ultimo a cui rinunceremmo".

## PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.