Sophos Rapid Response

Risposta immediata alle minacce attive

Sophos Rapid Response offre assistenza immediata, erogata da un team di esperti nella risposta agli incidenti, in grado di identificare e neutralizzare le minacce attive presenti nella rete di un'organizzazione.

Durante un attacco, ogni secondo è importante

Durante la risposta a una minaccia attiva, è essenziale ridurre quanto più possibile il tempo che intercorre tra l'indicatore di compromissione iniziale e la mitigazione completa della minaccia. Man mano che l'hacker percorre le varie fasi della catena di attacco, le organizzazioni affrontano una lotta contro il tempo per fare in modo che non riesca a raggiungere i propri obiettivi.

Sophos Rapid Response vi aiuta a uscire rapidamente dalla zona di pericolo, grazie all'assistenza del nostro team operativo 24/7 da remoto di esperti di risposta agli incidenti, analisi delle minacce e threat hunting, in grado di:

- Intervenire rapidamente per classificare, contenere e neutralizzare le minacce attive
- Espellere gli intrusi dalla vostra struttura informatica, per impedire che rechino ulteriori danni alle risorse
- Monitorare costantemente il sistema e rispondere agli incidenti 24/7 per potenziare il livello di protezione offerto
- Consigliare azioni preventive in tempo reale per risolvere la causa che ha dato origine al problema
- Installare rapidamente lo stack di tecnologie cloud Sophos nell'intero ambiente
- Analizzare dati supplementari ottenuti con tecnologie di altri vendor
- Fornire, dopo la risoluzione dell'incidente, un riepilogo dettagliato della minaccia che descrive le indagini svolte

Caratteristiche principali

- Identificazione e neutralizzazione rapida delle minacce attive
- Risposta agli incidenti e monitoraggio 24/7 per 45 giorni
- Referente dedicato e contatto per la risposta
- Riepilogo dopo la risoluzione dell'incidente con informazioni dettagliate di tutte le azioni intraprese
- Costi fissi, senza spese nascoste
- Sistema progettato per essere idoneo a una richiesta di rimborso assicurativo
- Transizione trasparente da Sophos Rapid Response a una subscription Managed Detection and Response (MDR)

Le caratteristiche di Sophos Rapid Response

Sophos Rapid Response include tutti i vantaggi di Sophos MDR Complete oltre ad altri vantaggi.

	Sophos Rapid Response
MDR Complete in modalità di risposta alle minacce "Autorizza"	✓
Monitoraggio, individuazione proattiva e risposta alle minacce 24/7	✓
Contatto dedicato per la risposta durante l'incidente e accesso alla linea di supporto diretta	✓
Analisi di dati supplementari ottenuti con tecnologie di altri vendor	✓
Preventivo immediato e attivazione dell'account il giorno stesso	✓
Riepilogo ufficiale delle minacce dopo la risoluzione dell'incidente, con i dettagli dell'indagine	✓

SOPHOS

Neutralizzazione delle minacce attive

Il team Sophos Rapid Response è specializzato nella neutralizzazione delle minacce attive. Che si tratti di un'infezione, di un tentativo di compromissione o di un accesso non autorizzato alle risorse che cerca di eludere i controlli di sicurezza, abbiamo già visto e bloccato di tutto.

I nostri esperti di risposta agli incidenti fanno parte del team Sophos Managed Detection and Response (MDR): il nostro servizio di threat hunting, rilevamento e risposta, operativo 24/7 e in grado di individuare proattivamente le minacce, svolgere indagini e implementare azioni di risposta per conto dei clienti come parte di un servizio completamente gestito.

Gli incentivi giusti

I tradizionali servizi di Incident Response (IR, risposta agli incidenti) prevedono costi orari e questo comporta il rischio di sottovalutare il tempo necessario per neutralizzare completamente una minaccia. Di conseguenza, implicano la necessità di acquistare ore aggiuntive. Ancora peggio, per i tradizionali servizi IR questo può rappresentare un incentivo a incrementare il numero di ore necessarie per la risposta.

Sophos Rapid Response offre un modello basato su un prezzo fisso, senza spese extra nascoste, che viene stabilito in base al numero di utenti e server presenti all'interno dell'ambiente. Inoltre viene fornito in modalità remota, per cui le attività di risposta possono essere avviate immediatamente. È nel nostro interesse, oltre che nel vostro, togliervi dalla zona di pericolo quanto più rapidamente possibile, in quanto il tempo non influisce sul costo.

Rapid Deployment

Per garantire la massima tempestività di risposta, il processo rapid deployment di Sophos è focalizzato sull'implementazione immediata degli agent Sophos MDR su tutti gli endpoint e i server individuabili.

Dopo aver sviluppato una strategia di sostituzione dei prodotti esistenti mediante l'uso di utilità di rimozione, un team di tecnici di distribuzione interverrà da remoto consultando ciascun cliente Rapid Response per intraprendere un piano di azione personalizzato che sfrutta strumenti di automazione per la distribuzione di massa nell'intera rete.

Il team collabora attivamente con i clienti per ottimizzare lo stato di integrità indicato dall'agent Sophos MDR per la rete, garantendo l'implementazione di configurazioni che seguono le best practice di settore, per accelerare le indagini.

La Metodologia Rapid Response

Una volta ricevuta l'approvazione per Rapid Response e una volta che il cliente ha accettato i termini e le condizioni del servizio, entriamo direttamente in azione. Rapid Response prevede quattro fasi: onboarding, valutazione, neutralizzazione e monitoraggio.

Onboarding

- Chiamata iniziale per stabilire le preferenze per la comunicazione e confermare se sono state già implementate misure correttive, e in tal caso quali
- Identificazione dell'estensione e dell'impatto dell'attacco
- Definizione di comune intesa di un piano di risposta strategico
- Installazione del software del servizio

Valutazione

- Valutazione dell'ambiente operativo
- Identificazione di eventuali indicatori di compromissione noti e delle attività svolte dagli hacker
- Raccolta di dati e inizio delle indagini
- Collaborazione per impostare un piano iniziale di attività di risposta

Neutralizzazione

- Rimozione dell'accesso degli hacker
- Prevenzione di ulteriori danni a risorse o dati
- Blocco di ulteriori attività di esfiltrazione dei dati
- Consigli su azioni preventive in tempo reale, per risolvere la causa che ha dato origine all'incidente

Monitoraggio

- Transizione al servizio Sophos MDR Complete
- Monitoraggio costante per individuare tentativi ricorrenti dello stesso incidente
- Riepilogo delle informazioni relative alle minacce, dopo la risoluzione dell'incidente

Riepilogo dettagliato delle minacce

Una volta neutralizzata la minaccia attiva nell'ambiente della vostra organizzazione, forniamo un riepilogo ufficiale delle nostre indagini, che include la descrizione dettagliata di tutte le azioni che abbiamo intrapreso e delle informazioni ottenute, nonché consigli per una strategia a lungo termine per la mitigazione di eventuali casi di minacce simili in futuro.

Monitoraggio E Risposta 24/7 Dopo La Risoluzione Dell'Incidente

Una volta risolto l'incidente e neutralizzata la minaccia immediata per l'organizzazione, spostiamo i clienti sul livello più alto del nostro servizio MDR: MDR Complete. Questo servizio garantisce l'individuazione proattiva delle minacce, l'indagine, il rilevamento e la risposta agli incidenti 24/7.

Qualora la minaccia si ripresentasse, oppure se dovesse emergerne una nuova, saremo pronti a implementare una risposta, senza alcun costo aggiuntivo. Se un attacco dovesse minacciare la vostra organizzazione nei 45 giorni successivi all'inizio della subscription, vi difenderemo fino al termine della validità di questa subscription.

Sei stato colpito da un cyberattacco?

Chiamaci in qualsiasi momento per parlare con i nostri esperti di Incident Response.

Australia +61 272084454

Canada +1 7785897255

Francia +33 186539880

Germania +49 61171186766

Italia +39 02 873 17993

Regno Unito +44 1235635329

USA +1 4087461064

Svezia +46 858400610

Se tutti gli esperti di risposta agli incidenti dovessero essere occupati, ti preghiamo di lasciare un messaggio e ti contatteremo il prima possibile.

Sei stato colpito da un cyberattacco?

Per maggiori informazioni, visita:
sophos.it/rapidresponse

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

22-11-24 DS-IT (DD)

SOPHOS