Sophos Rapid Response

Domande Frequenti

Devo utilizzare soluzioni Sophos per diventare cliente del servizio Rapid Response?
No, il servizio Sophos Rapid Response è disponibile sia per i clienti Sophos che per i clienti che non utilizzano soluzioni Sophos.

Stiamo affrontando un incidente attivo, come dobbiamo procedere?
Chiamate uno dei numeri locali in qualsiasi momento per parlare con i nostri esperti di risposta agli incidenti.

USA +1 4087461064

Australia +61 272084454

Canada +1 7785897255

Francia +33 186539880

Germania +49 61171186766

Regno Unito +44 1235635329

Svezia +46 858400610

Italia +39 0287317993

Quanto è rapido il servizio Rapid Response?
Molto rapido. Nella maggior parte dei casi, il processo di onboarding dei clienti richiede poche ore e la valutazione avviene entro 48 ore. Poiché il servizio è fornito completamente da remoto, la strategia di risposta viene implementata entro poche ore dal primo contatto con Sophos.

In che cosa consiste il processo di onboarding?
Il team Rapid Response può cominciare il processo di onboarding e avviare le indagini non appena riceve l'approvazione. Alle organizzazioni che non utilizzano Sophos XDR nel proprio ambiente, Sophos offre l'opzione di Rapid Deployment per un'implementazione rapida. Il team Rapid Deployment è composto da esperti specializzati nell'installazione rapida all'interno di ambienti nei quali è in corso un incidente attivo.

L'opzione Rapid Deployment prevede costi aggiuntivi?
No, Rapid Deployment è inclusa nel servizio.

Qual è la metodologia di 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
- Raccomandazioni in tempo reale sulle azioni preventive necessarie per risolvere il problema

SOPHOS

Domande Frequenti Su Sophos Rapid Response

Monitoraggio

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

In quali lingue è disponibile il servizio Rapid Response?
Attualmente il servizio viene offerto solamente in lingua inglese.

Sophos sostituisce o utilizza servizi di Data Forensic Incident Response (DFIR, risposta agli incidenti con indagine approfondita dei dati)?
Sophos può collaborare parallelamente con fornitori di servizi DFIR, come già ha fatto in diversi casi in passato. Sophos Rapid Response si focalizza sull'aspetto di risposta agli incidenti dei servizi DFIR e non offre tutti i servizi normalmente forniti dalle tradizionali soluzioni DFIR.

Sophos invia attrezzature? Gli esperti di risposta alle minacce visitano fisicamente le sedi dei clienti?
No, tutte le attività di risposta agli incidenti vengono svolte da remoto.

I clienti devono installare Sophos sui propri endpoint?
Sì. Il servizio Rapid Response viene fornito utilizzando Managed Detection and Response/Sophos XDR, per garantire massima efficacia di monitoraggio e risposta 24/7. Questo significa che dobbiamo anche disinstallare o disattivare temporaneamente la protezione endpoint di altri vendor.

Il team Rapid Response può cominciare a intraprendere azioni correttive per contenere e neutralizzare la minaccia anche prima che venga completata l'installazione. Il team utilizzerà tutti i dati disponibili e gli strumenti idonei come risorse complementari per la risposta.

Come vengono calcolati i costi?
I costi vengono calcolati in base al numero di utenti e server, per un periodo fisso di 45 giorni.

Sono previsti ulteriori costi?
No, il servizio non prevede spese nascoste.

Cosa succede al termine del periodo di validità del servizio Rapid Response?
Al termine del periodo stabilito, i clienti possono passare alla versione completa del servizio Sophos Managed Detection and Response (MDR), altrimenti la licenza scadrà.

È possibile implementare Rapid Response solo su un segmento dell'ambiente, oppure dobbiamo includere l'intero ambiente?
In alcune situazioni, il servizio Rapid Response può essere applicato solamente a un segmento dell'ambiente del cliente. Un esperto del team di Rapid Response sarà in grado di fornire ulteriori informazioni durante l'identificazione dell'ambito di estensione di ogni progetto.

Sophos può collaborare con un intermediario che rappresenta il cliente, ad esempio uno studio legale, secondo i termini dell'accordo?
Sì. Possiamo collaborare con un intermediario.

Sophos è in grado di determinare quali file sono stati esfiltrati/prelevati illecitamente durante un attacco?
Il servizio Rapid Response include il massimo impegno nello stabilire se durante un attacco sono stati esfiltrati file, e in tal caso quali. Tuttavia, non è possibile fornire una garanzia completa, in quanto il successo di tale operazione potrebbe dipendere dai dati disponibili durante l'indagine.

Sophos decifrerà i dati cifrati dal ransomware per conto del cliente?
No, questa attività non rientra nell'ambito del servizio Rapid Response.

Sophos aiuterà il cliente a negoziare o a effettuare il pagamento di un riscatto per i dati?
No, questa attività non rientra nell'ambito del servizio Rapid Response.

2022-09-14 (FAQ-PC)

SOPHOS