SOPHOS

Domande frequenti in ambito commerciale e tecnico - Sophos Emergency Incident Response

FAQ esterno

Panoramica Generale

Che cos'è Emergency Incident Response?
Sophos Emergency Incident Response è un servizio che ti aiuta ad affrontare un'emergenza informatica. Prevede la valutazione, l'isolamento e la comprensione rapida dell'incidente, nonché l'offerta di raccomandazioni per le attività di correzione. Il nostro team interfunzionale di esperti sfrutta gli anni di esperienza e le conoscenze maturate sul campo per valutare, isolare e neutralizzare le minacce attive, rimuovendo allo stesso tempo gli active adversary dai sistemi per prevenire ulteriori danni.

Inoltre, Emergency Incident Response ti aiuta a stabilire se la tua organizzazione ha subito un incidente e in tal caso a definirne la portata e l'impatto. Il servizio offre un'ampia scelta di attività di indagine per identificare la causa originaria degli incidenti, eseguire valutazioni per identificare la pericolosità dei comportamenti osservati, svolgere attività di threat hunting sfruttando l'intelligence sulle minacce, e assistere durante le negoziazioni in seguito a una richiesta di riscatto.

Chi può utilizzare Emergency Incident Response?
Qualsiasi organizzazione che stia affrontando un incidente di sicurezza attivo, un attacco recente che richiede ulteriori indagini, o attività sospette che devono essere esaminate per capire se si tratti di una minaccia.

Devo utilizzare già soluzioni Sophos per acquistare Emergency Incident Response?
No, Emergency Incident Response è disponibile sia per i clienti Sophos che per chi non utilizza soluzioni Sophos.

La mia azienda sta affrontando una violazione attiva. Come devo procedere?
Chiama uno di questi numeri in qualsiasi momento per parlare con uno dei nostri consulenti di incident response:

- Australia: +61 272084454
- Austria: +43 73265575520
- Canada: +1 7785897255
- Francia: +33 186539880
- Germania: +49 61171186766
- Italia: +39 02 94752 897
- Svizzera: +41 445152286
- Regno Unito: +44 1235635329
- Stati Uniti: +1 4087461064

Mandaci un'e-mail, scrivendo all'indirizzo: EmergencyIR@sophos.com.

Emergency Incident Response è un servizio remoto o in loco?
È disponibile sia l'opzione di usufruire del servizio da remoto, che in loco.

Quanto è rapido il servizio Emergency Incident Response?
Per la maggior parte dei clienti, l'onboarding richiede solo poche ore e la valutazione viene completata entro 48 ore. Poiché il servizio può intervenire completamente da remoto, la strategia di risposta viene implementata entro poche ore dal tuo primo contatto con Sophos.

Quanto tempo ci va per iniziare l'onboarding?
Il team Emergency Incident Response può avviare il processo di onboarding e le indagini non appena riceve la tua approvazione.

Qual è la metodologia di Emergency Incident Response?
Una volta che accetti il contratto di servizio, cominceremo con una chiamata iniziale. Se preferisci, possiamo anche procedere con una conversazione e-mail. L'indagine inizia non appena abbiamo compreso quali sono i tuoi obiettivi per il nostro incarico.

Emergency Incident Response include diverse categorie di intervento che possiamo offrire. Nel corso della chiamata esplorativa iniziale, collaboreremo con te per identificare le categorie richieste e concordare un numero di ore stimato.

Le categorie su cui ci focalizziamo includono: Gestione dell'intervento, Incident Response, Analisi forensi digitali, Valutazione dello stato di compromissione, Threat Hunting, Dati di intelligence e ricerca sulle minacce, Negoziazione del riscatto, Report sull'incarico, Supporto in loco (se applicabile), Business Email Compromise e Distribuzione del software.

In quali lingue è disponibile il servizio Emergency Incident Response?
Attualmente il servizio viene offerto in lingua inglese e giapponese. Devi avere una conoscenza di livello tecnico della lingua inglese o giapponese.

Sophos sostituisce o utilizza servizi di Digital Forensics and Incident Response (DFIR, incident response con analisi digitali forensi)?
Emergency Incident Response è un servizio DFIR. Non occorre coinvolgere un'altra azienda di sicurezza per la DFIR, poiché l'ambito dei servizi forniti attraverso Emergency Incident Response può includere indagini forensi digitali.

Devo installare tecnologie Sophos sui miei endpoint?
No, il servizio Emergency Incident Response può essere fornito utilizzando Sophos XDR; in alternativa, possiamo implementare il sensore di Sophos XDR parallelamente alla tua soluzione di protezione endpoint attuale. Entrambe le opzioni ci permettono di svolgere indagini sull'incidente.

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

Come vengono calcolati i costi?
Sophos fornirà una stima del numero di ore necessarie per rispondere all'incidente, basandosi su domande volte a definire l'ambito dell'intervento. Pagherai solo le ore effettive che utilizzerai.

Sono previsti ulteriori costi?
Se è richiesta la presenza in loco, ti verranno addebitate le spese della trasferta.

Possiamo implementare Emergency Incident Response solo su un segmento del nostro ambiente, oppure dobbiamo includere l'intero ambiente?
In alcune situazioni, il servizio Emergency Incident Response può essere applicato solamente a un segmento del tuo ambiente. Un esperto del team Emergency Incident Response sarà in grado di fornirti ulteriori informazioni durante l'identificazione dell'ambito di ogni progetto.

Sophos può collaborare con un intermediario che rappresenta la mia organizzazione, 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 Emergency Incident Response prevede 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 decrittograferà i dati crittografati dal ransomware per conto mio?
No, questa attività non rientra nell'ambito del servizio Emergency Incident Response.

Sophos mi aiuterà a negoziare o a effettuare il pagamento di un riscatto per i dati?
Emergency Incident Response include un'opzione di negoziazione del riscatto con i cybercriminali mediante l'intervento di personale esperto. Detto questo, Sophos non gestisce i pagamenti dei riscatti, ma può consigliare e collaborare con terze parti per questo scopo, se richiesto.

2025-06-03 (WP-NP)

SOPHOS