Brochure

Sophos Emergency Incident Response

Assistenza con servizio completo, dalle indagini iniziali fino al ritorno alla normalità operativa

Risposta immediata alle minacce attive

Se la tua azienda è sotto attacco, ogni secondo conta. Quando si verifica un incidente informatico, quello che ti serve sono rapidità ed efficienza, più esperienza e competenze di sicurezza multidisciplinari. Inoltre, devi avere un'ottima conoscenza e piena visibilità sul mutevole panorama globale delle minacce, nonché sulle più moderne tattiche e tecniche sfruttare dai cybercriminali.

Sophos Emergency Incident Response è un servizio che ti aiuta ad affrontare un'emergenza informatica. Prevede la valutazione, l'isolamento, la comprensione e la correzione rapida dell'incidente. 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. Sophos si basa su quello che ha appreso aiutando clienti in migliaia di casi per orientare miglioramenti e azioni di prevenzione consigliati, in grado non solo di risolvere la causa originaria dell'incidente, ma anche di incrementare la tua resilienza contro attacchi futuri.

Potenzia proattivamente le tue difese e il tuo profilo di sicurezza

Sophos Emergency Incident Response adotta un approccio collaborativo e interattivo, lavorando a stretto contatto con il tuo team per valutare rapidamente la situazione, isolare ed eliminare la minaccia secondo necessità, e fornire consigli pratici per tornare alla normalità operativa. Il nostro team individua ed elimina le minacce grazie a capacità come l'analisi forense digitale, la valutazione dei malware e le attività di threat hunting, più i dati di intelligence sulle minacce raccolti dai team di ricerca Sophos X-Ops e Counter Threat Unit. Coinvolgiamo esperti interdisciplinari (come penetration tester e ricercatori sulle minacce) per garantire la mitigazione dei rischi e il ritorno alla normalità operativa.

Rilevamento e indagine

Contatto e indagine iniziale

Per garantire la massima tempestività di risposta, Sophos si concentra sull'implementazione immediata di agenti in tutte le risorse individuabili. Questa assistenza remota per l'incident response permette di acquisire dati forensi per svolgere l'analisi iniziale, per sviluppare azioni di contenimento adeguate, e per determinare l'eventuale esigenza di ulteriori tecnologie al fine di incrementare la visibilità per l'intera durata dell'incarico.

I vantaggi per i clienti

- Aumenta il potenziale del tuo team con analisi digitali forensi, funzionalità di incident response e un'esperienza maturata sul campo.
- Riduci l'impatto di un incidente e il rischio che si ripresenti, acquisendo una comprensione completa della minaccia.
- Aumenta la visibilità, ottieni dati e trova rapidamente le risposte che cerchi, per stabilire quali azioni intraprendere.

Indagini più approfondite

Acquisizione di dati: risorse, servizi colpiti, impatto commerciale, altri vettori di attacco.

Analisi forense e delle minacce iterativa: ricercatori, threat hunter, penetration tester e analisti aiutano a ottenere una comprensione completa della minaccia.

Pianificazione delle attività di correzione: inizia a pianificare le attività di correzione, parallelamente e in sincronia con le indagini.

Riduzione della superficie di attacco: Sophos può fornire approfondimenti sugli autori degli attacchi, per verificare l'efficacia dei controlli e identificare eventuali altri punti di accesso, garantendo così una mitigazione completa dei rischi.

Negoziazione del riscatto: gli esperti di negoziazione in scenari di ransomware attingono alle proprie conoscenze sugli autori degli attacchi ransomware per facilitare la negoziazione e offrire consulenza su come recuperare i dati in maniera sicura ed economica.

Correzione

Protezione e verifica

Misure di protezione avanzata e mirata: il team Incident Response (IR) coordina e supporta attività tattiche di potenziamento dei controlli di sicurezza, per evitare una nuova infiltrazione nei sistemi da parte dei cybercriminali.

Contenimento: interruzione della connessione al centro di comando e controllo dei cybercriminali.

Rimozione degli intrusi: la rimozione dei cybercriminali da una rete isolata richiede l'eliminazione orchestrata di ogni loro traccia nella rete e il ripristino dei domini compromessi.

Recupero

Recupero dei sistemi e dei dati: per ripristinare i sistemi, sanificare i dati e riportare l'intera infrastruttura informatica alla normalità operativa, il team Sophos IR collabora con Partner di fiducia per fornire servizi di ripristino in maniera fluida e sicura.

Convalida dell'host: con la nostra tecnologia leader di settore basata sugli agenti, ti aiutiamo a garantire che gli host ripristinati siano pronti per il ritorno alla modalità di produzione.

Follow-up

Miglioramenti

Sophos fa tesoro delle lezioni apprese nel corso delle migliaia di incarichi che abbiamo completato, per orientare l'ottimizzazione dei processi di risposta consigliati e fornire raccomandazioni strategiche che contribuiscono a definire una roadmap di trasformazione della sicurezza. Al termine dell'incarico, possiamo compilare un report ufficiale delle nostre indagini sull'incidente, che include la descrizione dettagliata delle azioni intraprese e delle informazioni ottenute, nonché consigli per una strategia a lungo termine incentrata sul mitigare il rischio che minacce simili si ripresentino in futuro.

Caratteristiche del servizio

- Identificazione e neutralizzazione rapida delle minacce attive.
- Sviluppo rapido delle tecnologie.
- Acquisizione e analisi di dati forensi digitali per identificare gli indicatori di compromissione e intercettare le attività dei cybercriminali.
- Threat hunting per identificare le attività dannose correlate.
- Servizi tecnici, di gestione degli incidenti e di consulenza, offerti da remoto e in loco.
- Un team di incident response globale composto da professionisti altamente qualificati, con esperienza in scenari di attacco informatico comuni e meno comuni.
- Dati di intelligence sulle minacce specifici per l'incidente e approfondimenti sulle tattiche e tecniche attuali dei cybercriminali.
- Negoziazione del riscatto condotta da esperti.
- Report dopo la risoluzione dell'incidente, con informazioni dettagliate sulle azioni intraprese, sulle novità scoperte e sulle raccomandazioni fornite.

Perché scegliere Sophos per l'incident response?

Sophos affronta ogni incarico di cybersecurity di emergenza applicando l'ampia esperienza maturata sul campo. Offriamo assistenza completa per l'incident response a un'ampia selezione di organizzazioni appartenenti a diversi mercati verticali e che affrontano vari tipi di incidenti: da piccoli problemi che riguardano un unico sistema compromesso, fino a situazioni di crisi a livello dell'intera azienda che ostacolano o bloccano completamente le attività operative.

Il nostro team di professionisti di incident response vanta conoscenze e competenze maturate in scenari quali enti nazionali e militari, team di incident response di sicurezza informatica (CSIRT) a livello organizzativo, forze dell'ordine e servizi segreti. Agisce unendo la comprensione pratica delle più importanti prassi di cybersecurity ad attività di incident response in prima linea, attingendo dai dati di intelligence sulle minacce dei nostri team di ricerca X-Ops e Counter Threat Unit. Inoltre, utilizza i risultati dei nostri test e valutazioni della protezione, più le nostre analisi della sicurezza per accelerare le indagini e tornare con fiducia alla normalità operativa.

La tua azienda sta affrontando una violazione attiva?

Chiama in qualsiasi momento uno dei numeri riportati di seguito per parlare con i nostri esperti di risposta agli incidenti.

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

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

E-mail: EmergencyIR@sophos.com

Per saperne di più, visita

sophos.com/emergency-response

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

2025-06-04 BRIT (MP)

SOPHOS