Sophos Compromise Assessment

Individua le prove concrete di una violazione, prima che possano avere ripercussioni sulla tua organizzazione

L'anno scorso le imprese hanno investito in media 37 giorni e 2,4 milioni di $ per individuare le violazioni di sicurezza e riprendere le normali attività lavorative. Svolto da un team di esperti nella risposta agli incidenti di cybersecurity, il Sophos Compromise Assessment è il metodo più rapido ed efficace per identificare le attività degli hacker nel tuo ambiente IT. Il team è in grado di rilevare sia le attività attualmente in corso che quelle passate. La tua organizzazione potrà così intraprendere azioni rapide e decisive.

Identificazione Delle Attività Degli Hacker In Corso O Recenti

Condotto da un team di esperti di threat hunting e Incident Response, il Sophos Compromise Assessment stabilisce rapidamente se un hacker è riuscito a eludere le tue difese informatiche, quantifica il livello di rischio per la tua organizzazione e offre consigli dettagliati sulle azioni da intraprendere per eliminare la minaccia.

La vasta esperienza maturata nell'ambito della risposta alle minacce più avanzate permette al team Sophos Incident Response (IR) Services di identificare eventuali indicatori di compromissione (IoC), svolgendo indagini mirate sulle risorse potenzialmente compromesse. Il risultato è una valutazione rapida e accurata, che aiuta la tua organizzazione a gestire il rischio e la conformità, permettendoti allo stesso tempo di mantenere la piena capacità operativa.

Metodologia Della Sophos Compromise Assessment

Il team Sophos IR Services mantiene una comunicazione diretta con la tua organizzazione durante ogni fase della valutazione. Questo garantisce completa trasparenza sulla minaccia, sul livello di rischio e sulle azioni da intraprendere per risolvere l'incidente ed eliminare la causa originaria.

1. **Chiamata di coordinamento iniziale**: la valutazione comincia con uno scrupoloso scambio di informazioni sulla potenziale minaccia; vengono inoltre identificate le principali persone di riferimento e viene fornita conferma dell'ambito di implementazione del servizio e della procedura investigativa da seguire.
2. **Distribuzione degli strumenti di indagine**: installazione guidata della pluripremiata piattaforma Sophos basata sul cloud, per garantire l'acquisizione immediata dei dati sui dispositivi selezionati; questo permette al team Sophos IR Services di condurre una valutazione accurata dello stato di integrità del dispositivo.
3. **Indagine sulle minacce e valutazione del rischio**: se viene confermata la presenza di una minaccia attiva, il team Sophos IR Services effettuerà immediatamente una "Active Threat Call" (chiamata per minaccia attiva), coinvolgendo le persone di riferimento che hai nominato, per discutere del rischio che si verifichi un incidente di sicurezza più esteso e per definire le azioni più urgenti da intraprendere.
4. **Riepilogo della chiamata e report scritto**: riceverai dei documenti tecnici, più un riepilogo non tecnico che descrive nel dettaglio le prove dell'attività degli hacker e il livello di rischio, offrendo consigli pratici su come rimuovere la minaccia e risolvere la causa originaria del problema.

Tutte e quattro le fasi del Sophos Compromise Assessment vengono solitamente completate entro 7 giorni dalla chiamata di coordinamento iniziale.

Caratteristiche Principali

- Identificazione rapida della presenza di un hacker che agisce indisturbato nel tuo ambiente, senza essere stato rilevato
- Quantificazione del rischio potenziale che si verifichi un incidente di sicurezza esteso
- Comunicazione diretta con un team di esperti, specializzati in threat hunting e Incident Response in ogni fase dell'indagine
- Analisi dettagliata dell'attività degli hacker e del livello di rischio, con consigli su come rimuovere la minaccia e risolvere la causa originaria del problema
- Supporto per iniziative di gestione del rischio e rispetto della conformità, oltre alle dovute verifiche in caso di fusione o acquisizione

SOPHOS

Indagini Rapide E Accurate

Il Sophos Compromise Assessment svolge indagini per identificare un ampio spettro di attività degli hacker, che includono:

- Attività di rete sospette
- Movimenti laterali
- File anomali o dannosi
- Esecuzione automatica di malware
- Accesso non autorizzato
- Privilege escalation
- Elusione dei tentativi di difesa
- Furto di credenziali
- Esfiltrazione dei dati
- Script non verificati

Dopo La Valutazione

Se il team Sophos IR Services conferma che un cybercriminale è riuscito a eludere le tue difese informatiche, violando dati e sistemi aziendali, potrai optare per l'onboarding prioritario di Sophos Rapid Response. Questo servizio completo di Incident Response provvederà a classificare, isolare e neutralizzare la minaccia attiva nel tuo ambiente informatico. Un team di esperti di Incident Response operativo 24/7 da remoto entrerà rapidamente in azione per rimuovere gli hacker dal tuo ambiente e consiglierà azioni preventive in tempo reale per risolvere la causa originaria del problema.

Se non vengono individuati indizi di una violazione, Sophos Managed Detection and Response (MDR) continuerà a offrire alla tua organizzazione servizi di rilevamento e risposta 24/7. Il nostro team di threat hunter ed esperti di Incident Response lavora instancabilmente e incessantemente per individuare e confermare in maniera proattiva la presenza di potenziali minacce e incidenti. Il team intraprende azioni continue per fermare, isolare e neutralizzare le minacce in evoluzione, fornendo consigli pratici per risolvere l'incidente alla radice, al fine di migliorare il tuo profilo di integrità.

Sei stato colpito da un cyberattacco?

Sophos Rapid Response ti 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. L'attivazione richiede poche ore e nella maggior parte dei casi la valutazione viene completata entro 48 ore. Se stai affrontando una minaccia attiva, chiama uno dei numeri locali indicati di seguito in qualsiasi momento, per parlare con i nostri esperti di Incident Response.

Se stai affrontando una minaccia attiva, contatta il team Rapid Response, inviando un'e-mail all'indirizzo rapidresponse@sophos.com, oppure chiamando uno dei seguenti numeri locali:

Italia: +39 02 947 52897

Stati Uniti: +1 4087461064

Australia: +61 272084454

Canada: +1 7785897255

Francia: +33 186539880

Germania: +49 61171186766

Svezia: +46 858400610

Regno Unito: +44 1235635329

Austria: +43 73265575520

Svizzera: +41 445152286

Paesi Bassi: +31 162708600

Spagna: +34 913758065

Sei stato colpito da un cyberattacco?

Ottieni assistenza tempestiva con Sophos Rapid Response

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

2023-06-27 DS-IT (PC)

SOPHOS