PRESENTAZIONE DELLA SOLUZIONE

Sophos ITDR

Identity Threat Detection and Response

Sophos Identity Threat Detection and Response (ITDR) identifica e risponde alle minacce che riescono a sfuggire ai tradizionali controlli di sicurezza basati sull'identità. Completamente integrato in Sophos Extended Detection and Response (XDR) e Sophos Managed Detection and Response (MDR), Sophos ITDR aiuta a migliorare il profilo di sicurezza della tua organizzazione, monitorando continuamente il tuo ambiente alla ricerca di errori di configurazione e rischi di identità. Inoltre, fornisce dati di intelligence relativi alle sulle credenziali compromesse, ottenuti dal dark web.

Casi di utilizzo

1 | PROTEZIONE CONTRO LE MINACCE ALL'IDENTITÀ

Esito desiderato: neutralizzare gli attacchi basati sull'identità, prima che possano causare danni alla tua azienda.

La soluzione: negli ultimi 12 mesi, il 90% delle organizzazioni ha subito una violazione dell'identità[1]. Sophos ITDR permette di identificare proattivamente le minacce più sofisticate e protegge dal 100% delle tecniche "Credential Access" (Credenziali di accesso) di MITRE ATT&CK[2] nelle prime fasi della catena di attacco, rispondendo con rapidità e precisione. Gli analisti esperti di Sophos MDR sono in grado di indagare sulle attività ad alto rischio e di intraprendere immediatamente azioni per conto tuo, tra cui: la disattivazione di un utente, l'obbligo di reimpostare la password, il blocco di un account, la revoca delle sessioni e molto di più.

2 | RIDUZIONE DELLA SUPERFICIE DI ATTACCO DELL'IDENTITÀ

Esito desiderato: identificare e correggere gli errori di configurazione e le lacune di sicurezza basate sull'identità.

La soluzione: il 95% degli ambienti Microsoft Entra ID presenta errori di configurazione critici[3]. Se trascurate, queste vulnerabilità possono essere sfruttate dai cybercriminali per ottenere privilegi più elevati e sferrare attacchi basati sull'identità. Sophos ITDR analizza continuamente il tuo ambiente Entra ID per identificare all'istante errori di configurazione e lacune di sicurezza, offrendo consigli pratici per la correzione.

3 | INDIVIDUAZIONE DELLA FUGA E DEL FURTO DI CREDENZIALI

Esito desiderato: ridurre al minimo il rischio che le credenziali esposte vengano utilizzate per sferrare un attacco.

La soluzione: l'identità continua a essere uno dei principali vettori di accesso per il ransomware e Sophos ha osservato che negli ultimi 12 mesi il numero di credenziali rubate che sono in vendita in uno dei principali marketplace del dark web è raddoppiato[4]. Sophos ITDR monitora il dark web e i database delle violazioni, avvisandoti quando le credenziali diventano esposte, per ridurre il rischio che vengano utilizzate in un attacco futuro.

4 | IDENTIFICAZIONE DEI COMPORTAMENTI RISCHIOSI DEGLI UTENTI

Esito desiderato: comprendere e affrontare i comportamenti ad alto rischio degli utenti, per proteggere l'azienda.

La soluzione: monitorando la presenza di pattern di accesso insoliti e attività utente anormale puoi ridurre significativamente i tuoi rischi di cybersecurity e proteggere le tue risorse più preziose. Sophos ITDR identifica i comportamenti rischiosi che possono essere sfruttati dai cybercriminali (o che potrebbero indicare che le credenziali di un utente sono state compromesse) e fornisce dettagli sugli utenti della tua organizzazione per i quali sono stati recentemente generati avvisi di sicurezza Sophos.

Gartner Peer Insights Customers' Choice 2025

Uno dei vendor "Customers' Choice" 2025 di Gartner® Peer Insights™ per i servizi di Extended Detection and Response (XDR).

Tra i Leader nei G2 Overall Grid® Reports per MDR e XDR, in base alle valutazioni e alle recensioni dei clienti.

MITRE | ATT&CK® Evaluations

Ottimo Performer nelle valutazioni MITRE ATT&CK® per le categorie Enterprise Products (Prodotti Enterprise) e Managed Services (Servizi gestiti).

Scopri di più:
sophos.it/ITDR

[1] Studio condotto dalla Identity Defined Security Alliance (IDSA) 2024. | [2] In base alle capacità di rilevamento di Sophos, con mapping al framework MITRE ATT&CK.
[3] Dati raccolti da migliaia di interventi di incident response condotti da Sophos. | [4] Dati della Counter Threat Unit (CTU) di Sophos X-Ops, giugno 2024 - giugno 2025.

2025-09-16 SB-IT (MP)