SOPHOS

Casi di utilizzo: Sophos EDR e XDR

Disponibili con Intercept X Advanced with XDR, Intercept X Advanced with EDR, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with EDR

Ora è possibile trovare risposta alle domande critiche sulle IT operation e sul threat hunting, con la possibilità di intervenire quando richiesto. Le potenti funzionalità di queste soluzioni sono progettate per essere utilizzate sia dagli amministratori IT che dagli analisti di cybersecurity.

Gestione operativa dei sistemi di IT security e delle attività di threat hunting

- Scelta tra query SQL precompilate e completamente personalizzabili
- Possibilità di intraprendere rapidamente un'azione adeguata, non appena sono state raccolte tutte le informazioni richieste
- Include endpoint, server, firewall, e-mail, host di servizi cloud e molto di più

Sophos XDR

Casi di utilizzo per le IT operation

I casi di utilizzo per le IT operation aiutano a garantire le condizioni ottimali per salvaguardare l'integrità delle stesse. Quelli che seguono sono alcuni esempi di casi di utilizzo:

Controlli sullo stato di integrità del dispositivo

Identificazione dei dispositivi che mostrano problemi di performance, con la possibilità di accedervi da remoto per intraprendere l'azione più adeguata.

- Individuazione dei dispositivi con spazio limitato su disco, utilizzo elevato di memoria/CPU o in attesa di riavvio
- Accesso da remoto ai dispositivi per liberare spazio su disco, indagare sulle potenziali cause di un utilizzo elevato delle risorse e riavviare il sistema se necessario

Vulnerabilità

Identificazione dei dispositivi che presentano problemi o vulnerabilità che possono essere sfruttate da malware o hacker.

- Individuazione dei dispositivi con software che presentano vulnerabilità, servizi sconosciuti in esecuzione o estensioni del browser non autorizzate; inoltre è possibile rilevare le credenziali degli account che sono state condivise o prelevate illecitamente
- Accesso da remoto ai dispositivi per installare patch, condurre indagini, interrompere i servizi sconosciuti, disinstallare le estensioni del browser indesiderate e aggiornare le credenziali degli account cloud

Software indesiderato

Individuazione proattiva della presenza di software che potrebbe causare problemi di conformità o di produttività.

- Identificazione dei programmi indesiderati, ad esempio Spotify, Steam e BitTorrent
- Accesso da remoto ai dispositivi e disinstallazione dei software indesiderati

Errori di configurazione

Identificazione dei dispositivi e dei workload nel cloud che presentano problemi di configurazione e che potrebbero esporre i sistemi a rischi di sicurezza.

- Individuazione dei server su cui sono abilitati RDP e SSH, nonché dei security group nel cloud le cui porte di rete sono state lasciate aperte; inoltre, sono disponibili opzioni di monitoraggio e inventario degli host, dei container e di altri elementi nel cloud pubblico
- Accesso da remoto ai server, disattivazione di RDP/SSH e verifica della presenza di server in ascolto sulle porte aperte

Compliance

Identificazione e risoluzione dei problemi di conformità, sia per i sistemi on-premise che nel cloud.

- Individuazione dei file contenenti dati di natura sensibile e valutazione delle configurazioni degli ambienti AWS, Azure e GCP
- Accesso ai dispositivi da remoto per eliminare i file di natura sensibile e per verificare la sicurezza delle configurazioni del cloud rispetto agli standard CIS Benchmarks

Implementazione di progetti

Verifica dell'implementazione dei progetti IT, per assicurarsi che siano stati distribuiti su tutti i dispositivi.

- Visualizzazione dello stato di installazione dei software sui dispositivi, per valutare l'avanzamento dell'installazione
- Accesso da remoto ai dispositivi per garantire il completamento dell'installazione e il riavvio (se richiesto), al fine di applicare tutte le modifiche necessarie

Problemi della rete negli uffici (è richiesto XDR)

Visualizzazione e correzione dei problemi di rete in tutti gli uffici.

- Individuazione dei motivi alla base dei problemi che rallentano la performance della rete di un ufficio
- Identificazione dell'applicazione che causa il problema

Gestione dei dispositivi (è richiesto XDR)

Individuazione e identificazione dei dispositivi connessi all'ambiente IT dell'organizzazione.

- Visualizzazione di dispositivi non gestiti e non protetti, ad es. laptop, telefoni cellulari e appliance IoT
- Capacità aggiuntive di supervisione per i dispositivi obsoleti o non gestibili, come ad es. apparecchiature mediche specializzate

Preparazione per affrontare circostanze imprevedibili (è richiesto XDR)

Con 30 giorni di archiviazione nel cloud, anche le circostanze imprevedibili non saranno un problema.

- Possibilità di indagare sugli ultimi 30 giorni di attività di un dispositivo smarrito, per identificare gli eventi anomali
- Visualizzazione degli eventi del dispositivo, anche se è stato formattato o reso inutilizzabile

Casi di utilizzo per il threat hunting

Individuazione proattiva ed eliminazione delle minacce più velate ed elusive. Quelli che seguono sono solo alcuni dei casi di utilizzo possibili:

Attacchi alla rete

Identificazione dei processi che effettuano tentativi di accesso alla rete dalle caratteristiche insolite.

- Individuazione dei processi che effettuano tentativi di connessione su porte non standard o del traffico in uscita insolito, proveniente da un workload nel cloud
- Analisi dei security group nel cloud, per identificare le risorse esposte all'Internet pubblico
- Accesso dispositivi o workload da remoto, interruzione del processo e verifica della presenza di movimenti laterali

File modificati

Individuazione degli elementi che sono stati modificati in maniera inattesa.

- Identificazione dei processi che hanno recentemente modificato file o chiavi di registro
- Accesso da remoto al dispositivo, con possibilità di analizzare le modifiche e intraprendere azioni adeguate

Script offuscati

Gli attacchi a livello di memoria e indipendenti dai file sono un vettore di attacco molto comune.

- Analisi approfondita dei dettagli delle esecuzioni inattese di PowerShell
- Accesso da remoto al dispositivo, per eseguire ulteriori strumenti di analisi approfondita e interrompere i processi sospetti

Processi camuffati

Alcuni processi dannosi sono in grado di camuffarsi per eludere il rilevamento.

- Individuazione dei processi camuffati
- Accesso da remoto ai dispositivi, per interrompere i processi sospetti ed eseguire strumenti di analisi approfondita

Framework MITRE ATT&CK

Il framework MITRE ATT&CK è un modello comunemente utilizzato per identificare le tecniche di attacco.

- Utilizzo di query personalizzate o compilate da Sophos per identificare le tattiche e le tecniche di attacco utilizzate dagli hacker
- Possibilità di focalizzare le indagini in base alla tecnica identificata, per indagare ulteriormente su potenziali tipi o ambiti di attacco specifici

Impatto degli incidenti

Comprensione dell'impatto degli incidenti, con indicazioni sui dispositivi e sugli utenti che sono stati colpiti.

- Identificazione dei dispositivi nei quali è stato aperto un link di phishing
- Visualizzazione dei dispositivi che hanno caricato file da un sito di phishing, con possibilità di accedere da remoto a tali dispositivi per eseguire una disinfezione

Periodi di indagine estesi (è richiesto XDR)

30 giorni di archiviazione dei dati nel cloud, più 90 giorni sui dispositivi.

- Possibilità di svolgere indagini sui dati degli ultimi 30 giorni, senza che il dispositivo debba essere on-line
- Visualizzazione degli eventi dei dispositivi che sono stati resi inutilizzabili durante un attacco

Utilizzo di dati di rete (è richiesto XDR)

Integrazione dei dati di rete nelle attività di indagine e threat hunting.

- Verifica incrociata del traffico dannoso bloccato, con il confronto con altri indicatori di compromissione per capire il contesto degli attacchi estesi
- Utilizzo dei rilevamenti ATP e IPS del firewall per svolgere indagini sugli host e sui dispositivi sospetti

Utilizzo di dati della posta elettronica esaurienti (è richiesto XDR)

Integrazione dei dati della posta elettronica per ulteriori approfondimenti sul proprio ambiente informatico.

- Confronto tra le informazioni presenti nell'intestazione dell'e-mail e altri indicatori di compromissione, per comprendere meglio gli incidenti
- Identificazione e rimozione rapida dei file sospetti dai dispositivi e dalle cassette postali di O365

Per maggiori informazioni su Sophos XDR, EDR e sulle potenti capacità di protezione disponibili in Intercept X, visitate: Sophos.it.

26/03/21 UC-IT (MP)

SOPHOS