SOPHOS

Cas d'usages Sophos EDR et XDR

Disponible avec Intercept X Advanced with XDR, Intercept X Advanced with EDR, Intercept X Advanced for Server with XDR et Intercept X Advanced for Server with EDR

Sophos XDR

Obtenez les réponses à vos questions critiques relatives aux opérations informatiques et à la traque des menaces, et prenez les mesures nécessaires. Tant les administrateurs informatiques que les analystes de la cybersécurité peuvent tirer parti de cette puissante fonctionnalité.

Réalisez des opérations de sécurité informatique et de traque des menaces

- Choisissez parmi des requêtes SQL pré-écrites entièrement personnalisables
- Prenez rapidement des mesures dès que vous avez les informations dont vous avez besoin
- Couvre les systèmes endpoint, les serveurs, les pare-feux, la messagerie, les hébergements Cloud, etc.

Cas d'usages pour les opérations IT

Les cas d'usages pour les opérations IT maintiennent vos opérations informatiques au plus haut niveau. Voici quelques exemples :

Contrôle de l'intégrité de l'appareil

Identifiez les appareils qui ont des problèmes de performance, puis accédez-y à distance pour prendre les mesures nécessaires.

- Trouver les appareils qui ont un faible espace disque, une forte utilisation de la mémoire/CPU ou qui sont en attente de redémarrage.
- Accéder à distance aux appareils pour libérer de l'espace disque, analyser les causes de cette forte utilisation et redémarrer selon les besoins.

Vulnérabilités

Détectez les appareils qui ont des problèmes ou des vulnérabilités pouvant être exploitées par des malwares ou des attaquants.

- Localiser les appareils avec des failles logicielles, des services inconnus en cours d'exécution ou des extensions de navigateur non autorisées, et détecter les identifiants de comptes partagés ou volés.
- Accéder à distance aux appareils pour installer des correctifs, analyser et arrêter les services inconnus, désinstaller les extensions de navigateur et modifier les identifiants de comptes Cloud.

Logiciels indésirables

Identifiez les logiciels qui posent des problèmes de conformité ou de productivité.

- Trouver des programmes indésirables comme Spotify, Steam et BitTorrent.
- Accéder à distance aux ordinateurs et désinstaller les logiciels.

Oublis dans la configuration

Trouvez les appareils et les ressources Cloud mal configurés présentant des risques de sécurité.

- Identifier les serveurs avec des protocoles RDP et SSH activés, les groupes de sécurité Cloud avec des ports réseau restés ouverts, et surveiller et inventorier les hébergements de Cloud public, les conteneurs, etc.
- Accéder à distance aux serveurs, désactiver les protocoles RDP/SSH et vérifier la présence de serveurs surveillant les ports ouverts.

Conformité

Identifiez et corrigez les problèmes de conformité en local et dans le Cloud.

- Trouver des fichiers sensibles et évaluer les configurations pour les environnements AWS, Azure et GCP.
- Accéder à distance aux appareils pour supprimer les fichiers sensibles, garantir la conformité aux critères CIS des configurations de sécurité Cloud.

Déploiement de projets

Vérifiez si vos projets IT ont bien été déployés sur l'ensemble des postes.

- Vérifier si un logiciel particulier a bien été déployé sur l'ensemble des postes et mesurer la progression tout au long du déploiement.
- Accéder à distance aux appareils pour s'assurer que le déploiement a réussi et les redémarrer si besoin pour effectuer les changements nécessaires.

Problèmes de réseau au bureau (requiert XDR)

Consultez et corrigez les problèmes de réseau sur l'ensemble de vos sites.

- Comprendre pourquoi un bureau a des problèmes de réseau qui ralentissent les performances.
- Identifier l'application à l'origine du problème

Gestion des appareils (requiert XDR)

Identifiez les appareils dans l'environnement informatique de votre organisation.

- Voir les appareils non gérés et non protégés tels que les ordinateurs portables, les mobiles et les appareils connectés (IoT).
- Obtenir une surveillance supplémentaire des anciens appareils ou des appareils impossibles à gérer, tels que les équipements médicaux spécialisés.

Attendre l'inattendu (requiert XDR)

Avec 30 jours de stockage dans le Cloud, ne vous laissez pas surprendre par des événements inattendus.

- Revenir 30 jours en arrière pour détecter toute activité inhabituelle sur un appareil disparu
- Découvrir ce qu'il est advenu d'un appareil, même s'il a été réinitialisé ou détruit.

Cas d'usages pour la traque des menaces

Débusquez les menaces évasives et subtiles, et nettoyez-les rapidement. Voici quelques exemples de cas d'usages :

Attaques du réseau

Identifiez les processus qui tentent d'accéder au réseau de manière inhabituelle.

- Détecter les processus qui tentent de se connecter sur des ports non standard ou le trafic sortant inhabituel à partir d'une ressource Cloud.
- Analyser les groupes de sécurité Cloud pour identifier les ressources exposées à l'Internet public.
- Accéder à distance à l'appareil/ressource, arrêter le processus et analyser les mouvements latéraux.

Fichiers modifiés

Trouvez les éléments ayant été modifiés d'une manière inhabituelle.

- L'identification des processus qui ont récemment modifié des fichiers ou des clés de registre.
- Accéder à distance à l'appareil, analyser les modifications et prendre des mesures appropriées.

Scripts dissimulés

Les attaques sans fichier et basées sur la mémoire sont un vecteur d'attaque usuel.

- Passer au crible les données sur les exécutions PowerShell inattendues.
- Accéder à distance à l'appareil, lancer des outils d'analyses complémentaires et arrêter les processus suspects.

Processus déguisés

Certains processus malveillants se déguisent pour éviter d'être détectés.

- Détecter les processus qui se déguisent.
- Accéder à distance à l'appareil, arrêter les processus suspects et lancer des outils d'investigation.

Cadre MITRE ATT&CK

La cadre MITRE ATT&CK est un modèle habituellement utilisé pour identifier les techniques d'attaque.

- Utiliser vos propres requêtes ou les requêtes Sophos pour identifier les tactiques d'attaque et les techniques utilisées par les adversaires.
- Affiner vos investigations pour rechercher d'éventuelles attaques successives ou des zones à vérifier, en vous basant sur ces techniques identifiées.

Étendue de l'incident

Déterminez l'impact d'un incident et les appareils et les utilisateurs touchés.

- Identifier les postes sur lesquels un utilisateur a cliqué sur un lien dans un email de phishing.
- Voir quels postes ont téléchargé des fichiers à partir du site de phishing, y accéder à distance et les nettoyer.

SOPHOS

Prolonger les périodes d'investigation (requiert XDR)

Utilisez 30 jours de données dans le Cloud en plus des 90 jours de stockage de données sur l'appareil.

- Analyser 30 jours de données sans avoir besoin de remettre un appareil en ligne.
- Voir ce qui est arrivé aux appareils mis hors service lors d'une attaque

Utiliser des données réseau riches (requiert XDR)

Intégrez les données réseau pour la traque des menaces et vos investigations.

- Recouper le trafic malveillant bloqué avec d'autres IoC pour identifier une attaque plus large.
- Utiliser les détections ATP et IPS du pare-feu pour analyser les hôtes et les appareils suspects

Utiliser des données de messagerie riches (requiert XDR)

Intégrez les données des emails pour obtenir des informations supplémentaires sur votre environnement.

- Comparer les informations d'en-tête des emails avec d'autres IoC pour mieux comprendre un incident
- Identifier les fichiers suspects et les supprimer rapidement des appareils et des boîtes de réception O365.

Pour en savoir plus sur Sophos XDR, EDR et les capacités de protection puissantes d'Intercept X, rdv sur Sophos.fr.

21-03-26 UC-FR (MP)

SOPHOS