Managed Threat Detection

Complémentez votre protection Endpoint non Sophos existante avec la surveillance et la détection 24h/24 et 7j/7, sous la forme d'un service entièrement managé.

Bring Your Own Protection

Peu d'entreprises disposent des outils, personnels et processus internes nécessaires pour gérer efficacement leurs programmes de sécurité. Nous dépendons beaucoup de la protection Endpoint automatisée, mais que se passe-t-il si des cybercriminels parviennent à contourner cette protection ? Quelqu'un le remarquera-t-il avant qu'il ne soit trop tard ?

Sophos Managed Threat Detection surveille et détecte les menaces 24/7, pour que toute activité suspecte échappant à votre protection Endpoint ne passe pas inaperçue. Le service est conçu pour fonctionner en parallèle des produits de protection Endpoint non Sophos, ce qui permet aux entreprises d'utiliser leur propre protection tout en bénéficiant de la surveillance par des experts Sophos.

Détection

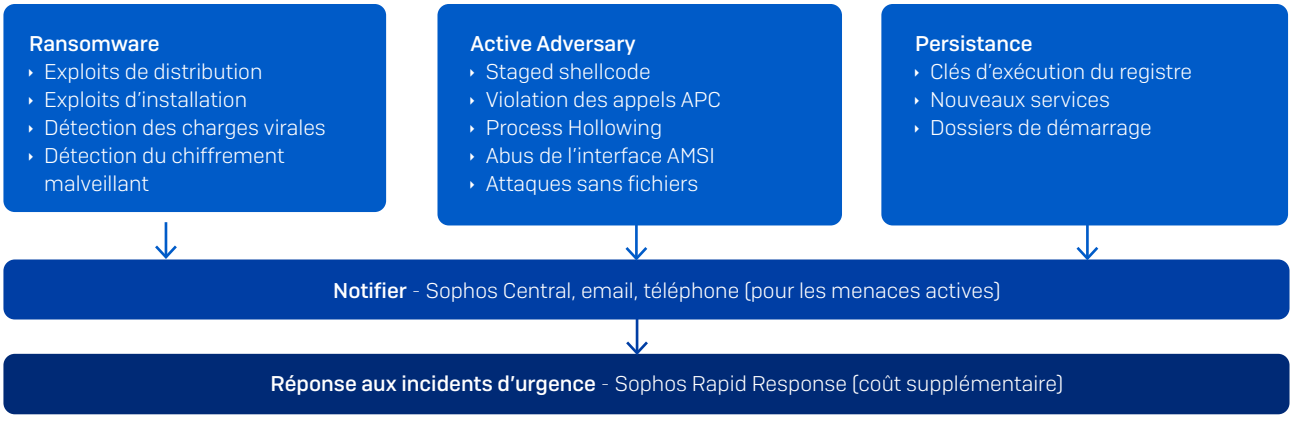
Managed Threat Detection est disponible en mode de réponse « Notifier ». Les clients recevront une alerte si une menace de niveau de gravité élevée échappe à leur solution de protection Endpoint. Cela inclut la détection de nombreux comportements observés avant une attaque de ransomware.

Voici quelques exemples d'événements détectés :

- Staged shellcodes tels que ceux couramment trouvés dans CobaltStrike Beacon ou Metasploit Meterpreter
- Nouvelle tâche planifiée qui exécute $PS, y compris les activités dans les emplacements couramment utilisés pour la persistance par les malwares et les cybercriminels (clés d'exécution du registre, services, éléments de démarrage de Windows, etc.)
- Ransomware et activité comportementale que d'autres produits de protection peuvent manquer

Avantages principaux

- Surveillance et détection des activités suspectes 24h/24 et 7j/7
- Conçu pour fonctionner en parallèle de produits de protection Endpoint tiers
- Mode de réponse aux menaces « Notifier »
- Validation par nos analystes de toutes les détections de niveau de gravité élevée
- Notifications contenant des recommandations de remédiation
- Sophos Rapid Response est disponible pour une réponse aux incidents supplémentaire



SOPHOS

Notification et réponse

Une communication claire est absolument essentielle lors de la gestion d'un programme d'opérations de sécurité. C'est pourquoi le service Managed Threat Detection fournit un flux constant d'informations, dont des rapports hebdomadaires et mensuels, des notifications par email et un tableau de bord dans Sophos Central.

Les clients recevront des notifications par email avec des mises à jour du statut des dossiers. Cela inclut des alertes lorsqu'une action est requise et lorsque les dossiers sont résolus. Tous les dossiers sont validés par un analyste et les notifications comprennent un résumé du cas, une liste des appareils affectés et des recommandations de remédiation.

De plus, des communications sont envoyées pour alerter les clients des dernières actualités du secteur, expliquant les dernières menaces découvertes, les mesures prises par Sophos et ce que les clients peuvent faire pour rester protégés.

Lorsque des menaces actives sont détectées dans l'environnement d'un client, les opérateurs Sophos le contactent par téléphone. Cela garantit que les informations critiques ne sont pas retardées. Les clients peuvent à tout moment mettre à jour leurs coordonnées et leurs préférences pour Managed Threat Detection dans leur tableau de bord Sophos Central. Ce dernier présente également un résumé de toute l'activité de Managed Threat Detection, offrant aux clients les informations les plus récentes, où et quand ils en ont besoin.

Si une assistance est nécessaire pour répondre à une menace, l'équipe Sophos Rapid Response est disponible en tant que service supplémentaire. Sophos Rapid Response fournit une assistance d'urgence rapide pour investiguer et neutraliser les menaces actives. Qu'il s'agisse d'une infection, d'une compromission ou d'un accès non autorisé tentant de contourner (ou ayant réussi à violer) vos contrôles de sécurité, notre équipe a déjà tout vu et tout stoppé avec succès. Les clients Sophos bénéficient d'un avantage en matière de rapidité puisque l'équipe Rapid Response aura un accès immédiat aux données télémétriques et à l'enregistrement des données fournies par les agents Managed Threat Detection.

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
Compatible avec protection Endpoint tierce	✗	✗	✓
Surveillance 24/7	✓	✓	✓
Détections contradictoires	✓	✓	✓
Rapports, tableau de bord	✓	✓	✓
Notification de la menace	✓	✓	✓
Connecteur MTR pour Sophos Firewall	✗	✓	✓
Connecteur MTR pour Sophos Cloud Optix	✗	✓	✗
Prise en charge de multiples OS	✓	✓	✗ (Win10/2012r2+ uniquement)
Traque des menaces sans indices, à l'initiative des analystes	✗	✓	✗
Diagnostic des systèmes endpoint Sophos	✓	✓	✗
Protection en temps réel	✓	✓	✗
Confinement et neutralisation	✓	✓	✗
Communication par téléphone	✗ (menaces actives uniquement)	✓	✗ (menaces actives uniquement)

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

21-07-13 DS-FR (MP)

SOPHOS