PRÉSENTATION DE LA SOLUTION

Sophos ITDR

Identity Threat Detection and Response

Sophos Identity Threat Detection and Response (ITDR) identifie et répond aux menaces qui contournent les contrôles traditionnels de protection des identités. Entièrement intégré à Sophos XDR et Sophos MDR, Sophos ITDR vous aide à améliorer la posture de sécurité de votre organisation, surveille en permanence votre environnement à la recherche de mauvaises configurations et de risques liés aux identités, et fournit des renseignements provenant du Dark Web sur les identifiants compromis.

Cas d'usages

1 | PROTÉGER CONTRE LES MENACES D'IDENTITÉ

Résultat souhaité : Neutraliser les attaques basées sur l'identité avant qu'elles n'aient un impact sur vos activités.

Solution : Au cours de l'année écoulée, 90 % des organisations ont été confrontées à une usurpation d'identité[1]. Sophos ITDR vous permet d'identifier de manière proactive les menaces sophistiquées et de vous protéger contre 100 % des techniques 'Credential Access' de MITRE ATT&CK[2] dès le début de la chaîne d'attaque, tout en répondant avec rapidité et précision. Nos analystes Sophos MDR expérimentés peuvent analyser les activités à haut risque et prendre immédiatement des mesures en votre nom, notamment désactiver un utilisateur, forcer la réinitialisation d'un mot de passe, verrouiller un compte, révoquer des sessions, etc.

2 | RÉDUIRE VOTRE SURFACE D'ATTAQUE

Résultat souhaité : Identifier et corriger les erreurs de configuration et les failles de sécurité liées aux identités.

Solution : 95 % des environnements Microsoft Entra ID présentent une erreur de configuration critique.[3] Si celle-ci n'est pas corrigée, les cybercriminels peuvent l'exploiter pour élever leurs privilèges et mener des attaques basées sur l'identité. Sophos ITDR analyse en continu votre environnement Entra ID afin d'identifier rapidement les erreurs de configuration et les failles de sécurité, et de vous fournir des recommandations pour y remédier.

3 | REPÉRER LES IDENTIFIANTS DIVULGUÉS OU VOLÉS

Résultat souhaité : Réduire le risque que des identifiants exposés soient utilisés pour mener une attaque.

Solution : L'identité reste l'un des principaux vecteurs d'accès pour les ransomwares. Sophos a observé que le nombre d'identifiants volés proposés à la vente sur l'une des plus grandes marketplaces du Dark Web a plus que doublé au cours de la seule année dernière.[4] Sophos ITDR surveille le Dark Web et les bases de données issues de vols, et vous alerte lorsque des identifiants ont été exposés afin de réduire le risque qu'ils soient utilisés dans une future attaque.

4 | IDENTIFIER LES COMPORTEMENTS À RISQUE DES UTILISATEURS

Résultat souhaité : Comprendre et gérer les comportements à haut risque des utilisateurs afin de protéger votre activité.

Solution : En surveillant les schémas de connexion inhabituels et les activités anormales des utilisateurs, vous pouvez réduire considérablement vos risques de cybersécurité et protéger vos actifs. Sophos ITDR identifie les comportements à risque que des acteurs malveillants pourraient exploiter, ou qui pourraient indiquer que les identifiants d'un utilisateur ont été compromis. La solution fournit des informations détaillées sur les utilisateurs de votre organisation qui ont été impliqués dans des alertes de sécurité Sophos récentes.

Gartner Peer Insights Customers' Choice 2025

Un « Customer's Choice » 2025 de Gartner® Peer Insights™ dans la catégorie Extended Detection and Response.

Un Leader dans les rapports Overall Grid® pour MDR et XDR de G2, selon les évaluations et les avis des clients.

MITRE | ATT&CK® Evaluations

Un Strong Performer dans les évaluations MITRE ATT&CK® dans les catégories Enterprise Products et Managed Services.

Pour en savoir plus : Sophos.fr/ITDR.

[1] Étude 2024 Identity Defined Security Alliance (IDSA). | [2] Basé sur les capacités de détection de Sophos mappées au cadre MITRE ATT&CK.
[3] Données recueillies à partir de milliers d'interventions menées par Sophos en réponse à des incidents. | [4] Données Sophos X-Ops Counter Threat Unit (CTU), juin 2024 – juin 2025.

2025-09-16 SB-FR (MP)