INFORME DE LA SOLUCIÓN

Sophos ITDR

Identity Threat Detection and Response

Sophos Identity Threat Detection and Response (ITDR) identifica y responde a las amenazas que eluden los controles tradicionales de seguridad de la identidad. Sophos ITDR, totalmente integrado con Sophos Extended Detection and Response (XDR) y Sophos Managed Detection and Response (MDR), le ayuda a mejorar la postura de seguridad de su organización, supervisa continuamente su entorno en busca de errores de configuración y riesgos de identidad, y proporciona información procedente de la Web Oscura sobre credenciales vulneradas.

Casos de uso

1 | PROTÉJASE DE LAS AMENAZAS DE IDENTIDAD

Resultado deseado: neutralizar las amenazas basadas en la identidad antes de que puedan afectar a su negocio.

Solución: el 90 % de las organizaciones sufrieron una filtración relacionada con la identidad en el último año.[1] Sophos ITDR le permite identificar de forma proactiva amenazas sofisticadas y protegerse contra el 100 % de las técnicas de acceso a credenciales de MITRE ATT&CK[2] en las primeras fases de la cadena de ataque y responder con rapidez y precisión. Los expertos analistas de Sophos MDR pueden investigar actividades de alto riesgo y tomar medidas inmediatas en su nombre, como desactivar un usuario, forzar el restablecimiento de una contraseña, bloquear una cuenta, revocar sesiones y mucho más.

2 | REDUZCA LA SUPERFICIE DE ATAQUE RELACIONADA CON LA IDENTIDAD

Resultado deseado: identificar y remediar errores de configuración y lagunas de seguridad basadas en la identidad.

Solución: el 95 % de los entornos de Microsoft Entra ID tienen errores de configuración críticos.[3] Si no se abordan, los ciberdelincuentes pueden aprovechar esas vulnerabilidades para aumentar sus privilegios y llevar a cabo ataques basados en la identidad. Sophos ITDR escanea continuamente su entorno de Entra ID para identificar rápidamente errores de configuración y lagunas de seguridad y ofrecer recomendaciones para solucionarlas.

3 | IDENTIFIQUE CREDENCIALES FILTRADAS O ROBADAS

Resultado deseado: minimizar el riesgo de que las credenciales expuestas se utilicen para ejecutar un ataque.

Solución: la identidad sigue siendo uno de los principales vectores de acceso del ransomware, y Sophos ha observado que el número de credenciales robadas puestas a la venta en uno de los mayores mercados de la Web Oscura se ha duplicado con creces en tan solo un año.[4] Sophos ITDR monitoriza la Web Oscura y las bases de datos de filtraciones, y le avisa cuando se exponen credenciales para reducir el riesgo de que se utilicen en un futuro ataque.

4 | IDENTIFIQUE LOS COMPORTAMIENTOS DE RIESGO DE LOS USUARIOS

Resultado deseado: comprender y abordar los comportamientos de alto riesgo de los usuarios para proteger su negocio.

Solución: al supervisar los patrones de inicio de sesión inusuales y la actividad anómala de los usuarios, puede reducir significativamente los riesgos de ciberseguridad y proteger sus recursos. Sophos ITDR identifica comportamientos de riesgo que podrían ser explotados por delincuentes o que podrían indicar que las credenciales de un usuario se han visto vulneradas. Además, proporciona información sobre los usuarios de su organización que han estado involucrados en alertas de seguridad recientes de Sophos.

Distinción Gartner® Peer Insights™ "Customers' Choice" 2025 para la detección y respuesta ampliadas.

Líder en los informes generales G2 Grid® para MDR y XDR según las puntuaciones y reseñas de los clientes.

Sólidos resultados en las evaluaciones MITRE ATT&CK® para productos empresariales y servicios gestionados.

Más información:
es.sophos.com/ITDR

[1] Estudio de la Identity Defined Security Alliance (IDSA), 2024. | [2] Según las capacidades de detección de Sophos asignadas al marco MITRE ATT&CK.
[3] Datos recopilados a partir de miles de intervenciones de respuesta a incidentes realizadas por Sophos. | [4] Datos de la Counter Threat Unit (CTU) de Sophos X-Ops, junio 2024 – junio 2025.

Gartner, Gartner Peer Insights 'Voice of the Customer': Extended Detection and Response, Peer Contributors, 23 de mayo de 2025. El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio descrito en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares. GARTNER es una marca de servicio y marca registrada de Gartner, Inc. y/o asociados en EE. UU. y en otros países, y PEER INSIGHTS es una marca registrada de Gartner, Inc. y/o asociados y se utiliza aquí con su permiso. Reservados todos los derechos.

2025-09-16 SB-ES (MP)