OPIS ROZWIĄZANIA

Sophos XDR

Ochrona przed wyrafinowanymi, wieloetapowymi atakami wielowektorowymi

Aktywni adwersarze to wysoko wykwalifikowani cyberprzestępcy, którzy przeprowadzają ataki na dużą skalę i stosują wyrafinowane taktyki mające na celu uniknięcie uruchomienia prewencyjnych rozwiązań zabezpieczających. Sophos Extended Detection and Response (XDR) zapewnia potężne narzędzia i informacje o zagrożeniach, które umożliwiają wykrywanie, badanie i neutralizowanie zagrożeń w całym ekosystemie IT za pomocą adaptacyjnej, natywnej dla sztucznej inteligencji, otwartej platformy Sophos.

Przykłady zastosowań

1 | ZACZNIJ OD NAJLEPSZEJ OCHRONY

Pożądany rezultat: powstrzymaj więcej zagrożeń na wczesnym etapie, aby zmniejszyć obciążenie zespołu.

Rozwiązanie: Skoncentruj działania dochodzeniowe, powstrzymując większą liczbę naruszeń, zanim do nich dojdzie. Sophos XDR zapewnia ponadprzeciętny poziom ochrony, umożliwiający szybkie blokowanie zaawansowanych zagrożeń, zanim nastąpi ich eskalacja. Wzmocnij swoje zabezpieczenia dzięki ochronie punktów końcowych klasy enterprise — obejmującej modele AI oparte na głębokim uczeniu, chroniące przed znanymi i nieznanymi technikami ataku, analizę behawioralną, mechanizmy ochrony przed ransomware oraz zabezpieczeniaprzed exploitami.

2 | CAŁKOWITA WIDOCZNOŚĆ POWIERZCHNI ATAKU

Pożądany rezultat: Uzyskaj wgląd w trudne do wykrycia zagrożenia w całym środowisku.

Rozwiązanie: Nasza otwarta, rozszerzalna architektura zapewnia widoczność całego obszaru ataku poprzez integrację informacji o zagrożeniach pochodzących z istniejących i przyszłych inwestycji w zabezpieczenia. Sophos XDR obejmuje gotowe integracje z rozbudowanym ekosystemem rozwiązań w zakresie punktów końcowych, zapór sieciowych, sieci, poczty elektronicznej, tożsamości, kopii zapasowych, bezpieczeństwa w chmurze i produktywności.

3 | PRZYSPIESZ DZIAŁANIA BEZPIECZEŃSTWA DZIĘKI SZTUCZNEJ INTELIGENCJI

Pożądany rezultat: Umożliwienie analitykom bezpieczeństwa szybszego neutralizowania zagrożeń.

Rozwiązanie: Narzędzia AI dostępne w Sophos XDR pomagają usprawnić procesy dochodzeniowe, dostarczając informacje w czasie rzeczywistym, kontekstualizując dane dotyczące zagrożeń i oferując zalecenia oparte na języku naturalnym. Zaprojektowany we współpracy z naszymi analitykami bezpieczeństwa pierwszej linii, asystent Sophos AI Assistant umożliwia Twojemu zespołowi wewnętrznemu korzystanie z rzeczywistych procesów roboczych i doświadczenia ekspertów Sophos. Wykorzystuj narzędzia AI do realizacji szerokiego zakresu zadań SecOps przy użyciu języka naturalnego lub predefiniowanych promptów: analizuj podejrzane polecenia, identyfikuj zasoby objęte incydentem, wzbogacaj dane o wywiad zagrożeń, twórz szczegółowe raporty i nie tylko.

4 | OTWARTA PLATFORMA ZAPROJEKTOWANA W CELU OPTYMALIZACJI I UJEDNOLICENIA

Pożądany rezultat: Skuteczna reakcja na zagrożenia pochodzące z wielu wektorów ataku.

Rozwiązanie: Uzyskaj jednolity widok całego ekosystemu IT w ramach zunifikowanej platformy wykrywania i reagowania, koncentrując działania analityczne na zdarzeniach o najwyższym priorytecie zamiast na szumie alertowym i nieistotnych powiadomieniach. Identyfikuj najbardziej krytyczne zagrożenia dzięki priorytetyzacji i analizie wspieranej przez AI oraz współpracuj w zespole, wykorzystując rozbudowane przepływy dochodzeniowe i narzędzia do zarządzania sprawami.

Gartner

Lider w raporcie Gartner® Magic Quadrant™ for Endpoint Protection Platforms 2025 – po raz 16. z rzędu

MITRE | ATT&CK® Evaluations

Sophos XDR konsekwentnie osiąga bardzo dobre wyniki w testach MITRE ATT&CK Evaluations dla rozwiązań klasy enterprise

G2

Lider w raporcie G2 Spring 2025 Overall Grid® dla rozwiązań klasy Extended Detection and Response

Dowiedz się więcej i rozpocznij bezpłatny okres próbny:
sophos.com/xdr

2025-09-12 SB-EN (NP)