

Sophos MDR

Całodobowa ochrona przed zagrożeniami zapewniana przez ekspertów

Sophos Managed Detection and Response (MDR) to w pełni zarządzana usługa świadczona przez ekspertów, którzy wykrywają cyberataki wymierzone w komputery, serwery, sieci, obciążenia w chmurze, konta e-mail, kopie zapasowe i inne elementy infrastruktury oraz reagują na nie. Nasi wysoko wykwalifikowani analitycy bezpieczeństwa powstrzymują zaawansowane ataki przeprowadzane przez ludzi i podejmują natychmiastowe działania w celu neutralizacji zagrożeń, zanim zakłócą one działalność firmy lub narazą poufne dane na niebezpieczeństwo.

Przykłady zastosowań

1 | MONITOROWANIE ZAGROŻEŃ 24/7

Pożądany rezultat: Rozszerzenie zespołu IT i bezpieczeństwa o ekspertów, którzy mogą reagować na zagrożenia w imieniu firmy.

Rozwiązanie: Analitycy bezpieczeństwa Sophos MDR monitorują, badają i reagują na zagrożenia 24 godziny na dobę, 7 dni w tygodniu – podejmując natychmiastowe, ręcznie sterowane działania w celu powstrzymania potwierdzonych zagrożeń. Sophos zatrudnia ponad 500 ekspertów ds. wykrywania zagrożeń i reagowania na nie, wspieranych przez osiem globalnych centrów operacyjnych ds. bezpieczeństwa.

2 | PRZYSPIESZ REAKCJĘ NA ZAGROŻENIA

Pożądany rezultat: skrócenie średniego czasu reakcji (MTTR) na potwierdzone zagrożenia.

Rozwiązanie: Sophos MDR pobiera dane telemetryczne dotyczące zagrożeń z całego środowiska IT i wykorzystuje sztuczną inteligencję oraz wiedzę specjalistyczną, aby wykrywać ataki w najwcześniejszym możliwym momencie. Nasi eksperci mogą w Twoim imieniu podejmować działania w odpowiedzi na zagrożenia, aby zakłócić, powstrzymać i wyeliminować atakujących, osiągając średni czas reakcji na zagrożenia wynoszący 38 minut – o 96% szybszy niż średnia branżowa.

3 | ZATRZYMAJ TO, CZEGO NIE WYKRYWAJĄ NARZĘDZIA BEZPIECZEŃSTWA

Pożądany rezultat: wykrywanie i blokowanie ataków, których nie są w stanie powstrzymać same narzędzia bezpieczeństwa.

Rozwiązanie: 55% ataków ransomware rozpoczyna się od wykorzystania przez atakującego legalnych danych uwierzytelniających użytkownika lub nieznannej luki w zabezpieczeniach. Sophos MDR przeprowadza proaktywne poszukiwania zagrożeń w celu identyfikacji zachowań atakujących i szybkiego eliminowania zagrożeń, których nie są w stanie powstrzymać same narzędzia.

4 | POPRAWA ZWROTU Z INWESTYCJI

Pożądany rezultat: Konsolidacja rozwiązań bezpieczeństwa w całym środowisku i uzyskanie większego zwrotu z inwestycji w technologie.

Rozwiązanie: Sophos MDR może zapewnić potrzebną technologię lub wykorzystać istniejące inwestycje w cyberbezpieczeństwo do wykrywania zagrożeń i reagowania na nie. Otwarta, natywna dla sztucznej inteligencji platforma Sophos gromadzi, filtruje i koreluje dane z szerokiej gamy narzędzi cyberbezpieczeństwa i IT, umożliwiając analitykom Sophos MDR szybkie, dokładne i przejrzyste eliminowanie potwierdzonych zagrożeń.

Uznanie branżowe



Firma Sophos została uznana za wybór klientów w raporcie Gartner® Voice of the Customer 2024 w kategorii zarządzanych usług wykrywania i reagowania



Najwyżej oceniana usługa zarządzanego wykrywania i reagowania według ocen i recenzji i klientów na platformie G2

Uznanie w branży



Najlepszy dostawca w ocenach MITRE ATT&CK dla usług zarządzanych

Dowiedz się więcej i poproś o indywidualną ofertę usług Sophos MDR:

www.sophos.com/MDR