Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X to jedyne w branży rozwiązanie XDR, które synchronizuje ochronę dla punktów końcowych, serwera, firewalla, poczty, chmury i usług Office365. Uzyskaj całościowy obraz środowiska swojej organizacji dzięki kompletnemu zestawowi danych i głębokiej analizie zagrożeń. Skorzystaj z narzędzia umożliwiającego wykrywanie, analizowanie i reagowanie na zagrożenia, które dedykowane jest zespołom SOC oraz administratorom IT.

Uzyskaj odpowiedzi na kluczowe pytania

Zarówno administratorzy IT, jak i specjaliści ds. cyberbezpieczeństwa szybko przekonają się o tym jakie możliwości daje wykorzystanie technologii XDR, wykonując codzienne operacje włącznie z polowaniem na zagrożenia.

Skorzystaj z najlepszej ochrony

Intercept X powstrzymuje zagrożenia, kiedy tylko pojawią się w Twojej sieci. Dzięki temu zespół IT poświęca mniej czasu incydentom bezpieczeństwa, które zostają automatycznie zatrzymane. Ponadto technologia XDR umożliwia dostęp do szczegółowej analizy zagrożeń oraz zapewnia informacje niezbędne do podejmowania szybkich, świadomych działań.

Skoncentruj swoją uwagę na kluczowych zagrożeniach

Skup się na ważnych kwestiach, korzystając z priorytetowej listy podejrzanych incydentów i konfiguracji, która zawiera kluczowe informacje o zagrożeniach. Na zaistniałe incydenty bezpieczeństwa możesz zareagować dzięki wykorzystaniu gotowych szablonów działania.

Zminimalizuj czas poświęcony na śledzenie zagrożeń i reakcję

Analiza prowadzona przez sztuczną inteligencję pozwala na szybkie zrozumienie zakresu i przyczyny zagrożenia i zminimalizowanie czasu reakcji. Kontroluj stan swojego urządzenia w czasie rzeczywistym oraz uzyskaj wgląd do historii danych sprzed 90 dni i do danych znajdujących się w Data Lake (do 30 dni wstecz).

Kontroluj bezpieczeństwo całej organizacji

Zapoznaj się ze stanem bezpieczeństwa całej swojej organizacji dzięki natywnej integracji danych z Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix i Microsoft Office 365.

Obsługa wielu platform i systemów operacyjnych

Kontroluj swoje środowisko, niezależnie od tego, czy znajduje się ono w lokalnie czy w chmurze, na platformie Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform czy Oracle Cloud Infrastructure.

W skrócie

-Uzyskaj odpowiedzi na pytania dotyczące bezpieczeństwa swojej organizacji

-Skup się na kluczowych zagrożeniach wykrytych dzięki wykorzystaniu AI

-Podejmuj zdalne działania naprawcze na konkretnych urządzeniach

-Uzyskaj całościowy obraz środowiska bezpieczeństwa w swojej organizacji, a w razie potrzeby uzyskaj bardziej szczegółowe dane

-Integracja pomiędzy poszczególnymi elementami systemu bezpieczeństwa

-Otrzymaj dostęp do biblioteki gotowych szablonów zawierających scenariusze odpowiedzi na zaistniałe incydenty bezpieczeństwa

Przykłady użycia

Działania IT

- Dlaczego stacja robocza działa powoli?
- Które urządzenia posiadają luki w zabezpieczeniach, nieznane usługi, bądź nieautoryzowane dodatki do przeglądarki?
- Czy na urządzeniach są programy, które należy usunąć?
- Zidentyfikuj w swojej sieci urządzenia niezarządzane oraz gości
- Dlaczego połączenie sieciowe w biurze działa wolno? Która aplikacja za to odpowiada?
- Przejrzyj historię aktywności do 30 dni wstecz na zaginionym lub zniszczonym urządzeniu.
- Zidentyfikuj urządzenia mobilne, które posiadają niezaktualizowane oprogramowanie.

Polowanie na zagrożenia

- Jakie procesy próbują nawiązać połączenie sieciowe na niestandardowych portach?
- Pokaż procesy odpowiedzialne za modyfikację plików lub kluczy rejestru
- Lista wykrytych IoCs zmapowanych do MITRE ATT&CK
- Prześledź historię urządzenia do 30 dni wstecz korzystając z danych zapisanych w Data Lake
- Użyj wykrywania ATP i IPS aby zbadać podejrzane hosty
- Porównaj informacje z nagłówka wiadomości email, SHAs i IoCs aby zidentyfikować ruch do złośliwej domeny
- Zidentyfikuj użytkowników z wieloma nieudanymi próbami uwierzytelnienia

Co zawiera Sophos XDR?

	Extended Detection and Response (XDR)
Dane pochodzące z wielu produktów zabezpieczających	✓
Możliwość wykrywania, śledzenia i reagowania na incydenty	✓
Lista najważniejszych zagrożeń i analiz prowadzonych przez sztuczną inteligencję	✓
Sophos Data Lake	✓
Czas przechowywania danych w Data Lake	30 dni
Informacje o stanie bezpieczeństwa w czasie rzeczywistym	✓
Okres przechowywania danych na dysku	do 90 dni
Gotowe szablony przeciwdziałania zagrożeniom	✓
Możliwości ochrony jakie daje Intercept X	✓