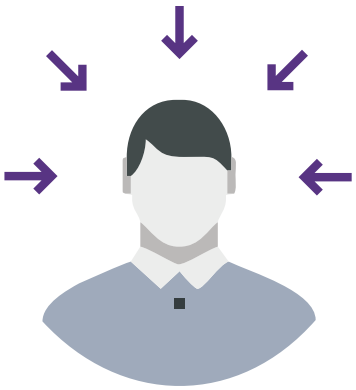
SentinelOne ActiveEDR

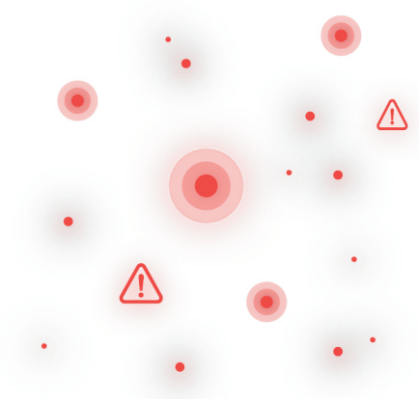
Wyzwania

Obecna wiedza i doświadczenie pokazują, że systemy antywirusowe i ochrona Endpoint Protection Platform (EPP) nie zapewniają skutecznego bezpieczeństwa w przedsiębiorstwach. W celu kompleksowej ochrony coraz więcej firm korzysta z dodatkowych usług, które mają za zadanie zapewnić wymagany poziom bezpieczeństwa. Niestety poleganie na rozwiązaniach chmurowych zwiększa tzw. dwell time, czyli czas przez jaki zagrożenie nie jest wykrywane w środowisku. Poleganie na łączności z usługami chmurowymi jest niewystarczające, gdyż złośliwe oprogramowanie potrzebuje tylko kilku sekund, aby zainfekować urządzenie, wyrządzić szkodę oraz usunąć po sobie ślady. Te zależności sprawiają, że dzisiejsze rozwiązania bezpieczeństwa są pasywne, ponieważ polegają na operatorach i usługach, które reagują zbyt późno.

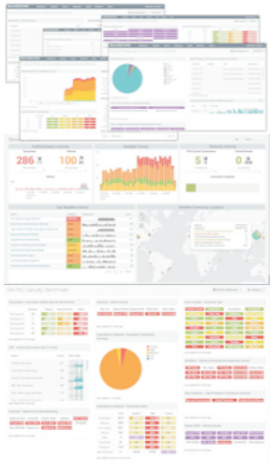
Zbyt mały personel



Zbyt dużo zagrożeń



Zbyt dużo produktów

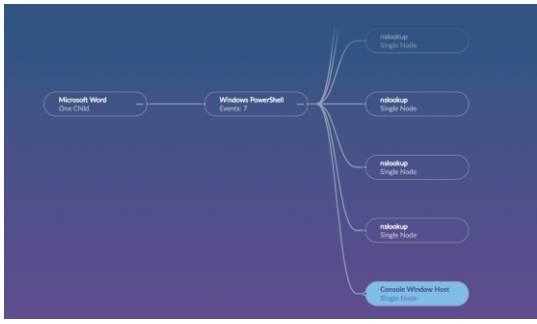


Platforma ochrony urządzeń końcowych SentinelOne łączy zapobieganie, detekcję i reagowanie w jednym (EDR), zbudowanym w tym celu agencie, wspomaganym przez uczenie maszynowe i automatyzację. Platforma zapewnia zapobieganie atakom i ich wykrywanie we wszystkich głównych wektorach oraz szybką eliminację zagrożeń dzięki w pełni zautomatyzowanym funkcjom reagowania. Zapewnia także kompleksową widoczność w środowisku urządzeń końcowych z analizami tworzonymi w czasie rzeczywistym.

T. +48 22 439 03 20
biuro@greeneris.com
www.greeneris.com

Rozwiązanie - Active EDR

Funkcjonalność ActiveEDR zastępuje tradycyjną ochronę antywirusową i jest realizowana przez zunifikowanego agenta SentinelOne, pojedynczą bazę kodu źródłowego oraz architekturę pojedynczej konsoli. Wychodząc poza tradycyjne rozwiązania antywirusowe oraz bazowe systemy EDR, ActiveEDR wykorzystuje autorską technologię TrueContext, która pozwala zespołom ds. bezpieczeństwa szybko zrozumieć źródło ataku i reagować samodzielnie bez polegania na zasobach zewnętrznych oraz usługach chmurowych. Dzięki ActiveEDR każdy, od nowicjusza po doświadczonych analityków, może automatycznie reagować na zagrożenia i bronić się przed zaawansowanymi atakami. Technologia ta umożliwia zespołom ds. bezpieczeństwa skupić się na ważnych alertach i wykorzystać ją do wspomagania swojej pracy.



Zróżnicowany pod każdym względem

Oferuje bogate w dane analizy i możliwość zautomatyzowanego reagowania na zagrożenia, łącznie z usuwaniem skutków ataku, a nawet możliwością całkowitego przywrócenia urządzenia po zaszyfrowaniu atakiem Ransomware.

Śledzenie ataków

Schemat w postaci drzewa przedstawiający przebieg ataku, pomaga zespołom analityków szybko ocenić wpływ każdego zagrożenia.

Reakcja i zapobieganie

Deep Visibility zapewnia możliwość podglądu każdej operacji wykonywanej przez agenta, łącznie z możliwością przeglądania danych historycznych.

Ochrona przed zagrożeniami ransomware, łącznie z odzyskaniem zaszyfrowanych danych.

Identyfikacja zagrożeń w czasie rzeczywistym

Widoczność zaszyfrowanego ruchu sieciowego bez konieczności korzystania z certyfikatów lub potrzeby wykorzystywania drogich urządzeń SSL.

Wykrywanie zagrożeń z technologią TrueContext

Monitorowanie dowolnego pliku i otrzymywanie powiadomień w przypadku dostępu i zmian.

Chcesz zobaczyć jak działa SentinelOne? Przygotujemy dla Ciebie zamknięte środowisko testowe, abyś mógł przekonać się o potencjale naszego systemu. Skontaktuj się z nami.

O Greeneris

Greeneris to spółka działająca na rynku polskim, specjalizująca się we wdrożeniach, świadczeniu usług z zakresu bezpieczeństwa IT, zarządzania mobilnością (Android, iOS) oraz innych kluczowych obszarów IT. Zatrudniamy certyfikowanych inżynierów oraz konsultantów, którzy swoją wiedzą i doświadczeniem pomagają w doborze właściwych rozwiązań. Działania firmy są udokumentowane licznymi wdrożeniami w wielu instytucjach i przedsiębiorstwach polskich, jak i korporacjach międzynarodowych działających na terenie kraju. Firma otrzymuje również regularnie wyróżnienia od producentów rozwiązań w obszarach swoich specjalizacji.

SentinelOne™

greeneris
creating innovation

T. +48 22 439 03 20
biuro@greeneris.com
www.greeneris.com