kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Managed Detection and Response

Większość zespołów ds. bezpieczeństwa stosuje podejście oparte na alertach dotyczących incydentów cyberbezpieczeństwa i reaguje tylko wtedy, gdy niepożądana sytuacja faktycznie nastąpi. Tymczasem nowe zagrożenia pozostają niezauważone, dając fałszywe poczucie bezpieczeństwa. Firmy w coraz większym stopniu widzą potrzebę proaktywnego wykrywania zagrożeń, które są niewidoczne, a mimo to nadal aktywnie działają w infrastrukturze organizacji.

Zalety produktu:

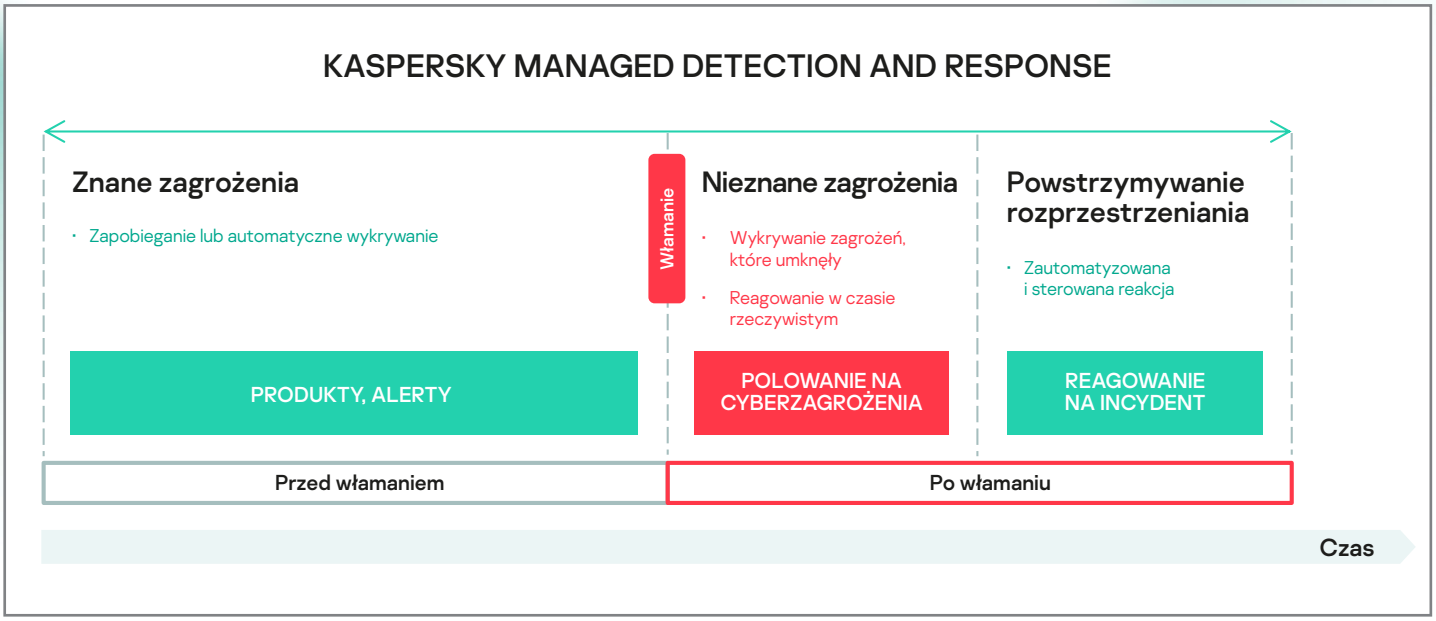
- Zapewnienie nieustannej ochrony przed nawet najbardziej innowacyjnymi zagrożeniami
- Mniejsze koszty ogólne ochrony i brak konieczności angażowania wielu wewnętrznych specjalistów ds. bezpieczeństwa
- Skupianie cennych zasobów wewnętrznych na tych zadaniach krytycznych, które naprawdę wymagają ich udziału
- Wszystkie najważniejsze zalety związane z posiadaniem własnego centrum operacji bezpieczeństwa bez konieczności faktycznego organizowania go

Rozwiązanie Kaspersky Managed Detection and Response (MDR) zapewnia całodobową i zaawansowaną ochronę przed coraz liczniejszymi zagrożeniami, które potrafią pokonywać automatyczne bariery zabezpieczające. W ten sposób nasz produkt pomaga organizacjom, które mają kłopot ze znalezieniem wyspecjalizowanego personelu lub dysponują ograniczonymi zasobami wewnętrznymi.

Niezrównany poziom możliwości wykrywania i reagowania wspierany przez jeden z najskuteczniejszych i najbardziej doświadczonych zespołów wykrywających zagrożenia w branży. W przeciwieństwie do podobnych ofert na rynku rozwiązanie Kaspersky MDR wykorzystuje opatentowane modele uczenia maszynowego, unikatową ciągłą analizę zagrożeń oraz udokumentowane wyniki skutecznych badań w zakresie ataków ukierunkowanych. Automatycznie wzmacnia ono odporność firmy na cyberzagrożenia, równocześnie optymalizując istniejące zasoby i przyszłe inwestycje w bezpieczeństwo IT.

Najważniejsze cechy produktu

- Szybkie i elastyczne wdrożenie natychmiast udostępnia funkcje bezpieczeństwa IT bez konieczności inwestowania w dodatkowy personel czy zwiększenie doświadczenia
- Skuteczna ochrona przed nawet najbardziej skomplikowanymi i innowacyjnymi zagrożeniami innymi niż szkodliwe programy zapobiega przestojom w działaniu firmy i minimalizuje ogólny wpływ incydentu
- W pełni zarządzana reakcja na incydent zapewnia szybką reakcję przy jednoczesnym zachowaniu pod kontrolą wszystkich działań w ramach reagowania
- Widoczność w czasie rzeczywistym wszystkich zasobów i stanu ich ochrony zapewnia nieustanną świadomość sytuacji poprzez różne kanały komunikacyjne



Rysunek 1. Kaspersky Managed Detection and Response

Obsługiwane produkty:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac*
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

Jak to działa

Kaspersky MDR sprawdza alerty produktu, aby zapewnić skuteczną ochronę automatyczną, a także proaktywnie analizuje metadane dotyczące aktywności systemu pod kątem wszelkich oznak aktywnego lub nadchodzącego ataku. Metadane te są gromadzone za pośrednictwem systemu Kaspersky Security Network i są automatycznie zestawiane w czasie rzeczywistym z analizą zagrożeń firmy Kaspersky w celu identyfikowania taktyk, technik i procedur używanych przez atakujących. Odpowiednie oznaki włamania umożliwiają wykrywanie ukrytych zagrożeń innych niż szkodliwe programy, naśladujących legalną aktywność. Produkt ten dostosowuje się do infrastruktury w ciągu pierwszych 2-4 tygodni i w tym czasie wymaga oznaczania przez użytkownika, co jest legalne.

W efekcie liczba fałszywych alarmów jest zminimalizowana. Produkt Kaspersky MDR ma dwie warstwy, aby spełniać potrzeby organizacji dowolnego rozmiaru i z dowolnej branży, o różnych poziomach dojrzałości ochrony IT (Rys. 2). Rozwiązanie **Kaspersky MDR Optimum** natychmiast zwiększa możliwości ochrony IT bez konieczności inwestowania w dodatkowy personel lub zwiększania doświadczenia i zapewnia odporność na ukryte ataki dzięki szybkiemu i kompleksowemu wdrożeniu. **Kaspersky MDR Expert** zawiera te same funkcje co wersja Optimum i zapewnia szerszą funkcjonalność oraz elastyczność doświadczonym zespołom ds. bezpieczeństwa IT, dzięki czemu mogą one zostawić uruchomienie i analizę incydentu na barkach firmy Kaspersky, a ograniczone zasoby wewnętrzne IT skupić na reagowaniu na zdarzenia krytyczne.

Rysunek 2.
Warstwy produktu Kaspersky MDR

Zawarta w rozwiązaniu MDR Optimum funkcja automatycznego polowania na zagrożenia używa opcji automatycznego wykrywania w oparciu o stosowne oznaki ataku, co umożliwia dalszą weryfikację, analizę i identyfikację nowych zagrożeń. Zarządzane polowanie na zagrożenia dostępne w rozwiązaniu MDR Expert polega na proaktywnym identyfikowaniu przez naszych doświadczonych ekspertów tych zagrożeń, które zdołały ominąć technologie wykrywania automatycznego.

Zestaw uzupełniających elementów opcjonalnych dostosowuje funkcjonalność produktu do konkretnych wymogów, zapewniając większą elastyczność wtedy, gdy jest ona potrzebna:

- Opcje elastycznego przechowywania i powstrzymywania ataku w celu spełnienia wymogów prawnych i związanych z kryminalistyką/e-wykrywaniem
- Narzędzie odpowiadające za reakcję na incydenty wykorzystuje całą wiedzę ekspercką firmy Kaspersky, aby rozwiązywać problemy związane z bezpieczeństwem
- Narzędzie kompleksowej oceny ryzyka włamania sprawdza, czy używane narzędzia kontroli zapewniają wystarczający poziom ochrony
- Praktyczne szkolenie dla analityków SOC dba o ogólne przygotowanie na incydent

Ochrona przed atakami ukierunkowanymi wymaga obszernego doświadczenia oraz nieustannej nauki. Niemal dziesięć lat temu firma Kaspersky jako pierwsza utworzyła specjalne centrum analizy skomplikowanych zagrożeń, a nasze produkty wykryły więcej wyrafinowanych ataków ukierunkowanych niż rozwiązania jakiegokolwiek innego dostawcy. Oparte na naszym unikatowym doświadczeniu rozwiązanie Kaspersky Managed Detection and Response maksymalizuje wartość produktów zabezpieczających od firmy Kaspersky, umożliwiając całkowicie zarządzane i indywidualnie dopasowane wykrywanie, priorytetyzację, analizę i reagowanie. W efekcie zapewnia wszystkie najważniejsze korzyści wynikające z posiadania własnego centrum operacji bezpieczeństwa, bez konieczności faktycznego organizowania go.

* Planowo wsparcie rozwiązania Kaspersky Endpoint Security for Mac zostanie wprowadzone w I kwartale 2021 r. Firma Kaspersky nie oświadcza ani nie zobowiązuje się w kwestii przewidywanej daty wydania. Jest ona podana wyłącznie w celach informacyjnych. Firma Kaspersky zastrzega sobie prawo do zmiany planów związanych z produktami w dowolnym czasie.

Informacje o cyberzagrożeniach: securelist.pl
Informacje ze świata bezpieczeństwa IT: kaspersky.pl/blog
Bezpieczeństwo IT dla korporacji: kaspersky.pl/korporacje
Portal Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.pl

Jesteśmy skuteczni. Jesteśmy niezależni. Jesteśmy transparentni. Zobowiązaliśmy się do budowania bezpieczniejszego świata, w którym technologia czyni nasze życie lepszym. Dlatego go chronimy, aby każda osoba wszędzie mogła korzystać z jego nieskończonych możliwości. Aktywuj cyberbezpieczeństwo dla lepszego jutra.

Sprawdzony.
Transparentny.
Niezależny.