Microsoft Security

3 powody przejścia na zintegrowaną ochronę przed zagrożeniami

Spis treści

Wprowadzenie

Przeciętne przedsiębiorstwo korzysta obecnie z ponad 30 różnych narzędzi zabezpieczających, często niepołączonych i „dodatkowych”.

Kwestia bezpieczeństwa znajduje się w punkcie zwrotnym. Cyberataki stają się coraz bardziej wyrafinowane, ponieważ organizacje nadal borykają się z wyzwaniami, takimi jak niedobór talentów i równoważenie kosztów, czy sprostanie presji związanej z pracą hybrydową.

Tymczasem rynek zabezpieczeń jest rozdrobniony i złożony bardziej niż kiedykolwiek wcześniej. Przeciętne przedsiębiorstwo korzysta obecnie z ponad 30 różnych narzędzi zabezpieczających, często niepołączonych i „dodatkowych”, które nie zapewniają centrom operacji bezpieczeństwa (SOC) odpowiedniej widoczności i właściwych informacji.

Specjaliści ds. bezpieczeństwa i zgodności chcą lepiej rozumieć najnowsze zagrożenia, ale muszą również wiedzieć, co działa, a co nie, i w jakich miejscach występują luki.

CISO, którzy chcą poprawić efektywność operacji zabezpieczeń, mogą patrzeć w przyszłość optymistycznie mimo natłoku wyzwań w zakresie bezpieczeństwa. Rozwiązaniem jest zintegrowane, kompleksowe podejście do ochrony przed cyberzagrożeniami, które pomoże organizacjom:

Powód 1: Osiągaj więcej mniejszym kosztem.

Konsoliduj rozwiązania punktowe i zmniejszaj obciążenie związane z operacjami związanymi z bezpieczeństwem (SecOps).

Powód 2: Zwiększ możliwości skoncentrowania się SecOps na ważniejszych zadaniach

Korzystaj z narzędzi, które zwiększają wydajność i sprawiają, że nawet młodsi analitycy mają większe możliwości niż kiedykolwiek.

Powód 3: Zwiększ wydajność pracowników

Chroń swoją organizację w sposób, który pozwoli pracownikom bez obaw tworzyć i wprowadzać innowacje.

Takie podejście jest możliwe dzięki integracji rozwiązania rozszerzonego wykrywania i reagowania (XDR) z natywnym dla chmury systemem zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (SIEM), który wykorzystuje sztuczną inteligencję (AI) i możliwości automatyzacji. Zintegrowane rozwiązanie może pomóc Twoim zespołom SOC osiągnąć większą przewidywalność, proaktywność i lepiej zapobiegać atakom w całym przedsiębiorstwie.

Powód 1

Osiągnij lepsze efekty niższym kosztem

Konsolidując narzędzia za pomocą zintegrowanego rozwiązania Microsoft, można również zaoszczędzić, płacąc tylko za to, czego się używa.

Wiele organizacji stosuje narzędzia zabezpieczeń, koncentrując się na najlepszych w swojej klasie rozwiązaniach punktowych. Niestety takie podejście może utrudnić specjalistom ds. bezpieczeństwa szybkie identyfikowanie zagrożeń i reagowanie na nie. Może to również mieć negatywny wpływ na wydatki na IT i wydajność użytkowników końcowych.

Ponieważ organizacje chcą osiągnąć więcej za mniej, pomocne może być zintegrowane podejście, takie jak SIEM i XDR Microsoft. Może zmniejszyć złożoność dzięki konsolidacji pojedynczych narzędzi — a ponieważ jest to rozwiązanie natywne dla chmury, integracja może również poprawić wydajność i skalowalność.

Konsolidując narzędzia za pomocą zintegrowanego rozwiązania Microsoft, można również zaoszczędzić, płacąc tylko za to, czego się używa. Można również zmniejszyć nadmierne wydatki na SecOps wymagane do zarządzania rozwiązaniami, zwiększając automatyzację i integrację.

> Rozpoczęcie procesu wdrażania nowych narzędzi zabezpieczających jest łatwe, ponieważ można oczekiwać, że luki będą duże. W miarę jego rozwoju szybko zdasz sobie sprawę, że narzędzia różnych dostawców mogą nakładać się na siebie. Takie nakładanie się może być pożądane w przypadku kontroli i równowagi, **ale może również wiązać się z wysokimi kosztami finansowymi**".
>
> **Jonathan Cassar,**
> dyrektor ds. technologii, MITA

1,6 mln USD

oszczędności rocznie dzięki konsolidacji rozwiązań

Microsoft zlecił firmie Forrester Consulting przeprowadzenie badania Total Economic Impact™ (TEI) i zbadanie potencjalnego zwrotu z inwestycji (ROI), jaki mogą osiągnąć przedsiębiorstwa dzięki wdrożeniu rozwiązań SIEM i XDR Microsoft. Oto niektóre z kluczowych ustaleń dotyczących hipotetycznej organizacji zatrudniającej łącznie 8000 pracowników i 10 specjalistów ds. bezpieczeństwa:

- **Oszczędność prawie 1,6 miliona USD rocznie dzięki konsolidacji rozwiązań**. Inwestycja w rozwiązanie SIEM i XDR Microsoft umożliwia obniżenie kosztów wcześniejszego rozwiązania SIEM (560 000 USD), powiązanej infrastruktury lokalnej (ponad 360 000 USD), trzech rozwiązań punktowych XDR (192 000 USD) oraz bieżących kosztów pracy związanych z zarządzaniem nimi (480 000 USD).
- **Zmniejszenie ryzyka naruszeń materialnych o 60 proc.** Dzięki bardziej wydajnym procesom badania i reagowania w zakresie bezpieczeństwa, ulepszonej automatyzacji reagowania na zagrożenia oraz zwiększonej zdolności do ochrony wszystkich środowisk komputerowych, w tym ochrony wielochmurowej, zmniejsza się ryzyko naruszeń, co przekłada się na roczne oszczędności w wysokości 1,6 mln USD.
- **Tworzenie zwrotu z inwestycji na poziomie 207 proc.** Reprezentatywne wywiady i analizy finansowe wykazały, że przedsiębiorstwo objęte badaniem osiąga korzyści w wysokości 17,68 mln USD w ciągu trzech lat w porównaniu z kosztami w wysokości 5,76 mln USD, co daje wartość bieżącą netto (NPV) 11,92 mln USD.

Powód 2

Zwiększ możliwości skoncentrowania się SecOps na ważniejszych zadaniach

Ważna jest integracja SIEM i XDR w celu korelowania alertów, priorytetyzacji najważniejszych zagrożeń i koordynowania działań w całym przedsiębiorstwie.

Zespoły SecOps są przytłoczone liczbą sygnałów, które muszą analizować, w tym wielu sygnałów o niskiej specyficzności, których wykrywanie i zwalczanie jest trudne lub niemożliwe. W miarę narastania zagrożeń przeciążone SOC ma trudności z nadążeniem, zwłaszcza przy próbie analizy danych z rozwiązań wielopunktowych. Nie da się wypełnić tych luk przez proste przydzielenie większej ilości zasobów, ponieważ na rynku jest zbyt mało wykwalifikowanych specjalistów ds. bezpieczeństwa.

Dlatego tak ważne jest zintegrowanie SIEM i XDR w celu korelowania alertów, priorytetyzacji najważniejszych zagrożeń i koordynowania działań w całym przedsiębiorstwie z wykorzystaniem zaawansowanej AI i automatyzacji do poaktywnego wykrywania zagrożeń i stosowania odpowiednich środków zaradczych.

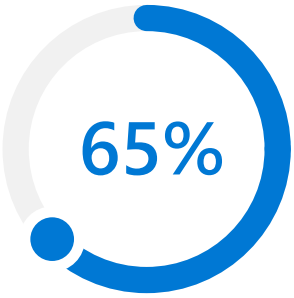
Weźmy na przykład pod uwagę, że pojedynczy sygnał niskiego poziomu może nie zostać zauważony przez tradycyjny SIEM. Jednak dzięki AI natywny dla chmury SIEM może automatycznie porównać ten sygnał z sygnałami z innych źródeł w całej organizacji, korelując go w wielu zestawach danych w celu wykrycia wieloetapowych ataków.

Zintegrowane rozwiązania SIEM i XDR uwalniają zasoby SecOps i jednocześnie zapewniają nawet młodszym analitykom większe możliwości oraz pewność siebie.

Następnie system normalizuje, analizuje i koreluje dane, obrazując jednocześnie sposób, w jaki cyberatak wniknął do infrastruktury wraz z osią czasu jego rozprzestrzeniania się. Dzięki temu zespoły SOC mogą zwizualizować naruszenie, używając jednej konsoli, i skutecznie rozwiązać problem.

> Wielu dyrektorów ds. bezpieczeństwa informacji nie zdaje sobie sprawy **z dodatkowego nakładu pracy w ich zespołach związanego z 20 różnymi interfejsami** lub rozwiązaniami punktowymi i ich rocznymi kosztami... my wyeliminowaliśmy wiele zachodu związanego z narzędziami dzięki jednemu dostawcy".
>
> **Terence Jackson,**
> dyrektor ds. bezpieczeństwa informacji i ochrony prywatności, Thycotic

Organizacja nie powinna potrzebować głębokiej wiedzy specjalistycznej, aby uwolnić wartość rozwiązania zabezpieczającego. Zintegrowane rozwiązania SIEM i XDR uwalniają zasoby SecOps i jednocześnie zapewniają nawet młodszym analitykom większe możliwości oraz pewność siebie.



Zintegrowane podejście SIEM i XDR Microsoft skraca czas badania zagrożeń o 65 proc.

Badanie Total Economic Impact™ (TEI) firmy Forrester zlecone przez Microsoft wykazało skuteczność tego rodzaju operacji zabezpieczeń w przedsiębiorstwie objętym badaniem.

- **Skrócenie czasu badania zagrożeń o 65 proc. i skrócenie czasu reakcji na zagrożenia o 88 proc.** Zintegrowane podejście do badania zagrożeń bezpieczeństwa i reagowania na nie SIEM i XDR Microsoft sprawia, że te przepływy pracy są skuteczniejsze dla specjalistów ds. bezpieczeństwa w przedsiębiorstwie objętym badaniem. Nie muszą już przechodzić od jednego narzędzia do innego w celu identyfikacji zagrożeń, a funkcje automatyzacji zabezpieczeń jeszcze bardziej poprawiają przebieg reakcji.

- **Skrócenie czasu tworzenia nowego zeszytu ćwiczeń o 90 proc. i czasu wdrażania nowych specjalistów ds. zabezpieczeń o 91 proc.** Zintegrowane podejście SIEM i XDR Microsoft sprawia, że dodatkowe przepływy pracy związane z bezpieczeństwem są również wydajniejsze. Ponieważ dzienniki SIEM są zintegrowane z całym pakietem rozwiązań, tworzenie zeszytów ćwiczeń jest prawie zautomatyzowane, a pojedyncze logowanie umożliwia nowym specjalistom ds. bezpieczeństwa wdrożenie się w czasie o prawie 16 tygodni krótszym.

Powód 3

Zwiększ wydajność pracowników

Zintegrowane rozwiązanie SIEM i XDR może pomóc Twojej organizacji zwiększyć wydajność użytkowników końcowych.

Oprócz wykonywania większej liczby zadań przy mniejszym wysiłku i zwiększenia wydajności zespołów SecOps zintegrowane rozwiązanie SIEM i XDR może pomóc Twojej organizacji zwiększyć wydajność użytkowników końcowych.

Zespoły SecOps wiedzą, że jeśli funkcje zabezpieczeń staną się zbyt skomplikowane, ludzie będą próbowali je obchodzić. Zatem gdy doświadczenia użytkowników końcowych wpływają negatywnie, a nie pozytywnie na wydajność pracowników, może to narazić organizację na większe zagrożenia bezpieczeństwa i wyższe koszty. Słabe lub utracone hasła, niezabezpieczony dostęp za pośrednictwem urządzeń osobistych lub nieograniczone udostępnianie danych wrażliwych to niektóre z wyzwań.

> [W przeszłości] przy podejrzeniu problemu używaliśmy narzędzi niewystarczająco ostrych. Wyłączaliśmy wszystkie urządzenia i blokowaliśmy dostęp, co negatywnie wpływało na firmę. Było to jasne dla wszystkich, ponieważ urządzenia nie działały. W Microsoft Sentinel dysponujemy skalpelem, dzięki któremu możemy z chirurgiczną precyzją reagować na zdarzenia. **W firmie zazwyczaj nawet nie wiedzą, że reagujemy na zagrożenie**, a to jest bardzo istotna miara sukcesu".
>
> **Rick Gehringer,**
> dyrektor ds. IT, Wedgewood

Prawie
68 000

Rozwiązania SIEM i XDR Microsoft poprawiły produktywność innych pracowników łącznie o prawie 68 000 godzin rocznie.

Zintegrowane podejście SIEM i XDR pomaga w dostarczaniu bezproblemowego środowiska użytkownika, które sprawia, że pracownicy są wydajni i dbają o bezpieczeństwo we wszystkich aspektach ich codziennej pracy. Może to zmniejszać negatywny wpływ na wydajność, np. na konieczność wyłączenia usług lub izolowania, a następnie zmiany obrazu urządzeń. Zintegrowane rozwiązanie SIEM i XDR tworzy również nowe możliwości dla wydajności użytkownika końcowego, takie jak samoobsługowe wsparcie bezpieczeństwa, lepsze pulpity zarządcze i raportowanie, a także zdolność reagowania i krótszy czas uruchamiania dzięki mniejszej liczbie agentów bezpieczeństwa.

W badaniu Total Economic Impact™ (TEI) firmy Forrester zlecone przez Microsoft w hipotetycznej organizacji zatrudniającej 8000 pracowników wykazano zwiększenie wydajności pracowników dzięki wdrożeniu SIEM i XDR Microsoft:

- **Poprawa produktywności innych pracowników łącznie o prawie 68 000 godzin rocznie.** Rozwiązania SIEM i XDR Microsoft chronią przed niekorzystnym wpływem na innych pracowników będącym skutkiem nieefektywnych procesów bezpieczeństwa. Na przykład przedsiębiorstwo oszczędza 4000 godzin rocznie dzięki nowej zdolności specjalistów IT do samoobsługi w zakresie aktualizacji zabezpieczeń i zaleceń. Umożliwia również zdalne rozwiązywanie problemów związanych z bezpieczeństwem na komputerach pracowników i zmniejsza liczbę działających na nich agentów bezpieczeństwa, oszczędzając prawie 64 000 godzin rocznie wydajności użytkowników końcowych.

Bezpieczeństwo stało się istotnym czynnikiem sukcesu technologicznego. Dlatego organizacje potrzebują środków bezpieczeństwa, które zapewnią jak największą odporność na nowoczesne ataki — aby chronić i umożliwiać produktywność i innowacyjność, które napędzają wzrost.

Uzyskaj zintegrowaną ochronę przed cyberzagrożeniami dzięki SIEM i XDR

Integracja wiodących produktów pozwala zapobiegać cyberzagrożeniom, wykrywać je i reagować na nie za pomocą jednego wszechstronnego rozwiązania.

Microsoft oferuje pierwsze i jedyne zintegrowane rozwiązanie SIEM i XDR, zapewniające kompleksową widoczność we wszystkich chmurach i platformach. Integracja wiodących produktów pozwala zapobiegać cyberzagrożeniom, wykrywać je i reagować na nie za pomocą jednego wszechstronnego rozwiązania.

Rozwiązania SIEM i XDR Microsoft wykorzystują potęgę AI i automatyzacji, a także głębokie, ciągłe inwestycje w wykrywanie i analizę cyberzagrożeń — dzięki codziennemu wglądowi w 43 biliony sygnałów. Dzięki integracji tych produktów zespoły SOC dysponują szerszym niż kiedykolwiek kontekstem, aby szybciej wykrywać i rozwiązywać krytyczne cyberzagrożenia:

Microsoft Sentinel

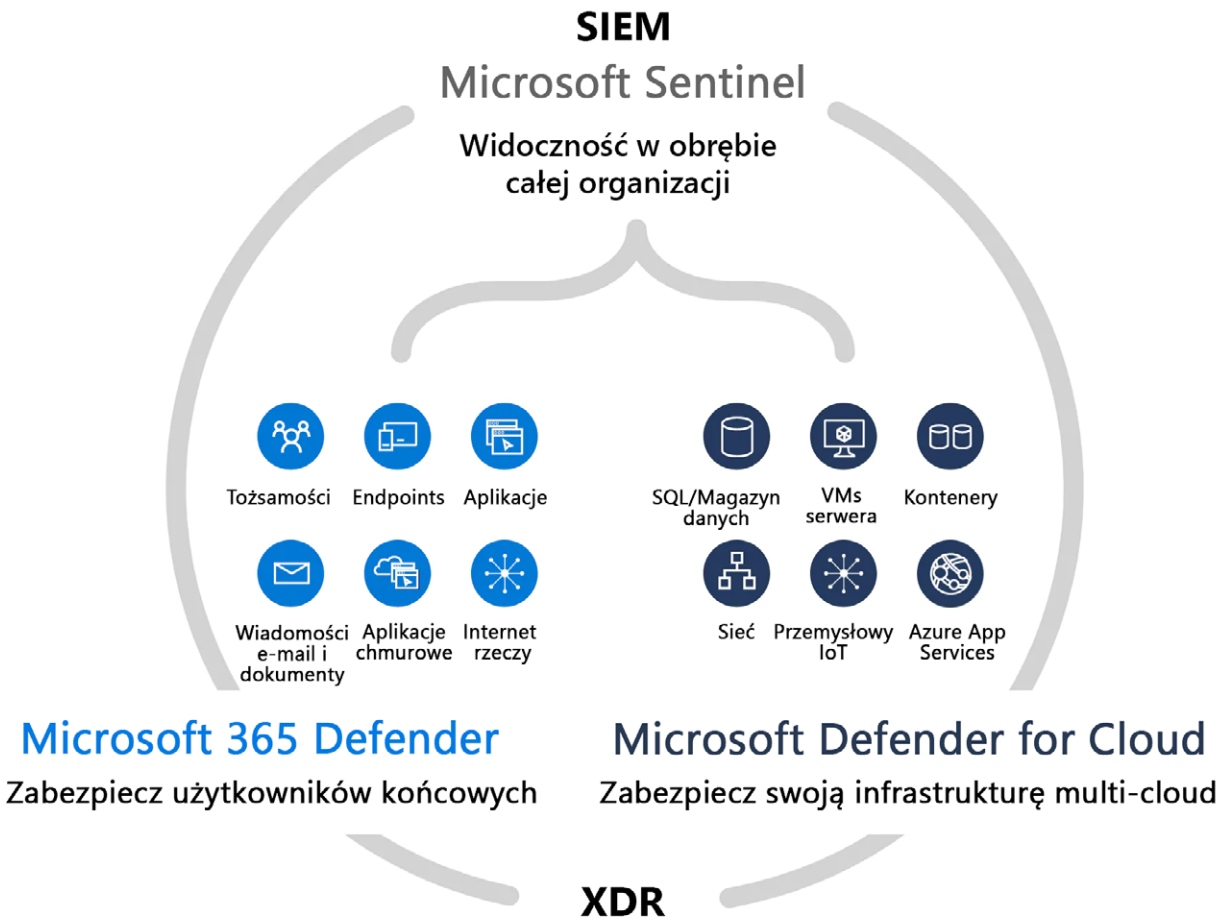
Uzyskaj ogólny wgląd w natywne rozwiązanie chmurowe SIEM Microsoft. Agregowanie danych dotyczących bezpieczeństwa z praktycznie dowolnego źródła i stosowanie AI w celu oddzielenia szumu od uzasadnionych zdarzeń, korelacja alertów w złożonych łańcuchach cyberataków oraz przyspieszenie reagowania na cyber-zagrożenia dzięki wbudowanym mechanizmom i automatyzacji.

Microsoft Defender XDR

Zapobieganie cyberatakom na tożsamości, urządzenia klienckie, aplikacje, pocztę e-mail, dane i aplikacje w chmurze oraz wykrywanie ich dzięki funkcjom XDR. Sprawdzanie cyberataków i reagowanie na nie dzięki gotowej, najlepszej w swojej klasie ochronie. Wykrywanie zagrożeń i łatwe koordynowanie reakcji przy użyciu jednego pulpitu zarządczego.

Microsoft Defender for Cloud

Ochrona rozwiązań wielochmurowych i funkcjonujących w chmurze hybrydowej dzięki wbudowanym funkcjom XDR. Zabezpieczenie serwerów, magazynu, baz danych, kontenerów i nie tylko. Możliwość skupienia się na tym, co najważniejsze, dzięki alertom z priorytetami.



Nie dodawaj zabezpieczeń. Wbuduj je.

Oddaj odpowiednie narzędzia i funkcje inteligentne w ręce odpowiednich osób. Broń się przed współczesnymi atakami za pomocą kompleksowego, natywnego i zintegrowanego rozwiązania.

Dowiedz się więcej o zintegrowanej ochronie przed cyberzagrożeniami Microsoft z SIEM i XDR >

Microsoft Security