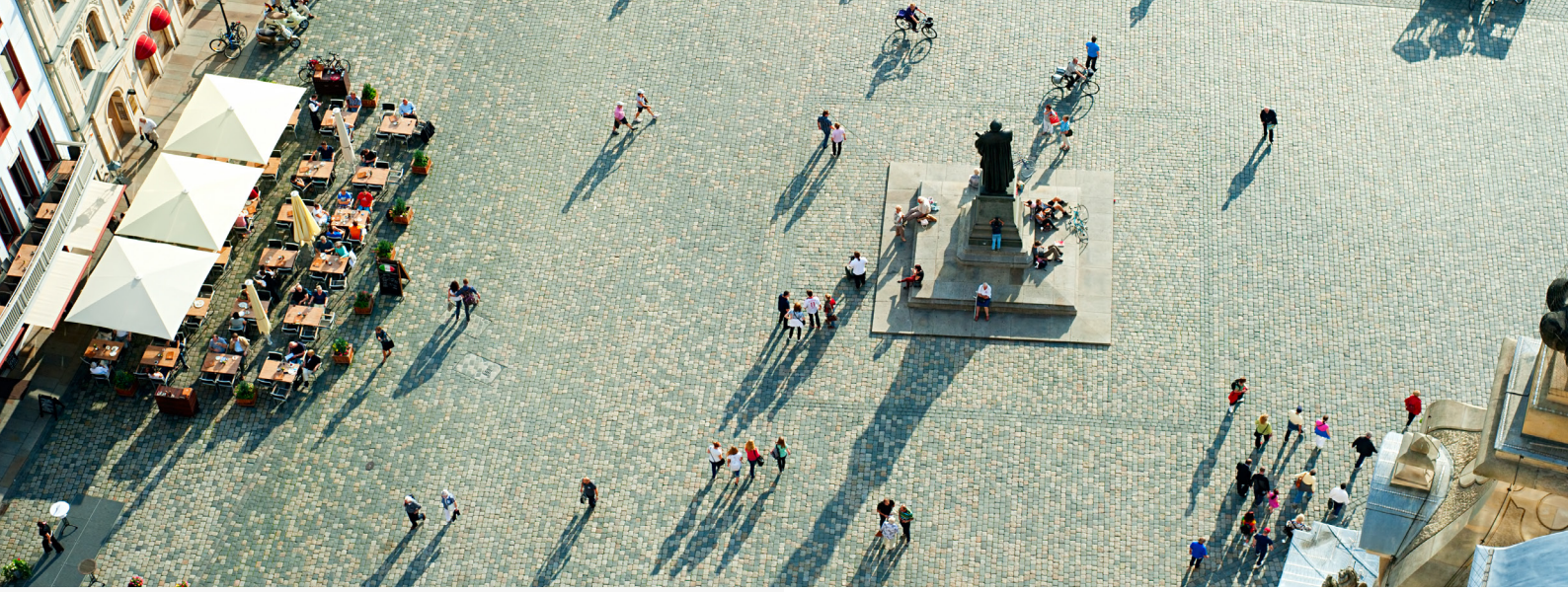
Przewodnik nabywcy

Jak wybrać odpowiednią platformę zabezpieczeń?

Zadaj właściwe pytania. Uzyskaj właściwe odpowiedzi.

IBM Security

IBM



Wybór odpowiedniej platformy zabezpieczeń

Znalezienie odpowiedniej dla przedsiębiorstwa platformy zabezpieczeń może być trudnym zadaniem. Na rynku cyberbezpieczeństwa termin „platforma” jest zresztą nadużywany, dlatego czasami niełatwo wśród nadmiaru informacji ustalić, które czynniki należy wziąć pod uwagę, gdy podejmujemy decyzję dotyczącą rozwiązania dla firmy. Wybór platformy wpłynie na poziom dojrzałości zabezpieczeń przedsiębiorstwa w kolejnych latach, więc taka decyzja powinna być przemyślana.

Zespoły ds. bezpieczeństwa zmagają się z wieloma problemami, takimi jak zbyt duża ilość danych, zbyt wiele narzędzi i zbyt mało dostępnych zasobów. Pora znaleźć inne sposoby połączenia danych dotyczących bezpieczeństwa, narzędzi i zespołów. Istnieje potrzeba zgromadzenia wszystkich elementów w jednym miejscu – a takie możliwości udostępnia właśnie zintegrowana platforma zabezpieczeń.

Jakie elementy powinna uwzględniać platforma zabezpieczeń

Aby znaleźć kompleksową, zintegrowaną platformę cyberzabezpieczeń, która sprawdzi się zarówno obecnie, jak i w przyszłości, należy wziąć pod uwagę następujące elementy:

- Zagadnienia związane z przenoszeniem danych
- Opcje wdrażania
- Niezbędne połączenia z innymi narzędziami
- Otwartość i możliwość przystosowania platformy
- Obsługiwane funkcje i usługi

Zastanówmy się nad odpowiedziami na kilka podstawowych pytań, dzięki którym można lepiej zrozumieć dostępne opcje wyboru platformy zabezpieczeń i w największym stopniu uwzględnić potrzeby przedsiębiorstwa.

1 Czy w celu pełnego wykorzystania możliwości rozwiązania konieczne jest przenoszenie danych?

W przypadku wielu platform zabezpieczeń należy na nie przenieść wszystkie dane, aby umożliwić do nich dostęp. Zapisanie wszystkich danych w jednym miejscu może wydawać się dobrym pomysłem, jednak proces taki bywa złożony i kosztowny. Ponadto wiążą się z nim istotne kwestie dotyczące prywatności i miejsca przechowywania danych.

Biorąc pod uwagę złożoność zagadnienia, korzystna może okazać się komunikacja platformy z systemami, w których dane znajdują się obecnie, bez potrzeby ich przenoszenia. Takie rozwiązanie stanowi uzupełnienie istniejących narzędzi i pozwala w większym stopniu wykorzystać wcześniejsze inwestycje, a zarazem zapewnić scentralizowany widok i dostęp do danych znajdujących się w różnych systemach.

2 Czy można wdrożyć platformę w środowisku lokalnym, w chmurze publicznej lub prywatnej?

Różne platformy zabezpieczeń są dostępne jedynie w postaci rozwiązań typu „oprogramowanie jako usługa" działających w chmurze. Być może takie podejście sprawdzi się w przypadku Twojego przedsiębiorstwa, jednak wiele firm nie jest gotowych na zastosowanie rozwiązania opartego wyłącznie na chmurze. Elastyczność zapewniana przez hybrydową architekturę wielochmurową może okazać się przydatna. Bardzo często obciążenia są uruchamiane nadal w środowisku lokalnym, dlatego platforma zabezpieczeń, która jest w stanie działać w takim środowisku, a także w chmurze publicznej lub prywatnej, potencjalnie daje wiele korzyści. Zamiast ograniczać się do jednej opcji wdrożenia, warto poszukać elastycznej architektury, którą da się wdrożyć w hybrydowym środowisku wielochmurowym.

3 Czy platforma obsługuje połączenia i integrację z narzędziami innych firm?

Przedsiębiorstwa używają obecnie bardzo różnorodnych systemów zabezpieczeń i trudno się spodziewać, że wszystkie będą pochodziły od jednego producenta. Niektóre platformy zabezpieczeń są konstruowane w taki sposób, aby integrowały się wyłącznie z narzędziami konkretnego dostawcy, co stanowi pewne ograniczenie. Jeśli firma używa narzędzi dostarczanych przez różnych producentów, powinna poszukać platformy wspierającej otwarte połączenia z wieloma systemami zabezpieczeń i narzędziami informatycznymi. Warto zwrócić uwagę na następujące elementy:

- Rozbudowany ekosystem partnerów
- Otwarty pakiet SDK
- Usługi wsparcia związane z tworzeniem własnych, niestandardowych połączeń

Dzięki temu łatwiej ustalić, czy dana platforma współpracuje z używanymi obecnie narzędziami i ogranicza konieczność ich całkowitej wymiany.

4 Czy platformę można dostosować do zmian w strategii zabezpieczeń?

Jednym z ważnych kryteriów wyboru platformy może być jej otwartość i elastyczność niezbędna do uwzględnienia zmian w strategii zabezpieczeń. Należy sprawdzić, czy rozwiązanie wspiera:

- Otwarte standardy
- Technologie Open Source
- Otwarte połączenia

Otwarta platforma komunikuje się z narzędziami innych firm, obsługuje niestandardowe połączenia i umożliwia programowanie. Pozwala to uniknąć uzależnienia od jednego dostawcy i zapewnić współdziałanie z różnymi systemami zabezpieczeń i narzędziami informatycznymi.

5 Czy platforma udostępnia podstawowe funkcje harmonizacji, automatyzacji i reagowania na incydenty?

Rozwiązania do harmonizacji i automatyzacji zabezpieczeń oraz reagowania na incydenty (SOAR) często są reklamowane jako platformy. Jednak funkcje SOAR mogą zyskać na wartości, jeśli zostaną zintegrowane w ramach głównej platformy zabezpieczeń, a nie udostępniane jako odrębne produkty. Warto wybrać platformę zabezpieczeń, w której opcje SOAR są częścią podstawowej funkcjonalności. Pozwoli to zwiększyć efektywność pracy zespołu ds. zabezpieczeń w ramach różnych przepływów pracy i scenariuszy.

6 W jaki sposób platforma pozwala zintegrować mechanizmy analizy zagrożeń?

Analitycy ds. bezpieczeństwa często korzystają z wielu źródeł informacji o zagrożeniach i różnych produktów do przeszukiwania danych operacyjnych oraz wsparcia analizy i podejmowanych decyzji. Warto sprawdzić, czy platforma udostępnia raporty związane z analizą zagrożeń oraz w jaki sposób mechanizmy analityczne są powiązane z innymi funkcjami. Dzięki integracji funkcji analizy zagrożeń w ramach platformy zabezpieczeń można zmniejszyć obciążenie analityków, pozwalając im podejmować szybsze, trafniejsze decyzje.

7 Czy oprócz oprogramowania dostawca oferuje dodatkowe usługi?

Platforma zabezpieczeń to narzędzie bogate w możliwości, jednak w przedsiębiorstwie może zaistnieć potrzeba skorzystania z dodatkowych usług związanych z realizacją konkretnej strategii zabezpieczeń. Na rynku istnieje wiele możliwości, jeśli chodzi o usługi zabezpieczeń, ale skorzystanie z oferty dostawcy platformy może ułatwić integrację takich dodatkowych usług z wybranym rozwiązaniem.

Analiza podstawowych potrzeb i oczekiwań związanych z platformą zabezpieczeń

Podejście oparte na platformie pozwala zoptymalizować wykorzystanie danych dotyczących bezpieczeństwa, narzędzi i zespołów. Na rynku dostępnych jest wiele opcji, dlatego określając kryteria wyboru platformy dla przedsiębiorstwa, należy odpowiedzieć sobie na kilka ważnych pytań:

- Czy można pozostawić dane w obecnych systemach?
- Czy możliwe jest wdrożenie w hybrydowej architekturze wielochmurowej?
- Czy potrzebne są otwarte mechanizmy integracji i połączeń z innymi systemami zabezpieczeń i narzędziami informatycznymi?
- Czy można łatwo dostosować platformę zgodnie ze zmianami w strategii zabezpieczeń?
- Czy przydatne byłyby funkcje harmonizacji, automatyzacji i reagowania na incydenty?
- W jaki sposób platforma uwzględnia mechanizmy analizy zagrożeń?
- Czy oprócz oprogramowania dostawca oferuje dodatkowe usługi?

IBM Cloud Pak for Security: zintegrowane zabezpieczenia dla hybrydowych środowisk wielochmurowych

IBM Cloud Pak for Security to otwarta, zintegrowana platforma zabezpieczeń, udostępniająca szczegółowe informacje o zagrożeniach występujących w wielu środowiskach i umożliwiająca realizację obecnych i przyszłych wymagań przedsiębiorstwa. Użytkownicy mogą szybko wyszukiwać zagrożenia, koordynować działania i automatyzować reakcje na incydenty bez konieczności przeprowadzania migracji danych.

IBM Cloud Pak for Security, dzięki zastosowaniu otwartych standardów i innowacyjnych technologii IBM, zapewnia dostęp do narzędzi oferowanych przez IBM i inne firmy, pozwalając wyszukiwać wskaźniki zagrożeń w chmurach i w środowiskach lokalnych. IBM bierze udział w rozwoju technologii Open Source zastosowanej w rozwiązaniu IBM Cloud Pak for Security. Przedsiębiorstwo nawiązało współpracę z kilkudziesięcioma firmami w ramach inicjatywy OASIS Open Cybersecurity Alliance, aby zwiększyć współdziałanie rozwiązań i ograniczyć zależność od pojedynczych dostawców.

IBM Cloud Pak for Security składa się z oprogramowania kontenerowego wstępnie zintegrowanego z platformą aplikacji korporacyjnych Red Hat OpenShift. Integracja taka umożliwia działanie zarówno w środowisku lokalnym, jak i w chmurach prywatnych lub publicznych. Dzięki uwzględnieniu funkcji SOAR rozwiązanie pozwala harmonizować i automatyzować reakcje na incydenty związane z bezpieczeństwem.

Więcej informacji o rozwiązaniu IBM Cloud Pak for Security

Odwiedź stronę WWW poświęconą rozwiązaniu IBM Cloud Pak for Security i poznaj sposoby identyfikowania ukrytych zagrożeń, podejmowania lepiej umotywowanych decyzji w oparciu o analizę ryzyka oraz ustalania priorytetów działań zespołu.

Jeśli potrzebne okażą się dodatkowe kompetencje i wiedza, skorzystaj z usług zabezpieczeń IBM i opracuj przemyślaną strategię działania, aby przeprowadzić transformację programu bezpieczeństwa.

IBM Polska Sp. z o.o.
ul. Krakowiaków 32
02-255 Warszawa

Strona główna IBM znajduje się pod adresem:
ibm.com