Analiza danych dotyczących bezpieczeństwa dla środowisk wielochmurowych

Rozwiązanie IBM Security QRadar SIEM

IBM

Spis treści

Rewolucja wielochmurowa nabiera rozpędu

Nowoczesne przedsiębiorstwo wymaga inteligentnych zabezpieczeń

Jak wykorzystać potencjał rozwiązań IBM Security™ QRadar®

Jak zyskać pełną widoczność usług przetwarzania w chmurze

Integracja rozwiązania QRadar z chmurą Amazon Web Services (AWS)

Lepsza widoczność chmury AWS zapewnia większe bezpieczeństwo

Integracja rozwiązania QRadar z platformą Microsoft Azure

Lepsza widoczność i przetwarzanie danych o zdarzeniach z milionów urządzeń

Integracja rozwiązania QRadar z platformą Google Cloud Platform

Szybkie wykrywanie anomalii i rozpoznawanie zagrożeń w czasie rzeczywistym

Monitorowanie rozwiązań SaaS

Monitorowanie danych z aplikacji SaaS z wykorzystaniem modułów QRadar DSM

Efektywne narzędzia dla zespołu odpowiedzialnego za bezpieczeństwo

Poznaj rodzinę produktów QRadar

Dlaczego warto wybrać rozwiązania IBM Security?

01

Rewolucja wielochmurowa nabiera rozpędu

Nowoczesne przedsiębiorstwo wymaga inteligentnych zabezpieczeń

W związku z tym, że coraz więcej przedsiębiorstw wdraża hybrydowe środowiska wielochmurowe, coraz więcej danych, aplikacji i obciążeń przenoszonych jest do chmury. Wzrasta liczba pracowników pracujących z domu, a interakcje przenoszą się ze świata fizycznego do wirtualnego. Należy więc oczekiwać, że wskaźniki wykorzystania chmur będą osiągać nowe rekordy.[1]

Firma analityczna Gartner przewiduje, że do 2022 roku sektor usług udostępniania chmur publicznych będzie rozwijać się w tempie wykładniczym. Najszybszy wzrost odnotuje segment infrastruktury jako usługi (IaaS), który zgodnie z przewidywaniami firmy Gartner osiągnie w 2022 roku wartość 76,6 mld USD.[2]

W takich przedsięwzięciach związanych z chmurą bezpieczeństwo powinno być sprawą priorytetową. Naruszenie bezpieczeństwa w chmurze może kosztować firmy ponad 50 000 USD w ciągu niespełna godziny.[3] Przedsiębiorstwa używające rozwiązań IaaS muszą proaktywnie zabezpieczać swoje systemy operacyjne, zarządzać konfiguracjami sieci oraz, oczywiście, chronić dane przetwarzane w tych systemach.

Aby zapewnić bezpieczeństwo newralgicznych informacji biznesowych, analitycy potrzebują pełnej widoczności całego środowiska informatycznego – sieci, aplikacji i działań – w systemie lokalnym i chmurze. Muszą również mieć możliwość wykrywania zagrożeń w czasie rzeczywistym oraz przypadków używania nieautoryzowanych usług w chmurze, a także sprawdzania, czy konta i zasoby w chmurze są skonfigurowane w sposób zapewniający bezpieczeństwo.

> 1 miliard utraconych rekordów

Błędy w konfiguracji środowisk chmurowych doprowadziły w 2019 roku do utraty ponad miliarda rekordów.[3]

> 50 000 USD straty w ciągu niespełna godziny

Naruszenie bezpieczeństwa w chmurze może kosztować firmy ponad 50 000 USD w ciągu niespełna godziny.[3]

02

Jak wykorzystać potencjał rozwiązań IBM Security QRadar

Jak zyskać pełną widoczność usług przetwarzania w chmurze

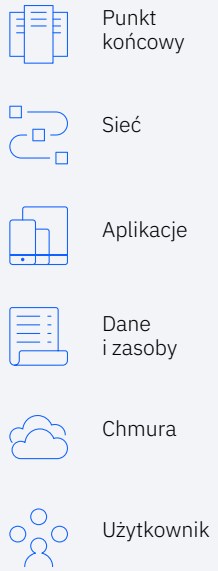
IBM Security QRadar to rozwiązanie do zarządzanie informacjami i zdarzeniami związanymi z bezpieczeństwem (ang. security information and event management – SIEM), które można głęboko zintegrować z wieloma usługami w chmurze, takimi jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365 i IBM Cloud®.

QRadar gromadzi i normalizuje informacje dotyczące bezpieczeństwa, pochodzące zarówno ze środowisk chmurowych, jak i lokalnych. Stosuje przy tym zaawansowane procesy analityczne, które umożliwiają automatyczne sortowanie milionów zdarzeń. Pomaga w wykrywaniu najbardziej krytycznych zagrożeń. Wysyła ważne alerty dotyczące potencjalnych incydentów, oparte na priorytetach, aby chronić środowiska lokalne i wielochmurowe środowiska hybrydowe.

Ponadto rozwiązanie to udostępnia analitykom bezpieczeństwa ujednolicony interfejs, na którym mogą oni śledzić najbardziej krytyczne zagrożenia, przeglądać chronologiczne łańcuchy zdarzeń prowadzące do poszczególnych alertów oraz uzyskiwać natychmiastowy wgląd w dane dotyczące potencjalnych ataków. Efektywne gotowe funkcje przyspieszają realizację wdrożeń i zwiększają ich skalowalność praktycznie w każdym obsługiwanym środowisku.

Dowiedz się, jak rozwiązanie QRadar może Ci pomóc w zabezpieczeniu środowiska chmurowego →

Zautomatyzowane wykrywanie i szeregowanie zagrożeń



Rozwiązanie IBM Security QRadar SIEM gromadzi, analizuje i koreluje dane z wielu źródeł w celu wykrywania i szeregowania najbardziej krytycznych zagrożeń, które wymagają badań.

03

Integracja rozwiązania QRadar z chmurą Amazon Web Services (AWS)

Lepsza widoczność chmury AWS zapewnia większe bezpieczeństwo

Około 76% przedsiębiorstw korzysta w mniejszym lub większym stopniu z chmury AWS[1]. W trakcie migracji z tradycyjnych, lokalnych systemów obliczeniowych do chmur zespoły odpowiedzialne za bezpieczeństwo potrzebują równie dobrej widoczności swoich chmurowych infrastruktur, aplikacji i danych, jak w środowiskach lokalnych.

Wykrywanie czynników ryzyka, które mogą zagrozić bezpieczeństwu danych
Nie wszystkie spośród największych wycieków danych, jakie miały miejsce w ciągu ostatnich lat, zostały celowo spowodowane przez cyberprzestępców. Niektóre były wynikiem błędów w konfiguracji zasobników (ang. bucket) usługi Amazon Simple Storage Service (Amazon S3), przez co dane wrażliwe stały się publicznie dostępne.

Za pomocą rozwiązania QRadar zespoły odpowiedzialne za bezpieczeństwo mogą proaktywnie skanować swoje środowiska AWS doraźnie lub w ramach programu regularnego skanowania. Pozwala im to aktywnie wyszukiwać takie błędy w konfiguracji, a w razie potrzeby alarmować analityków. Po otrzymaniu alertu specjaliści mogą rozpocząć działania w celu eliminacji luk i zapewnienia ochrony danych.

Wykrywanie zagrożeń dla danych i obciążeń w chmurze
W miarę jak coraz więcej danych wrażliwych i zasobów o znaczeniu newralgicznym jest przenoszonych do chmury, środowisko AWS staje się głównym celem hakerów. W przypadku uszkodzenia kont w systemie AWS, co może nastąpić bezpośrednio poprzez wyłudzenie danych (ang. spear phishing) lub na skutek eksploracji w poziomie, dane i obciążenia znajdujące się w chmurze AWS mogą zostać przejęte przez cyberprzestępców. Do skutecznego zapobiegania takim uszkodzeniom niezbędny jest ujednolicony system wczesnego ostrzegania o zagrożeniach. QRadar przekazuje dane dotyczące bezpieczeństwa pochodzące ze środowiska AWS, w tym z rozwiązań AWS CloudTrail, AWS CloudWatch oraz AWS Virtual Private Cloud (VPC) Flow Logs, do scentralizowanego rozwiązania służącego do analizy danych dotyczących bezpieczeństwa. Zespoły odpowiedzialne za operacje związane z bezpieczeństwem mogą wykorzystywać to rozwiązanie w celu śledzenia zagrożeń zewnętrznych i wewnętrznych z jednej konsoli.

QRadar może gromadzić dane dotyczące zdarzeń, pochodzące z rozwiązań zabezpieczających, z wykorzystaniem dołączanego pliku zwanego modułem **Device Support Module**.

Z wykorzystaniem obsługiwanych protokołów i modułów Device Support Module (DSM) rozwiązanie QRadar można zintegrować z następującymi komponentami środowiska AWS, co umożliwi zaawansowaną analizę bezpieczeństwa:

AWS CloudTrail. Integracja rozwiązania QRadar z tym komponentem zapewnia widoczność działań użytkowników poprzez rejestrowanie ich aktywności na kontach. Umożliwia obsługę kontrolowanych zdarzeń, których dane są gromadzone z zasobników usługi Amazon S3 oraz grupy katalogowej w systemie AWS CloudWatch Logs.

AWS Security Hub. W tym przypadku integracja umożliwia wykorzystanie zintegrowanego systemu funkcji analitycznych i mechanizmów obrony w czasie rzeczywistym. Dzięki temu zespoły odpowiedzialne za bezpieczeństwo zyskują lepszą widoczność priorytetowych alertów dotyczących bezpieczeństwa, a ponadto mogą przeprowadzać zautomatyzowane kontrole zgodności z przepisami, używając do tego celu jednego panelu kontrolnego centrum operacji bezpieczeństwa. Rozwiązanie QRadar zintegrowane z komponentem AWS Security Hub Amazon Findings Format (AFF) może zoptymalizować agregację zdarzeń obejmującą wiele funkcji bezpieczeństwa chmury AWS, instancji i rozwiązań zabezpieczających sieci AWS Partner Network (APN), co pozwala przeprowadzić bardziej dogłębną analizę bezpieczeństwa.

Amazon GuardDuty. Integracja rozwiązania QRadar z tym komponentem umożliwia użytkownikom analizowanie ciągłych strumieni metadanych, które są generowane na podstawie ich aktywności na kontach i w sieci, znalezionych w rejestrach zdarzeń usługi AWS CloudTrail, dziennikach Amazon VPC Flow Logs i dziennikach serwera DNS.

Amazon VPC Flow Logs. Ta integracja umożliwia klientom gromadzenie, przechowywanie i analizowanie dzienników przepływów w sieci. Można ją wykorzystać w celu monitorowania i rozwiązywania problemów związanych z łącznością i bezpieczeństwem, co pomaga w zapewnieniu prawidłowego działania reguł dostępu do sieci.

Amazon AWS Content Extension. To rozszerzenie w zakresie zawartości dodaje nowe funkcje analizy danych dotyczących zdarzeń do komponentu AWS wbudowanego w rozwiązanie QRadar. Przyspiesza również analizowanie danych dotyczących zdarzeń o znaczeniu newralgicznym. Dane, takie jak identyfikator instancji, nazwa pliku, nazwa roli lub nazwa pamięci masowej, są szybko udostępniane użytkownikom, aby umożliwić im monitorowanie zmian oraz zgłaszanie problemów dotyczących bezpieczeństwa środowisk chmurowych.

IBM Security QRadar Cloud Visibility. W ramach tej aplikacji dostępne są określone panele kontrolne środowiska AWS oraz następujące rozszerzenia:

- Uproszczone zarządzanie źródłami danych dzienników
- Zarządzanie tożsamością i dostępem (ang. identity and access management – IAM) dla kont, użytkowników i ról związanych z IAM
- Automatyczne wypełnianie struktury hierarchicznej sieci rozwiązania QRadar
- Wizualizacja dziennika Amazon VPC Flow Log
- Integracja z rozwiązaniami AWS Security Hub i Amazon Detective

Dlaczego warto używać rozwiązania QRadar do monitorowania środowisk AWS?

- Zapewnia scentralizowaną widoczność czynników ryzyka i zagrożeń we wszystkich wdrożeniach w chmurze
- Umożliwia analitykom bezpieczeństwa proaktywne wyszukiwanie błędów w konfiguracji, które wymagają podjęcia odpowiednich działań
- Eliminuje silosy, co ułatwia analizę całego łańcucha zdarzeń związanych z incydentem
- Wykorzystuje uczenie maszynowe do szybszego wykrywania użytkowników wysokiego ryzyka i zagrożeń wewnętrznych

Dowiedz się więcej o rozwiązaniu IBM Security QRadar Amazon AWS Content Extension →

04

Integracja rozwiązania QRadar z platformą Microsoft Azure

Lepsza widoczność i przetwarzanie danych o zdarzeniach z milionów urządzeń

Od lat liczba wdrożeń platformy Microsoft Azure systematycznie rośnie. Dziś z usługi tej korzysta 61% przedsiębiorstw i instytucji.[1] W miarę jak coraz więcej danych i obciążeń jest przenoszonych na tę platformę, konieczne jest dostosowanie procedur bezpieczeństwa do wymagań ochrony zasobów w tym nowym środowisku. QRadar udostępnia efektywne funkcje, które umożliwiają przekazywanie danych dotyczących bezpieczeństwa platformy Azure do programu analizy bezpieczeństwa obejmującego całe przedsiębiorstwo.

Z wykorzystaniem obsługiwanych protokołów i modułów DSM rozwiązanie QRadar można zintegrować z następującymi komponentami platformy Azure, co umożliwi zaawansowaną analizę bezpieczeństwa:

Azure Activity Logs. Jest to usługa rodzima platformy Azure umożliwiająca gromadzenie danych dotyczących zdarzeń, a w szczególności dużych ilości danych telemetrycznych. Dane te można łatwo przesłać do rozwiązania QRadar, co zapewni zespołom odpowiedzialnym za bezpieczeństwo głębszy wgląd w potencjalne czynniki ryzyka i zagrożenia w środowiskach Azure.

Azure Active Directory. Integracja rozwiązania QRadar z katalogiem Azure Active Directory umożliwia zespołom odpowiedzialnym za bezpieczeństwo monitorowanie tożsamości, zarządzanie dostępem oraz pozyskiwanie danych dotyczących zdarzeń ze źródeł zewnętrznych, takich jak pakiet Microsoft Office 365 i platforma Microsoft Azure.

Microsoft Graph Security API. Za pomocą protokołu QRadar Microsoft Graph Security API można odbierać alerty z interfejsu Microsoft Graph Security API, co umożliwia analitykom bezpieczeństwa szybkie badanie przypadków naruszenia ochrony danych.

Aplikacja QRadar Cloud Visibility. QRadar może wykrywać potencjalne problemy w środowiskach Azure i obsługiwać przypadki użycia dotyczące bezpieczeństwa. Po zarejestrowaniu naruszeń aplikacja QRadar Cloud Visibility pomaga użytkownikom w zarządzaniu nimi z panelu kontrolnego AzureOffense Overview.

Na panelu tym wyświetlane są dane dotyczące aktywnych naruszeń przedstawione w formie następujących wykresów:

- Wszyscy użytkownicy wg skali naruszeń
- Wszyscy użytkownicy wg powiązanych reguł
- Najpoważniejsze naruszenia
- Wszyscy użytkownicy wg liczby naruszeń
- Wskaźnik poziomu dla skali naruszeń

IBM Security QRadar Content Extension dla platformy Azure. W ramach tego rozszerzenia w zakresie zawartości dla platformy Azure dodawane są reguły, raporty i zapisane wyszukiwania, które umożliwiają wykorzystanie funkcji analizy zdarzeń rozwiązania QRadar dla wdrożeń na platformie Azure.

Celem tego rozszerzenia jest w szczególności usprawnienie takich procesów, jak zarządzanie bezpieczeństwem sieci, modyfikacja reguł bezpieczeństwa i zarządzanie siecią wirtualną.

Dlaczego warto używać rozwiązania QRadar do ochrony i monitorowania komponentów platformy Azure?

- Wykrywanie nieprawidłowych wzorców zachowań w całej infrastrukturze informatycznej przy użyciu reguł dotyczących bezpieczeństwa.
- Monitorowanie i diagnozowanie ruchu w sieci za pomocą grup bezpieczeństwa sieci Azure.
- Efektywniejsze zarządzanie sieciami wirtualnymi.
- Gromadzenie danych z dzienników zdarzeń i danych dotyczących bezpieczeństwa przepływów w sieci w bramach sieci lokalnej.
- Monitorowanie wydajności i używania aplikacji WWW działających na platformie Azure.

Dowiedz się więcej o rozwiązaniu QRadar Content Extension dla platformy Azure →

05

Integracja rozwiązania QRadar z platformą Google Cloud Platform

Szybkie wykrywanie anomalii i rozpoznawanie zagrożeń w czasie rzeczywistym

Google Cloud Platform jest jednym z czołowych rozwiązań w chmurze, używanym obecnie przez 35% firm (z tendencją rosnącą)[1]. Obejmuje pakiet usług w chmurze, które wykorzystują infrastrukturę Google. Dzięki zaawansowanym funkcjom rozwiązanie IBM Security QRadar można zintegrować z platformą Google Cloud Platform, co pozwala na gromadzenie, wyszukiwanie i analizowanie dużych ilości danych pochodzących z obciążeń przetwarzanych we wszystkich środowiskach, a także zapewnia scentralizowaną widoczność tych danych. Dzięki temu zespoły odpowiedzialne za bezpieczeństwo mogą skuteczniej wykrywać zagrożenia w każdym miejscu oraz na nie reagować.

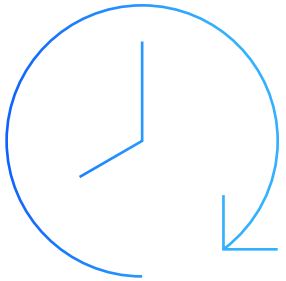
Z wykorzystaniem obsługiwanych protokołów i modułów DSM rozwiązanie QRadar można zintegrować z następującymi usługami platformy Google Cloud Platform, co umożliwi zaawansowaną analizę bezpieczeństwa:

Raporty działań związanych z pakietem Google G Suite. QRadar zapewnia widoczność zdarzeń związanych z kontrolą, które są generowane na platformie Google G Suite, w tym danych logowania, konta użytkownika oraz usług Google Drive i Google Admin.

Zespół odpowiedzialny za bezpieczeństwo zyska wgląd w następujące przypadki użycia:

- Wyłączenie konta z powodu podejrzanych działań
- Dane użytkownika pobrane w formie pliku CSV
- Cofnięcie uprawnień administratora przez użytkownika
- Dokonana przez osobę nieuprawnioną zmiana tajnego pytania lub odpowiedzi, które umożliwiają odzyskanie konta
- Dokonana przez osobę nieuprawnioną zmiana zezwoleń użytkownika na udostępnianie danych
- Dokonane przez osobę nieuprawnioną przeniesienie elementu z folderu źródłowego do folderu docelowego
- Zawieszenie użytkownika

Protokół Google Cloud Pub/Sub Protokół rozwiązania QRadar dla usługi Google Cloud Pub/Sub zapewnia lepszy wgląd we wszystko, co ma związek z usługą Pub/Sub. Umożliwia zespołom odpowiedzialnym za bezpieczeństwo szybsze działanie.



06

Monitorowanie rozwiązań SaaS

Monitorowanie danych z aplikacji SaaS z wykorzystaniem modułów QRadar DSM

Przedsiębiorstwa korzystają już z aplikacji typu „oprogramowanie jako usługa” (SaaS), które zapewniają im większą sprawność i elastyczność, umożliwiają szybszą pracę i pomagają w realizacji projektów generujących przychody. Liczba wdrożeń takich aplikacji cały czas rośnie. Firma Gartner przewiduje, że w 2022 roku wartość rynku tych chmurowych rozwiązań w formie usług osiągnie 143,7 mld USD.[2]

QRadar zapewnia lepszy wgląd w dane dotyczące używania aplikacji SaaS oraz umożliwia zespołom odpowiedzialnym za bezpieczeństwo efektywniejsze wykrywanie i blokowanie zagrożeń. Wbudowane moduły DMS pozwalają na bezproblemową integrację rozwiązania QRadar z innymi rozwiązaniami w środowisku użytkownika. Przed wdrożeniem moduły DSM są testowane i zatwierdzane przez zespół działu bezpieczeństwa IBM (IBM Security).

Rozwiązanie QRadar zostało zaprojektowane z myślą o pomocy zespołom odpowiedzialnym za bezpieczeństwo w monitorowaniu danych pochodzących z takich aplikacji SaaS, jak Salesforce.com, Office 365 czy środowiska Box. Gdy dane te zostaną wprowadzone do programu analizy bezpieczeństwa, zespół zyska lepszy wgląd w potencjalne zagrożenia i będzie mógł z wyprzedzeniem wykrywać incydenty, które stwarzają ryzyko dla danych w tych aplikacjach. Analitycy ds. bezpieczeństwa otrzymają lepsze narzędzie do wykrywania podejrzanych użytkowników wewnętrznych na wczesnych etapach ataku oraz zapobiegać przejęciu przez nich danych wrażliwych przechowywanych w aplikacjach i usługach.

Dowiedz się więcej o modułach DMS obsługiwanych przez rozwiązanie QRadar →

Rozwiązanie QRadar można zintegrować za pomocą modułów DSM z wieloma popularnymi rozwiązaniami SaaS i IaaS.

Amazon CloudTrail
Amazon CloudWatch
Amazon VPC Flows

Microsoft Azure Event Hubs

Microsoft Office 365

Box.com

Netskope Active

Cloudera Navigator

CloudPassage Halo

Skyhigh Networks

OpenStack

Cisco Cloud Web Security

VMware

Salesforce

Okta

Google Cloud Platform

Platforma Red Hat® Ansible®

07

Efektywne narzędzia dla zespołu odpowiedzialnego za bezpieczeństwo

Poznaj rodzinę produktów QRadar

Reasumując, rozwiązania IBM Security QRadar zostały zaprojektowane z myślą o zapewnieniu wglądu w newralgiczne dane, którego potrzebują przedsiębiorstwa w swoich coraz większych środowiskach chmurowych. Rozwiązania z tej rodziny umożliwiają połączenie wielu silosów danych na jednej platformie, co zapewnia ich pełną widoczność, a ponadto ułatwia analizę bezpieczeństwa i wykrywanie zagrożeń. Użytkownik może wykrywać nieprawidłowe zachowania w celu zabezpieczenia się przed atakami wewnętrznymi i zewnętrznymi, słabe punkty zabezpieczeń mogące przypadkowo narazić dane wrażliwe na ryzyko, a także przypadki używania nieautoryzowanych usług w chmurze.

Wszystkie te funkcje pomagają w uzyskaniu kompleksowego widoku systemu, sieci i aktywności użytkowników w całym przedsiębiorstwie. Mogą też dostarczyć inteligentnych informacji, które ułatwią proaktywne zwalczanie czynników ryzyka i zagrożeń.

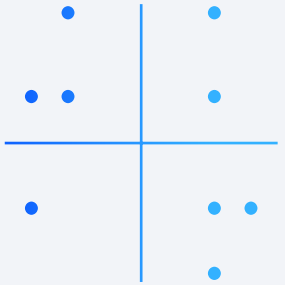
Rozwiązanie QRadar umożliwia centralne gromadzenie i analizowanie kanałów danych z wielu źródeł w różnych środowiskach, takich jak AWS, Azure, IBM Cloud, aplikacje SaaS, chmury prywatne i tradycyjne infrastruktury lokalne. Użytkownik może wdrożyć sprzęt i oprogramowanie lokalnie, zainstalować maszyny wirtualne w środowiskach IaaS lub korzystać z rozwiązania QRadar jako usługi w chmurze IBM.

W trakcie migracji do środowiska wielochmurowego firma może korzystać z tych samych możliwości w zakresie bezpieczeństwa, monitorowania i analiz w całym swoim środowisku.

Dowiedz się więcej →

IBM został umieszczony wśród liderów w najnowszym raporcie firmy Gartner „Magic Quadrant for Security Information and Event Management (SIEM)”**już po raz 11. z rzędu.**

Przeczytaj raport →



08

Dlaczego warto wybrać rozwiązania IBM Security?

IBM ma jedną z największych na świecie organizacji wyspecjalizowanych w badaniach i rozwoju oraz dostarczaniu produktów i usług w dziedzinie zabezpieczeń.

Dział zabezpieczeń IBM ma jedną z najbardziej zaawansowanych i najlepiej zintegrowanych na rynku ofert produktów i usług, które chronią systemy informatyczne przedsiębiorstw. Oferta ta, wspierana przez cenioną na całym świecie jednostkę badawczą IBM X-Force, obejmuje analizę danych dotyczących bezpieczeństwa, która pomaga firmom w kompleksowej ochronie infrastruktur, danych i aplikacji. Udostępnia też rozwiązania do zarządzania tożsamością i dostępem, ochrony bazy danych, tworzenia aplikacji, zarządzania ryzykiem, zarządzania punktami końcowymi, ochrony sieci i wiele innych. Są to rozwiązania pozwalające przedsiębiorstwom efektywnie zarządzać ryzykiem i wdrażać zintegrowane zabezpieczenia systemów mobilnych, przetwarzania w chmurze, mediów społecznościowych i innych architektur biznesowych.

Dział IBM Global Financing oferuje liczne opcje finansowania ułatwiające nabywanie technologii niezbędnych do rozwoju przedsiębiorstwa. Zapewnia zarządzanie produktami i usługami informatycznymi w całym cyklu życia, od zakupu do utylizacji. Więcej informacji można znaleźć na stronie ibm.com/financing.

Więcej informacji
Aby uzyskać więcej informacji o rozwiązaniu QRadar do analizy danych dotyczących bezpieczeństwa, należy skontaktować się z przedstawicielem IBM lub Partnerem Handlowym IBM albo skorzystać z serwisu WWW: ibm.com/security/security-intelligence/qradar.

IBM monitoruje **miliardy** zdarzeń dotyczących bezpieczeństwa dziennie **w ponad 130 krajach** i ma przeszło **3000 patentów w dziedzinie zabezpieczeń**.

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

Strona główna IBM znajduje się pod adresem:
ibm.com

Niniejszy dokument jest aktualny na dzień jego pierwszej publikacji i może zostać zmieniony przez IBM w dowolnym momencie. Nie wszystkie produkty są dostępne we wszystkich krajach, w których IBM prowadzi działalność.

1 „10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera", *Forbes*, 2 maja 2020 r.

2 „Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019", *Gartner*, 2 kwietnia 2019 r.

3 „Cloud Threat Landscape Report 2020", *IBM Security X-Force®* dział reagowania na wydarzenia i usług analitycznych (Incident Response and Intelligence Services), maj 2020 r.