Аналитика безопасности для мультиоблачных сред

Решение IBM Security QRadar SIEM

Содержание

01

Мультиоблачная революция набирает обороты

Современным предприятиям нужна интеллектуальная защита

Темпы внедрения гибридных мультиоблачных сред только нарастают, и вместе с этим всё больше данных, приложений и рабочих нагрузок переносится в облако. А с ростом популярности удаленной работы и переходом от личных встреч к виртуальному общению ожидается еще большее расширение сферы применения облачных технологий.[1]

По оценкам компании Gartner, экспоненциальный рост индустрии публичных облачных сервисов продолжится и в 2022 году. Самым быстрорастущим сегментом облачного рынка станет инфраструктура как услуга (IaaS). Gartner прогнозирует, что к 2022 году объем этого сегмента вырастет до 76,6 млрд долларов США.[2]

В таких облачных проектах безопасности должно быть отведено центральное место. Нарушения облачной безопасности могут нанести компаниям ущерб выше 50 000 долларов США менее чем за час.[3] Организациям, применяющим IaaS, необходимо обеспечить упреждающую защиту своих операционных систем, управление сетевыми конфигурациями и, естественно, безопасность данных в таких системах.

Чтобы обезопасить критически важную бизнес-информацию, аналитикам безопасности требуется полная прозрачность всей ИТ-экосистемы, включая сети, приложения и операции, как в локальной, так и в облачных средах. Нужно уметь обнаруживать угрозы в реальном времени, выявлять факты несанкционированного использования облачных сервисов и четко понимать, настроены ли облачные учетные записи и ресурсы должным образом для поддержания безопасности.

> 1 млрд утраченных записей

В 2019 году более миллиарда записей было утрачено вследствие неправильной настройки облачных сред.[3]

> 50 тысяч долларов США убытков менее чем за час

Нарушения облачной безопасности могут нанести компаниям ущерб выше 50 000 долларов США менее чем за час.[3]

02

Раскройте потенциал решений IBM Security QRadar

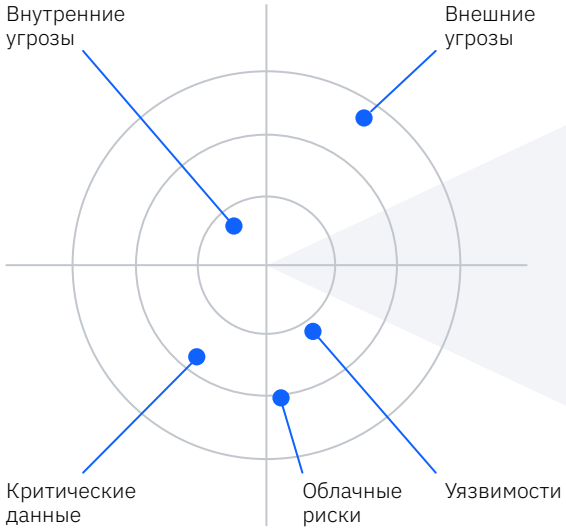
Полная прозрачность облачных сервисов

Решение IBM Security QRadar Security Information and Event Management (SIEM) обеспечивает тесную интеграцию с различными облачными сервисами, включая Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365, IBM Cloud и др.

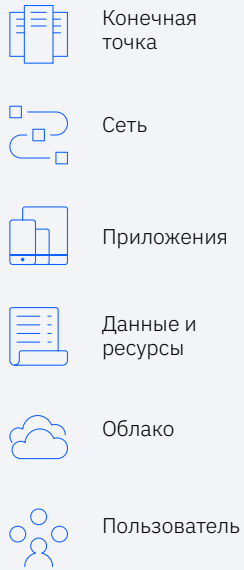
Это решение выполняет сбор и нормализацию информации о безопасности из облачных и локальных сред и применяет расширенную аналитику для автоматической сортировки миллионов событий. Оно помогает обнаруживать самые опасные угрозы и выдает приоритетные предупреждения о возможных инцидентах для защиты локальных и мультиоблачных гибридных сред.

Кроме того, аналитики безопасности работают с единым интерфейсом, который позволяет получать информацию о наиболее опасных угрозах, просматривать хронологическую цепочку событий, приведших к появлению каждого предупреждения, и оперативно анализировать потенциальные атаки. Мощный набор готовых функций помогает быстро развертывать и масштабировать решение практически в любой поддерживаемой среде.

Узнайте о том, как с помощью решения QRadar защитить облачную среду →



Автоматическое обнаружение и приоритизация угроз



Решение IBM Security QRadar SIEM осуществляет сбор, анализ и сопоставление данных из широкого круга источников для выявления и классификации наиболее серьезных угроз, требующих расследования.

03

Интеграция решения QRadar с Amazon Web Services (AWS)

Повышение прозрачности AWS для усиления безопасности

Примерно 76 % организацией в той или иной степени пользуются услугами AWS.[1] По мере перехода от традиционных вычислений в локальной среде к облачным вычислениям службам ИТ-безопасности необходимо обеспечивать в облаке такой же уровень прозрачности инфраструктуры, приложений и данных, как и в локальной среде.

Выявление рисков для данных
В последние несколько лет за некоторыми из крупнейших утечек данных стояли не злоумышленники. Многие утечки произошли в результате непреднамеренной ошибочной настройки корзин Amazon Simple Storage Service (Amazon S3), в результате чего конфиденциальные данные стали общедоступными.

С помощью решения QRadar специалисты по безопасности могут выполнять упреждающее сканирование сред AWS как на регулярной основе, так и по ситуации, для активного поиска ошибок в конфигурации и в случае их выявления направлять предупреждения аналитикам. Получив такие предупреждения, группы безопасности могут начать действовать с целью устранить ошибки и защитить свои данные.

Обнаружение угроз для облачных данных и задач
Сейчас, когда в облако переносится все больше конфиденциальных данных и критически важных ресурсов, главной целью злоумышленников становится AWS. В случае компрометации учетных записей AWS напрямую вследствие целевого фишинга либо в процессе бокового смещения данные и рабочие нагрузки AWS могут оказаться под контролем злоумышленника. Чтобы не допустить ущерба, важно заблаговременно получать предупреждения об угрозах. Решение QRadar собирает информацию о безопасности AWS, включая данные AWS CloudTrail, AWS CloudWatch и AWS Virtual Private Cloud (VPC) Flow Logs, и передает эти сведения в централизованную систему для анализа безопасности, с помощью которой специалисты по безопасности могут отслеживать внешние и внутренние угрозы.

Для сбора информации о событиях, поступающей от различных продуктов безопасности, в решении QRadar используется подключаемый модуль, называемый **Device Support Module**.

С целью расширенного анализа безопасности решение QRadar использует поддерживаемые протоколы и модули DSM для интеграции со следующими компонентами AWS:

AWS CloudTrail. Интеграция с QRadar обеспечивает прозрачность деятельности пользователей за счет регистрации действий, выполняемых с учетной записью. Поддерживаются события аудита, собираемые из корзин Amazon S3 и группы журналов AWS CloudWatch Logs.

AWS Security Hub. Интегрированная система аналитики и защиты в реальном времени предоставляет специалистам по безопасности расширенные возможности просмотра приоритетных предупреждений безопасности и автоматической проверки нормативного соответствия на единой сводной панели управления центром обеспечения безопасности (SOC). Благодаря поддержке AWS Security Hub Amazon Findings Format (AFF) решение QRadar может оптимальным образом собирать события из различных компонентов защиты AWS, экземпляров и решений для обеспечения безопасности AWS Partner Network (APN) с целью углубленного анализа безопасности.

Amazon GuardDuty. Благодаря этой интеграции пользователи получают возможность анализировать непрерывные потоки метаданных, генерируемых в учетных записях, и информацию о сетевой активности из событий AWS CloudTrail, журналов Amazon VPC Flow Logs и журналов серверов доменных имен (DNS).

Amazon VPC Flow Logs. Эта интеграция помогает клиентам собирать, хранить и анализировать журналы сетевых потоков. Ее можно использовать для мониторинга и устранения проблем с подключением и безопасностью для обеспечения надлежащей работы правил доступа к сети.

Amazon AWS Content Extension. Это расширение обеспечивает анализ дополнительных данных событий помимо тех, которые встроены в решение QRadar, и ускоряет анализ данных о критических событиях. Пользователи получают доступ к таким данным, как идентификатор экземпляра, имя файла, имя роли, имя хранилища и др., для мониторинга изменений и подготовки отчетности об относительной безопасности облачных сред.

Приложение IBM Security QRadar Cloud Visibility. Это приложение содержит дополнительные сводные панели и расширения для AWS, включая следующие:

- Упрощенное управление источниками событий
- Управление идентификационными данными и доступом (IAM) для учетных записей, пользователей и ролей IAM
- Автоматическое составление сетевой иерархии QRadar
- Визуализация Amazon VPC Flow Log
- Интеграция с AWS Security Hub и Amazon Detective

Зачем использовать решение QRadar для мониторинга сред AWS?

- Централизованное представление рисков и угроз в облачных средах
- Активный поиск аналитиками ошибок в конфигурациях, требующих реагирования
- Устранение разобщенности данных для понимания всей цепочки событий, связанных с инцидентом
- Машинное обучение для выявления пользователей с высоким уровнем риска и ускорения обнаружения внутренних угроз

Подробнее о IBM Security QRadar Amazon AWS Content Extension →

04

Интеграция решения QRadar с Microsoft Azure

Повышение прозрачности и обработка событий от миллионов устройств

В последние годы популярность Microsoft Azure непрерывно росла, и сейчас 61 % организаций заявляют о том, что они пользуются этой услугой.[1] В связи с переносом в Azure всё большего числа данных и рабочих нагрузок необходимо адаптировать методы обеспечения безопасности для защиты активов в этой новой среде. В решении QRadar предусмотрен мощный набор готовых функций для интеграции данных о безопасности Azure в корпоративную программу анализа безопасности.

С целью расширенного анализа безопасности решение QRadar использует поддерживаемые протоколы и модули DSM для интеграции со следующими компонентами Azure:

Azure Activity Logs. Собственная служба сбора событий Azure получает огромные объемы телеметрических данных и событий. Эту информацию можно легко направить в решение QRadar для углубленного анализа потенциальных рисков и угроз в средах Azure.

Azure Active Directory. Благодаря интеграции решения QRadar с Azure Active Directory специалисты по безопасности получают возможность вести мониторинг событий идентификации, управления доступом и безопасности из внешних ресурсов, таких как Microsoft Office 365 и Microsoft Azure.

Microsoft Graph Security API. С помощью протокола QRadar Microsoft Graph Security API организации могут получать предупреждения от Microsoft Graph Security API для более быстрого расследования нарушений.

Приложение QRadar Cloud Visibility. Решение QRadar может обнаруживать потенциальные проблемы в средах Azure и разрешать вопросы, связанные с безопасным использованием. Приложение QRadar Cloud Visibility с помощью сводной панели нарушений в среде Azure (Azure Offense Overview) помогает пользователям управлять такими нарушениями.

На этой панели представлены данные об активных нарушениях в виде следующих диаграмм:

- Все пользователи по важности
- Все пользователи по связанному правилу
- Самые серьезные нарушения
- Все пользователи по числу нарушений
- Показатель уровня важности

IBM Security QRadar Content Extension for Azure. Расширение QRadar Azure добавляет правила, отчеты и сохраненные поисковые запросы для увеличения имеющихся возможностей анализа событий QRadar для сред Azure.

Это расширение ориентировано на решение задач управления сетевой безопасностью, изменения правил безопасности и управления виртуальными сетями.

Зачем использовать решение QRadar для защиты и мониторинга компонентов Azure?

- Обнаружение аномального поведения и закономерностей в ИТ-инфраструктуре с помощью правил безопасности.
- Мониторинг и диагностика сетевого трафика с помощью групп сетевой безопасности Azure.
- Повышение эффективности управления виртуальными сетями.
- Сбор журналов событий и данных о безопасности сетевых потоков в шлюзах локальных сетей.
- Мониторинг производительности и использования веб-приложений в среде Azure.

Подробнее о QRadar Content Extension for Azure →

05

Интеграция решения QRadar с Google Cloud Platform

Оперативное выявление аномалий и обнаружение угроз в реальном времени

Платформа Google Cloud Platform является одним из ведущих облачных решений с растущей пользовательской базой, составляющей сейчас 35 %.[1] Решение предлагает ряд облачных сервисов на базе инфраструктуры Google. Решение IBM Security QRadar тесно интегрировано с Google Cloud Platform. Оно выполняет сбор, поиск и анализ сотен данных о рабочих нагрузках в разных средах и централизованное представление этих данных. Специалисты по безопасности могут быстрее обнаруживать угрозы и реагировать на них независимо от места их возникновения.

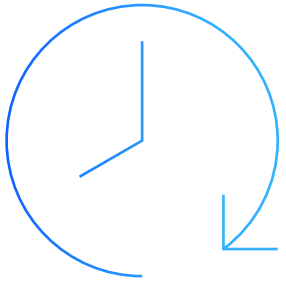
С целью расширенного анализа безопасности решение QRadar использует поддерживаемые протоколы и модули DSM для интеграции со следующими сервисами Google Cloud Platform:

Google G Suite Activity Reports. Решение QRadar обеспечивает прозрачность событий аудита, созданных в рамках платформы Google G Suite, включая входы в систему, учетные записи пользователей, Google Drive и Google Admin.

Служба ИТ-безопасности сможет получить ценную информацию в следующих сценариях использования:

- Учетная запись отключена вследствие подозрительных действий
- Информация о пользователе загружена с использованием файла в формате CSV
- Права администратора отозваны пользователем
- Пользователь изменил секретный вопрос или ответ для восстановления учетной записи
- Пользователь изменил разрешения на общий доступ
- Пользователь переместил объект из исходной папки в целевую папку
- Пользователь заблокирован

Протокол Google Cloud Pub/Sub. Протокол QRadar для Google Cloud Pub/Sub помогает повысить прозрачность всех действий, приводящих к созданию приемника в Pub/Sub, и тем самым ускорить реагирование.



06

Подробная информация о SaaS

Мониторинг данных от приложений SaaS с помощью модулей QRadar DSM

Предприятия уже используют программное обеспечение, предоставляемое в качестве услуги (SaaS), чтобы повысить гибкость, ускорить работу и поддерживать наиболее прибыльные проекты, и темпы внедрения SaaS продолжают расти. По прогнозам Gartner, объем продаж таких облачных решений на основе сервисов к 2022 году достигнет 143,7 млрд долларов США.[2]

Решение QRadar помогает организациям осуществлять контроль за использованием приложений SaaS и повышать эффективность обнаружения и блокирования угроз. Встроенные модули DSM предоставляют возможность интеграции с другими решениями, имеющимися в вашей среде. Перед развертыванием модулей DSM специалисты IBM Security выполняют их тестирование и проверку.

Решение QRadar призвано помочь вашим специалистам упростить мониторинг данных, поступающих от приложений SaaS, таких как Salesforce.com, Office 365, среды Box и др. Когда такие данные будут включены в программу анализа безопасности, ваши специалисты смогут более детально анализировать потенциальные угрозы и обнаруживать потенциальные инциденты, затрагивающие данные в этих решениях. Аналитики безопасности получат в свои руки инструменты, помогающие выявлять злоумышленников на ранних стадиях атак и не допускать компрометации конфиденциальных данных, которые хранятся в этих приложениях и службах.

Подробнее о модулях DSM, поддерживаемых в решении QRadar →

Решение QRadar поддерживает интеграцию с различными популярными предложениями SaaS и IaaS с использованием модулей DSM.

- 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
- Платформа Red Hat® Ansible®

07

Предоставьте своим специалистам по безопасности правильные инструменты

Ознакомьтесь с семейством продуктов QRadar

Подводя итоги, можно сказать, что решения IBM Security QRadar предоставляют важную информацию, необходимую для расширяющихся облачных сред. С помощью этого семейства решений вы сможете собрать на одной платформе разрозненные данные, чтобы обеспечить полную прозрачность, анализ безопасности и обнаружение угроз. Вы сможете выявлять аномальные действия, чтобы защититься от внутренних и внешних угроз, обнаруживать уязвимости, которые могут непреднамеренно подвергнуть опасности конфиденциальные данные, а также выявлять случаи несанкционированного использования облачных сервисов.

Все эти возможности помогают получить полное представление о системе, сети и действиях пользователей в организации, а также дают интеллектуальные средства для упреждающей борьбы с рисками и угрозами.

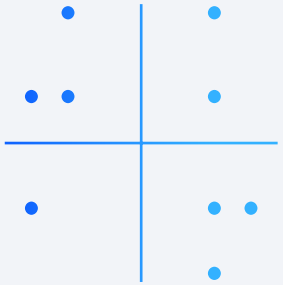
Решение QRadar осуществляет централизованный сбор и анализ потоков данных и информации об угрозах из различных источников в разных средах, включая AWS, Azure, IBM Cloud, приложения SaaS, частные облака и традиционные локальные инфраструктуры. На выбор предлагается локальное развертывание аппаратного или программного обеспечения, развертывание виртуальных машин в среде IaaS или использование решения QRadar в виде облачной услуги IBM.

При переходе в мультиоблачную среду вы можете использовать те же самые возможности для обеспечения безопасности, мониторинга и аналитики в масштабе всего предприятия.

Подробнее →

IBM признана лидером в области SIEM-систем в последнем отчете Gartner Magic Quadrant **– 11 лет подряд на первом месте.**

Прочитать отчет →



08

Почему именно решения IBM Security?

В состав IBM входит одна из крупнейших организаций в области аналитики безопасности, а также разработки решений по безопасности.

IBM Security предлагает целый спектр современных интегрированных продуктов и услуг в сфере корпоративной безопасности. Эти решения, основанные на признанных во всем мире результатах исследований подразделения IBM X-Force®, предоставляют аналитическую информацию в области безопасности, помогая организациям укреплять комплексную защиту инфраструктуры, данных и приложений. В этот пакет входят решения для управления идентификацией и доступом, для защиты баз данных, разработки приложений, управления рисками, управления конечными устройствами, обеспечения сетевой безопасности и т. д. Эти решения позволяют организациям эффективно управлять рисками и внедрять интегрированные средства защиты для мобильных, облачных сред, для социальных медиа и других бизнес-архитектур.

Кроме того, IBM Global Financing предлагает различные возможности финансирования при приобретении технологий, которые необходимы для развития вашего бизнеса. IBM обеспечивает управление всем жизненным циклом ИТ-продуктов и услуг, от приобретения и до вывода из эксплуатации. Более подробная информация: ibm.com/financing.

Дополнительная информация
Для получения дополнительной информации о решении по аналитике безопасности QRadar обратитесь к торговому представителю или бизнес-партнеру IBM либо посетите веб-сайт: ibm.com/security/security-intelligence/qradar.

IBM отслеживает **миллиарды** событий, связанных с информационной безопасностью, более чем в **130 странах мира**, а число патентов в сфере безопасности, полученных компанией, **составляет 3000**.

IBM Восточная Европа/Азия
123112 Москва
Пресненская наб., 10

Веб-сайт IBM:
ibm.com

Настоящий документ актуален по состоянию на момент публикации и может быть изменен IBM в любое время. Не все предложения могут быть доступны во всех странах, в которых IBM ведет свою деятельность.

Пользователь несет ответственность за оценку и проверку взаимодействия любых других продуктов и программ с продуктами и программами IBM. ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ЛЮБЫЕ ГАРАНТИИ ТОВАРОПРИГОДНОСТИ, СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ И ЛЮБЫЕ ГАРАНТИИ ИЛИ УСЛОВИЯ НЕНАРУШЕНИЯ ПРАВ. В отношении продуктов IBM действуют гарантии на основании положений и условий соглашений, в соответствии с которыми эти продукты предоставляются.

Заявление о добросовестной политике безопасности: в процесс обеспечения безопасности ИТ-систем входит защита систем и информации путем предотвращения, обнаружения и блокирования несанкционированного доступа к ним изнутри и снаружи организации. Несанкционированный доступ может привести к подмене, уничтожению, краже или неправомерному использованию информации, повреждению систем или их использованию в корыстных целях, в том числе для осуществления атак на других пользователей. Ни одну ИТ-систему или продукт нельзя считать абсолютно безопасными, равно как ни один продукт, услуга или мера безопасности не может обеспечить абсолютную эффективность в предотвращении несанкционированного доступа или неправомерного использования. Системы, продукты и услуги IBM предназначены для работы в комплексе законных мер по обеспечению безопасности, в который для максимальной эффективности обязательно будут входить другие процедуры и, возможно, будут задействованы другие системы, продукты и услуги. IBM НЕ ГАРАНТИРУЕТ, ЧТО СИСТЕМЫ, ПРОДУКТЫ И УСЛУГИ ПОЛНОСТЬЮ ЗАЩИЩЕНЫ ОТ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ ЛЮБОЙ ИЗ СТОРОН ИЛИ ЗАЩИТЯТ ВАШЕ ПРЕДПРИЯТИЕ ОТ ПОДОБНЫХ ЗЛОНАМЕРЕННЫХ ИЛИ ПРОТИВОЗАКОННЫХ ДЕЙСТВИЙ.

1 10 ключевых выводов из отчета RightScale о состоянии облачных технологий в 2020 году, подготовленного компанией Flexera, *Forbes*, 2 мая 2020 г.

2 По прогнозам Gartner, мировая выручка от публичных облачных сред вырастет в 2019 году на 17,5 %, *Gartner*, 2 апреля 2019 г.

3 Отчет об облачных угрозах за 2020 год, *IBM Security X-Force®* Incident Response and Intelligence Services, май 2020 г.