Особенности

- Использование надежного советника для расследования и классификации инцидентов безопасности с использованиемогромного объема информации
- Улучшенное понимание и идентификация сложных угроз безопасности с помощью обработки неструктурированных данных
- Ускоренный анализ большего количества данных безопасности, используя возможности когнитивных вычислений, предоставляемые IBM Watson for Cyber Security
- Решение сложных задан, связанных с анализом, скоростью и точностью при расследовании киберугроз.

Вооружите аналитиков по безопасности возможностями когнитивной системы ИТ-безопасности

Обнаруживайте угрозы и реагируйте на них в соответствующем масштабе и с непревзойденной скоростью

Известно ли вам, что в 2016 году типичный клиент, отслеживаемый IBM® Security, столкнулся с более чем 54 млн событий безопасности?[1] Крупные предприятия ежегодно расходуют 1,3 млн долл. США только на ошибочные срабатывания системы безопасности. Это равнозначно 21 000 часов расследований.[2] Среди данных, которые должны отслеживать аналитики, — более чем 75 000 известных уязвимостей программного обеспечения, о которых сообщается в Национальной базе данных уязвимостей.[3] Кроме того ежегодно публикуется более 1 млн бюллетеней, отчетов об угрозах и новостных статей.[4] Еще одна сложная задача — сортировка существующих данных. Типичная организация использует лишь 8 % неструктурированных данных, таких как блоги и видео. [5] Тем не менее, ожидается, что группы безопасности будут работать быстро.

IBM QRadar Advisor with Watson обеспечивает анализ безопасности на основе огромных объемов структурированных и неструктурированных данных. Это решение помогает преобразовать возможности центра операций по обеспечению безопасности (SOC), устраняя такие проблемы, как нехватка квалифицированных кадров, аварийные перегрузки, задержки реагирования на инциденты, устаревшая информация о безопасности и риски процессов, и может быть загружено за несколько минут из IBM Security App Exchange.

▸ Начать работу с бесплатной 30-дневной пробной версией QRadar Advisor with Watson.

«Уровень шума очень высок; человеческий мозг не может обрабатывать все изо дня в день. Нам нужна помощь, что-то вроде ИИ или когнитивных технологий».

— Чед Холмс (Chad Holmes), директор по киберстратегии, технологиям и развитию, Ernst & Young LLP

1 ‘IBM X-Force Threat Intelligence Index 2017,’ *(Индекс анализа угроз IBM X-Force, 2017 г.), IBM X-Force,* март 2017 г.
2 ‘The cost of malware containment,’ *(Затраты на сдерживание распространения вредоносного ПО), Ponemon,* январь 2015 г.
3 ‘National Vulnerability Database,’ *(Национальная база данных уязвимостей), Computer Security Resource Center,* Национальный институт стандартов и технологий, просмотрено 18 марта 2017 г.
4 ‘Когнитивная система безопасности помогает бороться с киберугрозами,’ *SecurityIntelligence,* 10 мая 2017 г.
5 ‘IBM Watson помогает бороться с киберпреступлениями,’ *IBM Corp.,* 10 мая 2016 г.

Используйте огромный объем знаний по безопасности

Решение Watson for Cyber Security, созданное на основе IBM Cloud, обеспечивает масштабную когнитивную систему безопасности, используя возможность анализировать и изучать неструктурированные данные, составляющие примерно 80 % всех данных,[1] которые не могут обрабатывать традиционные инструменты обеспечения безопасности.

Watson for Cyber Security использует базовую технологию Watson для сбора, анализа и изучения сведений о проблемах и угрозах безопасности на основе широкого спектра материалов, начиная с сообщений в блогах и научных публикаций и до предупреждений безопасности от правительственных учреждений. Используя обработку естественного языка, Watson for Cyber Security помогает понять естественный язык в неструктурированных данных, которые ранее были недоступны для систем обеспечения безопасности организации. Это позволяет анализировать информацию, относящуюся к конкретным инцидентам безопасности, помогая выявлять и анализировать угрозы. Работая и со структурированными, и с неструктурированными данными безопасности, Watson for Cyber Security расширяет возможности аналитиков получать новую информацию и быстро и более уверенно реагировать на угрозы.

Используя Watson for Cyber Security в качестве доверенного советника, аналитики безопасности могут анализировать инциденты безопасности, опираясь на постоянно растущий и адаптируемый комплекс знаний, выполняющий когнитивное исследование подозрительных действий и поведения и идентифицирующий как основные причины, так и дополнительные индикаторы нарушений и связанных с ними объектов угроз. Это мощное решение обучается, адаптируется и, в отличие от людей, не забывает данные, которые собирает. В результате оно может предоставить группам безопасности в 10 раз больше аналитической информации для выявления новых угроз.[1] Более того, являясь исключительно решением SaaS (ПО как услуга), Watson for Cyber Security не требует дополнительного оборудования или глубокой квалификации аналитиков на местах.

менее 1 минуты

необхдимо решению Watson for Cyber Security для комплексного анализа, на который сотрудник затратил бы более часа.[2]

Огромный объем знаний в области безопасности

Watson for Cyber Security отслеживает более 10 миллиардов соответствующих узлов безопасности, которые часто не замечают аналитики безопасности.

1 Кристи Шнайдер (Christie Schneider), "Самые большие проблемы с данными, о которых вы, возможно, даже не знаете," *блоги IBM Watson,* 25 мая 2016 г.

2 Результаты, полученные клиентами, которые принимали участие в программе бета-тестирования решения QRadar Advisor with Watson.

Анализ и идентификация сложных угроз безопасности

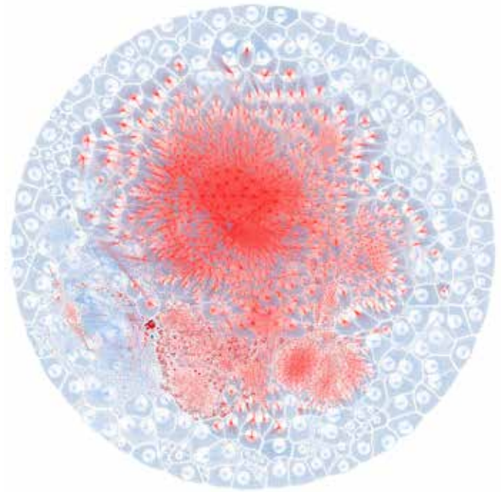
Платформа IBM QRadar Security Intelligence Platform анализирует миллионы событий и сетевых потоков в минуту для обнаружения современных угроз в рамках всего предприятия. Watson for Cyber Security расширяет возможности QRadar, используя функциональность когнитивных вычислений Watson. Решение предоставляет аналитикам безопасности доверенного советника для расследования и классификации инцидентов и аномалий безопасности на основе огромного количества структурированных и неструктурированных данных.

Принцип работы

Когда нарушение или инцидент QRadar делегируется в QRadar Advisor with Watson, решение сначала выполняет локальный сбор данных на основе характерных признаков нарушения для получения дополнительного контекста для инцидента, а затем разрабатывает запрос на исследование угрозы для выполнения анализа нарушения с использованием возможностей Watson for Cyber Security. Объединяя локальные и внешние знания, QRadar Advisor with Watson повышает эффективность и облегчает исследование угроз.

На основе характерных признаков, полученных в виде запроса на исследование угрозы из QRadar Advisor, Watson for Cyber Security использует свою обширную базу знаний, собранную из миллионов источников, включая источники информации об угрозах, веб-сайты, форумы и бюллетени, для дальнейшего анализа. Watson for Cyber Security получает информацию, собирает индикаторы нарушений и обнаруживает другие объекты угроз, связанные с первоначальным нарушением, такие как вредоносные файлы, подозрительные IP-адреса или неавторизованные объекты, и использует логику для определения отношений между этими объектами. QRadar Advisor with Watson затем усекает эту информацию, чтобы сосредоточиться на ключевых сведениях, относящихся к текущему нарушению.

Затем аналитики могут предпринять дальнейшие действия на основе анализа, предоставленного QRadar Advisor with Watson, отправив информацию о нарушении вместе с подтверждающими доказательствами и ключевыми сведениями, полученными от Watson, группе реагирования на инциденты для исправления.



QRadar Advisor with Watson опирается на более чем 1 миллион документов по безопасности, собранных Watson, чтобы описать весь контекст и область действия атаки.

- Узнайте, как технология IBM Watson помогла предупредить энергетическую компанию о текущей атаке.

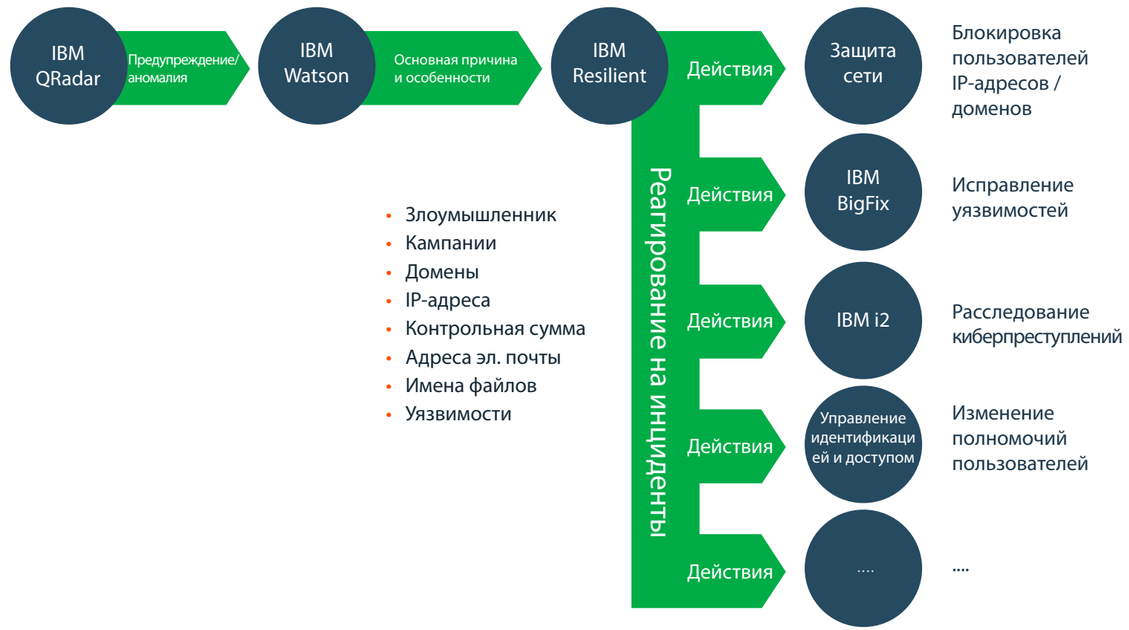
1 ‘Аналитический отчет об угрозах IBM X-Force Threat Intelligence Report, 2016 г.‘ *IBM Corp.*, февраль 2016 г.

2 ‘IBM 2016 Cost of Data Breach Study: Global analysis (IBM, 2016 г. Изучение стоимости нарушения безопасности данных: глобальный анализ),‘ *IBM Corp.*, июнь 2016 г.

Быстрый поиск по огромному объему знаний для ускорения реагирования на инциденты

Как показали недавние глобальные атаки на кибербезопасность, киберпреступники наносят удары быстро, часто неожиданно, и скорость — ваше самое главное оружие, чтобы противостоять им. Таким образом, решение QRadar Advisor with Watson будет полезно независимо от того, нужно ли помочь сформировать защиту против потенциальных угроз или обеспечить целенаправленную точность противодействия атаке, которая уже произошла. Оно позволяет использовать знаниях, которые есть в Watson о конкретном инциденте безопасности, оценить доказательства и предоставить аналитикам необходимую информацию для принятия дальнейших мер.

Ускорение комплексного процесса реагирования на инциденты



QRadar Advisor with Watson позволяет немедленно использовать когнитивный анализ безопасности и действовать на его основе.

«QRadar указал на нарушение со стороны пользователя, пытающегося подключиться к IP-адресу бот-сети. Аналитик безопасности вручную обнаружил 5 связанных индикаторов, а система Watson указала степень угрозы с использованием более 50 полезных индикаторов».

— крупная энергетическая компания.[1]

60раз

увеличение скорости, которое обеспечиваетQRadar Advisor with Watsonпо сравнению с исследованием угроз вручную.[1]

1 Результаты, полученные клиентами, которые принимали участие в программе бета-тестирования решения QRadar Advisor с Watson.

Обеспечьте анализ, скорость и точность

Аналитика: насущная необходимость

Некоторые потенциальные угрозы легко устранить. Попытка доступа к базе данных в выходной день может просто означать, что сотрудник работает из дома. Но в случае сложных атак могут помочь когнитивные методики, предлагаемые решением QRadar Advisor with Watson. Оно может собирать и сопоставлять огромные объемы доступных структурированных и неструктурированных данных безопасности для выявления новых шаблонов угроз, приоритизации угроз и предоставления надежных рекомендаций. QRadar Advisor with Watson делает выводы и проводит анализ на основе своей обширной базы данных по безопасности, чтобы представить информацию, наиболее актуальную для данного расследования.

Скорость: насколько нужно торопиться?

Даже наиболее точный анализ бесполезен, если выполнен слишком поздно. Возможность выявлять и анализировать угрозы за считанные минуты имеет важнейшее значение для надлежащего реагирования и предотвращения крупномасштабной атаки.

Watson обеспечивает когнитивное преимущество для обнаружения скрытых угроз с помощью автоматического анализа, позволяя аналитикам использовать большие объемы структурированных и неструктурированных данных в режиме реального времени при исследовании потенциальных угроз.

Точность: важно распознать

Надежность системы безопасности напрямую зависит от ее точности, как при согласованном обнаружении реальных угроз, так и при исключении ложных срабатываний. Поиск баланса может оказаться сложной задачей. Киберпреступники полагаются на доступ по тем же каналам, которые используют законные пользователи и приложения, поскольку знают, что вы не можете проверить каждый пакет заранее. QRadar Advisor with Watson обеспечивает вам преимущество в виде современных методов обнаружения и идентификации, позволяющих точно классифицировать инциденты и останавливать угрозы.

«…аналитики уровней 1 и 2 пришли к заключению, что это не инцидент безопасности. Исследование с помощью Watson содержало более ценную информацию. Система выполнила классификацию за считанные минуты и определила, что один из хостов нашего клиента подвергся DDoS-атаке».

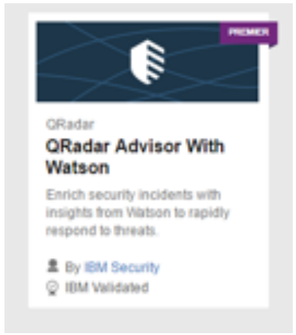
— клиент QRadar Advisor with Watson

- Смотрите видеоролик и узнайте, как решение QRadar Advisor with Watson выявило вредоносное ПО Poison Ivy.

30-дневная пробная версия QRadar Advisor with Watson

Узнайте, как возможности когнитивного анализа могут помочь вашей организации, установив это приложение. Решение QRadar Advisor with Watson доступно для текущих заказчиков QRadar в виде бесплатной 30-дневной пробной версии. Его можно установить за считанные минуты с IBM Security App Exchange, специализированного веб-сайта для расширений и дополнений приложений для продуктов IBM Security. По окончании пробного периода можно легко преобразовать пробную версию в подписку на услугу, используя лицензионный ключ.

Используйте QRadar Advisor with Watson с уверенностью
Киберпреступники используют шаблоны уязвимостей, и решение QRadar Advisor with Watson может помочь вам выявить и понять эти угрозы. После установки QRadar Advisor with Watson на стороне клиента с использованием локального или облачного экземпляра QRadar приложение безопасно связывается с его облачным партнером, Watson for Cyber Security. Ваши сетевые данные остаются полностью защищенными. QRadar Advisor with Watson не отправляет в облако файлы журналов или конфиденциальную корпоративную информацию. Вместо этого решение извлекает информацию из Watson, используя имена файлов и анонимные идентификаторы того типа, который многие организации уже используют для сканирования и других функций безопасности.



QRadar Advisor with Watson можно за считанные минуты загрузить с веюб-сайта IBM Security App Exchange.

Существующие заказчики могутзагрузить

бесплатную 30-дневную пробную версию

QRadar Advisor with Watson.

Преимущества решений IBM

Благодаря использованию лучших в отрасли когнитивных возможностей для обеспечения безопасности Watson может стать вашим доверенным советником в анализе огромных объемов структурированных и неструктурированных данных. QRadar Advisor with Watson обеспечивает совместную работу QRadar и Watson над огромными массивами данных. Решение поможет выявлять новые шаблоны угроз, обеспечивать более быстрый и точный анализ угроз безопасности и экономить драгоценное время и ресурсы для обеспечения безопасности предприятия. Решение QRadar Advisor with Watson может и удовлетворить сложные требования к безопасности, обеспечив современную аналитику, и дополнить возможности ограниченной группы безопасности. Оно предоставляет передовую технологию IBM, которая помогает снизить риск безопасности предприятия.

Дополнительная информация

Для получения дополнительной информации о решении QRadar Advisor with Watson обратитесь к представителю илибизнес-партнеру IBM либо посетите следующий веб-сайт: **ibm.com**/us-en/marketplace/cognitive-security-analytics

О решениях IBM Security

Подразделение IBM Security предлагает один из наиболее современных и интегрированных портфелей продуктов и услуг для обеспечения безопасности корпоративного уровня. Этот портфель, поддерживаемый всемирно известными исследованиями и разработками IBM X-Force, обеспечивает анализ безопасности и помогает организациям в формировании целостного подхода к защите людей, инфраструктур, данных и приложений, предлагая решения для управления идентификационными данными и доступом, обеспечения безопасности баз данных, разработки приложений, управления рисками, управления конечными устройствами, обеспечения безопасности сети и многое другое. С помощью этих решений организации могут эффективно управлять рисками и внедрить интегрированную систему безопасности для мобильных устройств, облачных систем, социальных сетей и других корпоративных бизнес- архитектур. Компания IBM обеспечивает работу одной из крупнейших в мире организаций по исследованиям, разработке и доставке решений безопасности, проводит мониторинг 15 миллиардов событий безопасности в более чем 130 странах в день, а также владеет более чем 3000 патентов в области безопасности.

IBM

IBM Восточная Европа/Азия
123317, М осква
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

WGS03087-RURU-01