IBM Security QRadar Incident Forensics
версия 7.2.6

Руководство пользователя

Примечание

Прежде чем начинать пользоваться этой информацией и поддерживаемым ею продуктом, прочтите информацию в разделе “Замечания” на стр. 39.

Информация о продукте

Этот документ относится к IBM QRadar Security Intelligence Platform V7.2.6 и к последующим выпускам, если не будет заменен обновленной версией данного документа.

Содержание

Введение в использование Экспертиза инцидентов IBM Security QRadar

Это руководство содержит информацию об исследовании инцидентов защиты с использованием Экспертиза инцидентов IBM® Security QRadar.

Для кого предназначена эта книга

Исследователи извлекают информацию из сетевого трафика и документов в экспертном репозитории. Эта информация используется при исследовании инцидентов защиты.

Техническая документация

Чтобы найти документацию по продукту IBM Security QRadar в Интернете, включая всю переведенную документацию, получите доступ к центру знаний IBM (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Информацию о том, как получить доступ к дополнительной технической документации в библиотеке продуктов QRadar, смотрите в документе Техническое замечание по получению доступа к документации IBM Security (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Как обратиться в службу поддержки заказчиков

Информацию о том, как обратиться в службу поддержки заказчиков, смотрите в документе Техническое замечание по поддержке и загрузке (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Заявление о рекомендуемых методах защиты

Защита ИТ-систем включает в себя защиту систем и информации за счет предотвращения, обнаружения и реакции на неправильный доступ из вашего предприятия и извне вашего предприятия. Неправильный доступ может привести к изменению, уничтожению, незаконному присвоению или неправильному использованию информации либо может вызвать повреждение или неправильное использованием ваших систем, включая использование для атак на других людей. Никакие ИТ-системы или продукты не должны считаться полностью защищенными, и никакой один продукт, служба или мера защиты не могут быть полностью эффективны для предотвращения неправильного использования или доступа. Системы, продукты и службы IBM разработаны как часть правомерного комплексного подхода к защите, который обязательно включает в себя дополнительные рабочие процедуры и может потребовать максимальной эффективности других систем, продуктов или служб. IBM НЕ ГАРАНТИРУЕТ, ЧТО КАКИЕ-ЛИБО СИСТЕМЫ, ПРОДУКТЫ ИЛИ СЛУЖБЫ ОКАЖУТСЯ НЕ ПОДВЕРЖЕНЫ ВРЕДНОМУ ИЛИ НЕЗАКОННОМУ ПОВЕДЕНИЮ ЛЮБОЙ СТОРОНЫ И НЕ ОБЕСПЕЧИВАЕТ ВАШЕМУ ПРЕДПРИЯТИЮ ЗАЩИТУ ОТ ТАКОВЫХ.

Пожалуйста, обратите внимание:

Использование этой Программы может затрагивать различные законы или нормативы, включая те из них, которые связаны с конфиденциальностью, защитой данных, наймом на работу и электронными взаимодействиями и хранением. IBM Security QRadar можно использовать только для законных целей и правомерным образом. Заказчик соглашается использовать эту Программу в соответствии с применимыми законами, нормативами и правилами политики и принимает на себя всю ответственность за их соблюдение. Лицензиат соглашается с тем, что он получил или получит все согласия, разрешения или лицензии, необходимые для правомерного использования им продукта IBM Security QRadar.

Примечание

Продукт Экспертиза инцидентов IBM Security QRadar предназначен, чтобы помочь компаниям улучшить среду защиты и данные. Если быть более точным, продукт Экспертиза инцидентов IBM Security QRadar обеспечивает компаниям помощь в исследовании и понимании того, что происходит в инцидентах защиты сети. Этот инструмент позволяет компаниям индексировать данные захваченных сетевых пакетов (PCAP) и производить в них поиск, а также содержит функцию, которая позволяет реконструировать такие данные обратно в их исходный вид. Эта функция реконструкции позволяет реконструировать данные и файлы, включая сообщения электронной почты, файлы и вложения изображений, телефонные звонки VoIP и веб-сайты. Дополнительная информация относительно возможностей Программы и ее функций, а также того, как их можно сконфигурировать, содержится в руководствах и прочей документации, прилагаемой к программе. Использование этой Программы может затрагивать различные законы или нормативы, включая те из них, которые связаны с конфиденциальностью, защитой данных, наймом на работу и электронными взаимодействиями и хранением. Продукт Экспертиза инцидентов IBM Security QRadar можно использовать только для законных целей и правомерным образом. Заказчик соглашается использовать эту Программу в соответствии с применимыми законами, нормативами и правилами политики и принимает на себя всю ответственность за их соблюдение. Лицензиат соглашается с тем. что он получил или получит все согласия, разрешения или лицензии, необходимые для правомерного использования им продукта Экспертиза инцидентов IBM Security QRadar.

Глава 1. Что нового для пользователей в Экспертиза инцидентов QRadar V7.2.6

В Экспертиза инцидентов IBM Security QRadar V7.2.6 появились новые инструменты исследования, которые помогут вам анализировать файлы и изображения, чтобы выявить подозрительное содержимое или поведение. Вы также можете проанализировать связи, показывающие взаимосвязи или соединения между веб-страницами и сотрудниками компании.

Анализ артефактов для подозрительного или несанкционированного содержимого

Анализ артефактов можно использовать для исследования инцидентов, например, чтобы установить, как система оказалась зараженной и были ли аналогичным образом подвергнуты риску другие активы.

Например, можно использовать возможности анализа файлов для восстановленных данных пакетов, чтобы увидеть список всех файлов и узнать, содержат ли они встроенные файлы или сценарии.

Вы можете посмотреть на файлы изображений, которые были помечены флагами, как те, в которых есть подозрительное содержимое и встроенные сценарии.

Эта оценка и распределение энтропии файлов поможет вам выявить аномалии файлов и обеспечит доказательства того, что данный файл содержит вредоносные (хакерские) программные средства, которые проскользнули незамеченными и отвечают за заражение систем.

Чтобы определить, могли ли быть затронуты другие системы, можно использовать анализ ссылок, чтобы быстро визуализировать все просмотренные веб-сайты и подмножество действий по доступу к зараженному веб-хосту.

 Узнать подробнее...

Глава 2. Исследования защиты

Используя Экспертиза инцидентов IBM Security QRadar, вы можете обнаруживать появляющиеся угрозы, определять их коренные причины и предотвращать их повторение. Используя инструменты экспертизы, вы сможете быстро направить свой анализ на выявление того, кто инициировал угрозу, как это было сделано и какие нарушения были произведены.

Будучи экспертным исследователем, вы можете производить повторную трассировку пошаговых действий кибер преступников и реконструировать неструктурированные сетевые данные, связанные с инцидентом защиты.

Когда ваша организация впервые узнает об угрозе, потенциальном риске в отношении защиты или нарушении совместимости, вы задает цели, чтобы оценить область, выявить вовлеченные объекты и понять мотивацию.

Вы можете использовать инструменты в Экспертиза инцидентов IBM Security QRadar в отдельных сценариях в исследованиях разного типа, например, исследованиях сетевой защиты, инсайдерском анализе, исследовании мошенничества и злоупотреблений, а также при сборе доказательств.

1. Восстановите и реконструируйте сетевые сеанса с IP-адреса и на IP-адрес.
2. В созданных инцидентах можно запросить категории атрибутов, чтобы собрать доказательства.

   При создании восстановления создается инцидент.
3. Используйте фильтры поиска, чтобы получить только ту информацию, которая вас интересует.
4. В зависимости от типа исследования выберите экспертный инструмент, который даст вам нужные доказательства.

Подозрительное содержимое

Можно использовать поиск, чтобы найти любой контекстный элемент или идентификатор, который, как вам известно, связан с атакующим или инцидентом. Если вы используете ключевое слово при поиске, будет возвращено подозрительное содержимое. Часть подозрительного содержимого может относиться к исследованию.

Поворот данных

Поворот данных достигается за счет того, что содержимое, возвращенное в результатах поиска, становится активной ссылкой. Например, если вы ищете слово `"Иван"`, результаты могут содержать сообщения электронной почты, написанные Иваном, чаты Ивана и более подробную контекстную информацию. Если вы щелкнете по сообщению электронной почты, чтобы его просмотреть, каждый актив или объект (например, вложения или ID компьютера, который использовал Иван) появится в виде ссылки. Исследователь может использовать эти ссылки, чтобы быстро провести расследование.

Цифровой оттиск

Используйте цифровой оттиск, чтобы проверить данные и отобразить взаимосвязи между объектами, например, IP-адресами, именами и MAC-адресами, на основе

частоты. Можно выбрать один или более результатов, чтобы увидеть частоту и направление взаимосвязи.

Досмотр

Используйте досмотр, чтобы увидеть временную шкалу действий, позволяющую произвести перетрассировку атаки. Досмотр перестроит сеанс и рассортирует документы по времени.

Фильтр содержимого

Используйте фильтр содержимого, чтобы взглянуть на подмножество категорий содержимого, например, веб-почту и порнографию, чтобы удалить шум или нерелевантную информацию при поиске.

Исследования защиты сети

Экспертиза инцидентов QRadar можно использовать для обнаружения и исследования злонамеренных операций, направленных на критически важные активы. Вы можете использовать встроенные инструменты экспертизы, которые помогут вам устранить нарушение защиты сети и предотвратить ее повторное появление.

Используйте инструменты исследований Экспертиза инцидентов QRadar, которые помогут вам определить, как произошло событие, свести к минимуму его влияние и выполнить все, что позволит предотвратить другое нарушение.

Нулевой пациент: Выявить источник атаки

В этом сценарии организацию оповещают о подозрительном нарушении. Она старается найти первоначальную точку атаки, чтобы выявить источник. Организация должна поместить затронутые нарушением объекты в карантин, чтобы не допустить распространения атаки на другие части организации.

Цели

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Определить тип атаки.
- Выявите первоначальную точку входа угрозы.
- Получить сведения о злонамеренной служебной нагрузке.
- Определите, как злонамеренная служебная нагрузка распространялась вне точки входа.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти симптоматические атрибуты, связанные со злонамеренной служебной нагрузкой.
2. Используйте категории содержимого, чтобы при помощи фильтра убрать содержимое, не связанное с исследованием.
3. Изучите подозрительное содержимое, которое продукт пометил флагами.

4. Используйте цифровые оттиски и визуализации, чтобы исследовать расширенные взаимосвязи злонамеренной служебной нагрузки, виновника или объекта назначения.
5. Используйте поворот данных и следуйте за связями данных, чтобы выявить "нулевого пациента".
6. Используйте досмотр, чтобы увидеть временную шкалу действий, позволяющую произвести перетрассировку атаки.

Скомпрометированные системы

В этом сценарии организацию оповещают о том, что одна или несколько ее систем были скомпрометированы такой кибер атакой, как утечка, фишинг, лобовая атака или внедрение SQL.

Цели

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Определить степень нарушений в организации.
- Понять тип рабочего риска нарушений в каждой системе.
- Вскрыть все периферийные действия, которые были выполнены при первоначальной атаке, чтобы обойти операции по очистке и обнаружение.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти злонамеренную служебную нагрузку или скомпрометированный актив.
2. Изучите подозрительное содержимое, которое продукт пометил флагами.
3. Используйте цифровые оттиски и визуализации, чтобы исследовать взаимосвязи объектов, возникшие из скомпрометированных систем.
4. Используйте досмотр, чтобы увидеть временную шкалу действий, позволяющую произвести перетрассировку атаки.
5. Выявите противоречия или подозрительные взаимодействия между категориями данных, используя поиск в произвольной форме, поворот данных и анализ подозрительного содержимого.

Данные, попавшие к неавторизованным объектам

В этом сценарии организацию оповещают о том, что конфиденциальные данные попали к неавторизованным объектам в организации или к внешним сторонам.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Определить характер и объем упущенных данных.
- Постараться понять, какие методы были использованы.
- Выявить виновников.
- Выявить источник утечки.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы находить идентификаторы упущенных данных.
2. Изучите подозрительное содержимое, которое продукт пометил флагами.
3. Проверьте полный объем упущенных или упускаемых данных, проверяя реконструкцию данных.
4. Используйте цифровой оттиск и визуализации, чтобы исследовать все затронутые взаимосвязи объектов.
5. Используйте досмотр, чтобы увидеть временную шкалу действий, позволяющую произвести перетрассировку атаки.
6. Используйте поиск в произвольной форме, чтобы определить мотивации при утечке данных.
7. Используйте поворот данных, чтобы найти утечки других данных, которые также могли быть упущены.

Исследования путем инсайдерского анализа

Используйте Экспертиза инцидентов QRadar, чтобы обнаруживать тайный сговор, саботаж и неправильное использование прав доступа. Выявите виновника, сотрудничающих с ним работников, определите, в каких системах есть нарушения и каковы потери данных в документах.

Неправильное использование прав доступа

В этом сценарии организацию оповещают о том, что один или несколько ее сотрудников неправильно используют учетные данные или используются как прокси, чтобы получить доступ к секретным системам и данным для выполнения неавторизованных операций.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Определить идентификатор пользователя.
- Выяснить, кто или что использует идентификатор для выполнения несанкционированных действий.
- Понять цель неправильного использования права доступа.
- Оценить, есть ли у объекта другие идентификаторы, которые также могут неправильно использоваться.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти идентификаторы, получающий доступ к секретным системам или данным.
2. Выясните, какие из этих попыток доступа являются подозрительными, анализируя подозрительное содержимое, выполняя поиск в произвольной форме, поворот данных и применяя фильтры к содержимому.

3. Просмотрите реконструкцию данных для содержимого, к которому осуществляется доступ.
4. Проследите все шаблоны доступа и оцените частоту в инструменте Досмотр.
5. Используйте цифровые оттиски, чтобы вскрыть алиасы, используемые одним объектом.

Тайный сговор

В этом сценарии организацию оповещают о том, что один или несколько акционеров сговариваются друг с другом или с внешними сторонами, чтобы выполнить операции, причиняющие вред организации.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Определить тайно сговаривающиеся объекты.
- Понять характер и шаблоны взаимодействий между сообщниками.
- Вскрыть содержимое, лежащее в основе схемы.
- Определить длительность действия схемы, чтобы понять область риска.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы находить идентификаторы затронутых объектов.
2. Изучите подозрительное содержимое, которое продукт пометил флагами.
3. Используйте цифровой оттиск, визуализации и фильтры содержимого, чтобы выявить взаимосвязи, которые могут оказаться подозрительными.
4. Используйте досмотр, чтобы отследить операции затронутых объектов и получить содержимое взаимодействий.
5. Выявите мотивы сговора, проверяя реконструированные документы.
6. Используйте поиск в произвольной форме и поворот данных, чтобы находить начало тайно согласующихся операций.

Саботаж

В этом сценарии организацию оповещают о том, что один или несколько акционеров пытаются нарушить операции. Акционер может использоваться как прокси.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Выявить саботажника.
- Постараться понять, какие методы применял саботажник.
- Оценить влияние и область нарушения.
- Выявить уязвимости, используемые саботажником.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти признаки саботажа.
2. Изучите подозрительное содержимое, которое продукт пометил флагами.
3. Используйте визуальную навигацию, цифровой оттиск и фильтры содержимого, чтобы изучить симптомы и обнаружить идентификаторы саботажника.
4. Используйте досмотр, чтобы отследить операции саботажника.
5. Используйте реконструкцию данных, чтобы обнаружить роли и мотивации саботажника.
6. Используйте реконструкцию данных, чтобы проверять содержимое, которое использовал саботажник.
7. Используйте поиск в произвольной форме, досмотр и анализ подозрительного содержимого, чтобы выявить скомпрометированные системы и процедуры, которые сделали саботаж возможным.

Исследования мошенничества и нарушений режимов

Используйте Экспертиза инцидентов QRadar для нахождения неавторизованных транзакций, несанкционированного распределения ресурсов, отклонений от протокола и уклонения от правового контроля.

Неавторизованные транзакции

В этом сценарии организацию оповещают о том, что неавторизованные транзакции отрицательно влияют на бизнес-операции в финансовом отношении.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Найти неавторизованные транзакции.
- Выявить затронутые объекты, которые отвечают за неавторизованные транзакции.
- Определить частоту и тенденции неавторизованных транзакций.
- Оценить область риска неавторизованных транзакций.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти все противоречивые или подозрительные транзакции.
2. Используйте поиск в произвольной форме и поворот данных, чтобы находить повторы этих транзакций.
3. Используйте поворот данных и цифровой оттиск, чтобы обнаруживать объекты, связанные с подозрительными транзакциями.
4. Вскройте содержимое транзакций, чтобы определить количественное значение, проверяя реконструированные документы.

Несанкционированное выделение ресурсов

В этом сценарии организация подозревает несанкционированное распределение ресурсов, которое отрицательно влияет на бизнес-операции в финансовом отношении.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Найти неправильное выделение ресурсов.
- Выявить затронутые объекты, которые отвечают за неправильное распределение ресурсов.
- Понять мотивацию несанкционированного распределения ресурсов.
- Оценить размер и область неправильно распределенных ресурсов.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме для нахождения взаимодействий, связанных с выделенными ресурсами.
2. Используйте поиск в произвольной форме, поворот данных и цифровой оттиск, чтобы найти идентификаторы объектов, производящих несанкционированное выделение ресурсов.
3. Обработайте содержимое затронутых взаимодействий, чтобы оценить мотивы, проверяя реконструированные документы и используя визуализации.
4. Используйте досмотр, чтобы произвести повторную трассировку операций по распределению и узнать количество неправильно выделенных ресурсов.

Отклонения от протоколов и действия в обход правовых регуляторов

В этом сценарии организацию оповещают о том, что были произведены действия в обход интересов бизнеса, протоколов ИТ и правовых регуляторов, что может оказать отрицательное влияние в финансовом отношении.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Оценить, какие протоколы или правовые регуляторы были обойдены.
- Выявить объекты, вовлеченные в такое поведение.
- Понять мотивацию этих объектов.
- Оценить, насколько глубоко распространилось это аномальное поведение.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти бизнес-процессы, управляемые протоколами или регуляторами.

2. Используйте поиск в произвольной форме, поворот данных и реконструкцию данных, чтобы создать перекрестные ссылки с документацией, в которой даны общие сведения о протоколах и способах правового контроля.
3. Используйте фильтры содержимого и поиск в произвольной форме, чтобы обнаружить конкретные экземпляры, в которых производились действия в обход протоколов/регуляторов.
4. Используйте цифровой оттиск, визуализации, поворот данных и фильтры содержимого, чтобы найти связанные идентификаторы объектов.
5. Используйте досмотр, чтобы повторно отследить операции объектов для изучения возможной мотивации.

Исследования сбора доказательств

Используйте Экспертиза инцидентов QRadar, чтобы оценить риск уязвимостей в организации, определить достоверность выявления угроз или виновных и уточнить методики защиты.

Достоверность при выявлении угроз

В этом сценарии организацию оповещают об определенной угрозе, использовании или уязвимости. Чтобы обосновать усилия по ликвидации последствий, которые в противном случае могли бы конкурировать с обычными бизнес-операциями, они хотят определить интервал достоверности для всех связанных рисков.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Оценить чувствительность к риску нарушения защиты.
- Определить, есть ли свидетельство риска нарушения защиты.
- Оценить область действия и денежное влияние риска защиты.
- Понять характер риска защиты.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, анализ подозрительного содержимого и поворот данных, чтобы находить угрозы, злонамеренную эксплуатацию или уязвимости с использованием потенциально направленных объектов в качестве отправной точки.
2. Используйте поиск в произвольной форме и поворот данных, чтобы скомпилировать вхождения.
3. Используйте поиск в произвольной форме, чтобы создавать перекрестные ссылки на документы, которые могут содержать информацию по влиянию.
4. Используйте цифровой оттиск и визуализации, чтобы выявить затронутые объекты.
5. Используйте досмотр, чтобы проанализировать действия, связанные с угрозой или виновным.

Уточнение практических методов защиты

Обнаружение нового и рискованного поведения дает организации повод оценить, являются ли достаточными существующие практические методы защиты. В этом

сценарии организация стремится оценить эффективность своих правил защиты в отношении рисков, с которыми она сталкивается.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Распознать новое или рискованное поведение.
- Оценить эффективность существующих правил защиты.
- Определить пробелы в защите, возникшие из-за динамических операций.
- Оценить эффективность предложенных практических методов защиты.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти новое или рискованное повешение, например, для мобильных пользователей и служб на основе облака, используя знания о домене и организации.
2. Изучите подозрительное содержимое и используйте инструмент Досмотр, чтобы создать перекрестные ссылки между этим поведением и существующими правилами или практическими методами защиты.
3. Используйте поиск в произвольной форме, досмотр, реконструкцию содержимого и визуализацию, чтобы проанализировать оповещения от правил защиты для определения частоты ложноположительных событий.
4. Используйте поиск в произвольной форме, досмотр, реконструкцию содержимого, поворот данных и визуализацию, чтобы обнаруживать ложноположительные события, которые не обнаруживаются с использованием существующих правил или методов защиты.

Оценка риска

В этом сценарии бюллетень защиты, в котором описаны отдельные уязвимости, способы эксплуатации или злонамеренное поведение, предлагает организации провести оценку рисков. Оценка рисков определяет, является ли организация восприимчивой к рискам, или она уже скомпрометирована.

Цель

Чтобы устранить проблему в этих исследованиях, у организации есть следующие цели:

- Оценить наличие выявленных уязвимостей в организации.
- Обнаружить злонамеренное присутствие внешних сторон.
- Вскрыть свидетельства любых нарушений.
- Определить, является ли организация жертвой использования не по назначению.
- Определить идентификатор пользователя.

Исследование

Используйте инструменты на вкладке **Экспертиза**, которые помогут вам произвести исследование.

1. Используйте поиск в произвольной форме, чтобы найти признаки уязвимостей, неправильного использования или другого злонамеренного поведения, указанного в бюллетене защиты.
2. Используйте поиск в произвольной форме, чтобы произвести исследование перекрестных ссылок или других данных, чтобы получить индикаторы.
3. Используйте досмотр, чтобы исследовать взаимодействия, которые могли эксплуатировать выявленные уязвимости.
4. Изучите подозрительное содержимое, которое продукт пометил флагами.
5. Используя реконструкцию данных, проверьте содержимое, которое лежит в основе потенциально рискованных взаимодействий.
6. Используйте досмотр, чтобы повторно отследить операции потенциально рискованных объектов.

Глава 3. Начинаем работу с исследованиями по экспертизе

Чтобы приступить к работе с исследованиями в области экспертизы в Экспертиза инцидентов IBM Security QRadar, используйте меню **Быстрый старт**, чтобы перемещаться от опции к опции и применять фильтр к данным, находящимся в репозитории экспертизы. Эта панель запуска содержит заранее заданные сводные запросы, которые можно использовать для запуска поиска или получения взаимосвязей для объекта.

Чтобы приступить к работе, выполните следующие рекомендации:

1. Начинайте восстановление экспертизы или поиск с нарушения на вкладке **Нарушения**.
   - Если вы щелкнете правой кнопкой мыши по любому IP-адресу и запустите восстановление экспертизы, экспертиза получит неструктурированные данные захвата для указанных диапазонов времени с устройства захвата, извлечет и перестроит документы, а затем добавит результаты в репозиторий экспертизы.
   - Если вы щелкнете правой кнопкой мыши по нарушению или любому IP-адресу и запустите поиск экспертизы, к репозиторию экспертизы будет применен фильтр и будет произведен поиск этого IP-адреса. После этого результаты будут показаны в основной сетке на вкладке **Экспертиза**. Вы можете уточнить свой поиск, построив запросы.

   Когда Экспертиза инцидентов QRadar получает требование поиска, этот продукт обрабатывает данные захвата пакетов и переводит их обратно в формат, отправленный предполагаемому получателю. Документы Microsoft Word, например, восстанавливаются как файлы Word. Телефонные звонки голос-по-IP восстанавливаются как аудиофайлы. Восстановленные файлы затем индексируются с использованием метаданных и содержимого файлов, чтобы сделать их доступными для поиска.
2. На вкладке **Экспертиза** щелкните по **Быстрый старт**.

   После того как вы произведете восстановление или поиск вместо выполнения поиска в произвольном формате и построения своих собственных запросов, вы сможете быстро начать исследование, используя заранее заданные запросы из меню **Быстрый старт** на вкладке **Экспертиза**. Например, можно посмотреть на категорию **Подозрительное содержимое** и запустить один из запросов, например, **оповещение объектов**. *Подозрительное содержимое* основано на заданном наборе правил для содержимого, который указывает на подозрительные операции. *Оповещение объекта* помечает флагом возможный вредоносный объект, участвующий в нарушении политики защиты.

   Категоризация содержимого и возможности фильтров помогают сократить объем возвращенных данных
3. В **сетке** выберите документы, которые в хотите увидеть.

   Экспертиза инцидентов QRadar возвращает приоритизированные результаты поиска. Аналогично тому, как оптимизация механизма поиска приоритизирует сайты при поиске в Интернете, наиболее часто встречающиеся вхождения появляются в начале списка.

   Вы можете начать изменять представление данных, щелкая по ссылкам и производя поиск метаданных, связанных с документом. Возможности изменения представления данных обеспечивают различные представления поиска и сводки данных.

4. Чтобы исследовать взаимосвязи между всеми действиями и инцидентом защиты, выберите в представлении документа ссылку и щелкните правой кнопкой мыши по **Получить взаимосвязи для**.

   После исследования атрибутов примените фильтр к информации, собранной путем соединения объектов.

5. Щелкните по **Цифровые оттиски**, чтобы пройти по следу идентификатора и собрать скомпилированный набор связей.

   Цифровой оттиск - это индекс метаданных, которые могут помочь идентифицировать подозрительных атакующих или грубых нарушителей, следуя по следам злоумышленников. При построении этих взаимосвязей Экспертиза инцидентов QRadar использует данные из сетевых источников, например, IP-адресов, MAC-адресов, а также портов TCP и протоколов. Продукт может найти такую информацию, как ID чатов, и может прочитать такую информацию, как идентификатор автора, из приложений по работе с текстом или электронными таблицами. Цифровой оттиск может помочь вскрыть взаимосвязи, связывая идентификатор объекта с идентификационной информацией для других пользователей или объектов.

Поиск и закладки в Экспертиза инцидентов QRadar

Исследователи используют Экспертиза инцидентов IBM Security QRadar для извлечения соответствующих данных из сетевого трафика и документов.

Поиск записей и пометка их закладками

Чтобы включить операцию интуитивной экспертизы, Экспертиза инцидентов QRadar получает данные пакета и загружает другое содержимое. Эта технология обеспечивает управляемое поиском исследование данных, реконструкцию сеансов и экспертную аналитику в помощь исследованиям инцидентов защиты.

Исследователи производят исследования с применением грубо детализированных действий, а затем переходят к тонкой настройке обнаруженных явлений в релевантный конечный набор результатов. Простой высокоуровневый подход заключается в том, чтобы сначала производить поиск многих записей и помечать их закладками. Затем делается упор на помеченные закладками записи, чтобы выявить конечный набор записей. Определите, какой материал имеет отношение к делу и корректируйте запросы, чтобы включать или исключать элементы. Используйте этот материал, чтобы дать подтверждение гипотезе.

При разработке новых подходов вы можете проследить их, используя другие методы. Можно использовать инструменты визуализации и анализа, чтобы вручную и автоматически оценивать релевантность результатов. Также можно использовать различные запросы, чтобы получить другой взгляд на ту же проблему.

Обработка результатов, отмеченных закладками

Когда вы найдете результаты, имеющие значение для вашего исследования, вы можете пометить результаты закладкой, чтобы изучить их глубже и принять относительно их окончательное решение. Помечайте закладками больше материалов, чем вам, как вы считаете, потребуется. Если у вас есть вопросы по материалу, пометьте его закладкой. Вы хотите устранить нерелевантный материал и сфокусироваться на том, что, как вы думаете, является релевантным.

После того как вы пометите закладкой набор результатов, которые вам показались релевантными, вы можете точнее настроить свое изучение.

1. Изучите каждый помеченный закладкой документ при помощи инструментов визуализации и анализа.
2. Вложите в документы примечания по делам и примите окончательное решение по каждому документу относительно его релевантности в деле.
3. Если запись не является релевантной, удалите закладку.

   В процессе исследования вы выявили релевантный материал в репозитории, и теперь у вас есть набор релевантных записей, помеченных закладками.
4. Напечатайте, экспортируйте или обработайте релевантные записи.

Поиск и исследование документов

Исследователи производят поиск документов, релевантных по отношению к подходу или гипотезе относительно того, как произошел инцидент защиты.

Поиски

Вместо того, чтобы вручную просеивать массы документов, большинство из которых не связано с делом, исследователи используют экспертный репозиторий для извлечения документов, удовлетворяющих интересующим исследователя характеристикам. Например, документ, появившийся в определенный период времени, относится к интересующей вас теме, или документ был отправлен или получен предположительным атакующим.

Поиск может быть специализированным. Например, "найти точную строку символов “Миссия Альфа”" - это специализированный поиск. Либо поиск может быть общим. Например, "найти все номера карт социального страхования, где бы они не существовали в репозитории" - это более общий поиск.

Поиски могут быть простыми и основанными только на одном критерии. Результаты сложного поиска должны удовлетворять нескольким условиям. Например, поиск всей электронной почты между двумя предположительными атакующими, касающейся определенной темы и исключающей электронную почту, содержащую вложения - это сложный поиск. Цель поиска - быстро и точно сократить число записей до пригодного для управления рабочего набора. При меньшем наборе документов, которые будет изучать исследователь, у документов будет более высокая вероятность их релевантности по отношению к делу.

Запуск восстановления для IP-адреса или порта

Можно запустить восстановление для одного или нескольких IP-адресов или портов. Если вы не введете IP-адрес или порт, будет восстановлен весь трафик TCP и UDP. Если ввести несколько IP-адресов или портов, нужно разделить их запятыми.

Ограничение: Кк правило, вы можете ввести около 7 адресов IPv4 и 7 портов или до 255 символов одновременно. Поля **IP-адрес** и **Порт** комбинируются с другими фразами, чтобы создать строку фильтра. Строка фильтра может содержать не более 255 символов.

Дела по экспертизе

Дела - это логические контейнеры для собраний импортированных документов и файлов захвата пакетов.

Дела создаются либо администраторами, либо исследователями, у которых есть полномочия на создание дел. Администраторы создают дела и назначают их

исследователям. Исследователи могут создать новое дело, когда они получают данные захвата пакетов из IP-адреса в IBM Security QRadar.

Задачи, связанные с данной:

“Выгрузка файлов pcap и документов из внешних систем в дела по экспертизе”
Вы можете выгрузить внешние данные в отдельные дела.

Собрания

Используйте собрания для группировки связанных данных из определенного источника, например, из файла данных захвата пакетов (packet capture, pcap), PDF или сетевого потока.

Собрания используются для идентификации групп связанных данных и управления ими. По завершении исследования вы сможете быстро удалить данные группы в собрании.

Собрания создаются либо администраторами, либо исследователями. Администраторы создают собрания для загрузки данных вручную в Экспертиза инцидентов IBM Security QRadar. Администраторы также добавляют собрания в дела. Исследователи могут создать новое собрание, когда инициируют получение данных захвата пакетов с IP-адреса в IBM Security QRadar.

Учтите следующие правила для собраний и имен собраний:

- Имена собраний должны быть уникальными.
- Дела содержат одно или несколько собраний.
- Собрания можно добавлять в несколько дел.
- Результаты поиска возвращают дубликаты данных, когда исследователю принадлежать два дела с одним и тем же собранием.
- Если окажется, что имя собрания не является уникальным при загрузке нового pcap, исходное собрание удаляется перед выгрузкой нового pcap.

Выгрузка файлов pcap и документов из внешних систем в дела по экспертизе

Вы можете выгрузить внешние данные в отдельные дела.

Прежде чем начать

Администратор должен включить защищенные разрешения FTP для пользователя, который хочет выгрузить внешние файлы.

Об этой задаче

Экспертиза инцидентов IBM Security QRadar может импортировать данные из любого доступного каталога в сети. Данные могут быть представлены в ряде форматов, включая следующие (но ими не ограничиваясь):

- Файлы стандартного формата PCAP из внешних источников
- Такие документы, как текстовые файлы, файлы PDF, электронные таблицы и презентации
- Файлы изображений
- Поток данных из приложений
- Поток данных из внешних источников PCAP

Вы можете выгрузить в дело несколько файлов.

Ограничение: Имя дела должно быть уникальным. Нельзя создать дело, имя которого совпадает с именем существующего дела.

Процедура

1. На FTP-клиенте выполните следующие шаги:
   a. Убедитесь, что в качестве протокола выбран протокол Transport Layer Security (TLS).
   b. Добавьте IP-адрес хоста Экспертиза инцидентов QRadar.
   c. Создайте вход в систему с использованием созданного имени пользователя Экспертиза инцидентов QRadar и пароля.
2. Соединитесь с сервером Экспертиза инцидентов QRadar и создайте новый каталог.
3. Чтобы передать по FTP и сохранить файлы pcap, создайте каталог `singles` в каталоге, созданном вами для дела, и перетащите файлы pcap в этот каталог.
4. Чтобы передать по FTP и сохранить файлы других типов, не являющиеся файлами pcap, создайте каталог `import` в каталоге, созданном вами для дела, и перетащите файлы в этот каталог.
5. Чтобы перезапустить FTP-сервер, введите следующую команду:

   ```
   etc/init.d/vsftpd restart
   ```
6. Чтобы перезапустить сервер, который перемещает файлы из области выгрузки в каталог Экспертиза инцидентов QRadar, введите следующую команду:

Результаты

Вы сможете увидеть свое дело в одном из инструментов на вкладке **Экспертиза**.

Запросы экспертного репозитория

Исследователи задают характеристики документов, которые их интересуют, для получения их из экспертной базы данных. Чтобы найти набор документов для исследования, используется несколько запросов.

Несколько запросов и изучение небольшого набора документов вручную - это лучше, чем просеивать весь репозиторий. Идеи относительно последующих запросов и уточненных запросов часто приходят во время изучения неподходящего документа.

Увеличенное количество и специфичность условий запроса приводят к более релевантным наборам результатов. Ваша цель - задать как можно больше известной информации о нужных вам результатах и быть как можно точнее, там где это возможно. В качестве критерия поиска можно ввести любое число условий запроса. Вы разделяете условия пробелом или логическим оператором. Если условия разделены просто пробелом, это предполагает логический оператор OR. Оператор OR означает, что нахождение любого из условий равным образом желательно. Результаты, удовлетворяющие большинству условий поиска, помещаются в начало списка, чтобы указать на силу соответствия условиям запроса.

Один критерий поиска также называют условием запроса. Поиски, как правило, содержат более одного условия запроса. Набор условий запроса для одного поиска также называется строкой запроса. Чтобы стать специалистом по формулировке запросов, потребуется практика, но это нетрудно. Это касается изучения только нескольких условий поиска и получения опыта по созданию и отрицанию условий в комбинации, которая даст вам то, что вы хотите. Поскольку строки запросов

сохраняются в экспертизе инцидентов QRadar, вы можете постоянно настраивать свои поиски по мере того, как вы лучше узнаете данные.

Задачи, связанные с данной:

“Визуализация отношений и связей” на стр. 30
Используйте окно Визуализировать, чтобы увидеть отношения между атрибутами в восстановленных документах. Например, можно изучить адреса электронной почты, которые связывались с конкретным адресом электронной почты.

Условия запроса в произвольной форме

Исследователи ищут точные вхождения строки символов, вводя условия поиска непосредственно в поле критериев поиска на вкладке **Экспертиза**. Можно использовать запросы с одним словом или с несколькими словами.

В следующей таблице описан тип запросов поиска, которые можно использовать.

Таблица 1. Типы запросов в произвольной форме

Тип запроса поиска	Описание	Пример
Запрос с одним словом	Поиск одного термина в документе.	щенки
Один запрос с символом подстановки	Поиск совпадения с одним или несколькими символами в середине или в конце условия запроса. **Ограничение:** Символы подстановки нельзя использовать в качестве первого символа при поиске.	te?t test* te*t
Запрос с несколькими словами	Указывает, что результаты поиска будут возвращены в порядке релевантности условий запроса. Документы, содержащие оба условия запроса, будут перечислены первыми, а после них будут идти документы, содержащий только одно из условий запроса. Документам, содержащим только одно условие запроса, присваивается ранг в соответствии с числом вхождений отдельного условия запроса.	бесплатные щенки
Запрос с несколькими словами с двойными кавычками	Задает совпадение с точной строкой. Документы, содержащие оба слова, но не в этом порядке и с иным удалением друг от друга, не будут возвращены в качестве результатов. Двойные кавычки обращают эти два слова в одну строку или одно условие запроса. Механизм поиска больше не видит эти два слова как отдельные.	"бесплатные щенки"
Запрос с несколькими словами, использующий оператор AND	Указывает, что соответствие будет признано, если оба условия запроса содержатся в документе. Условия запроса могут находиться в любом порядке, и им не нужно находиться близко друг от друга.	бесплатные AND щенки

Теги метаданных

Общие объекты помечаются тегами, чтобы обеспечить исследователям возможность быстро получить точные наборы результатов из релевантных документов.

В индексе экспертизы инцидентов можно использовать многие поля метаданных в зависимости от типа сеанса, документа или протокола.

Когда вы задает имя тега метаданных, оно должно быть точным и должно существовать в экспертном репозитории.

В следующей таблице перечислены типы поисков тегов метаданных.

Таблица 2. Поиски тегов метаданных

Тип поиска тегов метаданных	**Формат**	**Пример**
Стандартный	`MetadataTag:<значение>`	`ApplicationProtocol:http`
Символ подстановки	`MetadataTag:*`	`CreditCardNumber:*`
Диапазон	`MetadataTag:[<начальное значение> TO <конечное значение>`	`Duration:[30 TO 56]`

Понятия, связанные с данным:

“Аннотации к документам” на стр. 22
Исследователи помечают закладками документы и добавляют примечания к документам, чтобы отслеживать идеи и рациональные объяснения относительно документов в их деле.

Логические комбинации

Несколько условий запроса можно объединить друг с другом с использованием простых логических операторов для создания высокоспециализированных строк запросов. Будучи правильно сформатированными, эти строки запроса могут возвратить результаты, которые точно совпадают с тем, что ищет исследователь.

Базовые логические операторы - это AND, OR, NOT и (). Оператор AND указывает, что в документе должны выполняться оба условия запроса. Оператор OR указывает, что в документе может выполняться любое условие запроса. Оператор NOT задает отрицание или удаляет результаты, соответствующие отрицаемым условиям запроса. Оператор () позволяет группировать условия и значения запроса, чтобы применять функции к набору, применять несколько значений к одной функции или обеспечить удобство синтаксиса.

Логические операторы должны быть представлены в верхнем регистре.

В следующей таблице перечислены логические операторы и дан пример строки запроса.

Таблица 3. Логические операторы для строк запросов

Логический оператор	**Пример строки запроса**	**Пояснение к примеру**
AND	`TcpPort:80 AND Protocol:http`	Два условия запроса используются, чтобы найти весь стандартный веб-трафик. Если веб-тестирование происходит на порту 8080, это не будет соответствием, так как оба условия запроса не будут выполнены.

Таблица 3. Логические операторы для строк запросов (продолжение)

Логический оператор	Пример строки запроса	Пояснение к примеру
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	Три условия запроса используются, чтобы ограничить результаты результатами из собраний документов Yahoo, CNN и MSN в экспертном репозитории.
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	Поиск трафика с нестандартным использованием портов. Первое условие запроса ищет стандартный трафик HTTP, а второе условие запроса устраняет весь трафик, который использует принятые порты HTTP.

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		В этих запросах используются скобки, чтобы эффективно достичь сложных целей. Без скобок эти запросы будут длиннее и сложнее, чтобы их сформулировать и отладить.

Инструмент построителя запросов

Используйте инструмент построителя запросов, чтобы создавать поиски или управлять сохраненными поисками.

Инструмент построителя запросов графически помогает исследователям пройти процесс создания мощных поисков, которые используют категоризированные списки условий запроса с примерами.

Таблица 4. Параметры инструмента построителя запросов

Параметр	Описание
Выбор категории	Применяет фильтр к списку тегов метаданных, доступных в списке **Выбор поля**.
Выбор поля	Теги метаданных, используемые для пометок информации в экспертном репозитории.
Пример запроса	Позволяет запустить запрос, находящийся в поле **Ввод запроса** и сообщающий число результатов.
Создать	Позволяет заменить существующий запрос новым запросом, когда вы щелкнете по **Вставить запрос**.
AND	Объединяет новый запрос с существующим, когда вы щелкнете по **Вставить запрос**. Документы должны соответствовать обоим условиям запроса.
OR	Объединяет новый запрос с существующим, когда вы щелкнете по **Вставить запрос**. Документы должны соответствовать каждому из условий.

Исследователи могут сохранять и организовывать поиски в папках в файловой системе, что позволяет исследователям совместно использовать данные.

Исследователи используют описания или имена для сохраненных запросов для справок, управления и получения представления.

Функция **Использовать запрос** на вкладке **Запрос** используется для отправки сохраненного запроса в **Ввод критериев поиска**, записанный для выполнения.

Исследователи используют предыдущий список запросов, чтобы найти ранее выполненные запросы и повторно выполнить их, выбрав запрос, который они хотят выполнить, и щелкнув по **Вставить запрос**.

Инструмент фильтра запросов

Инструмент фильтра запросов использует активные данные, чтобы обеспечить визуальные ключи для построения постоянных фильтров.

Фильтр запроса является постоянным фоновым фильтром, который сокращает активный набор документов, опрашиваемый с использованием строки запроса. Используя фильтр, вы сокращаете набор доступных документов без перегрузки строки запроса статическими условиями запроса. В результате этого у вас будет больше возможностей управления с использованием строки запроса.

Фильтр запросов - это хорошая отправная точка, позволяющая начать исследование, благодаря спискам типов фильтров, не зависящих от дел, динамическому обновлению и сводке результатов в реальном времени. Списки типов фильтров заполняются всеми значениями, найденными в доступных вам делах. Вы сможете быстро увидеть, какие данные содержатся в принадлежащих вам делах. При выборе или очистке элементов списка типов фильтра автоматически обновляется сводка результатов. Вы сможете быстро увидеть эффективность фильтра и то, насколько большой набор документов остается при использовании фильтра.

Настройка фильтра запросов по умолчанию не рекомендуется для запросов, которые вы хотите использовать повторно. Для запросов, которые вы хотите оставить, создайте новый фильтр запроса. Если вы изменили фильтр запросов по умолчанию, вы должны по завершении операции произвести его сброс, чтобы не допустить ошибочного исключения документов из будущих запросов поиска.

Результаты для активных фильтров

Исследователи просматривают результаты от активных фильтров в разделе сводки результатов в инструменте фильтра запросов.

При изменении фильтра сводка обновляется. чтобы показать общее число документов и число доступных документов. Общее число документов - это число документов, доступных исследователю до применения фильтра. Число доступных документов - это число документов, доступных после применения фильтра. Исследователи используют эти числа, чтобы судить об эффективности их фильтра и правильно его скорректировать при его построении.

Фильтры поиска для инструмента фильтра запросов

Исследователи применяют к данным фильтр для назначенных им дел. Данные разделяются на группы по типу фильтра, например, по IP-адресу или по MAC-адресу.

Используя логический переключатель действия, исследователь может либо включать, либо исключать элементы, выбранные из списка.

У каждой группы фильтров поиска есть логический переключатель действия, который позволяет либо включить, либо исключить элементы, выбранные в списке. Если задано включение, элементы в списке объединяются с использованием логического

оператора AND, что означает, что каждый доступный документ содержит все выбранные элементы. Если задано исключение, используется логический оператор OR, что означает, что ни один из доступных документов не содержит ни одного из выбранных элементов.

Исследователи могут использовать группу **UserQuery**, чтобы сформулировать свои собственные строки запросов, которые нужно добавить в фильтр.

Ограничение числа возвращенных документов в поиске

Вы можете добавить фильтры в запросы Экспертиза инцидентов IBM Security QRadar, чтобы ограничить число или тип документов, которые вы видите на странице результатов поиска.

Процедура

1. На вкладке **Экспертиза** щелкните по значку **Фильтры запросов**.

   Данные разделяются на группы по типу фильтра.
2. В окне Фильтры поиска для каждого типа фильтра выберите, нужно ли включить документы в результаты поиска; для этого щелкните по **Включить** или по **Исключить**.
3. Чтобы найти элемент в группе фильтров, выполните следующие шаги:
   a. В столбце **Тип фильтра** разверните группу фильтров.
   b. В окне Поиск выберите критерии и щелкните по **Найти**.

      При поиске записи в группе фильтров **Веб-категория** будут показаны все соответствующие поля категории. Например, при поиске выражения **Веб-категория равно чат** будут показаны категории **Чат** и связанные категории, например, **Мгновенные сообщения**, **Веб-почта/Унифицированные сообщения**, **Механизмы поиска/Веб-каталоги/Порталы** и **Облако**.

Аннотации к документам

Исследователи помечают закладками документы и добавляют примечания к документам, чтобы отслеживать идеи и рациональные объяснения относительно документов в их деле.

Документы можно пометить закладками в главном окне результатов и в инструменте досмотра в хронологической таблица, в которой показана последовательность документов, обмен которыми производился во время взаимодействия. Поскольку запросы и исследования могут быть сложными, исследователи помечают закладками все записи, включая документы, представляющие мало интереса. Использование закладки устраняет необходимость заново создавать сложные запросы и строки исследования. Аннотации можно создать после установления закладки на запись.

При исследовании бывают случаи, когда вы хотите пройти двумя или более путями. Используйте функцию браузера, чтобы дублировать текущую вкладку, на которой вы находитесь. Дублирование вкладки позволит вам не запоминать, что нужно вернуться назад и пройти дополнительными путями, или не запоминать, как добраться до точки ответвления. Текущую вкладку можно дублировать столько раз, сколько потребуется. Пройдите по каждому отдельному пути на другой вкладке и пометьте закладками релевантные документы вдоль пути. Можно добавить примечание, которое укажет путь, ведущий к каждому помеченному закладкой документу.

Примечания - это способ записывать свои мысли во время исследования. Удалить примечания может только администратор. Примечания помечаются с

использованием ID пользователя исследователя и временной отметки их ввода. При экспорте документов примечания выводятся вместе с реконструированным документом и его атрибутами.

Понятия, связанные с данным:

“Теги метаданных” на стр. 18
Общие объекты помечаются тегами, чтобы обеспечить исследователям возможность быстро получить точные наборы результатов из релевантных документов.

Глава 4. Инструменты исследований

Исследователи используют инструменты Досмотр, Цифровые оттиски, Экспорт и Визуализация для управления данными различными способами.

Страница результатов поиска - это страница по умолчанию на вкладке **Экспертиза**. Результаты поиска доступны на вкладке **Таблица**. Исследователи используют результаты поиска в таблице, чтобы быстро находить документы и получать к ним доступ. На вкладке **Таблица** используйте инструменты Досмотр, Цифровые оттиски, Экспорт и Визуализация для дальнейшего исследования.

Индикатор строк

Индикатор строк обеспечивает уникальный идентификатор для каждого документа, возвращенного в наборе результатов. Используйте индикатор строк, чтобы отправить документ и все необходимые связанные документы в инструмент визуализации реконструированного представления.

Сортировка строк

Вы можете сортировать строки, показанные в таблице. Поскольку общее число результатов может оказаться больше числа результатов, показанных в таблице, произвести сортировку всего набора результатов нельзя.

Индикатор просмотренных документов

Индикатор просмотренных документов - это маленький кружок, цвет которого изменяется с красного на зеленый, чтобы указать, просмотрел ли исследователь документ.

Выбор документов

Исследователи используют показанный селектор документов для выбора числа документов, которые появятся в таблице результатов. Можно использовать оператор SELECT ALL для отправки документов в последующую функцию, и вы сможете отправить много документов для обработки или визуализации. При выборе документов с использованием показанного селектора документов вы выбираете все документы, а не только документы, присутствующие в таблице.

Визуализация сети и документов

Исследователи используют инструмент визуализации для выявления шаблонов, понимания того, в каких местах наблюдается больше всего конфликтов сетевого трафика и документов за указанный период времени, а также для просмотра подозрительного содержимого. Например, исследователи могут визуализировать шаблоны сетевого трафика, например, в случае серверов, доступ к которым осуществляется по окончании рабочего времени.

Инструмент VGrid делится на временные блоки. Подозрительное содержимое, например, сетевой трафик или документы, обозначено красным прямоугольником в таблице. Зеленый прямоугольник обозначает обычное содержимое. Ярко окрашенный блок указывает на больший объем трафика. Чем выше насыщенность цвета, тем больше объем трафика. Яркость временного блока связана с текущими

данными, показанными в VGrid. Например, ярко окрашенный временной блок станет темнее при загрузке других временных блоков с большим объемом данных.

Исследователи могут увидеть типы сетевого трафика и число документов для каждого временного блока, в котором есть содержимое.

Исследование сетевого трафика и документов во временном блоке

Исследователи могут захотите изучить отдельные документы, просмотренные веб-сайты или отправить электронную почту в течение заданного временного блока.

Процедура

1. На вкладке **Экспертиза** выберите вкладку **VGrid**.
2. Используйте одну из следующих опций, чтобы изучить содержимое временного блока:
   - Чтобы просмотреть типы сетевого трафика и число документов, установите указатель мыши на временной блок.
   - Чтобы произвести поиск содержимого во временном блоке, выберите один или несколько временных блоков. Щелкните правой кнопкой мыши и выберите **Поиск в выбранных временных блоках**.
   - Чтобы увидеть последовательность событий, выберите временной блок, а затем выберите **Досмотр**.
   - Чтобы визуализировать содержимое, выберите временной блок, а затем выберите **Визуализировать**.

Инструмент Досмотр

Используйте инструмент Досмотр, чтобы визуализировать последовательность событий в инциденте защиты по мере того, как они происходят.

Этот инструмент используется исследователями, чтобы увидеть, что просматривали предполагаемые атакующие и какие действия они выполняли. Инструмент досмотра отражает хронологическую последовательность действий в инциденте защиты в визуализаторе как в кино. Поскольку досмотр ориентирован во времени, выбор одного документа в окне результатов не показывает большое количество информации. Если выбрано слишком мало документов, разверните радиус времени около выбранных документов на вкладке **Атрибуты**. Разверните время, щелкнув по ссылке **Показать контекст**.

Исследователи могут применять к своим запросам фильтры на основе времени дела, протокола и IP-адреса.

На вкладке **Список** можно увидеть хронологический список отправленных и полученных документов. Пошаговое создание взаимодействия заново отражено в инструменте Досмотр.

Зеленые номера ID документов указывают, что документ был просмотрен исследователем, в то время как документы с красными номерами ID не были просмотрены.

Реконструированное представление документа

На вкладке **Представление** показано реконструированное представление документа, выбранное в левой части окна в представлении списка.

Эта мощная комбинация последовательности (слева) и реконструкции (справа) позволяет увидеть, что предполагаемые атакующие увидели и сделали в сети. Помимо видимых документов, которые прошли через сеть, досмотр также показывает закулисные согласования одного компьютера с другим и выполненные обмены сертификатами.

Задачи, связанные с данной:

Глава 5, “Исследование сетевого трафика для IP-адреса”, на стр. 37
Чтобы увидеть релевантное содержимое в переговорах, которые происходили во время инцидента защиты, вы можете восстановить и реконструировать сетевой трафик, связанный с IP-адресом. Также можно производить поиск в существующих случаях, связанных с IP-адресом.

Извлеченное содержимое документа

На вкладке **Текст** показано содержимое, извлеченное из документа. Содержимое документа не форматируется.

Это текст из функции индексирования механизма поиска.

Экспорт документов в Экспертиза инцидентов QRadar

В Экспертиза инцидентов IBM Security QRadar все экспортированные документы, кроме экспортированных документов pcap, включают в себя реконструированный документ, неструктурированный текст документа, атрибуты и примечания, вложенные в документ.

При экспорте документов pcap никакой реконструкции не производится. Например, когда вы экспортируете веб-страницу, загружается все, что скачал браузер во время основного соединения. Обычно во время основного соединения скачивается большая часть текстового содержимого. Однако большинство современных браузеров используют несколько соединений для загрузки большего числа элементов, например, таблиц стилей и изображений, которые не являются частью экспорта. При экспорте содержимое pcap не реконструируется в первую очередь.

Другим примером являются сложные протоколы, например, FTP и VOIP, в которых существует основная команда и управляющее соединение, а также отдельное соединение для передачи данных. Если вы экспортируете файлы pcap для вызова VOIP или скачивания FTP, данные не будут реконструированы, и вы можете получить результаты, которых не ожидаете.

Экспорт документов в виде файлов pcap

Документы можно экспортировать как файлы pcap с нескольких устройств Экспертиза инцидентов IBM Security QRadar и Захват пакетов IBM Security QRadar.

Ограничение: Содержимое, экспортируемое вами в формат pcap, не реконструируется.

Процедура

1. Чтобы экспортировать данные из выбранных документов, выберите переключатели рядом с документами в сетке восстановления на вкладке **Экспертиза** и нажмите на **Экспорт**.

   Для экспорта в формат pcap можно выбрать не более 25 документов.
2. В списке **Выбрать тип экспорта** щелкните по **PCAP**.

3. После экспорта всех документов для хоста Экспертиза инцидентов QRadar можно щелкнуть по **Загрузить**.
4. Если экспорт документа завершится неудачно, экспортируйте документ снова, щелкнув по сообщению **НЕУДАЧНО**.

Результаты

Если вы экспортируете один файл pcap, будет загружен файл pcap. Если вы экспортируете более одного файла pcap, файлы pcap будут собраны в сжатый файл (.zip) и сжатый файл будет загружен.

В каждом документе сохраняется IP-адрес хоста Экспертиза инцидентов QRadar и IP-адрес устройства Захват пакетов QRadar, с которого первоначально был взят документ. Если вы удалите хост Экспертиза инцидентов QRadar или переместите Захват пакетов QRadar, вам, возможно, не удастся выполнить экспорт.

Цифровой оттиск

Цифровой оттиск - это скомпилированный набор связей и отношений, обозначающих трассировку идентификатора. Цифровой оттиск реконструирует сетевые взаимосвязи, чтобы помочь выявить идентификатор атакующего объекта, определить, как он осуществляет взаимодействия и с чем.

Используйте инструмент Цифровой оттиск, чтобы быстро ответить на следующие важные вопросы:

- Что известно об этом предполагаемом атакующем, компьютере или IP-адресе?
- С кем общался этот предполагаемый атакующий?
- Кто находится в его сети контактов?
- Пытается ли предполагаемый атакующий замаскировать свою личность?

Электронные идентификаторы

Электронные идентификаторы, например, адреса электронной почты, адреса Skype, MAC-адреса, ID в чатах, ID в социальных сетях или ID в Твиттере, используются, чтобы идентифицировать объекты или людей. Известные объекты или физические лица, обнаруженные в сетевом трафике и документах, помечаются тегами автоматически.

Экспертиза инцидентов IBM Security QRadar коррелирует помеченные тегами идентификаторы, которые взаимодействовали друг с другом, чтобы создать цифровой оттиск.

Взаимосвязи собраний в отчетах о цифровых оттисках соответствуют постоянно собираемому электронному присутствию, связанному с атакующим, с объектом, относящимся к сети, или с любым термином метаданных цифрового оттиска. Исследователи могут щелкнуть по любому помеченному тегами цифровым оттиском идентификатору, связанному с документом. Полученный отчет о цифровых оттисках приводится в табличном формате и организован на основе типов идентификаторов.

Получение информации о взаимосвязях

В отчете о цифровых оттисках показаны взаимодействия между *центральным идентификатором* и всеми остальными идентификаторами. *Центральный идентификатор* - это электронный идентификатор, который является интересующим вас источником в инциденте защиты.

Высший идентификатор во многих категориях обычно является указателем на центральный идентификатор в этом типе или в этой категории идентификаторов. Например, если идентификатор является MAC-адресом, адрес электронной почты, к которому относится большинство взаимодействий, вероятно, принадлежит предположительному атакующему, который является владельцем компьютера. Однако, если IP-адреса назначаются динамически, вы также должны исследовать IP-адреса, назначенные в течение диапазона времени.

Корреляции между другими категориями и центральным идентификатором, как правило, менее сильные. Прежде чем вы решите выполнить действие на основе цифрового оттиска, проверьте данные с использованием независимых источников. Используйте инструмент Цифровой оттиск, чтобы расширить радиус исследования до большего числа подозрительных атакующих и объектов.

Исследование взаимосвязей для отслеживания следов идентификаторов

Цифровой оттиск реконструирует сетевые взаимосвязи, чтобы помочь вам выявить атакующий объект и другие объекты, с которыми он взаимодействует.

Инструмент Цифровой оттиск показывает распределение частоты для коррелированных событий. Инструмент показывает взаимосвязи между объектами и подсчитывает число отношений. Чем выше это число, тем сильнее взаимосвязь. Например, если вы просматриваете взаимосвязи между адресом электронной почты и другими объектами, вы сможете увидеть, кто с кем общается. Вы можете просматривать IP-адреса, связанные с адресом электронной почты, IP-адреса, которые посещал подозреваемый, а также другие имена, связанные с адресом электронной почты.

В распределенных средах можно указать, что вы хотите увидеть взаимосвязи для одного узла в вашей организации.

Процедура

1. Выберите результат из списка документов в сетке восстановления и щелкните по вкладке **Цифровой оттиск**.
2. Выберите в списке элемент, который вы хотите исследовать.

   По умолчанию, отчет о цифровых оттисках представлен в табличном формате и организован по типам идентификаторов. Будут показаны все идентификаторы, которые взаимодействовали с центральным идентификатором. Взаимодействующие идентификаторы организованы по типам идентификаторов и рассортированы по частоте взаимодействия.
3. Если вы увидите интересующий вас идентификатор, выберите его.

   Идентификаторы - это гиперссылки, и их можно использовать как центральный идентификатор другого отчета. Создается другая вкладка, и на экране появится новый центральный идентификатор. Вы сможете увидеть, с кем взаимодействует данный предположительный атакующий и с кем взаимодействуют эти вторичные взаимодействующие. Вы можете расширить радиус исследования до большего числа подозрительных атакующих и объектов, с которыми они взаимодействуют.
4. Чтобы увидеть другой хост, выберите IP-адрес в списке **Выбрать удаленный хост**.

   В распределенных установках можно выбрать хост Экспертиза инцидентов QRadar, а затем просмотреть цифровой оттиск. В представлении по умолчанию находится первичный хост, но вы можете выбрать любой вторичный хост, связанный с хостом Экспертиза инцидентов QRadar.

5. Чтобы увидеть визуализацию связей и отношений для взаимодействий центрального идентификатора с другими идентификаторами, щелкните по вкладке **Визуализировать данные**.

Инструмент визуализации

Вы можете визуально изучать связи и отношения между несколькими атрибутами и категориями данных.

Используйте окно Визуализировать, чтобы увидеть реляционную карту метаданных из выборки в одном документе, двух документах или большем числе документов. Если используются большие выборки документов, исследователь получит сложное представление взаимосвязей метаданных и относительной частоты. Исследователи могут затем пройти эти пути, чтобы более подробно исследовать инцидент защиты.

Визуализацию выбранных документов можно легко перестроить с использованием другого отношения, изменив одно или оба отношения.

В визуализации показано каждое отношение, содержащееся в выбранных документах, и показана частота отношения. Каждый узел соответствует отдельной части метаданных, связь с которой есть в выбранных документах. Размер передает относительную частоту по сравнению с другими узлами. Ссылки показывают соединения, найденные между отдельными частями метаданных, и передают частоту за счет размера. Исследователи могут использовать узлы для идентификации возможных путей дальнейшего исследования.

Визуализация отношений и связей

Используйте окно Визуализировать, чтобы увидеть отношения между атрибутами в восстановленных документах. Например, можно изучить адреса электронной почты, которые связывались с конкретным адресом электронной почты.

Процедура

1. В таблице восстановления включите переключатели для документов, которые вы хотите исследовать, и щелкните по **Визуализировать**.
2. Выберите схему, число документов, которые нужно показать, и отношения между атрибутами, которые вы хотите увидеть, и щелкните по Обновить.
3. Используйте элементы управления масштабом, чтобы увидеть больше или меньше сведений на изображении.
4. Чтобы выполнить новый поиск или изменить активный фильтр, щелкните правой кнопкой мыши по узлу.

   В контекстном меню можно возвратить эту часть метаданных назад, чтобы выполнить новый поиск. Вы также можете изменить активный фильтр, чтобы включить или исключить метаданные.

   Ограничение: Можно просмотреть до 9999 документов одновременно в одном окне Визуализировать.

Анализ артефактов для подозрительного или несанкционированного содержимого

Аналитик защиты может искать угрозы, избежавшие обнаружения, проанализировав реконструированные артефакты, например, файлы и изображения. Чтобы понять связь между сотрудниками и артефактами, также можно изучить связи, идущие к этим файлам и изображениям и от них.

Пример - Использование анализа артефактов для поиска источника атаки (нулевой пациент)

Джон работает аналитиком защиты в компании Replay Industries. Оказалось, что заражено несколько компьютеров, несмотря на все применяемые меры защиты. После того, как он выявляет эти компьютеры и помещает их в карантин, Джону нужно выяснить, как эти системы оказались заражены и были ли аналогичным образом подвергнуты риску другие активы.

Восстановление пакетов из IP-адреса

Начав с IP-адресов и примерного интервала времени, когда все произошло, Джон может использовать Экспертиза инцидентов QRadar, чтобы восстановить релевантные данные пакетов.

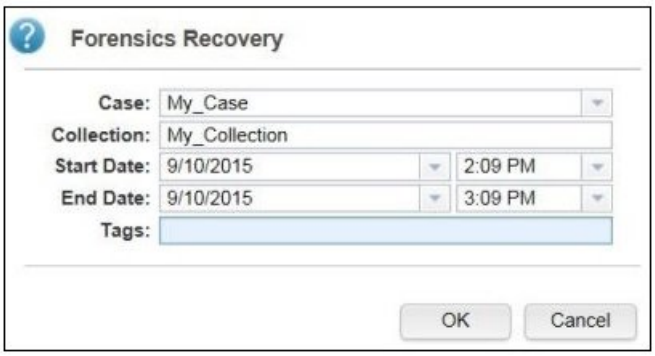


Рисунок 1. Восстановление из IP-адреса

Анализ файлов

Производя поиск исполняемого содержимого, Джон начинает с использования возможностей анализа файлов, включенных в Экспертиза инцидентов QRadar. Он видит список всех файлов, узнает, как часто они отправлялись, содержали ли они встроенные файлы или сценарии, а также какова у них оценка энтропии. Джон быстро находит файл изображения, который компонент Экспертиза инцидентов QRadar пометил флагом и как подозрительное содержимое, и как файл со встроенным сценарием.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

Рисунок 2. Атрибуты анализа файлов

Оценка энтропии файлов измеряет случайность данных и используется, чтобы найти зашифрованную вредоносную программу; распределение энтропии также четко показывает, что часть файла - это не то, что там должно быть. Дополнительный анализ доказывает, что данный файл содержит новую форму вредоносной программы, которая проскользнула незамеченной мимо существующих средств защиты и отвечает за заражение систем.

На следующей диаграмме энтропия используется в качестве индикатора дисперсии бит на байт. Поскольку каждый символ в данных состоит из 1 байта, значение энтропии указывает на изменчивость символов и дисперсию способность блока данных к сжатию. Отклонения в значениях энтропии в файле могут указывать, что в файлах скрыто подозрительное содержимое. Например, высокие значения энтропии

могут говорить о том, что данные сохранены в зашифрованном и сжатом состоянии, а более низкие значения могут указывать на то, что во время выполнения служебная нагрузка расшифровывается и сохраняется в разных разделах.

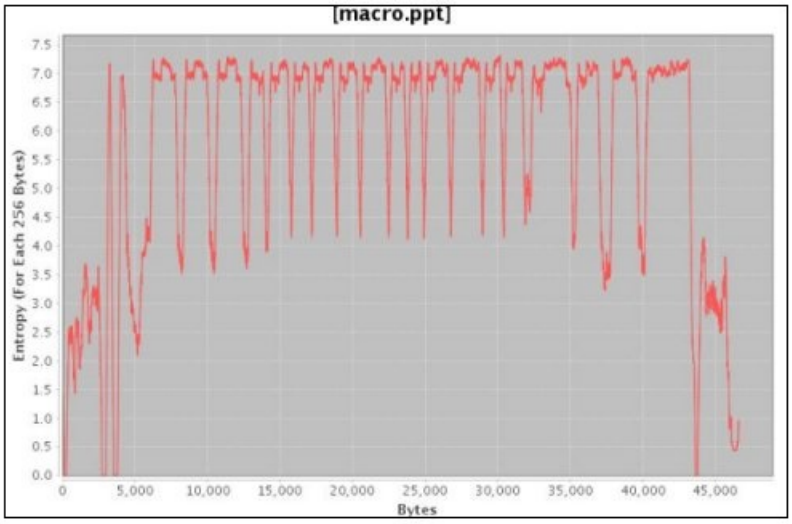


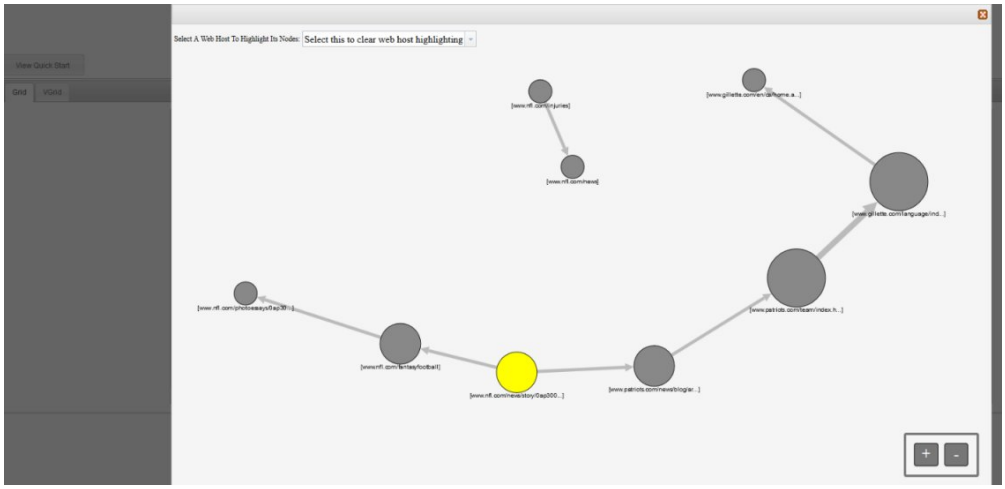
Рисунок 3. Пример графика энтропии файлов, где показаны встроенные сценарии

Джону теперь нужно понять, откуда поступил этот файл, и у кого еще он может оказаться. Джон использует Экспертиза инцидентов QRadar, чтобы быстро найти веб-сервер, который передал зараженный файл изображения. Веб-страница, о которой идет речь, популярна как широковещательный канал для самых последних новостей о широкоизвестной команде НФЛ, и она оказалась подвергнута риску. Даже несмотря на то, что веб-сайт содержал много изображений, было только одно содержащее встроенную вредоносную программу изображение, которое было ранее найдено Джоном путем анализа файлов.

Анализ ссылок для визуализации взаимодействий с веб-сайтом

Чтобы определить, могли ли быть затронуты другие системы, Джон использует анализ ссылок, чтобы быстро визуализировать все просмотренные веб-сайты и, невзирая на большой объем трафика с веб-сайтами для компаний, с которыми вела свою деятельность компания Replay, можно ясно увидеть небольшое подмножество действий по доступу к зараженному веб-хосту. Джон анализирует эти ссылки, чтобы узнать, какие другие серверы в его сети использовались для доступа к этому веб-хосту.

В своем исследовании Джон использует узлы на графике, где представлены веб-страницы, а стрелки между узлами соответствуют взаимосвязям или транзакциям между веб-страницами, чтобы быстро оценить шаблоны трафика и увидеть, как перемещались документы. Чем больше узел, тем больше ссылок есть у документа в его пути, а чем больше стрелка ссылки, тем больше раз эта ссылка использовалась.



Поскольку этот сайт является популярным сайтом новостей о НФЛ, не удивительно, что есть ряд других серверов, которые связывались с этим веб-хостом и потенциально могли быть затронуты.

Анализ изображений

Чтобы сузить набор серверов, которые загружали вредоносный файл изображения, Джон переключается на анализ изображений и быстро находит все отправленные или принятые файлы изображений.

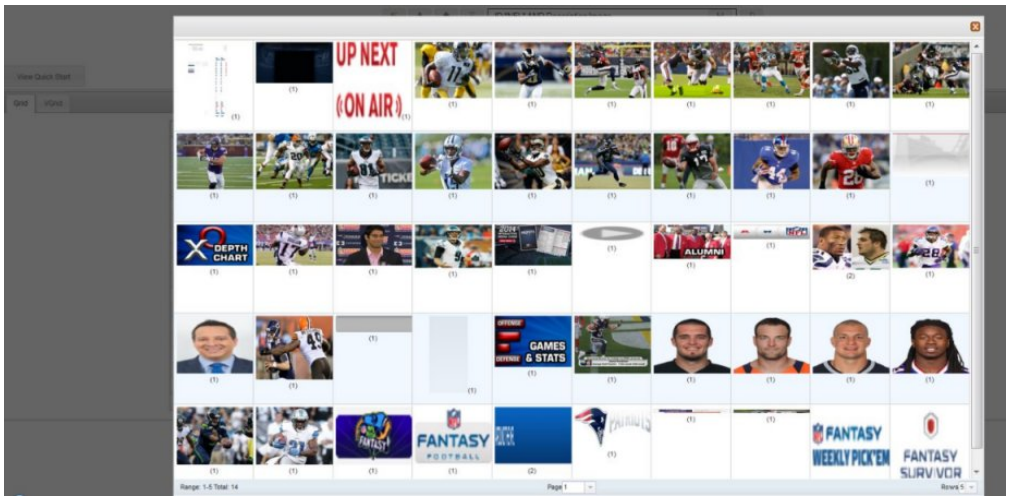


Рисунок 4. Пример анализа изображений

Джон быстро убеждается в том, что все его зараженные серверы и два сервера, о которых он не знал, имели доступ к дискредитированному файлу изображения.

Джон также устанавливает, что несколько других серверов, которые получали доступ к тому же веб-сайту, не загрузили зараженный файл. Теперь у Джона есть нужная ему информация, чтобы объявить карантин для этих двух дополнительных серверов и создать новый хэш файла для зараженного файла, которые компания Replay Industries может выгрузить и использовать совместно с другими пользователями в IBM X-Force Exchange.

Анализ файлов для поиска встроенного содержимого и вредоносных действий

Чтобы исследовать файлы на скрытые угрозы, вы можете посмотреть на значения энтропии файлов, загрузить встроенные файлы и сценарии для дальнейшего анализа и просмотреть документ и его атрибуты.

Поскольку нарушители могут скрыть содержимое двоичных файлов в файлах контейнеров, можно использовать анализ файлов в Экспертиза инцидентов IBM Security QRadar, чтобы изучить, содержали ли файлы встроенные сценарии или другое двоичное содержимое.

Энтропия файлов означает степень случайности данных в файле и позволяет определить, содержит ли файл скрытые данные или подозрительные сценарии. Шкала случайности - от 0 (неслучайный файл) до 8 (полностью случайный файл, например, шифрованный файл). Чем больше может быть сжат блок, тем ниже значение энтропии; чем меньше можно сжать блок, тем выше значение энтропии.

На следующей диаграмме энтропия используется в качестве индикатора дисперсии бит на байт. Поскольку каждый символ в данных состоит из 1 байта, значение энтропии указывает на изменчивость символов и дисперсию способность блока данных к сжатию. Отклонения в значениях энтропии в файле могут указывать, что в файлах скрыто подозрительное содержимое. Например, высокие значения энтропии могут говорить о том, что данные сохранены в зашифрованном и сжатом состоянии, а более низкие значения могут указывать на то, что во время выполнения служебная нагрузка расшифровывается и сохраняется в разных разделах.

Процедура

1. На вкладке **Экспертиза** выберите один или несколько восстановленных файлов в представлении **Сетка**.
2. В меню инструментов исследования в верхней части сетки щелкните по **Анализ файлов**.

   В результатах каждая строка сетки содержит данные анализа для документа, например, имя файла, описание, информацию о том, обнаружено ли подозрительное содержимое, и значения энтропии.
3. Чтобы рассортировать файлы по определенному атрибуту, например, энтропии, щелкните по заголовку соответствующего столбца.
4. В списке файлов щелкните правой кнопкой мыши по файлу, чтобы произвести дальнейшую оценку
   - Чтобы проверить документ и его атрибуты, щелкните по **Показать документ**.
   - Чтобы проверить график энтропии и узнать, может ли встроенный файл или сценарий содержать вредоносную программу, щелкните по **Показать энтропию**.

     Значения энтропии можно использовать как указание на то, может ли файл содержать вредоносное содержимое. Например, текстовые файлы ASCII, как правило, обладают высокой способностью к сжатию, и у них низкие значения энтропии. Шифрованные данные, как правило, мало способны к сжатию, и обычно у них высокое значение энтропии. Вредоносные программы часто упаковываются и скрываются как в файлах, так и в изображениях.
   - Чтобы загрузить встроенные файлы, щелкните по **Извлечь встроенные файлы** и выберите файлы, которые нужно загрузить.

     Эта опция доступна только для документов со встроенными файлами или сценариями. Файлы загружаются в каталог загрузки вашего веб-браузера. Будьте осторожны, чтобы не открыть потенциально вредоносные сценарии в незащищенной среде.

Анализ изображений на скрытые угрозы или подозрительную активность

Просмотренные изображения сортируются на основе размера и релевантности со значением частоты в скобках. Этот анализ может оказаться полезным, если сотрудник использует ресурсы компании для поиска неподходящих, ограниченных или запрещенных изображений. Например, изображения могут быть связаны с самолетами, некоторыми зданиями или положениями, которые являются объектами назначения для нарушений безопасности.

Используя анализ изображений, вы можете просматривать наиболее релевантные изображения из одного или нескольких документов в одном или нескольких захваченных файлах пакетов на одном экране вместо того, чтобы пришлось открывать каждый документ и просматривать изображения.

Процедура

1. На вкладке **Экспертиза**, в представлении **Сетка** выберите один или несколько восстановленных документов, содержащих изображение в описании.
2. В меню инструментов исследования в верхней части сетки щелкните по **Анализ изображений**.

   В результатах версии миниизображений всех изображений, содержащихся в документах, показаны в порядке релевантности. Число в скобках рядом с изображением указывает число экземпляров изображения в документе. Если вы установите курсор на миниизображение, изображение станет больше.
3. Щелкните правой кнопкой мыши по изображению для дальнейшего изучения
   - Чтобы проверить изображение и его атрибуты, щелкните по **Показать документ**.
   - Чтобы проверить график энтропии и узнать, может ли изображение содержать вредоносную программу, щелкните по **Показать энтропию**.

     Значения энтропии можно использовать как указание на то, может ли файл содержать вредоносное содержимое. Например, файлы растровых изображений и текстовые файлы ASCII, как правило, обладают высокой способностью к сжатию, и у них низкие значения энтропии. Шифрованные данные, как правило, мало способны к сжатию, и обычно у них высокое значение энтропии. Вредоносные программы часто упаковываются и скрываются как в файлах, так и в изображениях.

Анализ ссылок для поиска соединений и взаимосвязей

При анализе ссылок ссылки показывают общность между веб-сайтами, которые просматривались. При исследовании инцидентов защиты вы сможете быстро увидеть, есть ли перекрывание и как люди взаимодействуют друг с другом.

Например, если вы считаете, что группа злоумышленников работает совместно, но не знаете, как, вы сможете взглянуть на набор документов от рядя пользователей и использовать анализ ссылок, чтобы увидеть общие веб-страницы. После этого вы можете исследовать отдельные веб-сайты.

Процедура

1. На вкладке **Экспертиза** выберите одну или несколько веб-страниц в представлении **Сетка**.
2. В меню инструментов исследования в верхней части сетки щелкните по **Анализ ссылок**.

Если между веб-сайтами существует связь, на цитоскопической диаграмме будут показаны веб-страницы в виде кружков (узлов) и ссылки на веб-страницы и с веб-страниц в виде стрелок. Чем больше узел, тем больше ссылок есть у документа в его пути, а чем больше стрелка ссылки, тем больше раз эта ссылка использовалась. Выбранные узлы выделены желтым цветом.

3. Чтобы исследовать связь с отдельного веб-хоста, выберите веб-хост в списке **Выбрать веб-хост**.

   Узлы, соответствующие веб-страницам с выбранного веб-хоста, показаны как темно-серые кружки.

4. Чтобы увеличить или уменьшить размер кружков (узлов) и стрелок, используйте элементы управления увеличением (+) или уменьшением (-).

   Вы также можете прокрутить данные вверх или вниз, пользуясь колесиком на мыши, чтобы увеличить или уменьшить размер узлов и стрелок.

5. Чтобы переместить один или несколько узлов, щелкните мышью и перетащите узлы.

   Можно перетащить весь график, щелкнув в любом месте фона, нажав кнопку мыши и перетащив график.

Запуск восстановления со страницы документа Атрибуты

При просмотре вкладки **Атрибуты** для документы можно запустить восстановление для IP-адреса или порта.

Процедура

1. Выполните поиск на странице Поиск на вкладке **Экспертиза**.
2. В списке возвращенных документов щелкните по одному из них, чтоб его открыть.
3. Перейдите на вкладку **Атрибуты**.
4. Щелкните по IP-адресу или порту.
5. В меню щелкните по **Запустить восстановление для**.

Глава 5. Исследование сетевого трафика для IP-адреса

Чтобы увидеть релевантное содержимое в переговорах, которые происходили во время инцидента защиты, вы можете восстановить и реконструировать сетевой трафик, связанный с IP-адресом. Также можно производить поиск в существующих случаях, связанных с IP-адресом.

При реконструкции сетевого трафика из IP-адреса создается инцидент. Исследователи могут визуализировать последовательность событий из инцидента защиты или просматривать документы в инциденте.

Экспертиза инцидентов IBM Security QRadar индексирует все доступные сетевые данные, данные файлов, метаданные и текстовые символы, которые находятся в каждом восстановленном файле.

В распределенных внедрениях несколько устройств захвата и Экспертиза инцидентов QRadar являются хостами для захваченных и обработанных данных. Вы можете просматривать агрегированные результаты восстановления инцидентов или результаты по хостам и устройствам захвата.

Процедура

1. Чтобы создать случай и получить данные с устройств захвата пакетов, в QRadar, щелкните правой кнопкой мыши по IP-адресу и выберите **Запустить экспертное восстановление**.
   a. В следующей таблице представлены рекомендации по параметрам восстановления данных:

Таблица 5. Параметры восстановления данных

Параметр	Описание
Регистр	Дело, используемое для исследования. **Ограничение:** Имя дела должно быть уникальным.
Совокупность	Восстановленные данные группируются в собрание и связываются с делом. **Ограничение:** Имя собрания должно быть уникальным. Если имя собрания существует в деле, исходное собрание будет удалено.
Дата начала	Начальная дата и время захвата пакетов данных.
Дата завершения	Конечная дата и время захвата пакетов данных.
Теги	Теги метаданных, используемые для быстрого получения точных наборов результатов из релевантных документов. **Ограничение:** Символ # не разрешается. Можно использовать другие специальные символы, например, $, %,*.

   b. Нажмите на **OK**, а затем щелкните по вкладке **Экспертиза**.

      Устранение ошибок: Если вы увидите сообщение о том, что у вас нет разрешения на восстановление данных, убедитесь, что у вашего профиля защиты есть доступ к IP-адресу. В некоторых случаях, если вы использовали символ # в поле **Теги**, вы можете увидеть сообщение.

   c. Щелкните по значку треугольника, чтобы увидеть инциденты.
   d. Чтобы визуализировать последовательность событий для инцидента, щелкните по **Перейти к результатам страницы досмотра**.

e. Чтобы увидеть документы в инциденте, щелкните по **Перейти к результатам страницы поиска**.

2. Чтобы производить поиск в существующих случаях для IP-адреса, в QRadar, щелкните правой кнопкой мыши по IP-адресу и щелкните по **Запустить экспертный поиск**.
   a. На вкладке **Экспертиза** щелкните по значку инцидентов (треугольнику).
   b. Чтобы исследовать агрегацию операций, связанных с инцидентом, выделите дело, установив на него указатель мыши, а затем щелкните по значку поиска.
   c. Чтобы исследовать действия по хостам Экспертиза инцидентов QRadar и устройствам захвата в распределенных внедрениях, разверните запись **Дело**, а затем разверните запись **Собрание**.
   d. Чтобы увидеть хронологический список взаимодействий в инциденте, выделите собрание, установив на него указатель мыши, а затем щелкните по значку досмотра.

Понятия, связанные с данным:

“Реконструированное представление документа” на стр. 26
На вкладке **Представление** показано реконструированное представление документа, выбранное в левой части окна в представлении списка.

Замечания

Данная публикация разработана для продуктов и услуг, предлагаемых в США.

IBM может не предоставлять в других странах продукты, услуги и аппаратные средства, описанные в данном документе. За сведениями о продуктах и услугах, предоставляемых в вашей стране, обращайтесь в местное представительство IBM . Ссылки на продукты, программы или услуги IBM не означают и не предполагают, что можно использовать только указанные продукты, программы или услуги IBM . Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако при этом пользователь сам несет ответственность за оценку и проверку работы продуктов, программ и услуг, которые получены не от IBM.

IBM может располагать патентами или рассматриваемыми заявками на патенты, относящимися к предмету данной публикации. Получение данного документа не означает предоставления каких-либо лицензий на эти патенты. С запросами по поводу лицензий обращайтесь в письменной форме по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

По поводу лицензий, связанных с использованием наборов двухбайтных символов (DBCS), обращайтесь в отдел интеллектуальной собственности IBM или направьте запрос в письменной форме по адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Приведенный ниже абзац не относится к Великобритании и к тем странам, в которых подобные положения не соответствуют местному законодательству:

КОРПОРАЦИЯ INTERNATIONAL BUSINESS MACHINES ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ОТСУТСТВИЯ НАРУШЕНИЙ, КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ КАКОЙ-ЛИБО КОНКРЕТНОЙ ЦЕЛИ. В ряде стран для некоторых сделок не допускается отказ от явных или предполагаемых гарантий; в таком случае данное положение может к вам не относиться.

В приведенной здесь информации могут встретиться технические неточности или типографские опечатки. В публикацию время от времени вносятся изменения, которые будут отражены в следующих изданиях. IBM может в любой момент без какого-либо предварительного уведомления внести изменения в продукты и/или программы, описанные в настоящей публикации.

Любые ссылки в этой публикации на веб-сайты, не принадлежащие IBM, приведены только для удобства и никоим образом не служат для их поддержки. Материалы на этих веб-сайтах не входят в число материалов по данному продукту IBM и весь риск пользования этими веб-сайтами несет сам пользователь.

IBM оставляет за собой право на использование и распространение любых предоставленных вами сведений любыми приемлемыми способами, не принимая на себя никаких обязательств перед вами.

Если обладателю лицензии на данную программу понадобятся сведения о возможности: (i) обмена данными между независимо разработанными программами и другими программами (включая данную) и (ii) совместного использования таких данных, он может обратиться по адресу:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Такую информацию можно получить при соблюдении определенных условий, включая в некоторых случаях уплату определенной суммы.

IBM предоставляет лицензионную программу, описанную в данном документе, и все прилагаемые к ней лицензионные материалы на основании положений Соглашения между IBM и Заказчиком, Международного Соглашения о Лицензиях на Программы IBM (IBM International Program License Agreement) или любого эквивалентного соглашения между IBM и заказчиком.

Все приводимые здесь данные о производительности были получены в контролируемой среде. Поэтому результаты, полученные в других операционных средах, могут заметно отличаться от приведенных. Некоторые измерения производились в системах разработчиков, и нет никаких гарантий, что в обычно используемых системах результаты будут такими же. Кроме того, результаты некоторых измерений были получены экстраполяцией. Реальные результаты могут быть другими. Пользователи должны проверить данные в своей собственной среде.

Информация, касающаяся продуктов других компаний (не IBM) была получена от поставщиков этих продуктов, из опубликованных ими заявлений или из прочих общедоступных источников. IBM не производила тестирование этих продуктов и никак не может подтвердить информацию о точности их работы и совместимости, а также прочие заявления относительно продуктов других компаний (не IBM). Вопросы относительно возможностей продуктов других компаний (не IBM) следует адресовать поставщикам этих продуктов.

Все заявления о будущих планах и намерениях IBM могут быть изменены или отменены без уведомлений, и описывают исключительно цели фирмы.

Все приведенные здесь цены IBM - это розничные цены, установленные IBM; они действительны на текущий момент и могут быть изменены без предварительного уведомления. Цены дилеров могут отличаться от них.

Эта информация может содержать примеры данных и отчетов, иллюстрирующие типичные деловые операции. Чтобы эти примеры были правдоподобны, в них включены имена лиц, названия компаний и товаров. Все эти имена и названия являются вымышленными, и всякое сходство с именами, названиями и адресами, используемыми в реальной предпринимательской деятельности, являются не более чем совпадением.

При просмотре этого документа на компьютере фотографии и цветные иллюстрации могут быть не видны.

Товарные знаки

IBM, логотип IBM и ibm.com - товарные знаки или зарегистрированные товарные знаки International Business Machines Corp., зарегистрированные во многих странах мира. Прочие имена продуктов и услуг могут быть товарными знаками IBM или других компаний. Текущий список товарных знаков IBM есть в Интернете на странице "Copyright and trademark information" (Информация об авторских правах и товарных знаках) по адресу: www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT и логотип Windows - товарные знаки Microsoft Corporation в США и/или других странах.

Замечания, касающиеся политики конфиденциальности

В программных продуктах IBM, включая программы как решения служб (“Программные Предложения”), могут использоваться cookies или другие технологии для сбора информации по использованию продукта, чтобы помочь конечному пользователю в работе, настроить взаимодействия с конечным пользователем или для иных целей. Во многих случаях никакой личной идентификационной информации Программные Предложения не собирают. Некоторые из наших Программных Предложений могут помочь вам производить сбор личной идентификационной информации. Если в таком Программном Предложении используются cookies для сбора личной идентификационной информации, ниже представлена конкретная информация об использовании cookies в данном предложении.

В зависимости от внедренных конфигурации это Программное Предложение может использовать cookies сеанса, которые собирают ID сеанса каждого пользователя для управления сеансом и аутентификации. Эти cookies можно отключить, но при их отключении также будут устранены функции, которые они поддерживают.

Если конфигурации, внедренные для этого Предложения относительно программ, обеспечивают вам, как заказчику, возможность собирать информацию для идентификации личности от конечных пользователей через cookies и другие технологии, вы должны обратиться за местной юридической рекомендацией о том, существуют ли какие-либо законы, применимые к такому сбору данных, включая все требования относительно замечаний и согласований.

Более подробную информацию об использовании различных технологий, включая cookies, для этих целей смотрите на странице политики конфиденциальности IBM по адресу: http://www.ibm.com/privacy, и в Заявлении об электронной конфиденциальности IBM по адресу: http://www.ibm.com/privacy/details, в разделе “Cookies, Web Beacons and Other Technologies” (Cookies, веб-маяки и другие технологии) и в документе “IBM Software Products and Software-as-a-Service Privacy Statement” (Заявление о конфиденциальности программных продуктов IBM и программ в качестве услуг) http://www.ibm.com/software/info/product-privacy.

Глоссарий

Этот глоссарий содержит термины и определения для программ и продуктов Экспертиза инцидентов IBM Security QRadar.

В данном глоссарии используются следующие перекрестные ссылки:

- *Смотрите* - ссылка с непредпочтительного термина на предпочтительный синоним термина либо с сокращения на полную форму термина.
- *Смотрите также* - ссылка на связанный или противоположный термин.

Другие термины и определения смотрите на веб-сайте терминологии IBM (откроется в новом окне).

“A” “B” “C” “D” “E” на стр. 44 “F” на стр. 44 “H” на стр. 44 “I” на стр. 44 “M” на стр. 44 “O” на стр. 44 “P” на стр. 44 “R” на стр. 44 “C” на стр. 44 “B” на стр. 45 “V” на стр. 45

A

аномалия
Отклонение от ожидаемого поведения сети.

атака Любая попытка неавторизованного лица нарушить работу компьютерной программы или сетевой системы. Смотрите также атакующий.

атакующий
Пользователь (человек или компьютерная программа), который пытается нанести ущерб информационной системе или получить доступ к информации, не предназначенной для общего доступа. Смотрите также атака.

B

логический оператор
Встроенная функция, которая задает логическую операцию AND, OR или NOT при оценке наборов операций. Логические операторы - это &&, || и !.

путь Элемент веб-интерфейса, показывающий положение пользователя на сайте. Обычно это ряд гиперссылок, появляющихся вверху или внизу страницы. Эти ссылки указывают на страницы, которые просматривались, и позволяют пользователю перейти назад в начальное расположение.

C

устройство захвата
Смотрите устройство захвата пакетов.

дело Информация, содержащаяся в базе данных и относящаяся к конкретному исследованию.

категория
Набор элементов, сгруппированных в соответствии с конкретным описанием или классификацией. Категориями могут быть разные уровни информации в измерении.

центральный идентификатор
Элемент категории, с которым взаимодействовали все остальные идентификаторы. Центральный идентификатор - это центральный элемент в исследовании.

собрание
Отдельный именованный набор данных, связанный с делом. Например, упорядоченный набор захваченных сетевых пакетов.

постоянно собираемое электронное присутствие
Онлайновый идентификатор атакующего в виде собрания связанных цифровых оттисков.

беседа Реконструированный с помощью экспертизы поток данных между двумя или более сетевыми конечными точками. Например, беседа в социальной сети.

D

очистка
Процесс, посредством которого осуществляется декомпиляция данных захвата пакетов, так что все принятые данные будут собраны в виде отчета о результатах.

цифровой оттиск
Отчет, состоящий из помеченных тегами

идентификаторов, связанных друг с другом в индивидуальном деле.

взаимосвязь цифровых оттисков
Взаимосвязь между помеченными тегами идентификаторами, связанными с делом.

инспектор домена
Особый инспектор, назначенный для разбиения и извлечения данных экспертизы с определенных веб-сайтов доменов, например, Facebook или Gmail.

E

шифрование
В компьютерной безопасности: Процесс преобразования данных в непонятный вид, так чтобы либо было невозможно получить исходные данные, либо можно было их получить только с использованием процесса расшифровки.

F

запись потока
Запись переговоров между двумя хостами.

исследователь экспертизы
Пользователь, который извлекает релевантные данные из сетевого трафика и документов в экспертный репозиторий.

H

гипотеза
Предлагаемое объяснение инцидента на основе доступных свидетельств, собранных в дело. Гипотеза должна быть проверяемой и опровергаемой.

I

идентификатор
Собрание атрибутов из источника данных, соответствующее сотруднику, организации, месту или элементу.

инцидент
Смотрите инцидент защиты.

принятый сетевой трафик
Захваченный сетевой трафик, обработанный процессом сбора экспертизы.

M

метаданные
Данные, описывающие характеристики данных; описательные данные.

реляционная карта метаданных
Карта, на которой показаны связанные метаданные из документов дела.

O

нарушение
Отправленное сообщение или сгенерированное событие в ответ на отслеживаемое условие. Например, нарушение предоставляет информацию о том, когда была нарушена политика или когда производилась атака на сеть.

P

устройство для захвата пакетов
Автономное устройство, которое перехватывает и записывает в журнал данные трафика.

информация о захвате пакетов
Информация о данных трафика, собранная устройством захвата.

инспектор протокола
Особый инспектор, назначенный для извлечения данных экспертизы из таких сетевых протоколов, как HTTP или FTP.

R

задание восстановления
Процесс, который восстанавливает запрошенные данные захвата и переадресует их на устройство очистки для приема.

C

инцидент защиты
Событие, в котором нарушаются, компрометируются или атакуются обычные сетевые операции.

суперпоток
Один поток, состоящий из нескольких потоков с аналогичными свойствами, чтобы повысить мощность обработки путем сведения к минимуму ограничений хранения.

инструмент Досмотр
: Инструмент, который показывает хронологическую последовательность действий в инциденте защиты в визуализаторе.

B

трафик
: Во взаимодействиях с передачей данных: Количество данных, переданных после определенной точки в пути.

след
: Цифровые оттиски, связывающие физических лиц, вовлеченных в дело, с физическими лицами вне дела.

V

уязвимость
: Возможность нарушения безопасности в операционной системе, системной программе или компоненте прикладной программы.

Индекс