Как использовать механизм табличных списков в MaxPatrol SIEM

ptsecurity.com

Содержание

Резюме

В этом документе мы расскажем, ка́к эффективно использовать механизм табличных списков в MaxPatrol SIEM на примерах его применения в таких процессах, как процессы управления событиями, инцидентами и активами.

Механизм накопления данных и обмена ими между различными правилами обогащения и корреляции, реализованный с помощью табличных списков, позволяет повысить эффективность корреляционных правил MaxPatrol SIEM и облегчает сбор информации для последующего обогащения событий, инцидентов и активов.

Приведенная здесь информация будет полезна:

- специалистам, занимающимся разработкой корреляционных правил;
- операторам мониторинга событий;
- специалистам по инвентаризации активов;
- специалистам по внедрению MaxPatrol SIEM;
- другим специалистам, использующим MaxPatrol SIEM в своей работе.

Несколько фактов о табличных списках

MaxPatrol SIEM собирает и обрабатывает большое количество информации от различных источников данных; одним из способов накопления и обработки информации об активах, событиях и инцидентах является механизм табличных списков. Используя информацию из табличных списков в правилах корреляции, обогащения или для ручного анализа, можно повысить эффективность работы с MaxPatrol SIEM и существенно сократить трудозатраты операторов системы.

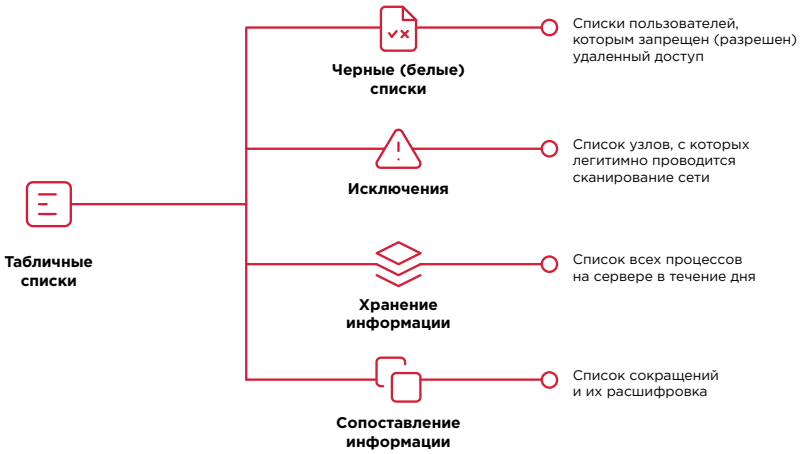
Табличный список представляет собой двумерный массив данных, в котором оператор MaxPatrol SIEM может определить состав полей и сроки хранения записей. В зависимости от целей использования табличные списки можно разделить на следующие типы:

- списки активов;
- табличные списки, заполняемые правилами корреляции;
- табличные списки, заполняемые правилами обогащения;
- репутационные списки;
- справочники.

Подробное описание табличных списков приведено в таблице ниже.

	Списки активов	**ТС, заполняемые правилами корреляции**	**ТС, заполняемые правилами обогащения**	**Репутационные списки**	**Справочники**
Тип данных	Информация об активах	Любая информация	Любая информация	Индикаторы компрометации	Любая информация
Запись данных	Автоматически обновляется при обращении к ТС	При выполнении правила корреляции	При выполнении правила обогащения	Автоматически, при получении информации из внешних источников	Ручной ввод данных и возможность импорта данных
Чтение данных	Правила корреляции (обогащения), ручной просмотр				
Срок хранения данных	—	Устанавливается при создании ТС	Устанавливается при создании ТС	—	—
Примеры реализации	Список всех активов, на которых установлено определенное ПО	Список всех активов, на которых были зафиксированы попытки подбора пароля и которые входят в определенную группу (ИСПДн, ЗОКИИ и т. п.)	Список, содержащий расшифровку сокращений в наименовании оборудования («WS-123» >«Рабочая станция, кабинет 123»)	Репутационный список Positive Technologies или иного вендора	Список активов, которые являются важными по результатам оценки рисков ИБ

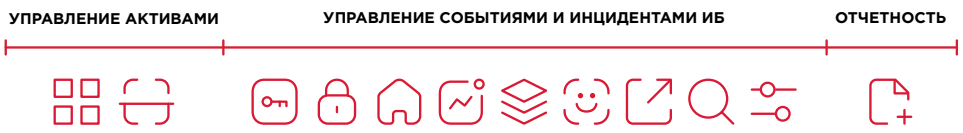
Табличные списки также можно разделить по способу применения, например черные, белые списки, списки исключений. Примеры разделения табличных списков по способу применения приведены на рисунке ниже.



Практические кейсы использования табличных списков

Табличные списки используются в процессах управления ИБ, автоматизируемых при помощи MaxPatrol SIEM (управление активами, событиями и инцидентами ИБ). Поскольку табличные списки служат основой для обмена информацией между процессами, зачастую соотнести табличный список с определенным процессом не представляется возможным; например, в кейсе ниже «Выделенные категории активов» табличный список используется для передачи информации из процесса управления активами в процессы управления событиями и инцидентами ИБ.

Однако табличные списки в приведенных ниже кейсах мы постарались условно разбить на группы, в зависимости от процессов управления ИБ, в которых они используются в большей степени.



Выделенные категории активов

Практически в любой организации имеются информационные системы персональных данных (ИСПДн), а в некоторых компаниях — значимые объекты критической информационной инфраструктуры (ЗОКИИ). Для идентификации активов рекомендуем применять механизм группировки, реализованный в MaxPatrol SIEM.

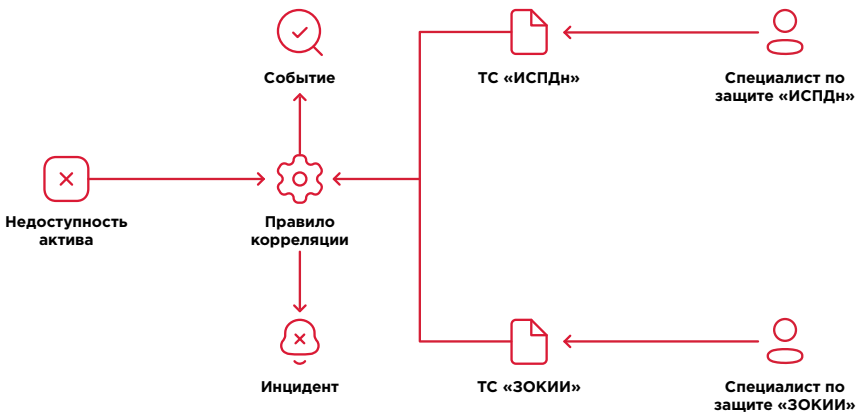
Для эффективной организации работы с выделенными категориями активов рекомендуем использовать табличные списки, придерживаясь следующего подхода:

- выделите две группы активов (с ИСПДн и ЗОКИИ), используя табличные списки;
- назначьте ответственными за актуализацию табличных списков с группами активов — ответственных за обеспечение безопасности ИСПДн и ЗОКИИ.

Для реализации подобного сценария использования создавайте табличные списки, содержащие списки выделенных групп активов (в данном случае: один для ИСПДн, другой для ЗОКИИ). В созданных табличных списках должна содержаться информация, позволяющая однозначно идентифицировать актив (IP-адрес, DNS-имя и т. п.), входящий в выделенную категорию (ИСПДн или ЗОКИИ).

Работу с табличными списками организуйте через Knowledge Base MaxPatrol SIEM, что позволит привлечь к актуализации созданных табличных списков специалистов, занимающихся непосредственно защитой ИСПДн и ЗОКИИ.

Рассмотрим использование табличных списков в правилах обработки событий, связанных с недоступностью актива. В правиле, обрабатывающем события, в котором MaxPatrol SIEM не может получить информацию с актива, добавим проверку принадлежности актива к определенной группе; соответственно, если актив относится к ЗОКИИ, то будет зарегистрирован инцидент, требующий дальнейшего реагирования и расследования, если же актив относится к ИСПДн, будет зарегистрировано событие, которое не требует немедленной реакции (см. рисунок ниже).



Еще одним примером применения табличных списков является их использование в правилах обработки событий, связанных с вирусным заражением: в правиле корреляции, обрабатывающем события от антивирусной системы, зададим разную степень опасности инцидента при обнаружении вредоносного ПО: для ЗОКИИ — высокая опасность, для ИСПДн — средняя, а для рабочих станций низкая[1]. В результате для разных групп активов будут созданы инциденты разной степени опасности, что позволит установить приоритет обработки инцидентов и реагировать в первую очередь на инциденты, опасные для определенной группы активов.

1 Конкретные значения зависят от характера инфраструктуры, активов и от других параметров и подбираются отдельно для каждой организации.

Группировку активов можно также выполнять по степени их значимости на основе информации, полученной от подразделений организации. Например, на основе информации, полученной от отдела ИТ, можно выполнить следующую группировку:

- периметр сети;
- ключевые серверы;
- ядро сети;
- инфраструктурные серверы;
- рабочие станции.

Создав табличный список для таких групп активов, можно установить различную степень опасности инцидентов: например, сканирование портов для оборудования на периметре сети не будет являться опасным инцидентом, тогда как для остальных групп, особенно для серверов и ядра сети, — это инцидент высокой степени опасности.

Подобный подход позволит эффективно организовать работу с активами за счет гибкой настройки правил корреляции и избегания лишней коммуникации между подразделениями при актуализации состава групп выделенных активов.

Сканирование активов на уязвимости

При сканировании активов на уязвимости, например с помощью внешнего сканера защищенности, MaxPatrol SIEM зарегистрирует данную активность и в зависимости от параметров правил корреляции может зарегистрировать до нескольких десятков инцидентов. Для предотвращения подобной ситуации может использоваться табличный список с исключениями, в который вносятся сканирующие узлы. Однако такой подход повышает риск целевой атаки, которая не будет впоследствии детектирована MaxPatrol SIEM (если для атаки будут использованы сканирующие узлы).

Для снижения подобных рисков рекомендуем следующий подход:

- в качестве исключений используйте несколько параметров сканирования;
- актуализацию исключений возложите на специалистов, проводящих сканирование на уязвимости.

Для реализации такого подхода рекомендуем создать табличный список, содержащий следующие поля:

- «сканирующий узел»;
- «временной интервал»;
- «сканируемые активы».

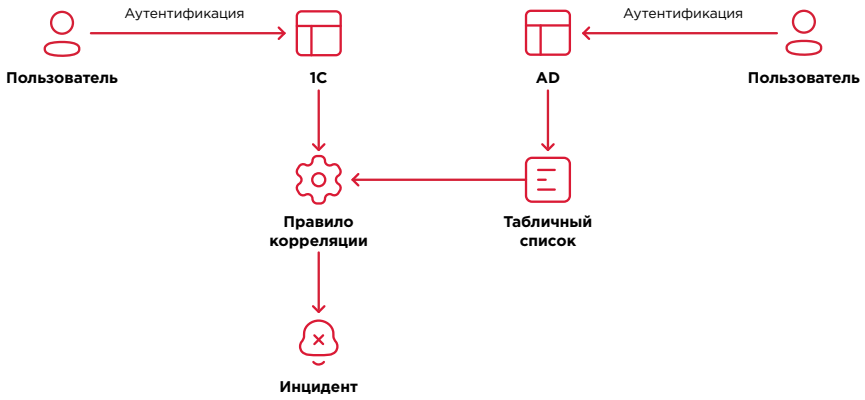
Созданный табличный список будет актуализироваться с помощью механизма Knowledge Base MaxPatrol SIEM специалистами, проводящими сканирование на уязвимости. В результате использования табличного списка в правилах корреляции будут учитываться назначенные исключения только в строго заданных рамках, и в случае нелегитимной активности со сканирующего узла (несовпадение времени и (или) целей сканирования) MaxPatrol SIEM сможет детектировать данную активность и зарегистрировать инцидент.

Контроль авторизованных пользователей

Для выявления инцидентов, связанных с несанкционированным доступом к информационным ресурсам, необходимо обладать сведениями о пользователях, которые в настоящий момент авторизованы в информационных системах организации. В качестве механизма агрегации такой информации рекомендуем использовать механизм табличных списков.

Рассмотрим на примере. В организации для общей идентификации и авторизации пользователей используется Active Directory, а для локальной идентификации и авторизации — механизм SSO. Событие, когда пользователь не авторизован в AD, но при этом авторизуется в информационной системе (например, в «1С») должно рассматриваться как инцидент ИБ, поскольку в подобном случае возможна либо атака злоумышленников, либо нарушение внутренних регламентов организации (вход под чужой учетной записью).

Для обнаружения таких инцидентов используйте табличные списки, содержащие информацию о пользователях ИС. В правиле, обрабатывающем события входа-выхода пользователей AD, заполняется табличный список, в котором содержатся имена всех пользователей, которые авторизованы в AD на текущий момент. В дальнейшем этот список используется в правилах корреляции, например при обработке событий входа в «1С»: правило корреляции обращается к табличному списку аутентифицированных в AD пользователей, и в случае, если пользователь не авторизован в AD, регистрируется инцидент (см. рисунок ниже).



Такой сценарий позволит отслеживать инциденты, связанные с попытками несанкционированного доступа к информационным ресурсам, а также с несанкционированной передачей учетных данных между сотрудниками организации.

Контроль физического доступа

Практически во всех офисах, ЦОД, на производственных объектах развернута СКУД, которая контролирует физический доступ сотрудников в помещения организации. Использование информации, собранной со СКУД, позволяет выявлять потенциальные инциденты, связанные с несанкционированным доступом к информационным системам организации.

Для реализации такого сценария рекомендуем создать табличный список, содержащий идентификатор сотрудника и время его прохода через контрольный пункт, оборудованный СКУД. Этот табличный список будет актуализироваться правилом обработки событий СКУД и использоваться при обработке событий входа пользователя в ИС.

Рассмотрим применение табличных списков на примере системы банк-клиент, АРМ которой расположены в выделенном помещении организации:

- при получении события авторизации в банк-клиенте MaxPatrol SIEM проверяет табличный список, в котором содержатся записи о сотрудниках, находящихся в помещении;
- в случае если сотрудник, авторизованный в банк-клиенте, не находится в помещении, регистрируется инцидент.

Подобное применение табличных списков позволит детектировать инциденты, связанные с несанкционированным удаленным доступом к информационным системам организации, а также инциденты, связанные с несанкционированной передачей учетных данных между сотрудниками организации.

Еще одним вариантом использования табличных списков при интеграции со СКУД является контроль присутствия сотрудников в офисе в нерабочее время. Для реализации такого способа рекомендуем создать:

- табличный список с графиком работы;
- табличный список с выходными и праздничными днями.

При обработке событий входа в офис данная информация позволит выявлять аномальную активность сотрудников, например приход в неурочное время (ночь, праздники), вход утром — и выход на следующий день и т. п. Для снижения числа ложных срабатываний рекомендуем дополнительно создать табличный список с исключениями (ночные смены, внеурочная работа и т. п.).

Локация и окружение удаленного пользователя

При использовании сотрудниками удаленного доступа к корпоративным информационным ресурсам риск несанкционированного доступа существенно повышается. Для эффективного выявления инцидентов, связанных с несанкционированным удаленным доступом, необходимо хранить и анализировать информацию об окружении удаленного пользователя: откуда происходит подключение, идентификаторы пользователя и оборудования, перечень используемого ПО.

Для решения такой задачи рекомендуем создать табличный список, в который правилами обработки событий удаленных подключений будет вноситься информация о локации, из которой подключается пользователь, его идентификаторе и используемых им ПО и ОС[2].

В правилах корреляции будет осуществляться проверка соответствия параметров удаленного входа предыдущим параметрам пользователя, и в случае резкого расхождения (например, если пользователь последние несколько раз подключался с IP-адреса одного провайдера и использовал Windows, а сейчас подключился с IP-адреса другого провайдера и использует Linux) будет создаваться инцидент, требующий дальнейшего анализа со стороны операторов MaxPatrol SIEM.

Подобный сценарий использования табличных списков в правилах корреляции позволит выявлять инциденты, связанные с несанкционированным удаленным подключением к ресурсам организации, на ранних этапах кибератаки.

2 Реализация подобного сценария будет зависеть от применяемых технологий удаленного подключения и может потребовать разработки дополнительных коннекторов для сбора необходимой информации.

Анализ целевых атак

Целенаправленные атаки представляют серьезную угрозу для любой организации, поскольку направлены на конкретную компанию и плохо регистрируются стандартными алгоритмами СЗИ. Для идентификации целевых атак необходимо непосредственное участие аналитиков ИБ, которые анализируют различную информацию, собранную как из открытых источников, так и с помощью СЗИ организации, в том числе информацию о внешних сканированиях или попытках перебора паролей на ресурсах организации.

Рекомендуем сохранять собранную информацию для последующего анализа в табличных списках, в которых будут определены как минимум следующие поля:

- «источник атаки»;
- «время проведения атаки»;
- «тип атаки».

Время хранения записей в таком табличном списке должно быть сопоставимо с глубиной ретроспективного анализа, который будут проводить аналитики ИБ.

Информация, накопленная в табличном списке, будет использована в дальнейшем аналитиками ИБ:

- при выявлении трендовых кибератак на организацию;
- выявлении интереса к организации со стороны различных группировок злоумышленников (APT-группировок);
- анализе случаев сканирования внешних ресурсов организации.

Используя отчеты, построенные на основе табличного списка, аналитики смогут ретроспективно (после получения новых данных об атакующих) выявлять целевые атаки на организацию.

В качестве примера рассмотрим аналитику по активностям APT-группировок. Проанализировав отчет и выделив основные типы и источники атак, аналитик ИБ сможет провести поиск по сохраненной в табличном списке информации об атакам и попытках атак на организацию. В случае выявления адресов либо методик, совпадающих с теми, которые использовались в последних атаках APT-группировок, необходимо провести дальнейший анализ для выявления возможной атаки.

Для отслеживания информации об атаках на организацию рекомендуем добавить данные из табличного списка на виджет MaxPatrol SIEM. Использование виджетов позволит оперативно получать информацию о текущей ситуации с атаками на внешний периметр организации и оперативно предпринимать действия по реагированию на такие атаки.

Типовые сценарии использования

Расшифровка сокращений

Одним из вариантов использования табличных списков при обогащении данных об активах является сопоставление принятых в организации наименований оборудования. Зачастую в организациях принято именование серверов типа «SRV001-SLQ». С помощью табличных списков можно сопоставить наименования серверов с их назначением, для этого рекомендуем создать табличный список, в котором будут определены поля «имя сервера» и «назначение сервера».

Создав табличный список и загрузив в него информацию, предоставленную отделом ИТ, можно решить следующие задачи:

- группировать активы по назначению (например, все серверы CRM);
- отслеживать появление серверов без назначения;
- использовать информацию о назначении серверов в правилах корреляции событий.

Идентификация пользователей

В большинстве случаев в карточке инцидента (события) содержится идентификационная информация пользователя, с которым связаны инцидент или событие, в виде «ivanov.ii@company.net». Подобное представление требует от операторов MaxPatrol SIEM определенных временных ресурсов для однозначной идентификации пользователя. Для упрощения работы операторов рекомендуем объединить идентификационные данные пользователя с его именем и должностью. Для этого рекомендуем создать табличный список со следующими полями:

- «логин пользователя»;
- «ФИО»;
- «должность».

Наполнение такого табличного списка можно организовать следующими способами:

- ручное заполнение на основе информации, предоставленной со стороны HR;
- ручной импорт данных (в формате CSV), выгруженных из HR-системы;
- автоматическая загрузка данных из атрибутов учетной записи AD.

Созданный табличный список будет использоваться в правилах обогащения, что позволит указывать имя и должность пользователя в любых инцидентах (событиях), которые содержат информацию о логине пользователя, а также позволит сократить трудозатраты операторов MaxPatrol SIEM.

Работа с ложными срабатываниями

Табличные списки зачастую используются для снижения количества ложных срабатываний. Например, есть правило корреляции, при срабатывании которого регистрируется инцидент при соединениях между рабочими станциями по портам, которые использует вредоносное ПО. При этом в организации развернута устаревшая (legacy) клиент-серверная система, которая использует один из таких портов, что приводит к возникновению множества ложных срабатываний. Одним из вариантов снижения числа ложных срабатываний является исключение конкретного порта из правила корреляции, однако это может привести к пропуску реальных инцидентов. Для избегания подобной ситуации рекомендуем создать табличный список, в котором будут отражены все возможные легитимные соединения по данному порту, после чего использовать его в правиле корреляции. Такой подход позволит существенно снизить количество ложных срабатываний и при этом сохранит возможность обнаружения вредоносной активности.

Контроль ПО

В целях контроля использования ПО рекомендуем использовать табличные списки следующими способами:

- табличный список с перечнем запрещенного ПО — для детектирования запуска ПО, запрещенного в организации;
- табличный список с перечнем подозрительного ПО — для использования в качестве индикатора инцидента (например, запуск cmd.exe на рабочей станции HR еще не является инцидентом, но требует дополнительного анализа);
- табличный список с перечнем разрешенного ПО — для использования в тех случаях, когда точно известно, какое ПО может быть запущено, например, на серверах, компонентах АСУ ТП, банкоматах, терминалах.

Во всех указанных случаях необходимо помнить об обработке исключений для предотвращения ложных срабатываний, подобные исключения также рекомендуем устанавливать с использованием табличных списков; например, можно установить перечень пользователей, которые имеют право запускать определенное ПО, или задать технологические окна для обслуживания банкоматов.

Запрещенные соединения

Специалисты по ИБ могут создавать списки IP-адресов, соединение с которыми запрещено в организации, например IP-адресов серверов управления ботнетами, серверов обновлений ПО (при использовании централизованного обновления), IP-адресов, с которых ранее производились атаки на периметр организации. Добавив подобные IP-адреса в соответствующие табличные списки, их можно использовать в правилах корреляции для выявления таких инцидентов, как включение рабочей станции в ботнет, обход запретов на межсетевом экране, для выявления некорректной конфигурации ПО и т. п.

Рекомендации по использованию

Для эффективного использования табличных списков рекомендуем придерживаться следующих принципов.

Избегайте избыточности в табличных списках: используйте только необходимый минимум информации.

Рассмотрим на примере: есть несколько правил обогащения, которым необходима информация о соответствии логина пользователя и его имени, и правило, в котором необходимо сопоставление логина пользователя с именем, должностью, подразделением, офисом и т. п. Создание и использование для всех правил одного табличного списка со всей необходимой информацией может привести к тому, что выполнение всех этих правил потребует дополнительных ресурсов, соответственно для последнего правила рекомендуем создать отдельный табличный список с необходимой информацией, а для остальных — использовать табличный список, в котором будут храниться только логин и имя пользователя.

Группируйте информацию в табличных списках по правилам корреляции и обогащения, в которых они применяются, а также по целям использования (белый, черный список, хранение информации, исключения).

Например, в правиле корреляции необходимо использовать список пользователей, которым разрешен удаленный доступ к сети организации, при этом данный список совпадает со списком привилегированных пользователей, который используется в другом правиле корреляции. Использование одного табличного списка в двух вышеописанных правилах корреляции может привести к последующим ошибкам в самих правилах, например если

с течением времени изменится подход организации к предоставлению доступа и удаленный доступ будет разрешен не только привилегированным пользователям. Поиск и устранение ошибок могут потребовать большого количества времени и ресурсов, особенно если с момента написания правила прошло много времени, поэтому даже если списки на текущий момент совпадают, не используйте один и тот же список для двух разных целей.

При использовании табличных списков для исключений по возможности ограничивайте область действия данных исключений.

Рассмотрим на примере: MaxPatrol SIEM регистрирует много ложных срабатываний, связанных с подозрительными процессами, в основном на рабочих станциях инженеров АСУ ТП, поскольку на них используется устаревшее ПО и ПО собственной разработки. Простое решение — добавить рабочие станции в исключения — может привести к пропуску реальных инцидентов, а значит необходимо добавить в исключения конкретное ПО на конкретных рабочих станциях.

Основные выводы

Табличные списки представляют собой гибкий и эффективный механизм обмена, агрегации и хранения информации в MaxPatrol SIEM.

Табличные списки позволяют:

- хранить и поддерживать в актуальном состоянии информацию об атрибутах активов (значимость, признак категории информации и т. п.);
- эффективно использовать данные, импортируемые из иных систем организации;
- хранить информацию для последующего ретроспективного анализа;
- управлять ложными срабатываниями;
- поддерживать списки исключений;
- хранить и поддерживать в актуальном состоянии информацию для обогащения событий и инцидентов.