Как использовать статические и динамические группы активов в MaxPatrol SIEM

ptsecurity.com

Содержание

Резюме

В этом документе мы расскажем, как использовать группировку активов в MaxPatrol SIEM, чтобы повысить эффективность процессов управления активами, событиями и инцидентами ИБ.

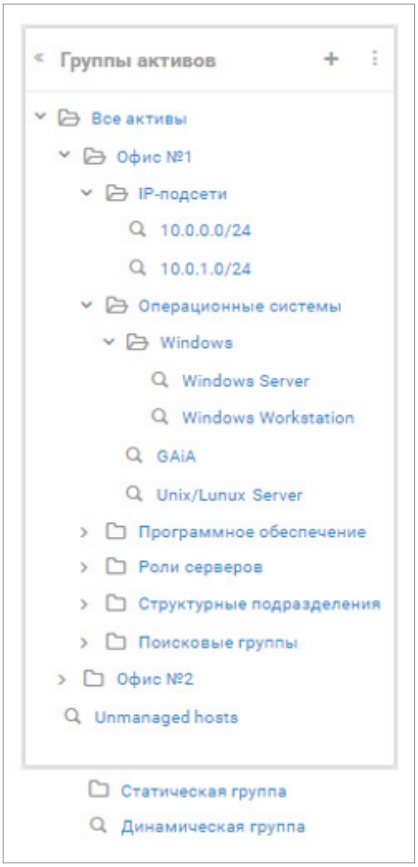
Опрос о трудозатратах специалистов на работу с SIEM-системами, проведенный Positive Technologies[1], показал, что каждый третий специалист:

- систематизирует и анализирует происходящее внутри организации;
- обновляет сведения об ИТ-инфраструктуре;
- настраивает источники событий и следит за их работоспособностью.

Систематизация сведений об активах, автоматический поиск и аудит активов, акцентирование внимания на действительно важных изменениях в ИТ-инфраструктуре организации позволяют существенно упростить повседневную работу операторов MaxPatrol SIEM и сосредоточиться на выявлении инцидентов ИБ и реагировании на них.

Приведенная здесь информация будет полезна вне зависимости от того, являетесь ли вы оператором MaxPatrol SIEM или только задумываетесь о пилотном проекте или внедрении системы.

Несколько фактов о группах активов в MaxPatrol SIEM



Группировка в MaxPatrol SIEM

В MaxPatrol SIEM используется иерархическая структура групп активов, в которой предусмотрены следующие типы групп:

- системные группы;
- пользовательские группы, которые могут быть динамическими или статическими.

Вендором предустановлены две системные группы активов. Первая группа содержит все активы, известные MaxPatrol SIEM, вторая содержит активы, которые не попали ни в одну из пользовательских групп, что указывает оператору системы на наличие активов, о которых недостаточно информации.

Все пользовательские группы создаются оператором и входят в состав системной группы «Все активы».

Статические и динамические группы

Для эффективной систематизации активов рекомендуем использовать сочетание статических и динамических групп. Статические группы формируют логическую структуру групп. Группы создаются таким образом, чтобы объединять активы на основе обобщающего признака, например по территориальному признаку или используемой ОС. Статические группы наполняет активами оператор — вручную или с использованием динамических групп.

1 С результатами опроса можно ознакомиться на сайте Positive Technologies: ptsecurity.com/ru-ru/research/analytics/siem-report-2019/#id6

Динамические группы служат для поиска активов на основе имеющихся в MaxPatrol SIEM сведений — например, на основе типа узла, IP-адреса, DNS-имени, открытых портов, ОС, состава ПО. Поиск выполняется на основе фильтров, задаваемых оператором при создании группы. Например, можно создать статическую группу «ОС», в состав которой будут входить динамические группы, каждая из которых будет отдельно осуществлять поиск активов под управлением Windows, Unix или macOS.

Практические кейсы использования групп активов

Группы активов в процессе управления активами

Группировку активов рекомендуем использовать для решения следующих задач процесса управления активами:

- систематизация сведений об активах;
- присвоение значимости активам;
- автоматизация поиска и аудита активов;
- мониторинг состояния активов.

Систематизация сведений об активах

Систематизация позволяет упростить оператору поиск информации об активах, что положительно сказывается на сроке принятия решений, связанных как с процессом управления активами, так и с процессами управления событиями и инцидентами ИБ.

В первую очередь рекомендуем выполнить группировку активов по территориальному признаку на основе статических групп, например: страна > область > город > площадка. Если MaxPatrol SIEM обслуживает единственную площадку организации, рекомендуем сразу перейти на следующий уровень группировки.

Следующий уровень группировки включает в себя несколько отдельных статических групп и входит в состав каждой площадки (при наличии нескольких площадок в организации).

Рекомендуем применять следующий базовый набор признаков группировки:

- IP-подсети;
- операционные системы;
- структурные подразделения;
- роли серверов;
- программное обеспечение;
- поисковые группы.

Внутри групп активов находится последний уровень группировки, формируемый на основе динамических групп, обеспечивающих наполнение статических групп активами в автоматическом режиме. Если отсутствует возможность периодического сканирования актива, его можно внести в статическую группу вручную. Примеры групп активов приведены в таблице ниже.

Предложенная нами структура групп может изменяться под нужды любой организации для повышения уровня детализации, как правило путем добавления вложенных статических групп, например:

- **операционные системы:**
  - Windows:
    - Windows Workstation;
    - Windows Server;
    - и т. п.

В состав этих групп активов войдут динамические группы, соответствующие версиям ОС семейства Windows.

Таблица 1. Примеры динамических групп

СТАТИЧЕСКИЕ ГРУППЫ	ПРИМЕРЫ ВЛОЖЕННЫХ ДИНАМИЧЕСКИХ ГРУПП	ЦЕЛЬ ИСПОЛЬЗОВАНИЯ
Структурные подразделения	Топ-менеджмент, HR, бухгалтерия	Определение значимости активов на основе принадлежности к структурному подразделению, а также определение ответственных лиц и сведений о расположении актива
Роли серверов	AD, СУБД, application server	Мониторинг серверной группы и определение значимости на основе роли сервера
IP-подсети	IP-подсети организации (10.0.0.0/24, 10.0.1.0/24 и т. п.)	Автоматизация поиска активов
Операционные системы	Windows, Unix/Linux, macOS, GAiA	Группировка для направленного аудита активов и сбора событий с определенных типов ОС
Программное обеспечение	«1С», SAP, Zabbix	Группировка для направленного аудита активов и сбора событий с определенного типа ПО
Поисковые группы	Открыт удаленный доступ, выявлено запрещенное ПО	Автоматический поиск активов, потенциально нарушающих политику ИБ организации или характеризующих подозрительную ситуацию

Актуализация информации об активах

MaxPatrol SIEM выполняет периодический сбор информации об активах на основе задач аудита, которые в качестве целей могут использовать IP-адреса, DNS-имена или группы активов. Использование динамических групп в этом случае позволяет добиться двух преимуществ. Первое обусловлено тем, что группы обновляются автоматически и оператору не требуется постоянно корректировать цели для задач аудита. Второе преимущество — скорость сбора данных — достигается с помощью точного выбора и настройки методов сбора данных для сгруппированных активов.

Мониторинг состояния активов

В связи с тем, что работа операторов однообразна, они часто пропускают изменения активов, кажущиеся им повседневными. Для снижения подобных рисков рекомендуем настроить поисковые группы MaxPatrol SIEM, оповещающие оператора о фиксации определенного состояния актива, например:

- открыты запрещенные сетевые порты;
- выявлено запрещенное ПО;
- активна учетная запись локального администратора;
- узел имеет статический IP-адрес (не получает через DHCP).

Приоритизация активов

Для снижения трудоемкости операций при присвоении (переопределении) значимости активам в MaxPatrol SIEM предусмотрена возможность задания значимости целым группам активов. Активы, в свою очередь, наследуют значимость от групп, участниками которых они становятся, при этом теряют значимость, покидая группы. Благодаря этой функциональности актив всегда будет иметь максимальную величину значимости среди собственного и наследуемых значений.

При присвоении значимости активам рекомендуем придерживаться следующих принципов:

- задавайте базовую значимость всем активам с помощью групп;
- для критически важных активов задавайте значимость вручную;
- поисковым группам задавайте повышенную значимость.

Примеры присвоения значимости активам приведены в таблице ниже.

Таблица 2. Примеры присвоения значимости активам

ГРУППА АКТИВОВ	ЗНАЧИМОСТЬ	НАЗНАЧЕНИЕ ЗНАЧИМОСТИ
Все активы	Низкая	Назначается базовая значимость всем активам
Офис № 1	Не назначена	Неэффективно присваивать значимость активам, поскольку оценить ее по данным критериям группировки невозможно
• IP-подсети	Не назначена	
• Операционные системы	Не назначена	
Структурные подразделения	Не назначена	Назначается вложенными группами
• Топ-менеджмент	Высокая	Определяется владельцами активов
• Бухгалтерия	Высокая	
• HR	Низкая	
Роли серверов	Не назначена	Назначается вложенными группами
• Domain Controller	Высокая	Определяется владельцами активов
• Terminal Server	Высокая	
• File Server	Средняя	

Группы активов в процессах управления событиями и инцидентами ИБ

Наличие информации об активах в MaxPatrol SIEM и применение механизма группировки позволяют решить ряд задач процессов управления событиями и инцидентами ИБ:

- автоматизация активного сбора событий;
- учет особенностей активов при корреляции событий;
- предварительная группировка событий;
- локализация затронутых инцидентом участков ИТ-инфраструктуры.

Автоматизация активного сбора событий

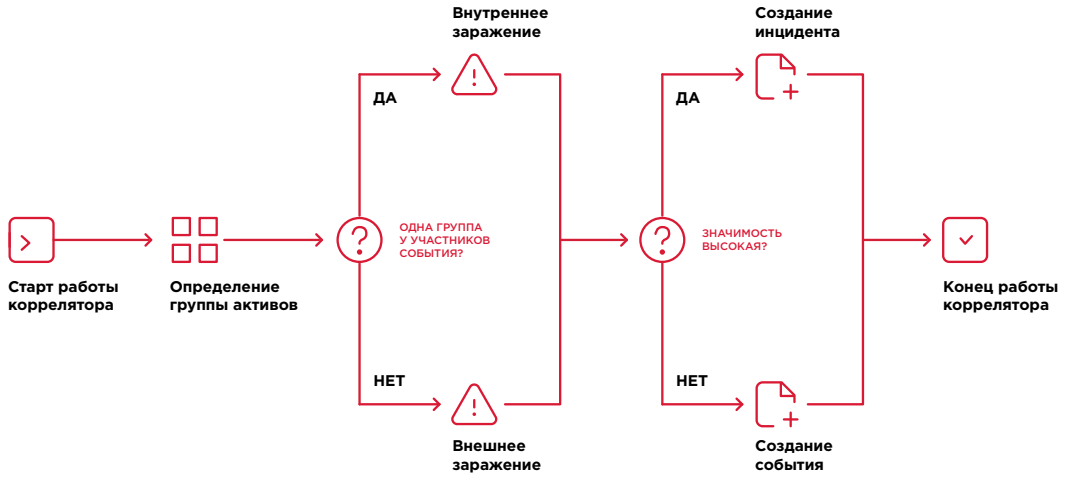
Активные методы сбора событий требуют формирования пары «метод сбора событий <—> цель сбора событий (источник)». По аналогии с аудитом активов для автоматизации сбора событий рекомендуем операторам MaxPatrol SIEM в качестве целей использовать группы активов, имеющие в своем составе источники событий. При этом стоит учитывать, что методы сбора событий непосредственно связаны с ПО, с которого происходит сбор, а значит формирование групп во многом зависит от источников событий, подключаемых к MaxPatrol SIEM.

Если после аудита будет выявлен источник событий на активе, то он автоматически попадет в соответствующую ему группу источников, и MaxPatrol SIEM будет собирать события с данного источника без дополнительных действий со стороны оператора.

Использование групп активов в правилах корреляции

Тонкая настройка правил корреляции снижает количество ложных срабатываний, тем самым снижая нагрузку на операторов в части разбора событий, ошибочно признанных инцидентами.

При обработке событий правило корреляции может запрашивать у MaxPatrol SIEM дополнительную информацию об активах и их членстве в группах. Для примера рассмотрим часть алгоритма правила корреляции, определяющего тип заражения вредоносным ПО (внутреннее, внешнее) и порядок создания инцидента (см. рисунок ниже). Внутреннее заражение — распространение вредоносного ПО по сети организации, внешнее — заражение путем загрузки вредоносного ПО из интернета или посредством загрузки с флеш-накопителей работников организации.



Предварительная группировка событий и инцидентов ИБ

При работе с событиями и инцидентами рекомендуем операторам MaxPatrol SIEM использовать сформированные группы активов в качестве первичного фильтра событий по источнику и участникам события. Например, если необходимо выполнить поиск инцидентов в серверной группе, можно выбрать группы по IP-адресам серверов или группы по ролям серверов.

Определение масштаба влияния инцидента на инфраструктуру

Одним из важных этапов работы с инцидентом ИБ является определение затронутых им участков ИТ-инфраструктуры.

При регистрации инцидента с ним автоматически сопоставляются активы-участники, перечень которых определяет правило корреляции, и связанные с ним события. На основе этой информации MaxPatrol SIEM указывает в карточке инцидента все группы активов, связанные с активами — участниками инцидента. Этот механизм упрощает оператору процесс локализации затронутых участков ИТ-инфраструктуры организации за счет полученных знаний о смежных активах. Например, произошел инцидент заражения сервера SAP сетевым червем. При изучении карточки инцидента оператор может получить сведения о том, что он является членом групп «Подсеть 10.15.64.0/24», «Серверы», «SAP» и т. п. Анализируя возможности вредоносного ПО и принятые меры защиты, можно сделать вывод о том, что червь потенциально может распространиться по активам подсети. Используя полученную информацию и возможности предварительной группировки активов, событий и инцидентов можно выполнить проверку затронутых активов.

Если в процессе расследования оператор вручную прикрепит активы к инциденту, система автоматически предоставит оператору обновленные сведения о группах, затронутых инцидентом.

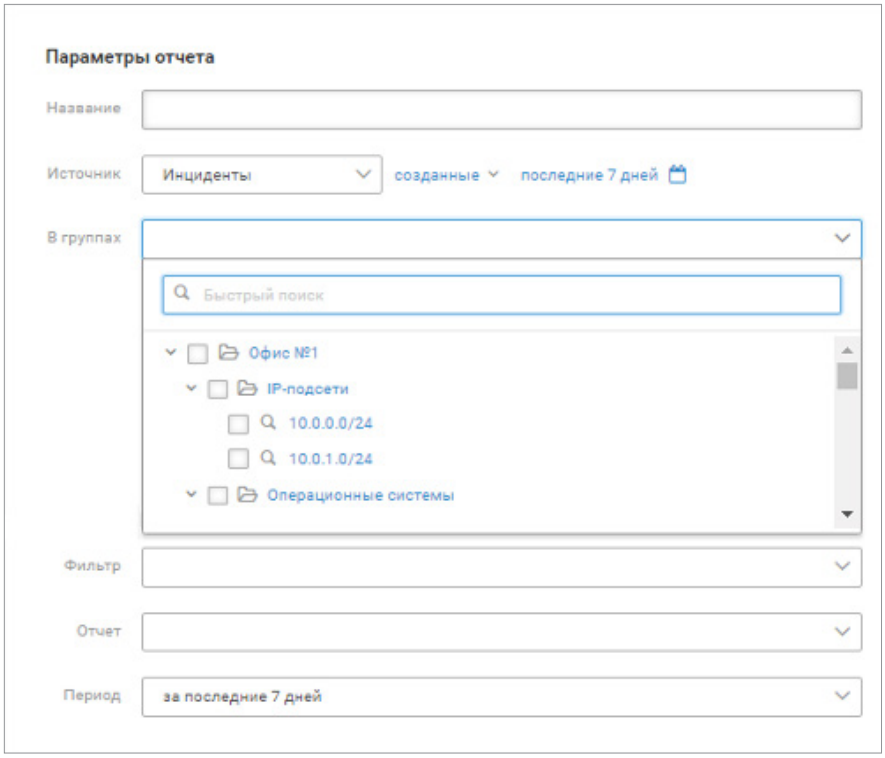
Разграничение доступа и отчетность

Ограничение доступа к информации

Доступ к сведениям об активах, событиях и инцидентах обеспечивается на основе созданных групп активов. Это позволяет предоставлять оператору доступ к информации, связанной только с выбранными группами, а значит отдельные категории пользователей не смогут ознакомиться с недоступной для них информацией. Например, оператор площадки № 1 не сможет анализировать события площадки № 2 или часть персонала не сможет получать доступ к информации о критически важных активах и связанных с ними событиях и инцидентах.

Формирование отчетности

MaxPatrol SIEM позволяет формировать отчетность по процессам управления активами, событиями и инцидентами ИБ. Функция группировки активов обеспечивает возможность предварительной фильтрации информации, поступающей в отчет.



Инструкция по применению

Для эффективного использования механизма группировки активов рекомендуем придерживаться чек-листа, приведенного ниже.

ЧЕК-ЛИСТ

ПРЕДВАРИТЕЛЬНЫЙ ЭТАП

- [ ] Проведение первичного сканирования
- [ ] Уточнение полученных сведений об активах

- [ ] Формирование структуры статических групп
- [ ] Формирование динамических групп
- [ ] Разграничение доступа к информации на основе групп
- [ ] Разработка правил корреляции на основе групп
- [ ] Определение и присвоение значимости активам
- [ ] Настройка автоматического аудита активов
- [ ] Формирование структуры статических групп
- [ ] Настройка автоматического сбора событий

Основные выводы

Группировка активов в MaxPatrol SIEM является не просто эффективным, но и необходимым инструментом при построении и функционировании процессов управления ИБ в любой организации. Использование групп активов позволяет значительно снизить трудозатраты операторов системы:

- на инвентаризацию и мониторинг активов;
- сбор и обработку событий;
- выявление и реагирование на инциденты ИБ;
- формирование отчетности,

что оказывает непосредственное влияние на сроки принятия решений, связанных с соответствующим процессом управления ИБ.