Детектирующая логика: как на раннем этапе заложить порядок в SIEM

Зуев Владимир, АО «Россельхозбанк»

Что такое корреляционное правило?

Корреляция - «синхронное поведение» или «взаимозависимость» двух или нескольких параметров в рассматриваемой системе;

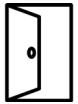
Правило в SIEM - набор тестов, который проходят события при поступлении в SIEM;

'21 МЕНЯЕМСЯ ВМЕСТЕ

Зачем систематизировать управление правилами?

Измеримость и управляемость покрытия

Упрощение масштабирования



Оптимизация управления исключениями

Создание единой точки накопления знаний

'21 МЕНЯЕМСЯ ВМЕСТЕ

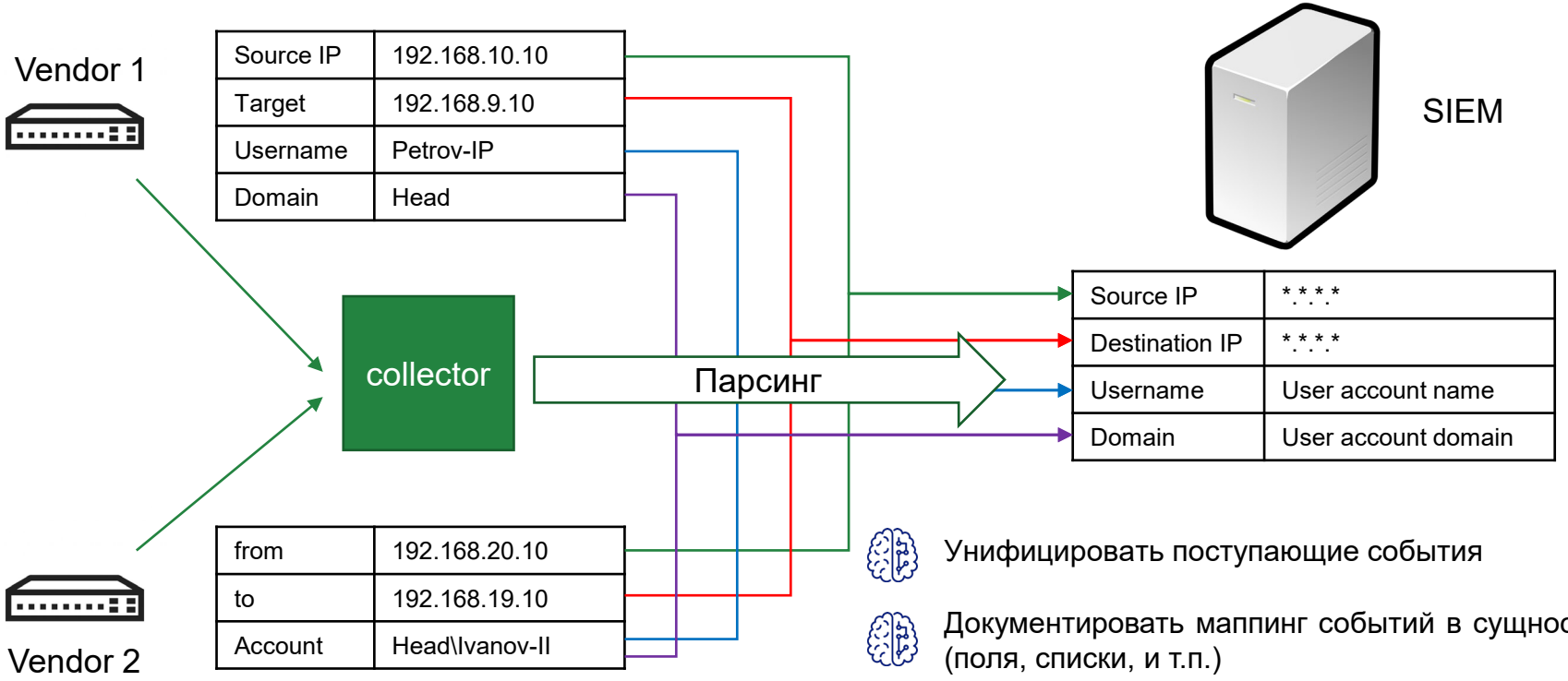
Обязательные аттрибуты каждого правила

Правило

Имя правила	Группа пользователей	Уязвимости
Сценарий выявления (use case)	Источники событий	Элемент Mitre ATT&CK
Логическое правило	Зависзависимые сущности	Ссылки на сценарии реагирования
Описание SIEM правила	Ключевые особенности	Используемые исключения

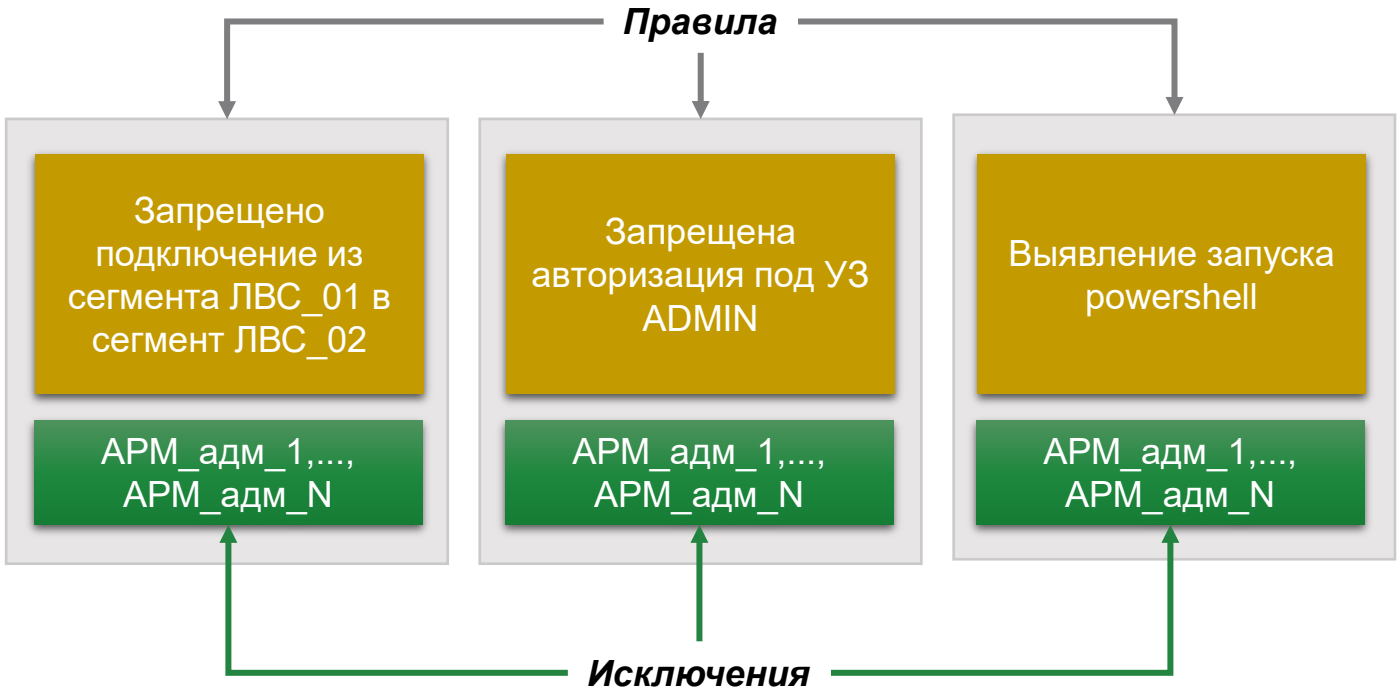
'21 МЕНЯЕМСЯ ВМЕСТЕ

Управление источниками



- Унифицировать поступающие события
- Документировать маппинг событий в сущности SIEM (поля, списки, и т.п.)
- Учитывать в архитектуре SIEM не только что и как подключаем в виде источника, но и какие события приходят от источников

Управление исключениями



Управление исключениями

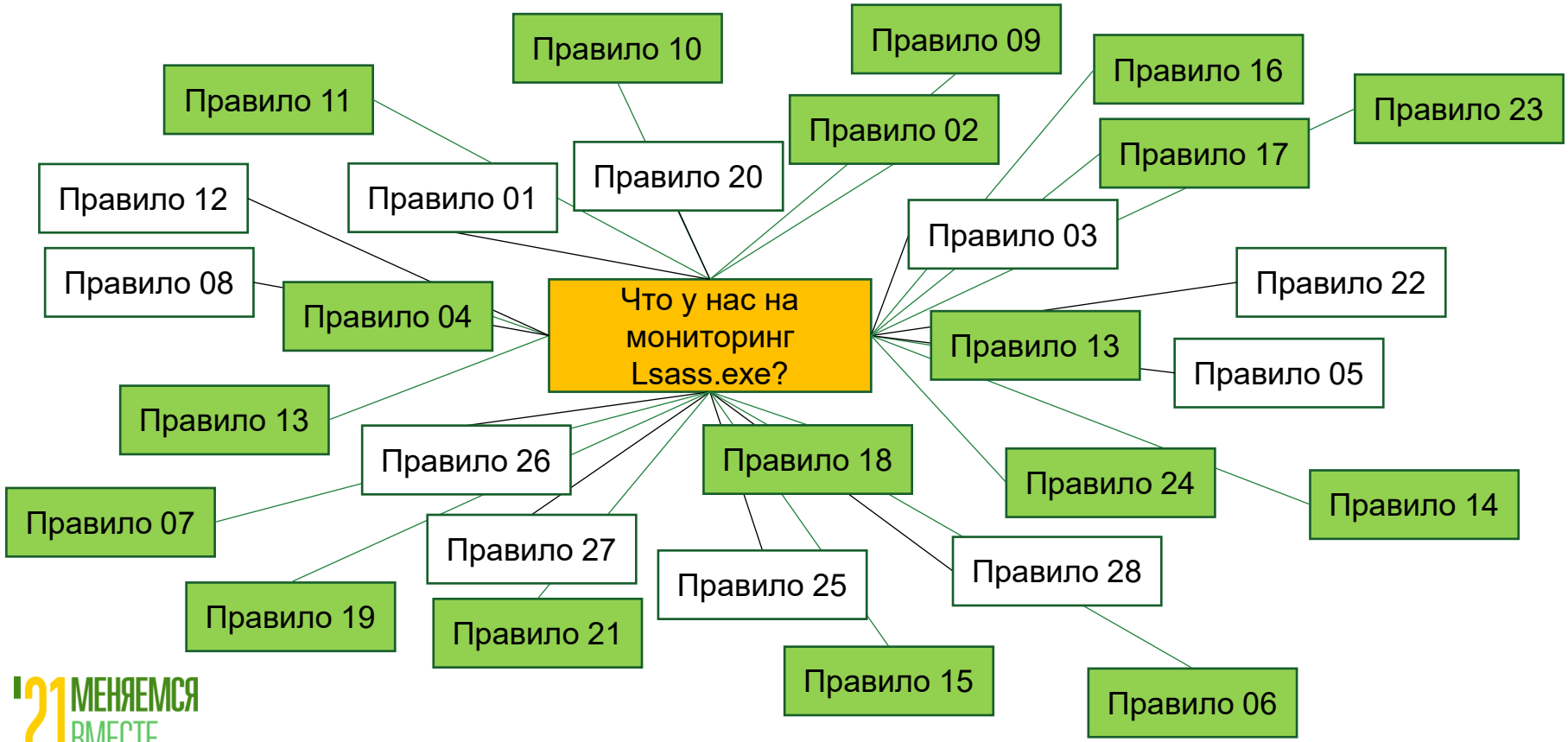
Появился новый администратор

- Вносить в каждом правиле новый АРМ администратора в исключения
- Создать список АРМ администраторов и включать этот список в необходимые правила

- Хранить исключения отдельно как обособленные сущности
- Детально документировать и хранить подтверждения
- Относиться критически и аккуратно вписывать в правила
- Применять единый подход к работе с исключениями

'21 МЕНЯЕМСЯ ВМЕСТЕ

Стандартизация в работе



'21 МЕНЯЕМСЯ ВМЕСТЕ

Варианты систем хранения

Что должна уметь?

- поиск по параметрам, используемым в правилах\сценариях;
- управление версиями правил\сценариев;
- возможность одновременной работы нескольких пользователей;
- интеграция с системой управления заявками.

Confluence

GitLab

'21 МЕНЯЕМСЯ ВМЕСТЕ

Полезные советы

- Используейте как основную сущность – сценарии выявления (Use cases);
- Помните и понимайте, что поддержание правил и сценариев в актуальном состоянии требует ресурсов;
- Процесс разработки и накопления базы правил должен отличаться в зависимости от этапа жизненного цикла SIEM системы или построения SOC;
- Аналитик SIEM должен набираться в штат одним из первых, а не последний когда все готовы и «ждут правил» чтобы стартовать;
- Выстраивание системы работы с правилами - большой объем работы, но её игнорировани гарантирует боль на дистанции;
- Аналитики с режимом работы 5\2 не вносят правки в правила в пятницу вечером (регламентируйте работы);

'21 МЕНЯЕМСЯ ВМЕСТЕ

Спасибо за внимание!

E-mail: zuevvm@rshb.ru
Tg: @Kpzrr

'21 МЕНЯЕМСЯ ВМЕСТЕ