Батетников Илья

Эксперт MP10

Валерий Горбачев

Руководитель направления внедрения средств защиты информации АО "ДиалогНаука"

Гибкий процесс управления уязвимостями на базе MaxPatrol VM

ТОП-4 векторов проникновения

НКЦКИ

1. Эксплуатация уязвимостей на периметре
2. Подрядчики и системы, имеющие сопряжение с целевой инфраструктурой
3. Фишинг
4. Обычное ВПО как точка входа для профессиональных кибергруппировок

Как прошел 2022?

Методичка НКЦКИ

Как определить какие обновления устанавливать?

25227 новых CVE

Без учета уязвимостей в Отечественном, Китайском ПО, и других уязвимостей без CVE,

Методики ФСТЭК

оценки уровня критичности уязвимостей программных, программно-аппаратных средств
тестирования обновлений безопасности программных, программно-аппаратных средств.

Проекты методик ФСТЭК

оценки защищенности уже не ПО, как две предыдущие, а целой информационной систем
оценки защищенности целой организации

Проверка обновлений

ФСТЭК анонсировал тестирование обновлений

Log4Shell (CVE-2021-44228)

Exchange (CVE-2022-41080)

...

Результаты пилотных проектов MaxPatrol VM 2022

в 100%

организаций обнаружены трендовые уязвимости

около 600 трендовых уязвимостей обнаружено в пределах пилотной зоны

на 1 актив высокой степени значимости в среднем приходится

2 трендовые уязвимости

10% выявленных трендовых уязвимостей

содержалась на активах высокой степени значимости

47 трендовых уязвимостей

приходилось на каждые 100 активов

Исследование основано на результатах 27 пилотных проектов MaxPatrol VM, которые проводились в 2022 году

Как начался 2023?

Проект методики ФСТЭК

Как построить процесс управления уязвимостями

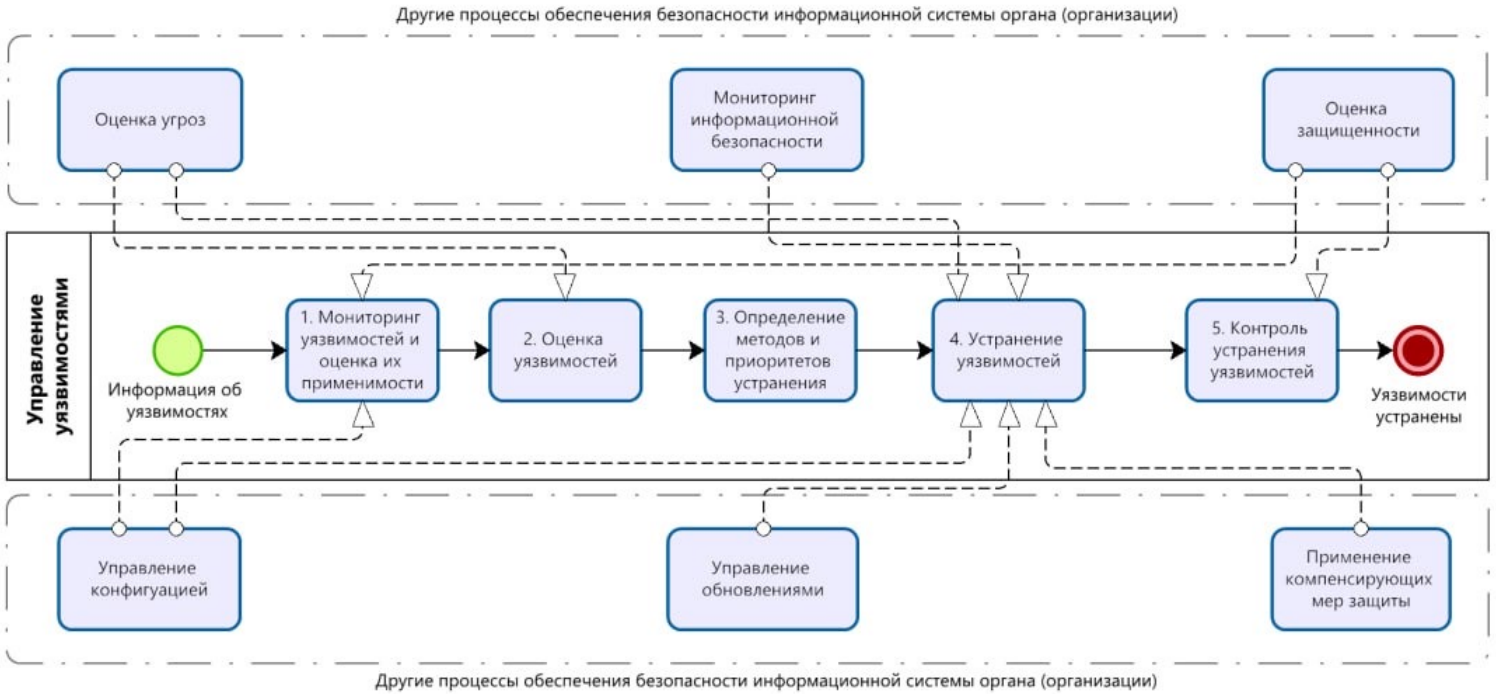
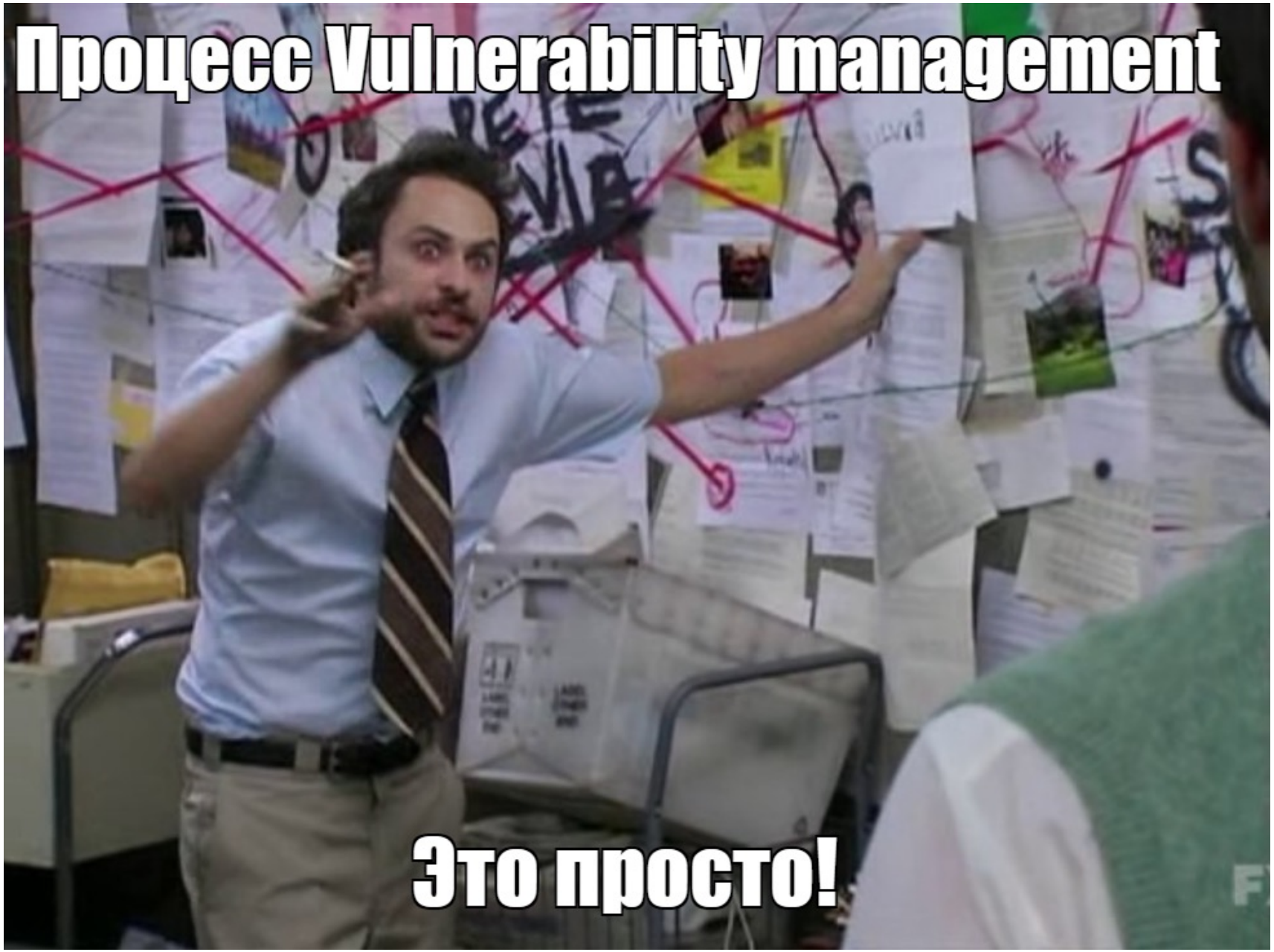


Рисунок 2.2. – Схема Процесса


Процесс Vulnerability management
Это просто!

Как должно быть

Процесс VM

Плановая обработка уязвимостей

- В IT-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с IT-отделом

Особо опасные уязвимости

- Фокус ИБ и IT смещается на трендовые уязвимости и те, что имеют эксплойт* и расположены на важных активах
- О сроках устранения каждой уязвимости служба ИБ и IT-отдел договариваются отдельно

- **Эксплóйт** —программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые злоумышленниками для атаки.

Управление уязвимостями

VM

01
Следим за постоянной актуализацией данных об активах

02
Оцениваем и классифицируем активы

03
Договариваемся с IT и фиксируем политики

04
Система определяет и сортирует уязвимости

05
Следим за устранением уязвимостей и за соблюдением политик

06
Смотрим общие метрики, оцениваем тренд по компании

Выделение особо опасных уязвимостей.

Оперативное реагирование на них вне процесса.

Обработка Особо Опасных

MaxPatrol VM

MaxPatrol VM

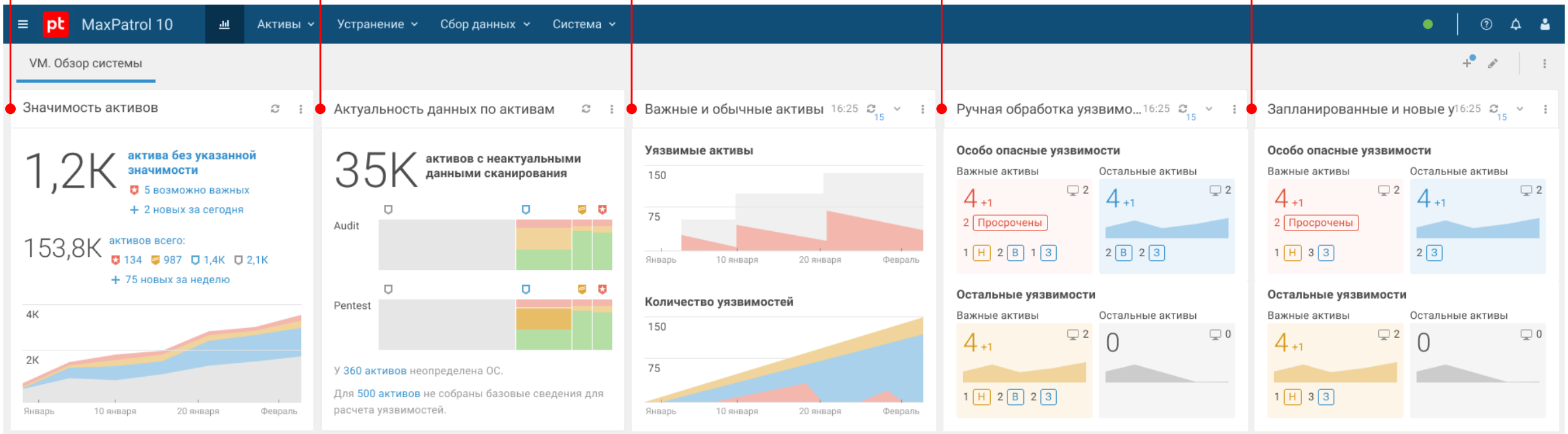
VM нашел все активы в сети. Приоритизируйте их, чтобы знать, что важно

Получайте свежую информацию об активах и их уязвимостях. Задайте политики сканирования

Контролируйте, что происходит на важных активах. Отслеживайте появление новых активов

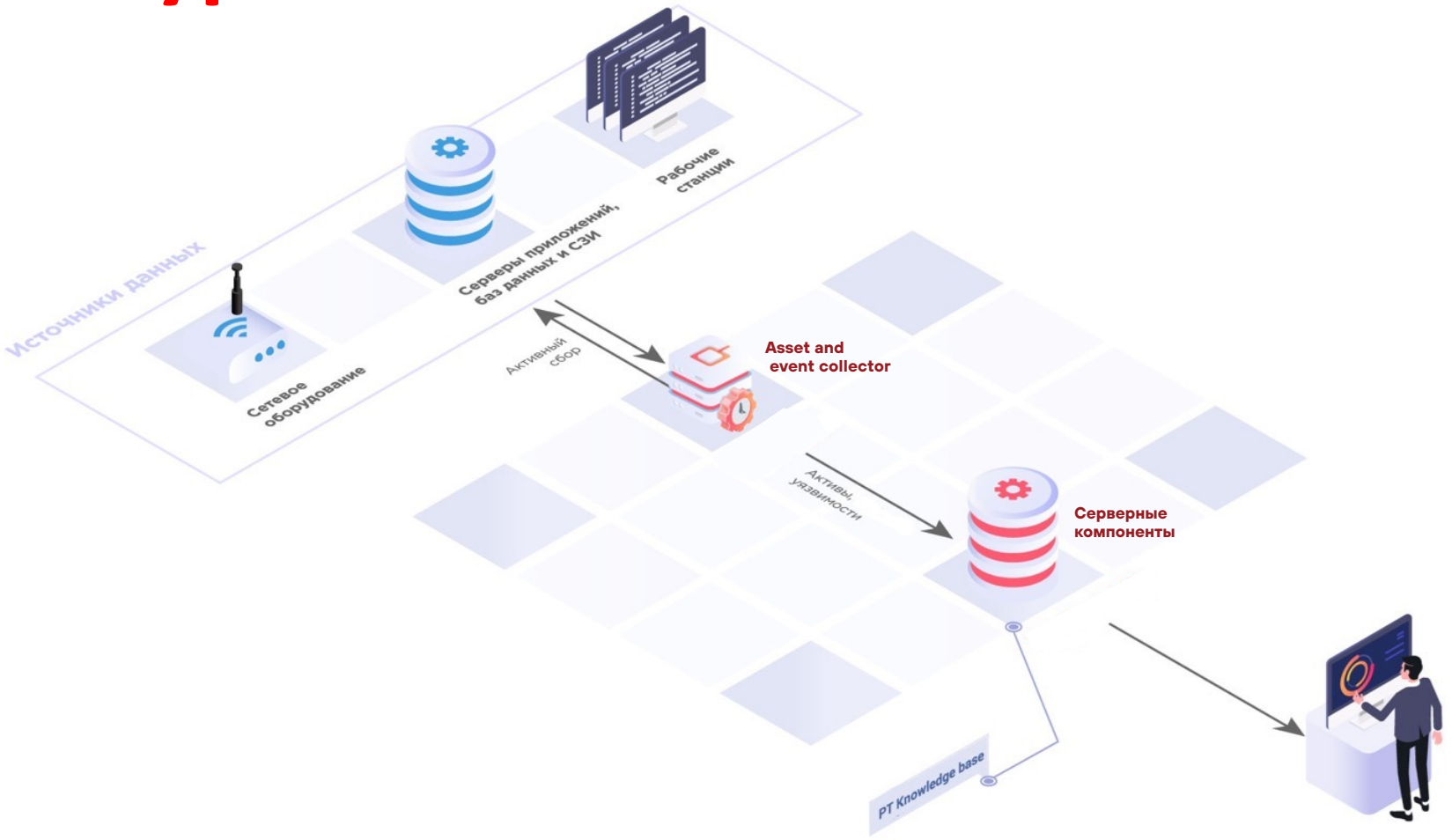
Обычные уязвимости исправляет IT-отдел в рамках политик. Специалист по ИБ смотрит только за особо опасными уязвимостями

Специалист по ИБ смотрит за нарушением политик. Контролируте своевременное устранение



Архитектура и лицензирование

Архитектура MaxPatrol VM



Варианты поставки и модель лицензирования

Поставка:

- ПО (можно развернуть в виртуальной среде или на физическом сервере заказчика)
- Программно-аппаратный комплекс

Годовое лицензирование:

1. Enterprise-архитектура.

Базовая лицензия по количеству активов (на 1, 2, 5, 10, 20, 50 или 100 тысяч активов)

HA (Лицензия на кластерную конфигурацию MaxPatrol VM) по количеству активов строго соразмерно базовой лицензии (на 1, 2, 5, 10, 20, 50 или 100 тысяч активов)

Non-production лицензия для развертывания конфигурации MaxPatrol VM для непродуктивных задач: восстановление из рез. копий, тестирования интеграций, отладки правил корреляции и т.п.

2. Инфраструктурные лицензии:

- **Server** — управляющий сервер
- **Лицензия для выявления уязвимостей активов** для неограниченного количества DataCollectors (на 100, 250, 500, 1 000 и 5 000 активов)
- **Лицензия для проверки соответствия стандартам** (на 100, 250, 500, 1 000 и 5 000 активов)
- **Лицензия на мобильный сканер MaxPatrol VM**, предназначенный для поиска уязвимостей в изолированных сетях и последующим переносом информации на основную инсталляцию (на 100, 250, 500, 1 000 активов)
- **Индустриальные лицензии** предназначенные для работы компонентов в технологических сетях передачи данных

MaxPatrol 10

Сочетание двух продуктов повысит уровень защищенности компании: даст возможность коррелировать события с уязвимостями и оперативно на них реагировать

ЭКСПЕРТИЗА PT

В ПАКЕТАХ ЭКСПЕРТИЗЫ:

- правила выявления атак
- рекомендации по реагированию
- обновления параметров сбора и обработки событий ИБ

В БАЗЕ ЗНАНИЙ:

- правила расчета уязвимостей
- трендовые уязвимости
- рекомендации по устранению выявленных уязвимостей

ВОЗМОЖНОСТИ

MAXPATROL SIEM

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ В РЕАЛЬНОМ ВРЕМЕНИ

- Сбор и анализ событий
- Выявление актуальных атак
- Расследование сложных инцидентов

MAXPATROL VM

ПОСТРОЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ, РЕЗУЛЬТАТЫ КОТОРОГО ВИДНЫ

- Обнаружение и приоритизация уязвимостей
- Настройка политик сканирования и устранения уязвимостей
- Контроль защищенности

ОСНОВА

SECURITY ASSET MANAGEMENT

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений