POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES

Использование решений Positive Technologies в процессе управления уязвимостями

Олег Матыков

руководитель отдела проектных решений

Positive Technologies

Вебинар

Процесс управления уязвимостями

Уязвимость – это характеристика, которая может быть использована нарушителем при проведении атаки на ИТ-актив и привести к реализации угрозы.

Процесс управления уязвимостями – циклические действия, направленные обнаружение и классификацию уязвимостей, а также на их устранение или снижение последствий их эксплуатации.

Проблемы процесса управления уязвимостями

- Процесс не документирован, поиск и устранение проводятся бессистемно
- Процедуры сканирования и устранения не синхронизированы
- Процесс управления уязвимостями регламентирован, но автоматизирован неэффективно

Документирование процесса управления уязвимостями

Документирование процесса УУ

1. Политика управления уязвимостями
2. Процедура управления уязвимостями
3. Настройки системы управления уязвимостями
4. Инструкции пользователей (для каждой роли)
5. Дополнения в должностные инструкции
6. Приказ о внедрении системы управления уязвимостями

Документирование процесса УУ

Политика управления уязвимостями – небольшой документ с описанием границ процесса управления уязвимостями, цели и задачи, основные принципы процесса. Может быть частью общей политики ИБ.

Процедура управления уязвимостями – подробное описание шагов процесса и контроля эффективности процесса. Роли и функции

Документирование процесса УУ

Настройки системы управления уязвимостями – документирование настроек информационных систем УУ

Инструкции пользователей - перечень задач роли и описание основных функции

Дополнения в должностные инструкции – обязанности в рамках процесса УУ

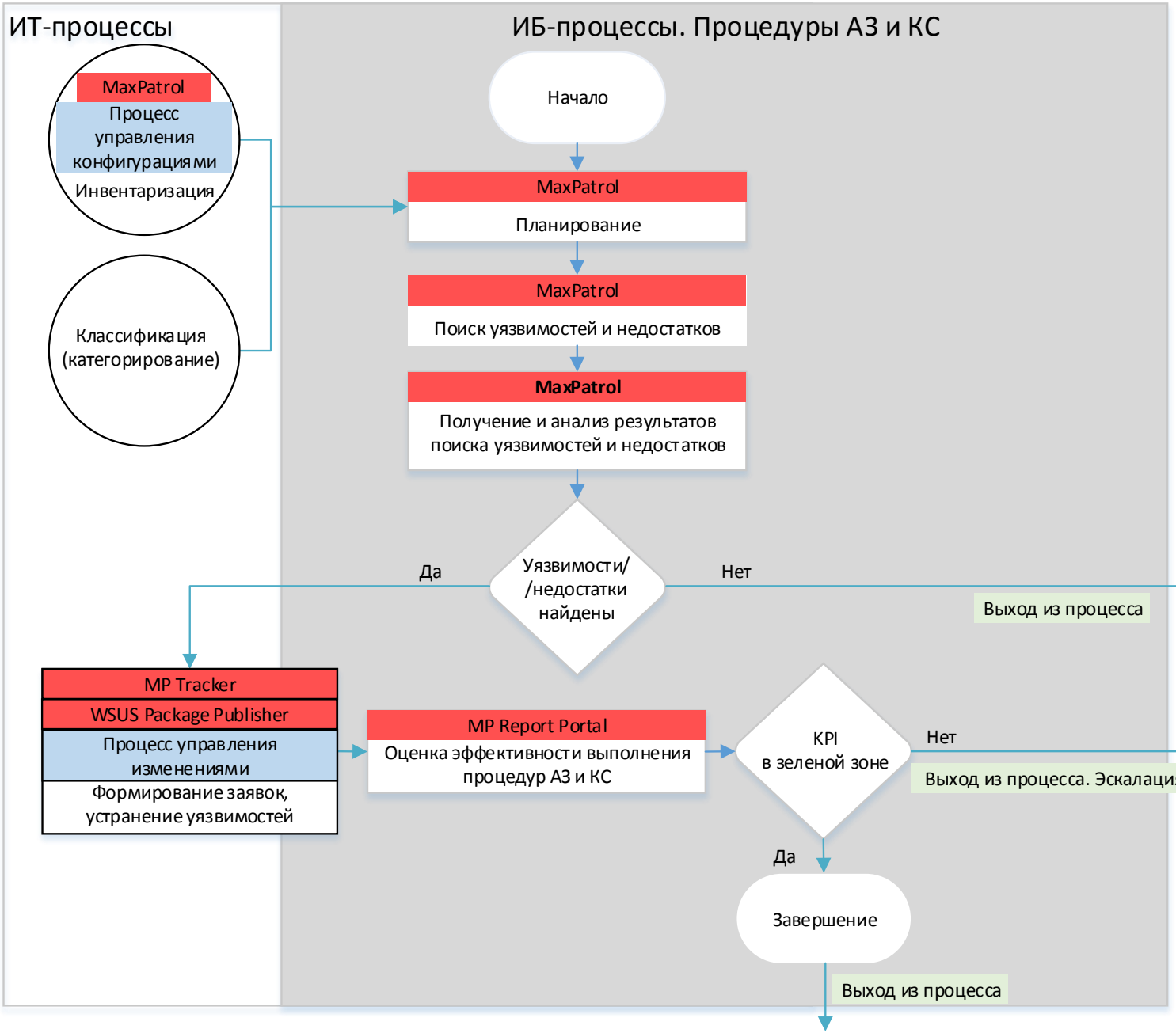
Приказ о внедрении системы управления уязвимостями – формально закрепляет ответственность сотрудников

Возможности автоматизации процесса управления уязвимостями

Управление уязвимостями

Инструменты для управления уязвимостями

Пример с решениями Positive Technologies


ИТ-процессы
ИБ-процессы. Процедуры АЗ и КС
MaxPatrol
Процесс управления конфигурациями
Инвентаризация
Классификация (категорирование)
Начало
MaxPatrol
Планирование
MaxPatrol
Поиск уязвимостей и недостатков
MaxPatrol
Получение и анализ результатов поиска уязвимостей и недостатков
Уязвимости/ /недостатки найдены
Да
Нет
Выход из процесса
MP Tracker
WSUS Package Publisher
Процесс управления изменениями
Формирование заявок, устранение уязвимостей
MP Report Portal
Оценка эффективности выполнения процедур АЗ и КС
KPI в зеленой зоне
Нет
Выход из процесса. Эскалация
Да
Завершение
Выход из процесса

Как это выглядит на практике

Автоматизация процедур анализа защищенности

Применяемые средства

MaxPatrol

- инвентаризация компонентов ИС
- планирование поиска уязвимостей и недостатков
- поиск уязвимостей и недостатков
- анализ результатов выполнения процедур АЗ и КС
- выпуск отчетов

MP Tracker и WSUS Package Publisher

- управление изменениями (интеграция с Service Desk)

MP Report Portal

- оценка эффективности выполнения процедур АЗ и КС

Участники процесса

- Владелец актива
- Ответственный за обеспечение безопасности – лицо, осуществляющее контроль состояния информационной безопасности ИС
- Ответственный за техническое обслуживание – лицо, которое обеспечивает эффективную (с точки зрения соответствия полноты технической поддержки бизнес-процессов компании) работу ИС на различных стадиях жизненного цикла

(Категорирование активов)

Уровень критичности напрямую связан с ценностью актива для компании и определяет уровень требований по обеспечению его защиты, в том числе — к своевременности выявления уязвимостей, которая, в свою очередь, определяется периодичностью сканирования

Критерии оценки уровня критичности (потенциального воздействия от потери конфиденциальности, целостности и доступности информации):

- нарушение законов и (или) подзаконных актов
- финансовые потери
- снижение эффективности бизнеса
- негативное воздействие на репутацию

Планирование поиска уязвимостей

Это не только расписание сканирования

Периодичность и характер проводимых проверок определяются:

- уровнем критичности (значимости) актива
- целями проверки (поиск уязвимостей, аудит, контроль соответствия стандартам)
- доступными способами сбора данных (используемые механизмы ОС, протоколы взаимодействия, учетные записи)
- рисками, связанными с выбранным способом сбора данных

Поиск уязвимостей и недостатков или коротко о MaxPatrol

Режимы сканирования:

- Механизм тестирования на проникновение (Pentest)
- Системные проверки (Audit)
- Контроль соответствия стандартам (Compliance)

Анализ результатов сканирования

Предварительный анализ результатов сканирования проводится для определения:

- ошибки идентификации
- ошибок проброса порта
- ложных срабатываний
- ошибок сканирования

Форма представления результатов

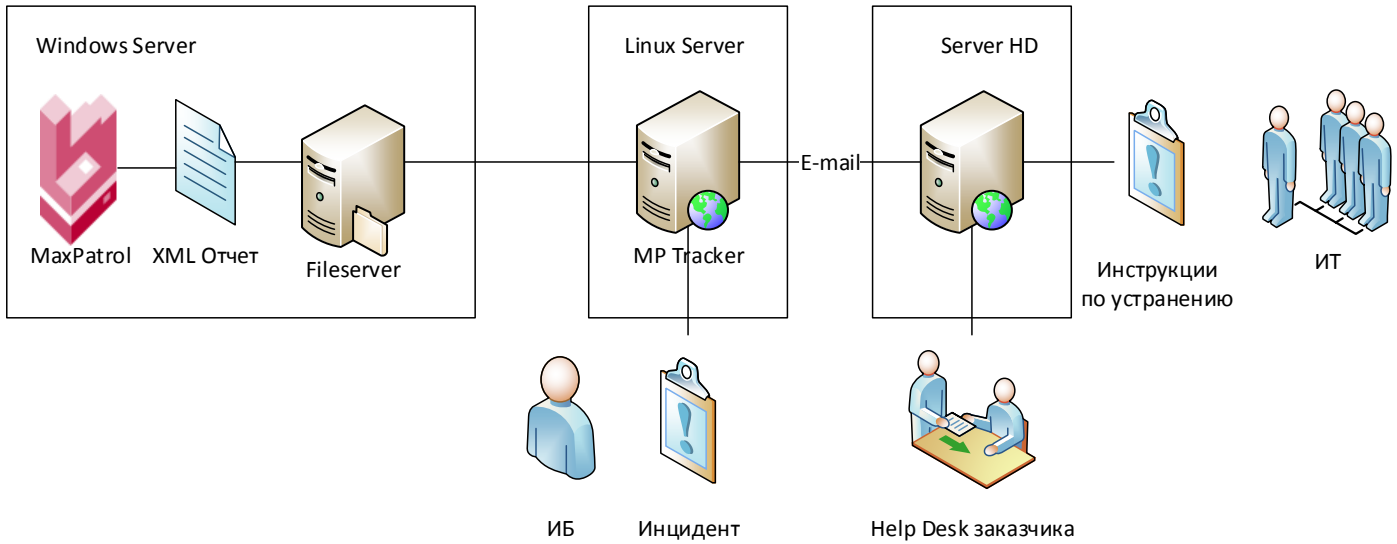
Представление информации о текущем уровне защищенности ИС и присутствующих в ней уязвимостях возможно в виде:

- документа сканирования MaxPatrol
- отчета MaxPatrol
- выгрузка данных во внешнюю систему:
  - MS Excel
  - трекинговую систему MP Tracker
  - портал отчетности MP Report Portal

Управление изменениями

Основная задача:
уменьшение или исключение отрицательного воздействия на ИС событий информационной безопасности — обнаруженных уязвимостей и недостатков ИС

MP Tracker — система учета и отслеживания заявок
WSUS Package Publisher — средство формирования и установки обновлений



Работа с заявками

При формировании и обработке заявки должны учитываться (в порядке следования):

- категория ИС (определяет уровень критичности системы и должна лежать в основе формирования задач сканирования в MaxPatrol)
- наименование платформы
- наименование ПО
- уровень уязвимости (для выделенного ПО определяется по информации, импортированной из MaxPatrol в MP Tracker; в MaxPatrol присваивается на основании уровня CVSS)

(Управление обновлениями)

- настройка подсистемы управления обновлениями:
  - определение перечня ПО, для которого должны быть получены обновления
  - определение перечня обновлений для ПО
  - определение группы потребителей обновлений
  - тестирование и распространение обновлений
- настройка политики запроса обновлений для потребителей
- создание тестовой среды и распределение клиентов по группам на основе функциональности, уровня риска и т. п.
- создание пакетов обновления и установки ПО производителей, отличных от Microsoft
- контроль успешности установки обновлений

Эффективность процесса

Оценка эффективности процедур АЗ и КС включает:

- определение целей и задач ИБ
- выбор процессов, необходимых для совершенствования
- определение лиц, участвующих в АЗ и КС
- формирование показателей эффективности (метрик)
- настройка источников событий
- привязка к уровню зрелости ИС
- включение в процедуру внутреннего контроля (аудита)

Метрики

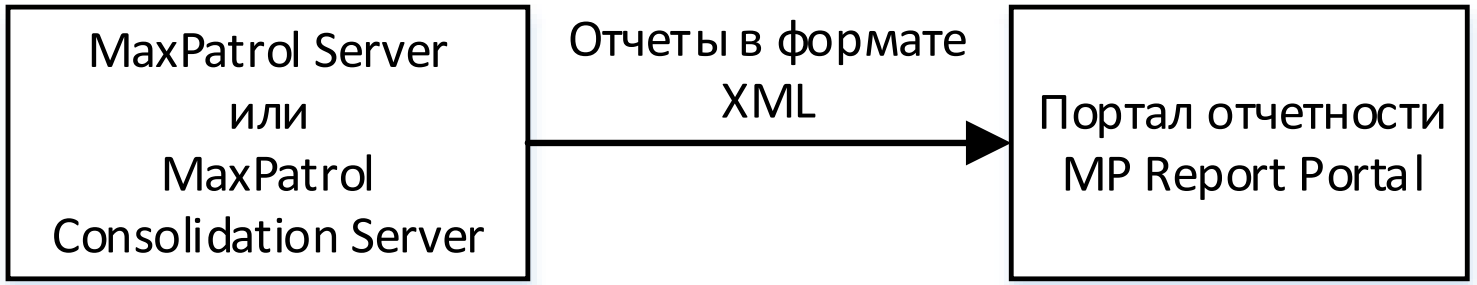
Сведения по метрикам необходимо получать с определенной периодичностью для создания корректной картины изменений

Примеры:

- доля устраненных уязвимостей
- выполнение плана сканирования
- контроль инфраструктуры
- соответствие стандартам

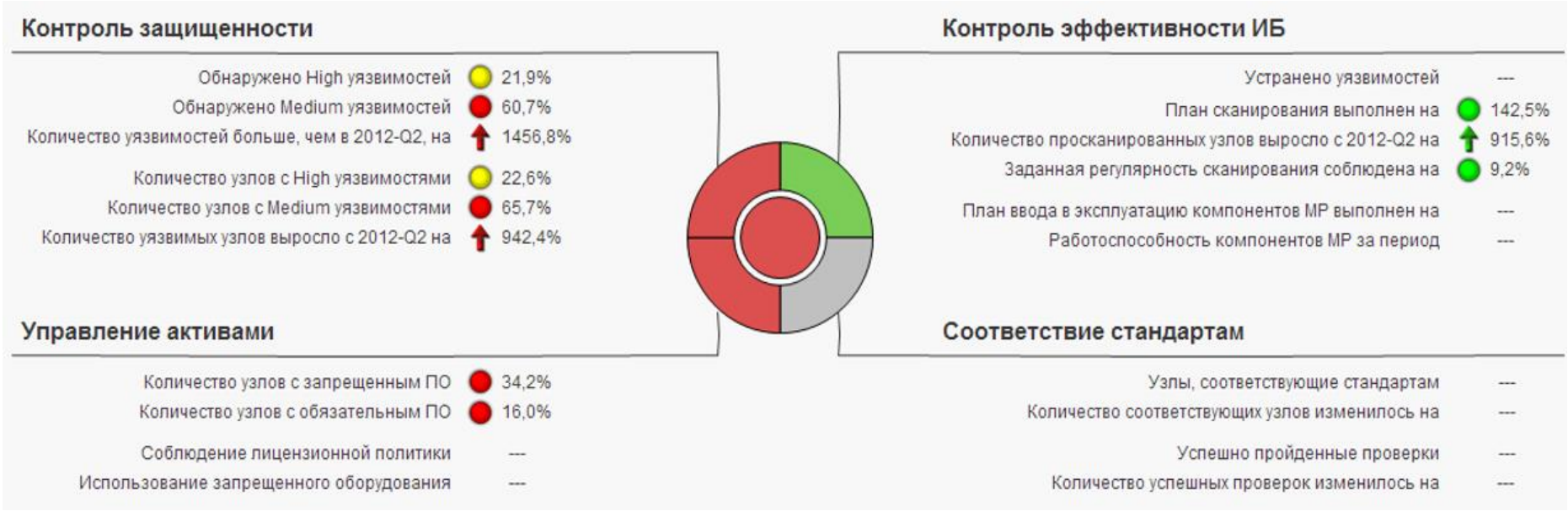
Портал отчетности. Схема работы

Портал отчетности MP Report Portal консолидирует и отображает настроенные показатели информационной безопасности по всей инфраструктуре компании в целом с возможностью детализации по регионам



- СУБД MS SQL Server
- MS Management Studio
- MS IIS 7
- QlikView

Показатели информационной безопасности



А по подробнее?

Качаем документ:
«Рекомендации по применению процедур АЗ и КС с использованием MaxPatrol.pdf»

Конец рассказа
Спасибо за внимание

Олег Матыков

Руководитель отдела проектных решений

omatykov@ptsecurity.ru

POSITIVE TECHNOLOGIES