ДЕМОНСТРАЦИЯ ВОЗМОЖНОСТЕЙ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА УГРОЗЫ НОВОЙ ВЕРСИИ ПРОДУКТА MAXPATROL EDR

Владимир Соловьев
Руководитель направления внедрения СрЗИ АО «ДиалогНаука»
26.10.2023

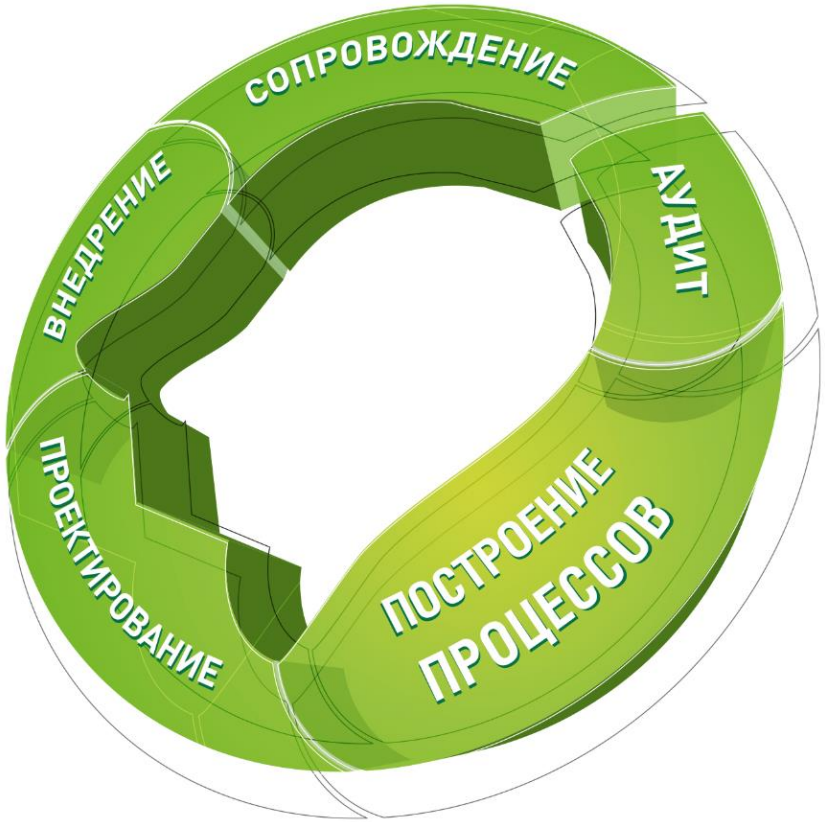
ДиалогНаука

ДиалогНаука

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН.
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB.
- В настоящее время – системный интегратор в области информационной безопасности.

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

- 152-ФЗ и GDPR
- Объекты КИИ (187-ФЗ)
- Положения Банка России
- ГОСТ 57580
- PCI DSS
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

MaxPatrol EDR

Защита конечных устройств от сложных и целевых атак

MAXPATROL EDR

MaxPatrol EDR защищает конечные устройства от сложных и целевых атак во всех популярных ОС, включая отечественные, предоставляет гибкую настройку политик и правил, а также мощные механики обнаружения

- На ранних этапах выявляет развивающиеся на устройствах атаки, которые могут пропустить другие средства ИБ
- Собирает максимум данных с узлов и обнаруживает киберугрозы
- Останавливает злоумышленника за считанные секунды
- Помогает аналитикам SOC и руководителям ИБ расследовать и предотвращать атаки, когда злоумышленники нацелены на конечные устройства и случайные действия сотрудников

Молниеносная реакция на узлах в автоматическом или в ручном режиме: остановка процесса, удаление файлов, изоляция устройства, отправка файладля динамического анализа в Sandbox, синкхолинг

Своевременное и непрерывное обнаружение ВПО за счет экспертизы PT ESC, предотвращение техник атак из матрицы MITRE ATT&CK: топ-50 для Windows, топ-20 для Linux

Легкое встраиваниев гетерогенные IT-инфраструктуры, единый агентдля сбора телеметриии информации об уязвимостяхна узлах, поддержка популярных зарубежных и российских ОС

Гибкая настройка агентов с учетом особенностей инфраструктурыи сети организации, идеальный баланс между нагрузкой на узлы и обеспечением требований SOC

БОЛЬШЕ ЧЕМ СЕНСОР

1

АВТОНОМНАЯ РАБОТА

Агенты способны проводить анализ и выполнять реагирование самостоятельно, без обращения к серверу управления или доступа в Интернет

2

ПОДДЕРЖКА ОТЕЧЕСТВЕННЫХ ОС

Доступен для всех популярных ОС, включая отечественные (Astra Linux, РЕД ОС, Альт и др.)

3

РУЧНОЕ ИЛИ АВТОМАТИЧЕСКОЕ РЕАГИРОВАНИЕ

Богатый выбор действий, которые можно полностью автоматизировать: остановка процесса, удаление файлов, изоляция устройства, отправка на анализ, синкхолинг

4

СВОЕВРЕМЕННОЕ И НЕПРЕРЫВНОЕ ОБНАРУЖЕНИЕ

Поставляется с набором экспертных правил от PT ESC, благодаря чему способен обнаружить актуальные угрозы, включая тактики и техники из матрицы MITRE ATT&CK (топ-50 для Windows и топ-20 для Linux), даже в полностью автономном режиме.

Новые пакеты экспертизы поставляются непрерывно

5

ОБНАРУЖЕНИЕ УГРОЗ В ДИНАМИКЕ

Обнаруживает атаки с использованием легитимных инструментов: PowerShell, WMI, CMD, CLI, BASH, которые могут пропустить традиционные средства защиты, основанные на сигнатурном анализе

6

ПОМОЩЬ ДРУГИМ СРЕДСТВАМ ИБ

Единый агент собирает телеметрию и информацию об уязвимостях на узлах, не требуя предоставления привилегированных учетных записей со стороны IT-подразделения, и передает их на обработку в другие СЗИ

ПОДХОДИТ ДЛЯ РАЗНЫХ ОРГАНИЗАЦИЙ

1

ЭКОНОМИТ РЕСУРСЫ И ВРЕМЯ СПЕЦИАЛИСТОВ

Построение эшелонированной защиты на базе комплексных решений или интеграции нескольких продуктов не всегда вписывается в бюджет организации. MaxPatrol EDR позволяет начать решать задачу защиты устройств сотрудников и компании без чрезмерных затрат, постепенно выстраивая процессы и уровни киберзащиты

2

АВТОМАТИЗИРУЕТ ФУНКЦИИ РЕАГИРОВАНИЯ

Часто EDR-решения предполагают активное участие человека и не подразумевают автоматические реакции, кроме остановки процессов или удаления файлов. В MaxPatrol EDR можно управлять логикой и пользоваться всеми доступными опциями реагирования как вручную, так и автоматически

3

ПРЕДОСТАВЛЯЕТ ПРИВЫЧНУЮ ЛОГИКУ И ИНТЕРФЕЙС

MaxPatrol EDR создан в едином стиле с другими продуктами Positive Technologies и предоставляет те же сущности, авторизацию, сервисы и кросс-продуктовые сценарии, что и, например, MaxPatrol SIEM или MaxPatrol VM, обеспечивая пользователю легкий старт

4

НЕ КОНФЛИКТУЕТ С ДРУГИМИ СЗИ

Организации могут использовать несколько защитных решений, дополняя экспертизу разных вендоров без влияния на бизнес-процессы

5

УЧИТЫВАЕТ ОСОБЕННОСТИ ИНФРАСТРУКТУРЫ

Позволяет гибко настраивать модули обнаружения и политики. Обеспечивает идеальный баланс между нагрузкой на узлы и обеспечением требований SOC

6

РАБОТАЕТ В ЗАКРЫТЫХ СЕГМЕНТАХ

Обеспечивает однонаправленную передачу данных для контуров с разной степенью доверия. Поставка обновлений экспертизы возможна через промежуточный сервер

ИСПОЛЬЗУЕТ ЭКСПЕРТИЗУ POSITIVE TECHLONOGIES

ПОСТАВЛЯЕТСЯ С НАБОРОМ ЭКСПЕРТИЗЫ ДЛЯ ОБНАРУЖЕНИЯ АКТУАЛЬНЫХ УГРОЗ:

500 + правил корреляции

5000 + YARA-правил

ПОЗВОЛЯЕТ СОЗДАВАТЬ И ИСПОЛЬЗОВАТЬ СОБСТВЕННЫЕ КОРРЕЛЯЦИОННЫЕ И YARA-ПРАВИЛА

ВЫЯВЛЯЕТ ПОДОЗРИТЕЛЬНЫЕ ДЕЙСТВИЯ В ПОСЛЕДОВАТЕЛЬНОСТИ СОБЫТИЙ

ОБРАБАТЫВАЕТ ПОСТУПАЮЩИЕ СОБЫТИЯ И ОБОГАЩАЕТ ИХ ПОЛЕЗНОЙ ИНФОРМАЦИЕЙ:

- **определяет** уровень привилегий учетных записей, от имени которых запускаются процессы
- **извлекает** параметры командной строки при запуске
- **фиксирует** контрольные суммы процессов и исполняемых файлов
- **отслеживает** цепочки подозрительных действий

Автоматизирует реагирование на инциденты ИБ:

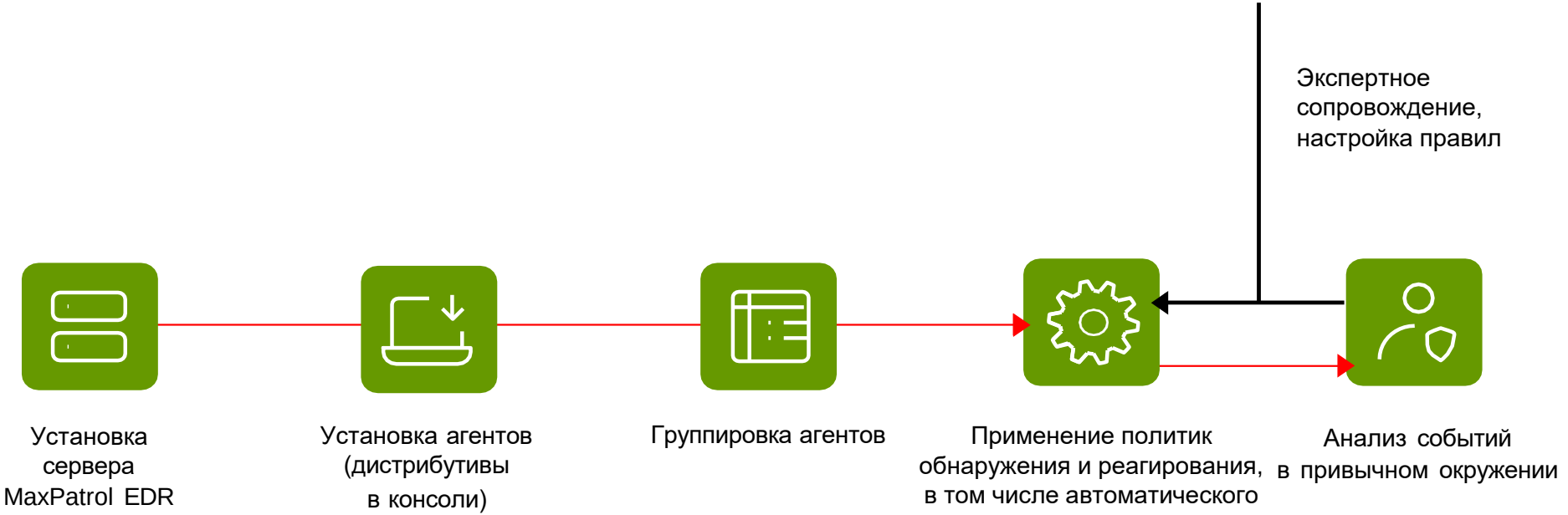
Помогает снизить требования к ресурсам и компетенциям SOC с помощью автоматизации рутинных процессов реагирования на типовые угрозы ИБ. Это позволяет сократить сроки обработки инцидентов, использовать время и навыки аналитиков для решения наиболее важных задач

Оператор системы может выполнить реагирование на угрозу вручную или собрать необходимые для анализа данные максимально оперативно

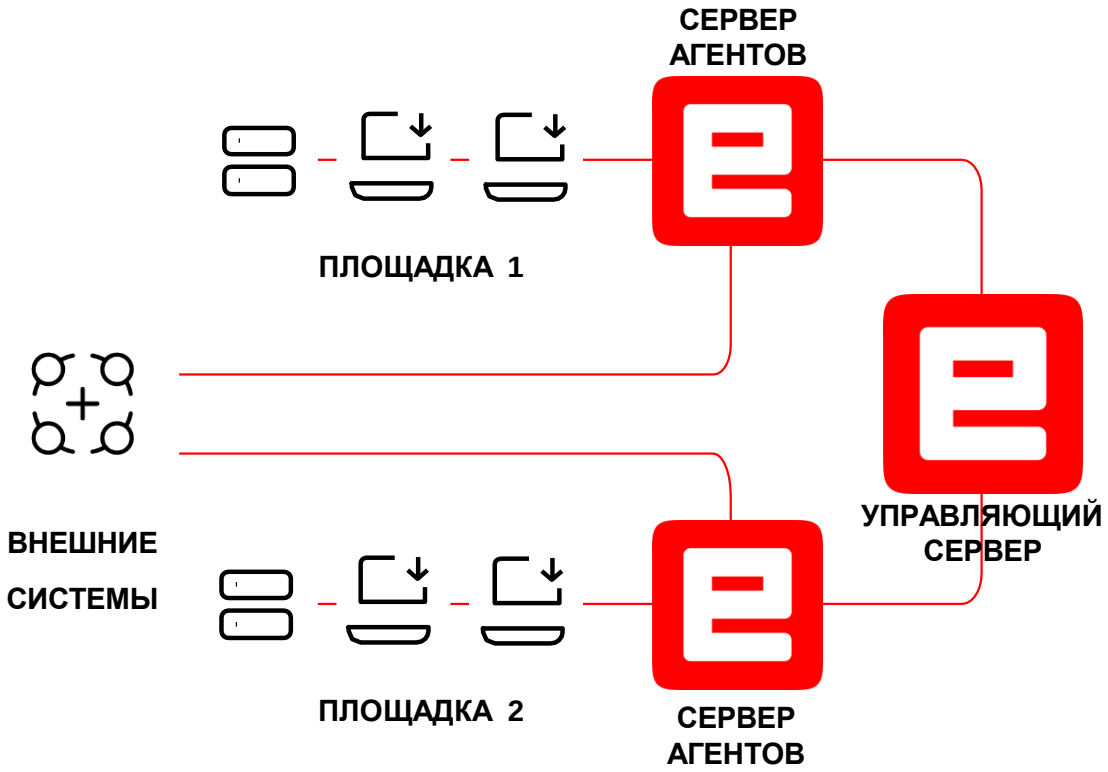
MaxPatrol EDR

ПРИНЦИП РАБОТЫ

НАЧАТЬ ПРОСТО



КАК УСТРОЕН MAXPATROL EDR: АРХИТЕКТУРА



- **MaxPatrol EDR** состоит из серверной части и агентов, устанавливаемых на конечные устройства
- **Серверная часть** состоит из двух программных компонентов: управляющего сервера и сервера агентов
- **Управляющий сервер —** основной компонент системы, который позволяет конфигурировать ее через веб-интерфейс
- **Сервер агентов —** приложение для управления агентами и модулями, а также взаимодействия с внешними системами (MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, сторонний syslog)
- **Агент —** приложение, которое устанавливается на конечное устройство для обеспечения работы модулей и связи с сервером агентов
- **Агенты поддерживают установку на Windows, Linux, macOS**

КАК УСТРОЕН MAXPATROL EDR: МОДУЛИ

Модуль — приложение, которое запускается на конечном устройстве для выполнения основных функций продукта

1

МОДУЛИ ДОСТАВКИ И УСТАНОВКИ

- Установщик Sysmon
- Модуль импорта и экспорта файлов на узле
- Модуль доставки параметров auditd

2

МОДУЛИ СБОРА

- Сбор данных и реагирование
- Сбор данных из журнала событий Windows
- Сбор событий из auditd

3

МОДУЛИ ОБНАРУЖЕНИЯ

- YARA-сканер **почти 5000 правил**
- Коррелятор **300+ правил корреляции**

4

МОДУЛИ ИНТЕГРАЦИИ

- Отправка событий на сервер syslog
- Отправка отчетов в MaxPatrol VM
- Проверка файлов в PT Sandbox
- Отправка файлов во внешние системы

5

МОДУЛИ РЕАГИРОВАНИЯ

- Удаление файлов
- Изоляция узлов
- Завершение процессов
- Выполнение команд с сервера
- Блокировка IP-адреса
- Синкхолинг опасных доменов
- Очистка автозагрузки
- Поиск по хешам файлов

MAXPATROL EDR: ОБНАРУЖЕНИЕ

- Доставка и установка инструментов для расширенного мониторинга на конечные устройства
- Комбинирование автономных механизмов обнаружения:
  - Статический анализ
  - Поведенческий анализ
- Реагирование на угрозы
- Многоэтапные проверки — последовательный автоматический запуск механизмов обнаружения
- Гарантированное хранение артефактов для расследования
- Дополнительные проверки артефактов во внешних системах

ОБНАРУЖИВАЕТ САМЫЕ ПОПУЛЯРНЫЕ ТЕХНИКИ ИЗ МАТРИЦЫ MITRE ATT&CK

- **Топ-50** для Windows
- **Топ-20** для Linux

ПРЕДОСТАВЛЯЕТ ВОЗМОЖНОСТЬ ГРАНУЛЯРНОЙ НАСТРОЙКИ СИСТЕМЫ

- Баланс между глубиной обнаружения и нагрузкой
- Фильтрация событий перед отправкой в SIEM-систему

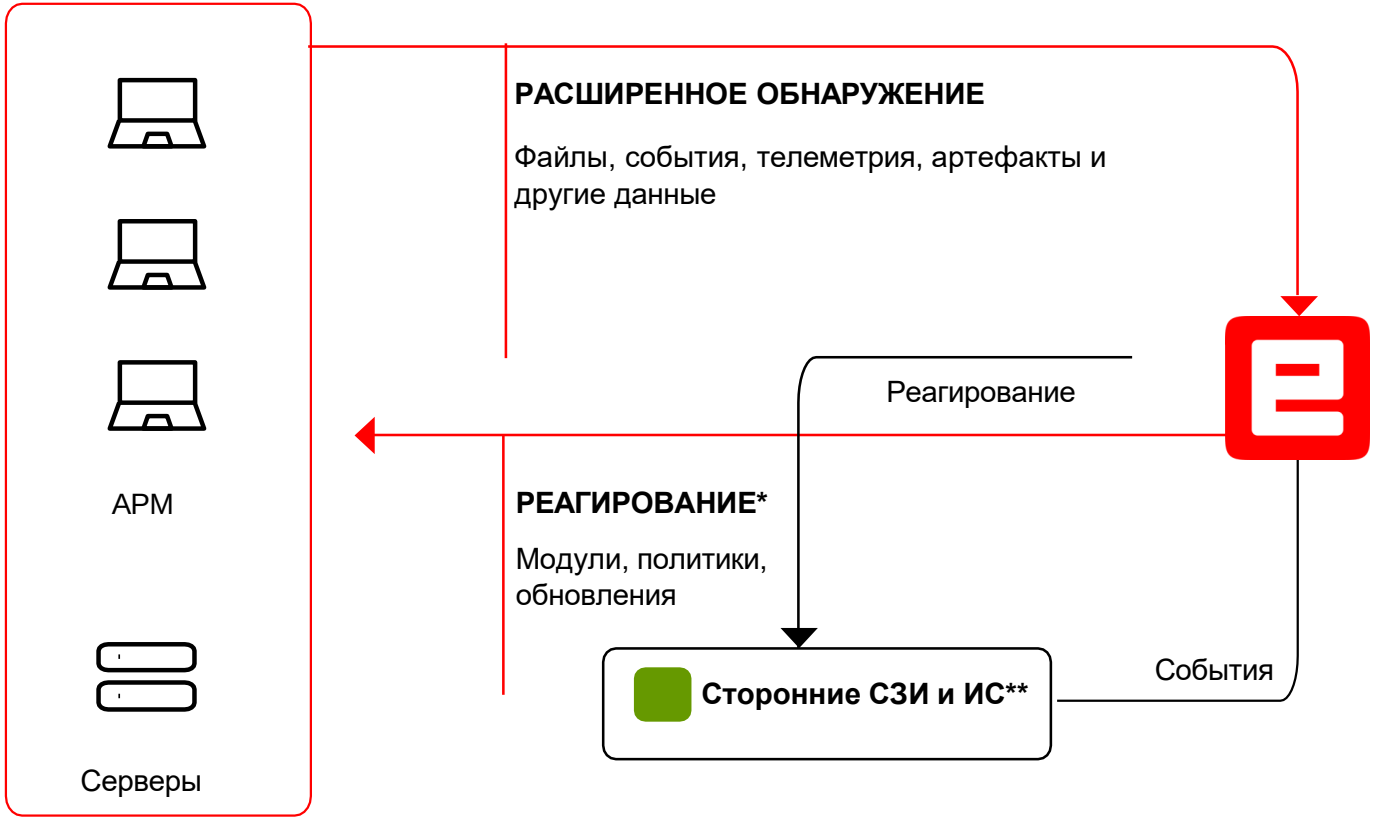
MAXPATROL EDR: РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

- Обнаружение угроз и реагирование (Windows)
- Обнаружение угроз (Windows, Linux)
- Реагирование на угрозы
- Интеграция с сервером syslog
- Интеграция с PT Sandbox (проверка)
- Интеграция с PT Sandbox (проверка и реагирование)

Политика определяет набор устанавливаемых на агент модулей, а также их параметры, включая действия по реагированию, отправке данных во внешние системы и т. д.

Готовые шаблоны политик обнаружения угроз и реагирования MaxPatrol EDR основаны на рекомендациях экспертного центра PT ESC. Они позволяют экономить ресурсы аналитиков, упрощая внедрение и эксплуатацию продукта, предоставляют возможность максимально гибко управлять функциями агентов

КАК РАБОТАЕТ MAXPATROL EDR

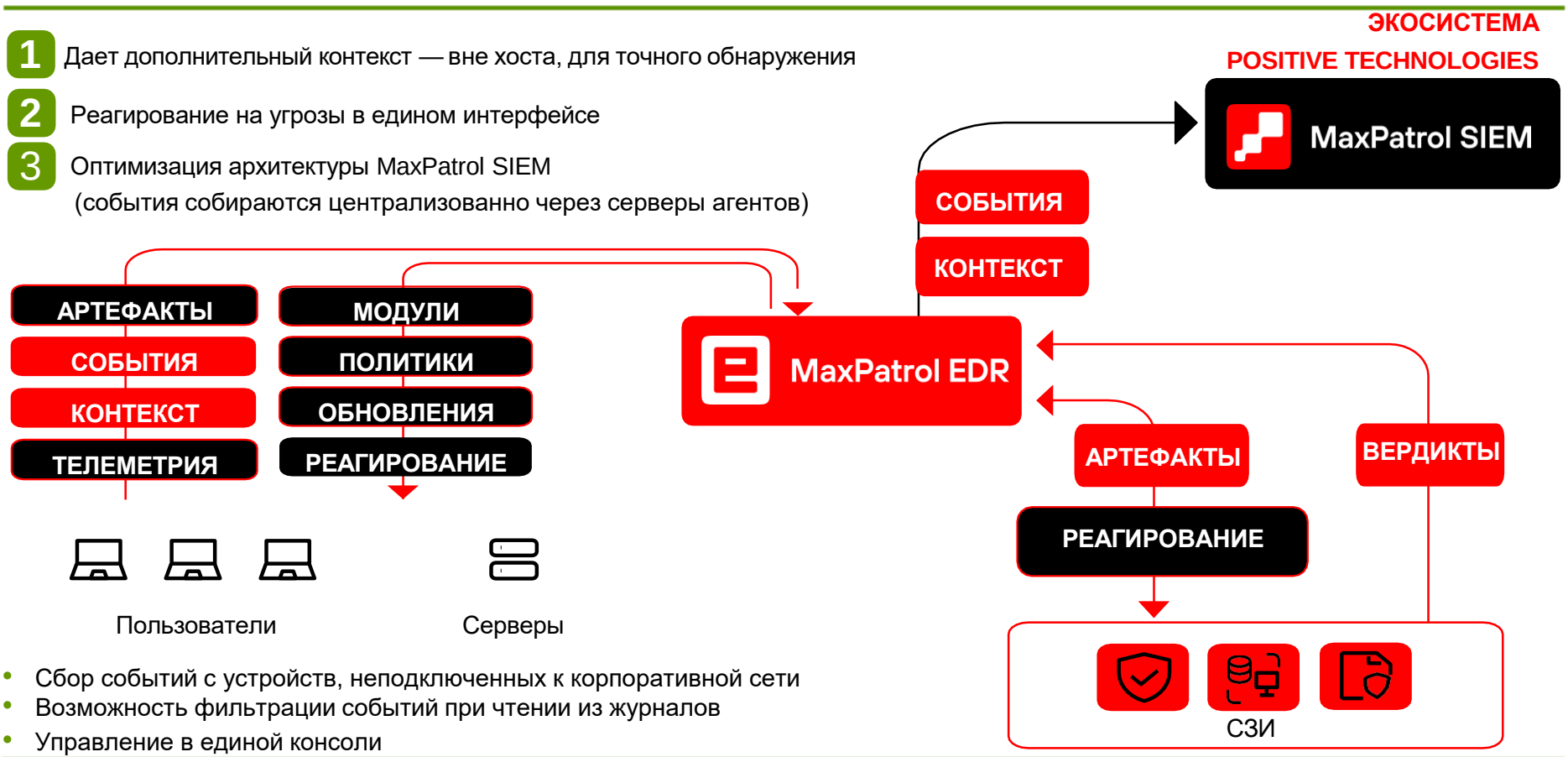


* Реагирование может происходить как в автоматическом режиме (если допустимо и предусмотрено политикой), так и в ручном

** Интеграция путем добавления кастомных функциональных модулей в продукт через Positive Technologies и партнеров вендора

MAXPATROL EDR + MAXPATROL SIEM

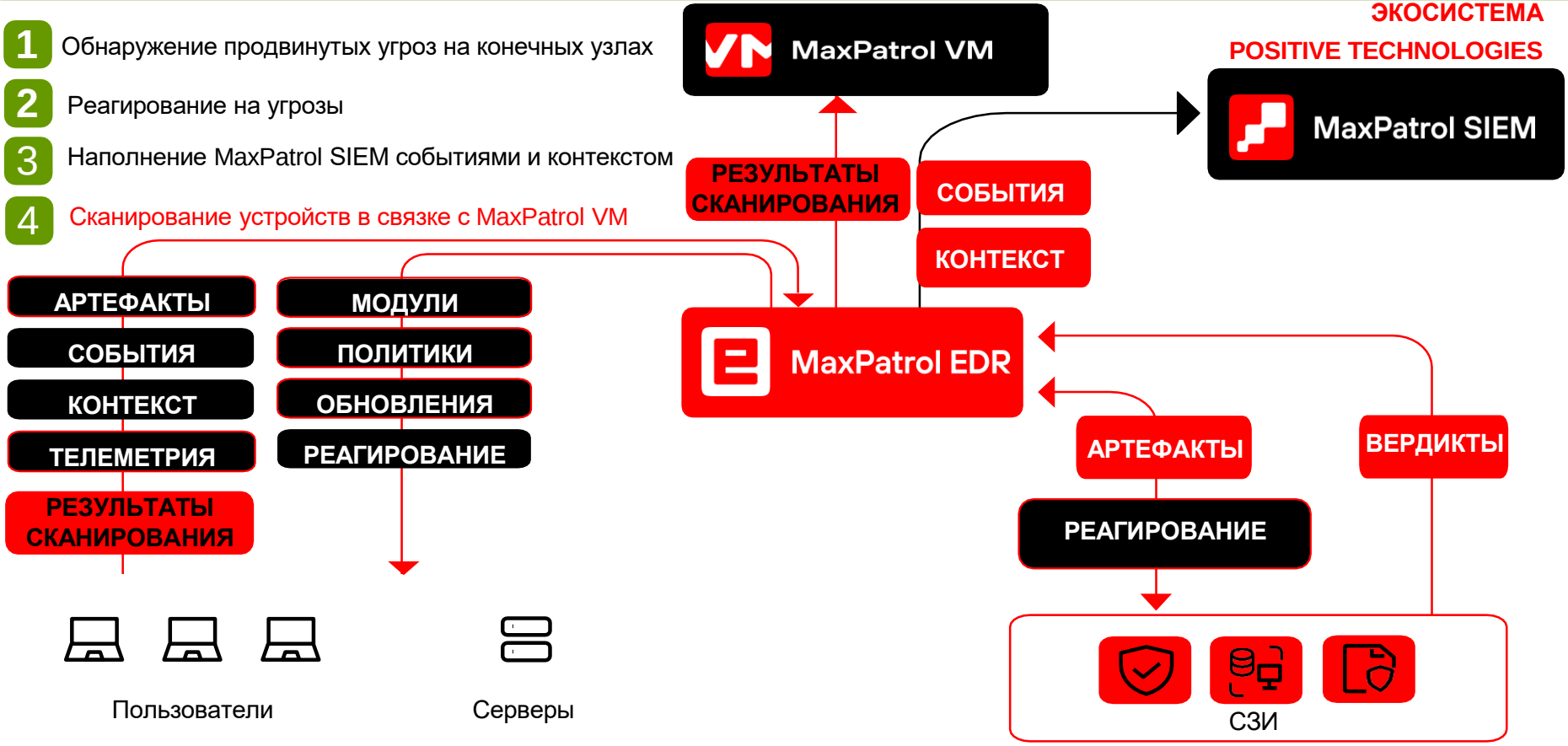
1. Дает дополнительный контекст — вне хоста, для точного обнаружения
2. Реагирование на угрозы в едином интерфейсе
3. Оптимизация архитектуры MaxPatrol SIEM
   (события собираются централизованно через серверы агентов)



- Сбор событий с устройств, неподключенных к корпоративной сети
- Возможность фильтрации событий при чтении из журналов
- Управление в единой консоли

MAXPATROL EDR + MAXPATROL SIEM + MAXPATROL VM

1. Обнаружение продвинутых угроз на конечных узлах
2. Реагирование на угрозы
3. Наполнение MaxPatrol SIEM событиями и контекстом
4. Сканирование устройств в связке с MaxPatrol VM



MAXPATROL EDR + PT SANDBOX

Файлы, подлежащие дополнительной проверке, передаются от агента серверу агентов MaxPatrol EDR, а далее — в PT Sandbox для подробного статического и поведенческого анализа.
Результат анализа становится доступен на всех агентах.

Иногда защиту от атак можно реализовать только с применением комплекса из агентского решения и сетевой песочницы. Например, защиту от доставки продвинутого ВПО через защищенные сквозным шифрованием каналы связи, такие как Telegram. Пример такой успешной атаки Lazarus доступен по QR-коду

MaxPatrol EDR

Демонстрация работы

ВОПРОСЫ?

115230 Москва,
1-й Нагатинский проезд, д. 10, стр. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: MarketingDepartment@dialognauka.ru