

ОБЗОР РЕЛИЗА · R28

Рост производительности, цифровой помощник и поведенческий анализ

Ключевые обновления MaxPatrol SIEM, вошедшие
в релиз R28, и планы продуктовой команды
на ближайшее будущее

Существенный рост производительности

За последние месяцы команда продукта существенно оптимизировала работу сервиса корреляции. Изменения уже вошли в актуальные релизы и проверены на ряде нагруженных on-premise инсталляций заказчиков.

25–50%

снижение потребления
RAM коррелятором

до 40%

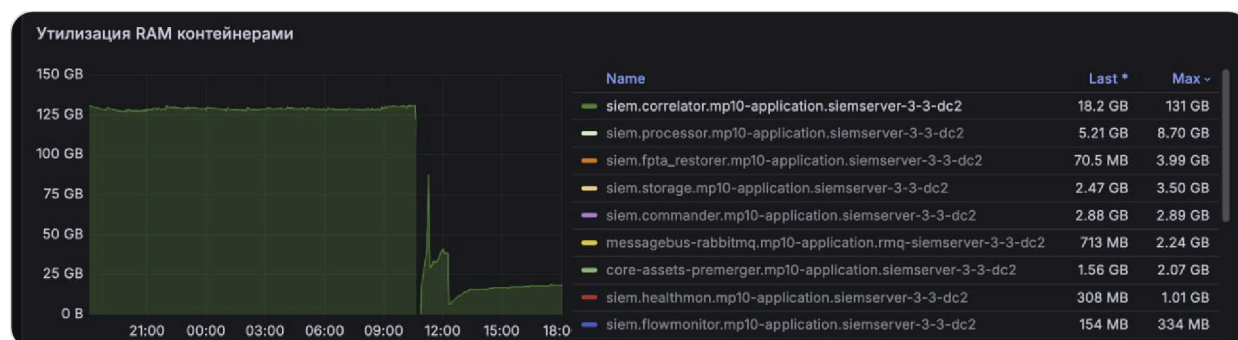
снижение нагрузки на CPU

40 ГБ + 5 ядер

высвобождено в одном
из рабочих контуров

Рисунок 1 — Утилизация RAM контейнерами до и после перехода на обновленный коррелятор

Потребление памяти снизилось примерно со 130 ГБ до 15–20 ГБ



Источник: мониторинг рабочего контура заказчика.

Конкретный результат зависит от состава и интенсивности потока событий, правил корреляции и архитектуры внедрения, поэтому эффект для каждой инсталляции необходимо оценивать отдельно.

Что это означает для заказчика

- ✓ повышение запаса производительности существующей инфраструктуры
- ✓ сокращение требований к вычислительным ресурсам
- ✓ снижение затрат на дальнейшее масштабирование
- ✓ обработка большего потока событий без пропорционального роста мощностей

Цифровой помощник PT Naira

В MaxPatrol SIEM появился цифровой помощник PT Naira, который помогает аналитикам быстрее выполнять повседневные задачи.

Возможности PT Naira

- Диалог с помощником в формате чата
- 🔍 Помощь в расследовании: объясняет события, правила корреляции, скрипты, процессы и срабатывания MaxPatrol BAD
- ⚡ Ускорение подключения новых источников за счет генерации правил нормализации

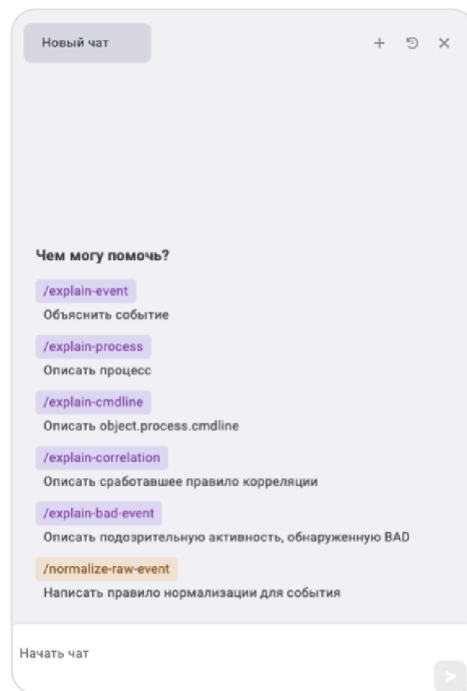


Рисунок 2 — Интерфейс PT Naira

до 50%

снижение времени на расследование инцидента

до 90%

снижение трудозатрат на написание правил нормализации

Новые возможности в MaxPatrol BAD

В новой версии расширены механизмы поведенческого анализа.

Расширенный анализ Unix-подобных систем

Unix-like-активы в инфраструктуре теперь под контролем поведенческого анализа

Обнаружение источников аномалий на разных узлах

Упростили поиск источника активности, который вызывает аномалии на разных узлах

Объединение данных из связанных событий

Данные об активности процесса автоматически обогащаются дополнительным контекстом

Благодаря этому MaxPatrol BAD

- ✓ автоматически приоритезирует наиболее опасные события
- ✓ ускоряет расследование инцидентов за счет расширенного контекста
- ✓ выявляет атаки, которые не обнаруживаются правилами корреляции

Дополнительные ВОЗМОЖНОСТИ И ПЛАНЫ

Дополнительные возможности релиза R28

Конвертер Sigma-правил → XP

Отображение экспертной метаинформации в PT KB: сценарии, MITRE ATT&CK, связи

Дополнительная разметка критичных алертов

Поддержка новых версий Astra Linux — 1.7.8, 1.7.9 и 1.8.4

Планы продуктовой команды на R28.1

В ближайшем релизе команда продукта продолжит развитие платформы. Среди ключевых направлений:

- Оптимизация потребления ресурсов
- Обновленные дашборды и виджеты
- Пакеты экспертного контента
- Поддержка ClickHouse в качестве storage
- Log management
- Поддержка «Ред ОС 8.0»

Обновлений в R28 значительно больше, чем вошло в этот обзор. Если хотите подробнее разобраться в новых возможностях или обсудить, как использовать их в работе с заказчиками, дайте знать — организуем отдельную встречу с командой продукта.