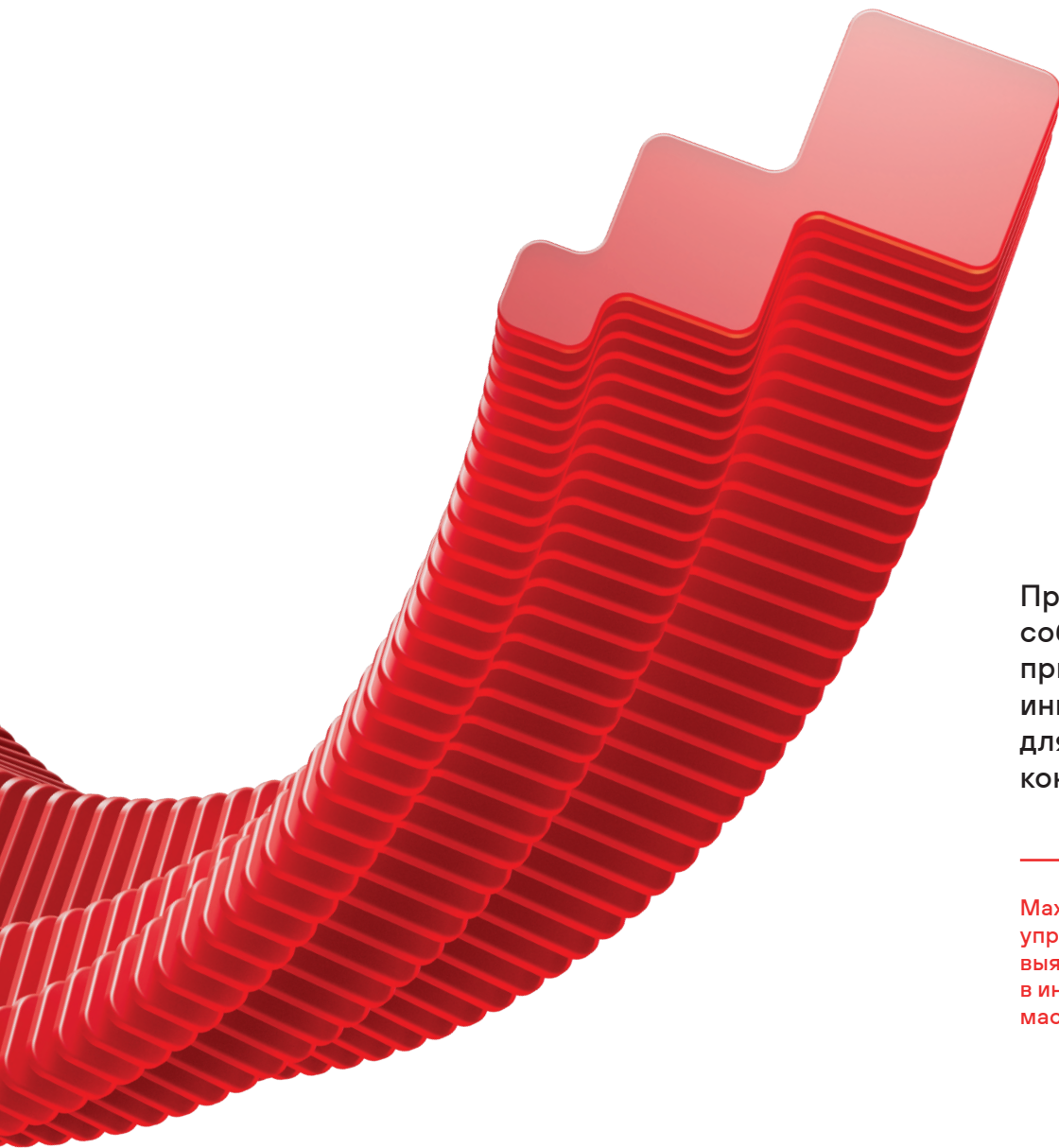


MaxPatrol SIEM



Превращает поток событий в список приоритизированных инцидентов с нужным для расследования контекстом

MaxPatrol SIEM – система управления событиями ИБ, которая выявляет комплексные кибератаки в инфраструктурах любого масштаба.

MaxPatrol SIEM знает:



Где искать

Технологии Asset Management позволяют видеть обновления инфраструктуры в реальном времени и контролировать полноту и качество сбора событий ИБ.



Что искать

Экспертиза PT ESC покрывает больше 70% техник из матрицы MITRE ATT&CK, а ML-модуль MaxPatrol BAD выявляет даже неизвестные атаки и аномалии.



Что делать дальше

Собирает контекст атаки и дает возможность реагировать на нее из карточки события

Уникальные технологии в MaxPatrol SIEM



MaxPatrol BAD

AI/ML-помощник, который выявляет аномалии и 0-day атаки, включая атаки с использованием ИИ, приоритизирует инциденты, дает контекст и ускоряет расследования.



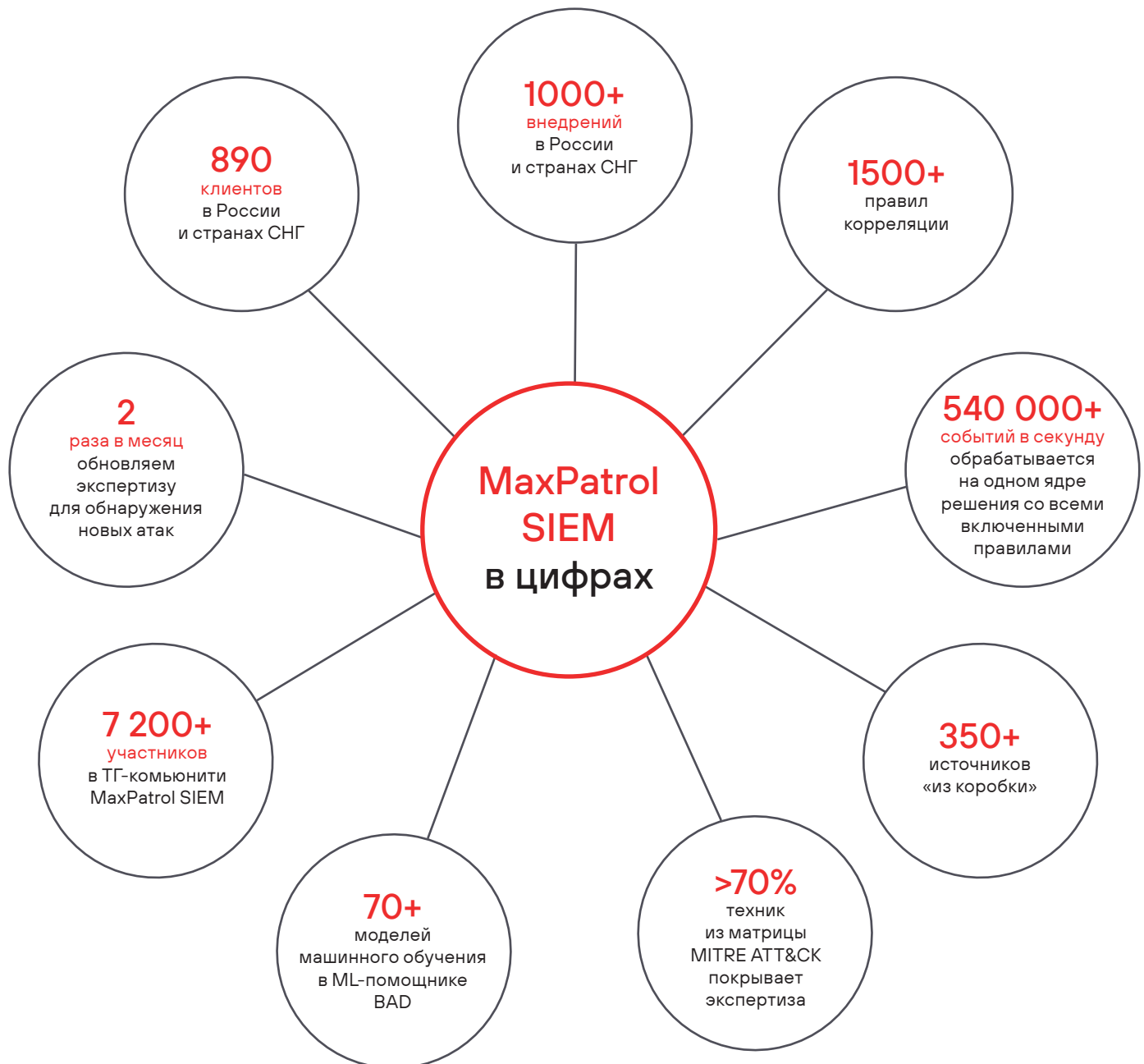
СУБД LogSpace

Первая российская СУБД, разработанная специально для SIEM-систем. Позволяет хранить больше данных, чем опенсорсные аналоги с теми же ресурсами.



Контроль источников

Встроенный мониторинг источников позволяет контролировать число событий в потоке, и оценивать полноту и качество поступающих событий для максимального качества детекта.



Оставьте заявку на демо
Оцените возможности MaxPatrol SIEM в вашей инфраструктуре



Присоединяйтесь к комьюнити MaxPatrol SIEM
Будьте в курсе последних новостей

