Павел Гончаров
Бизнес-лидер MaxPatrol SIEM

Результативный MaxPatrol SIEM

01

SIEM-системы бывают разные

Выбор есть всегда

Важно не ошибиться в критериях

Для **формальног**о выполнения требований регуляторов

«Бесплатный» долгострой имени главного специалиста по ИБ

Устанавливается на «оптимальные» с точки зрения компании аппаратные ресурсы

«Недорогой»

Работает на результат

Создан **побеждать** в **баттл-картах**

02

Видение результата

SIEM. Назначение

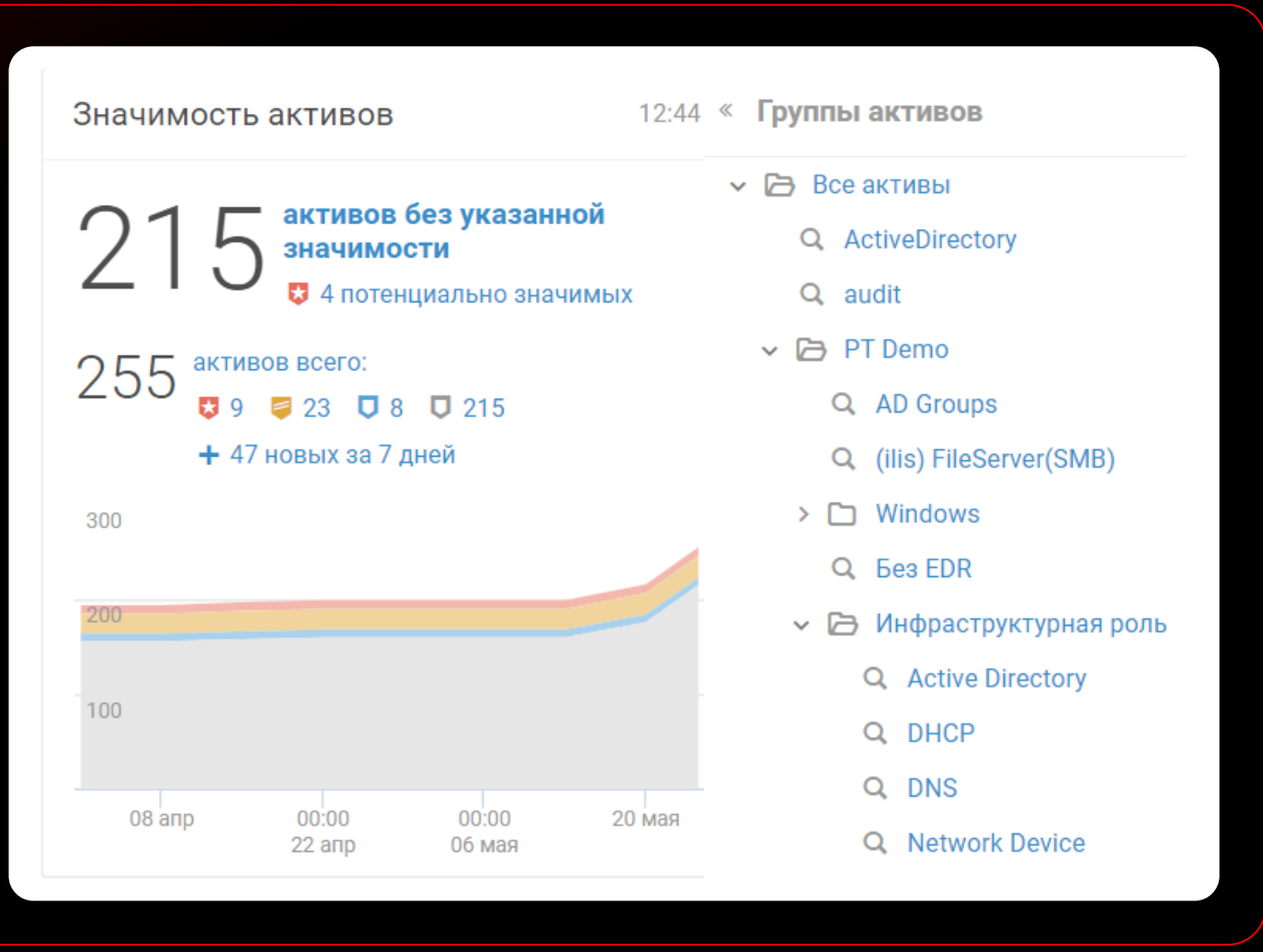
Выявление попыток нарушения киберустойчивости компании

03

Технологии

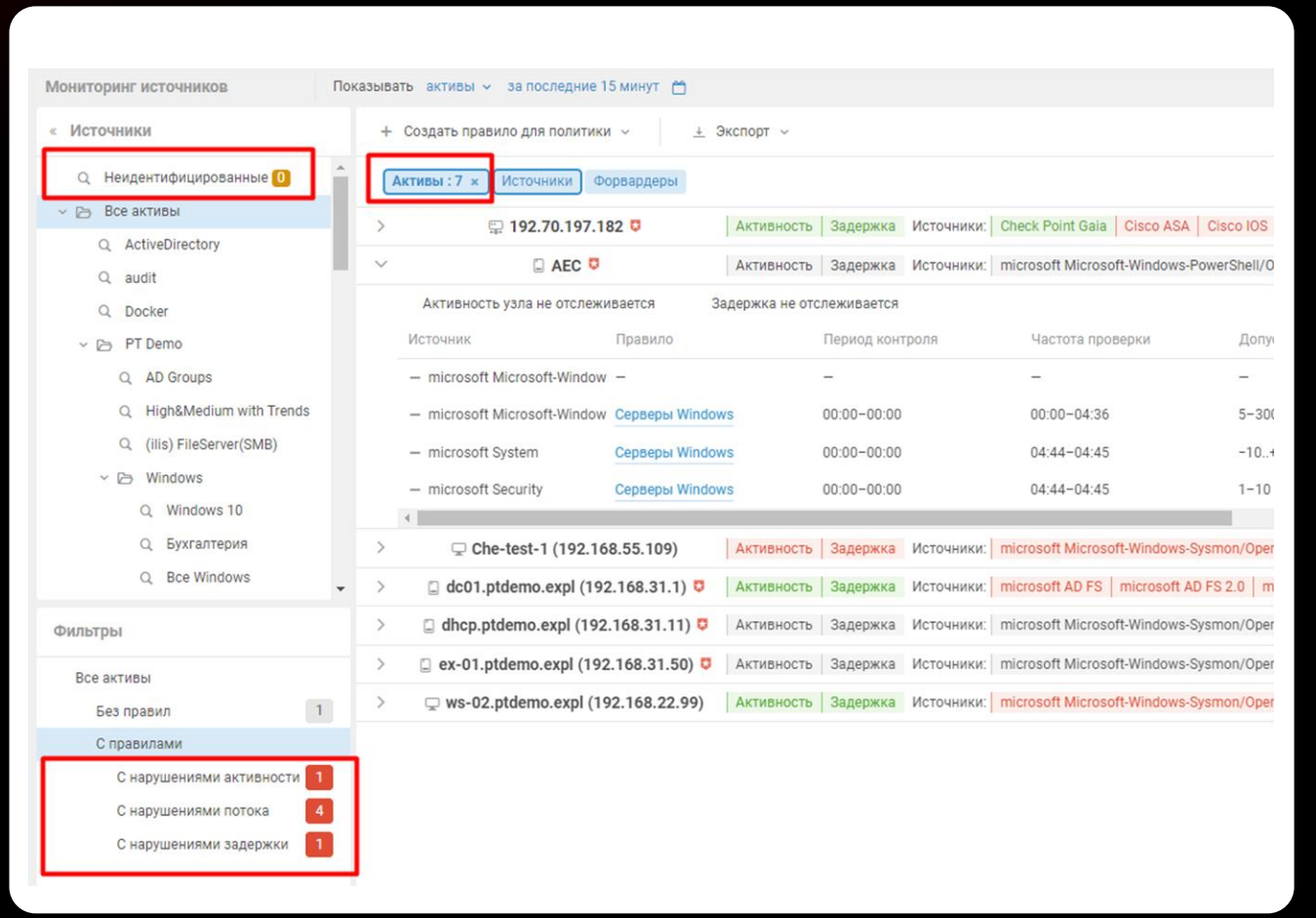
Активы как объекты защиты

- Узнает все о вашей инфраструктуре
- Даст рекомендацию о важности активов
- Учтет значимость при выявлении инцидентов



Мониторинг источников

- События
  под контролем
- Рекомендации
  экспертов-практиков



BAD — неутомимый помощник

График работы — 24/7

ФОТ ≈ равен зарплате студента 2–3 курса

Рабочее место — 1–2U 19” rack-mount

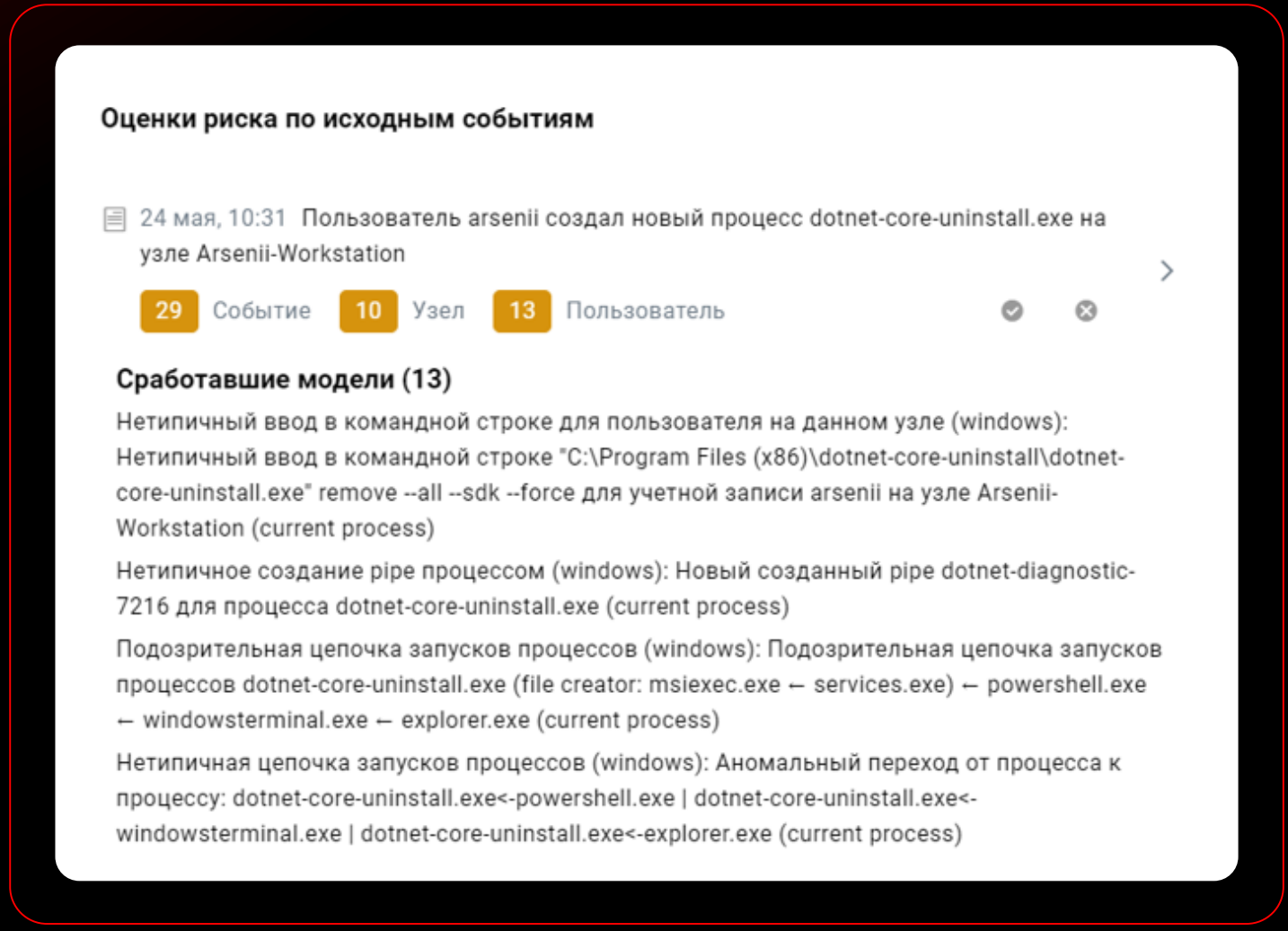
49
ML-моделей

14
типов систем

- Windows и Sysmon
- Security Center
- SQL Server
- 1C:Enterprise
- Keycloak
- Passwork
- Auditd
- TeamCity
- VMware vSphere (ESXi)
- Check Point Gaia
- Cisco (IOS, ASA, FWSM, PIX)
- FortiGate
- OpenVPN
- Artyfactory

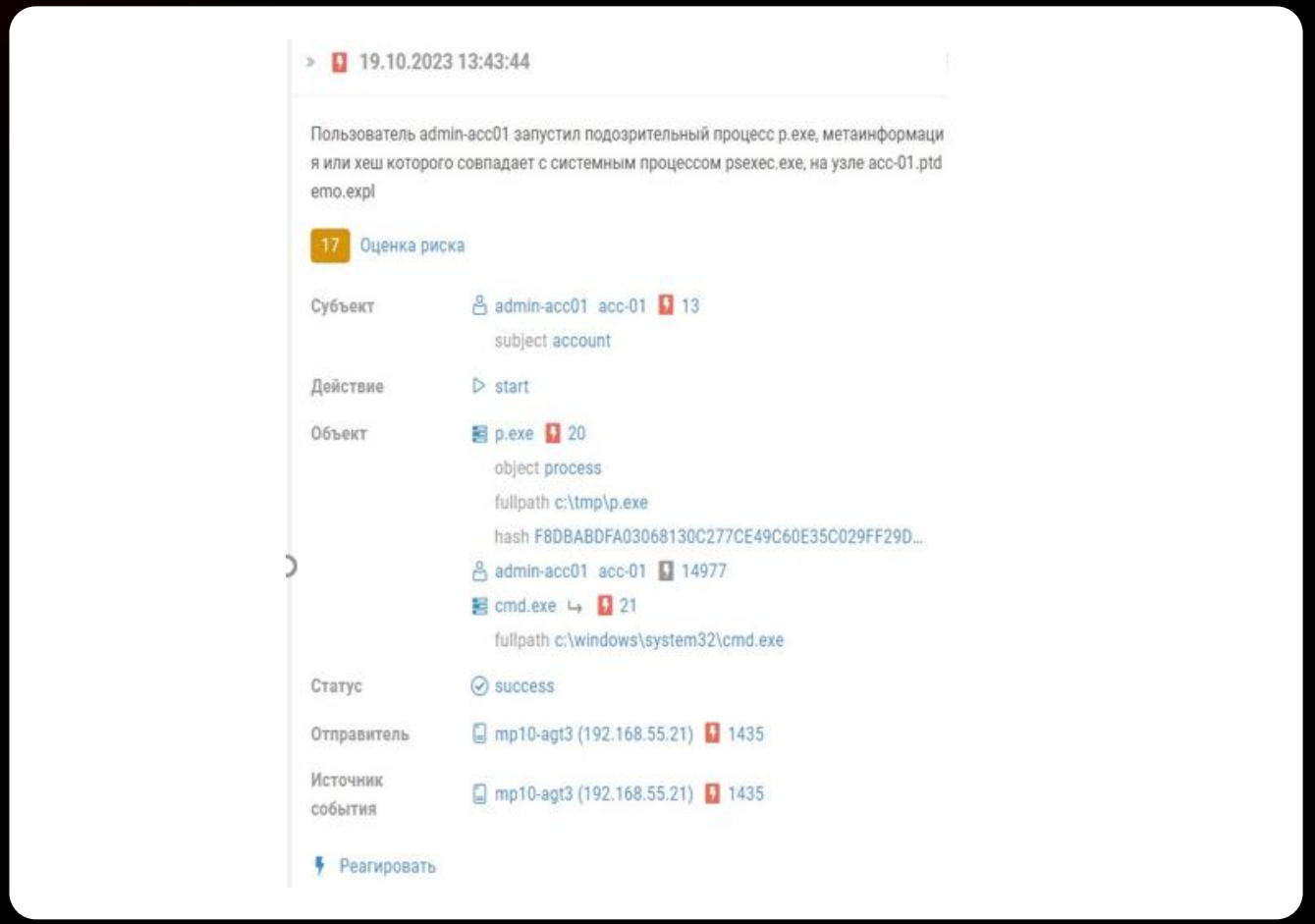
BAD — неутомимый помощник

- Дополнительная уверенность в результате мониторинга
- Выявление попыток обхода правил корреляции
- Помощь в приоритизации и принятии решений
- Обнаружение неизвестных атак и аномалий



Фокус на контексте атаки

- Обязательные данные для понимания контекста происходящего
- Настройка карточки события под пользовательские сценарии
- Возможность быстрой реакции при интеграции с MaxPatrol EDR



04

Доверься экспертам:

практика с полей бесценна

MaxPatrol SIEM. Экспертиза

Уже 9 лет более 70 экспертов PT Expert Security Center работают над созданием и совершенствованием контента для MaxPatrol SIEM

345
Источников «из коробки»

1271
правило корреляции

8965
правил нормализации

97
правил обогащений

287
техник из матрицы MITRE ATT&CK покрывает экспертиза MaxPatrol SIEM «из коробки»

199
табличных списков

05

Результативный MaxPatrol SIEM

MaxPatrol SIEM

Работает на результат

- Знает инфраструктуру
- Непрерывно собирает события ИБ
- Контролирует полноту и качество событий
- Обнаруживает известные и неизвестные атаки
- Помогает экспертам компании развивать свои знания
- Выявляет попытки нарушения киберустойчивости

Внимание, опрос!

Спасибо!