Сергей Сухоруков
Лидер продуктовой практики MaxPatrol SIEM

Результативный MaxPatrol SIEM

01

SIEM'ы 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 заказчика **аппаратные ресурсы**

«Недорогой»

Создан **побеждать в баттл картах**

Работает на Результат

02

Видение результата

SIEM. Назначение.

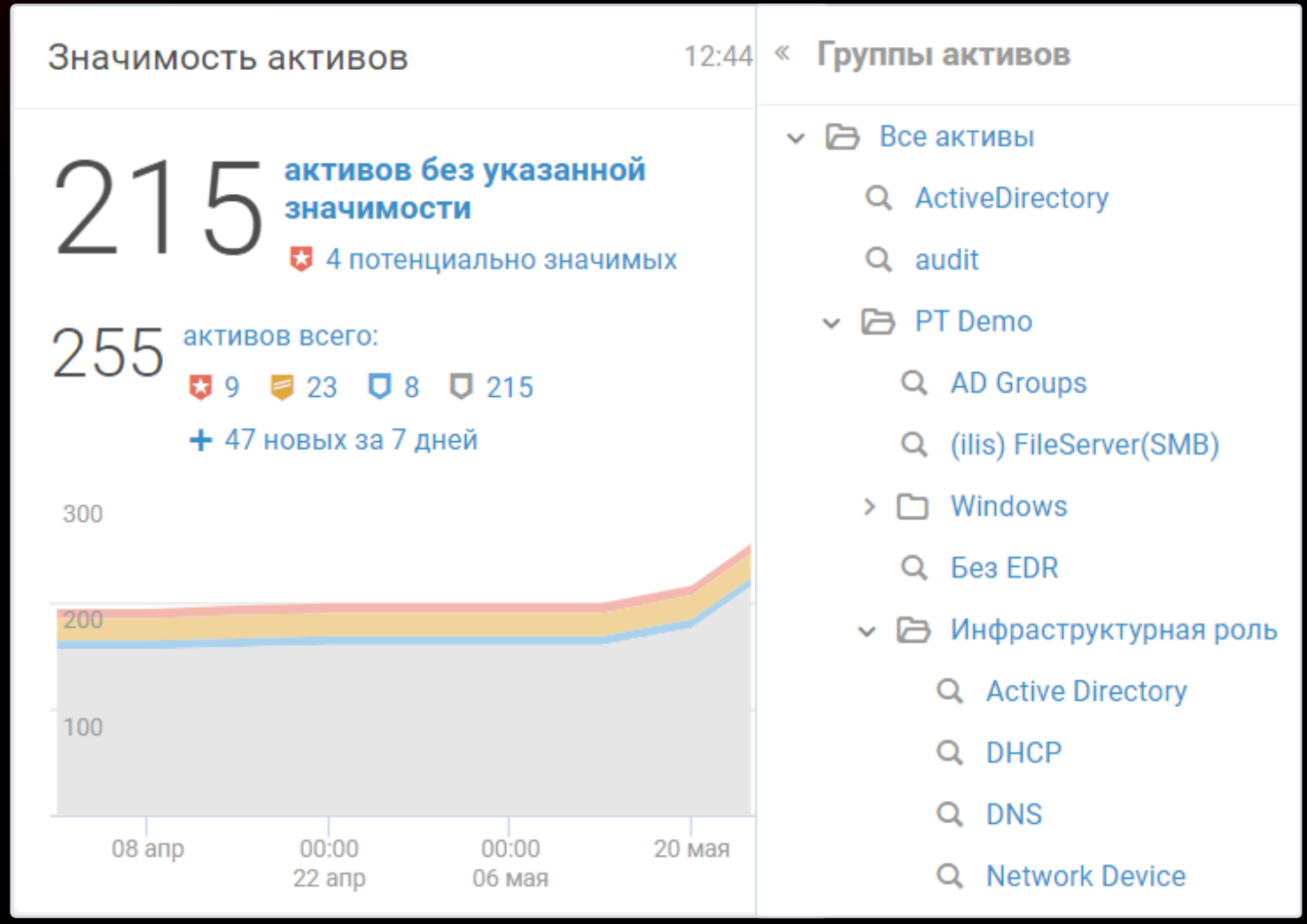
Выявление попыток нарушения киберустойчивости компании

03

Технологии

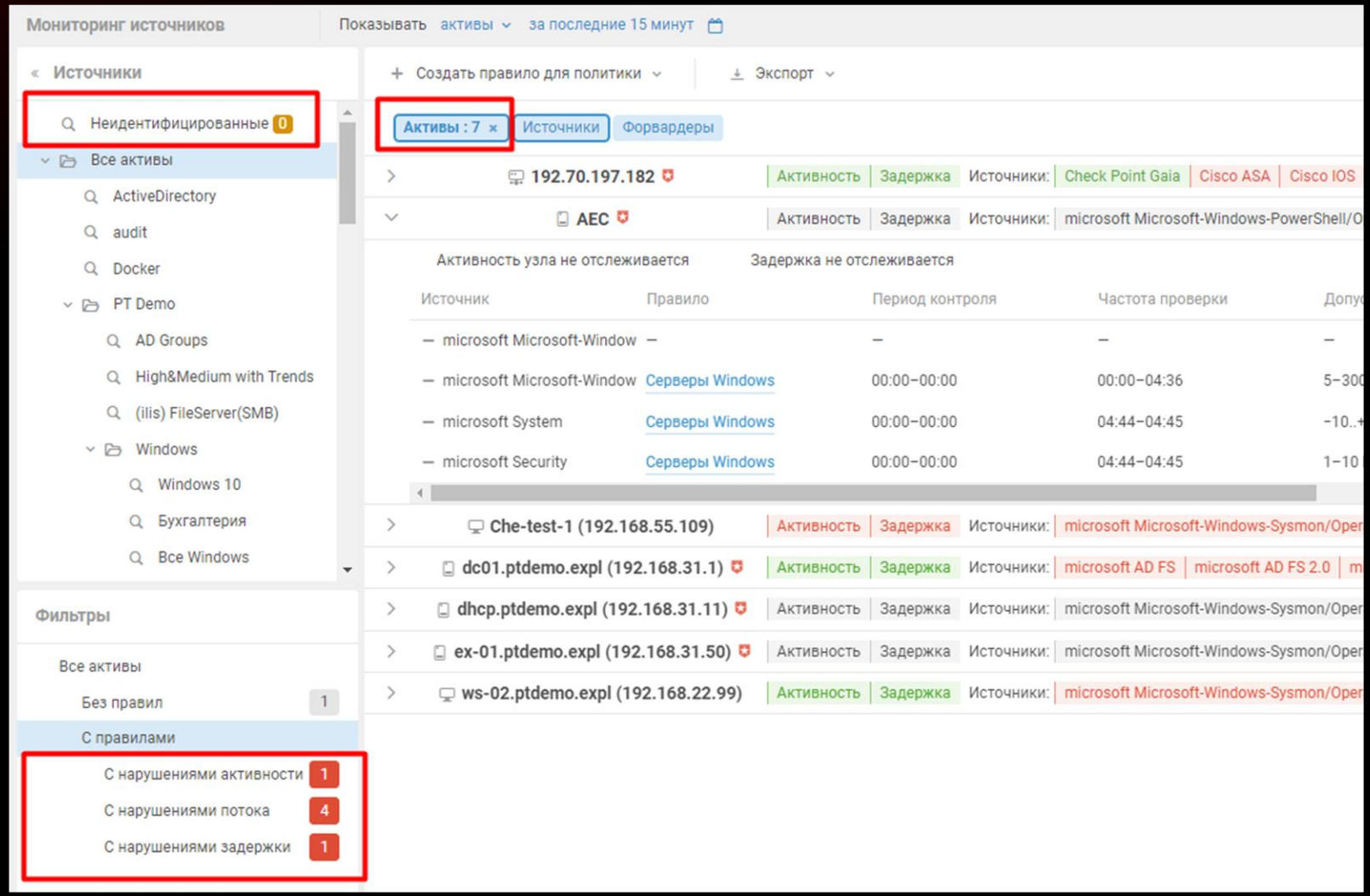
Активы как объекты защиты

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



Мониторинг источников

- События под контролем
- Рекомендации практических экспертов



BAD неутомимый помощник

График работы 24x7

ФОТ ~ = зарплата студента 2-3 курса

Рабочее место 1-2U 19” Rack mount

49

ML моделей

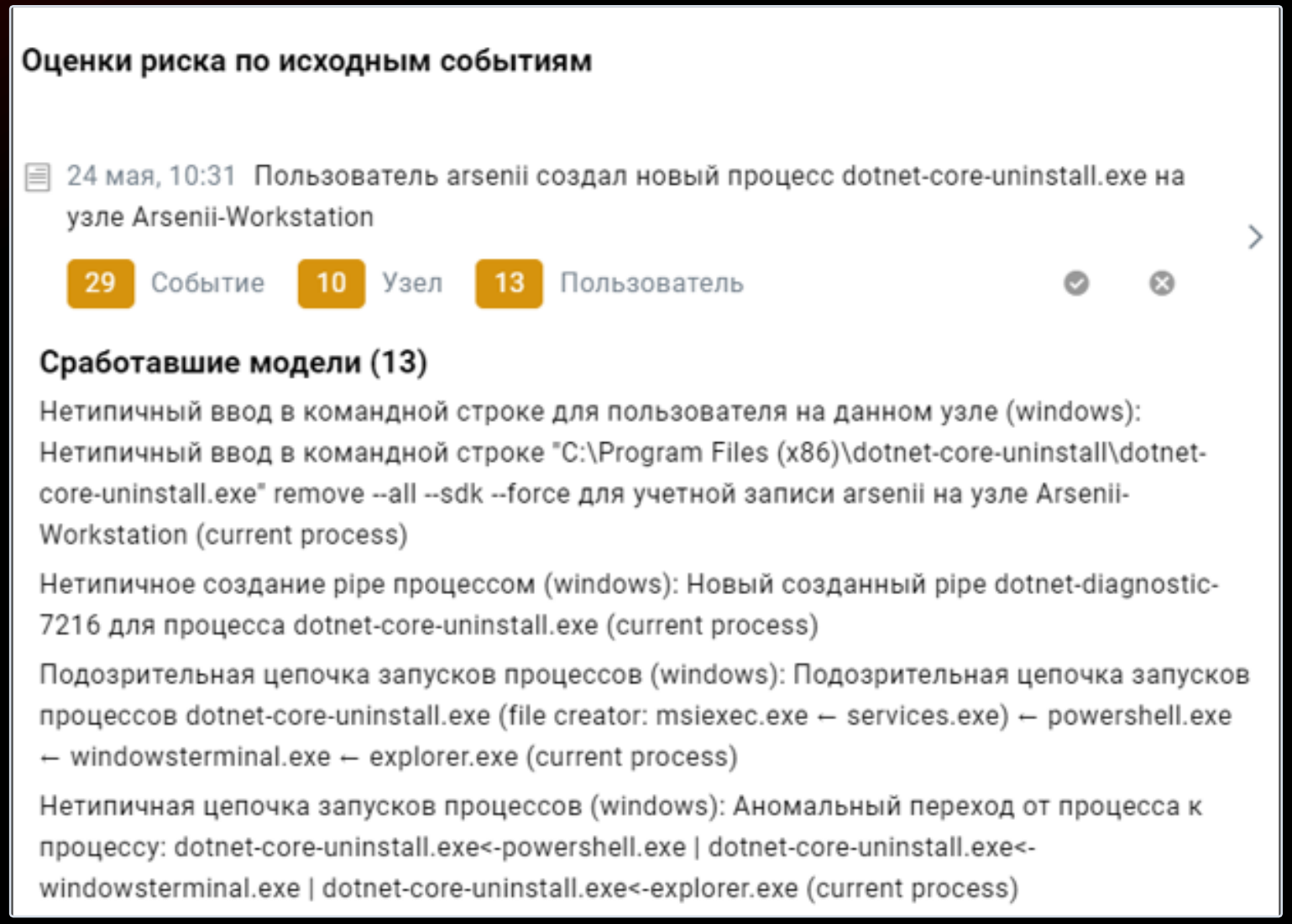
14

типов систем

- windows+sysmon
- security_center
- sql_server
- 1c_enterprise
- keycloak
- passwork
- auditd
- vsphere (ESX)
- checkpoint gaia
- cisco (ios,asa,fwsm,pix)
- fortigate
- openvpn
- artyfactory
- teamcity

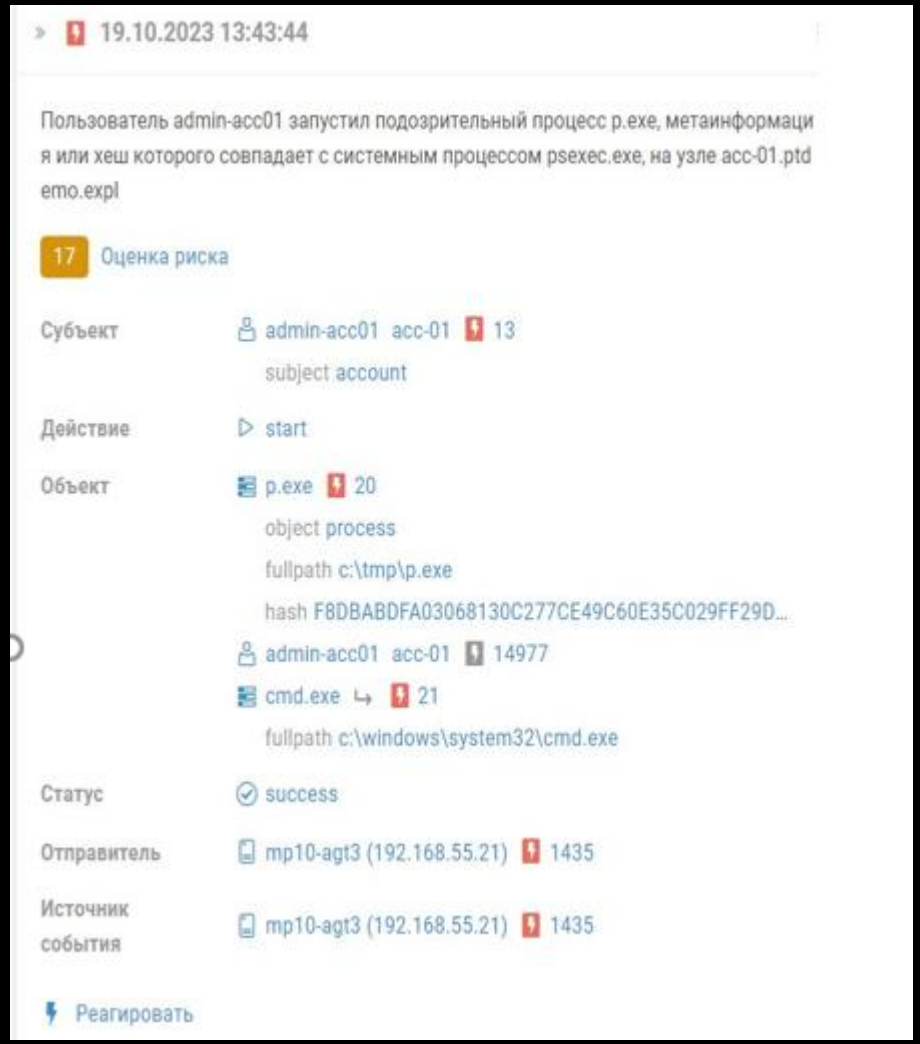
BAD неутомимый помощник

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



Фокус на контексте атаки

- Обязательных 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

344
источников «из коробки»

1181
правил корреляции

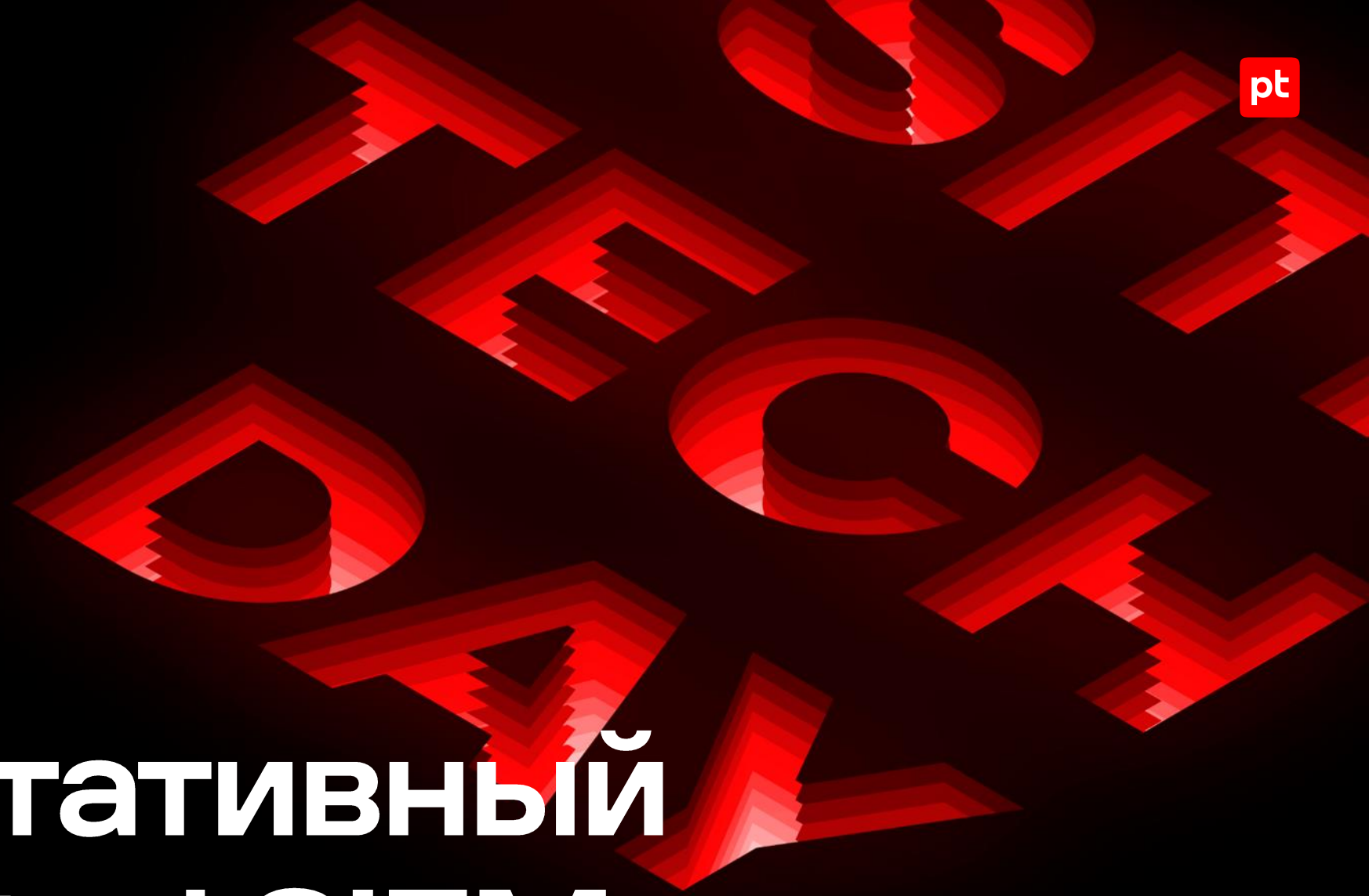
8876
правил нормализации

84
правил обогащений

182
табличных списка

284
техник из матрицы MITRE ATT&CK покрывает экспертиза MaxPatrol SIEM «из коробки»

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
- Развивает внутренних экспертов
- Выявляет попытки нарушения киберустойчивости

Спасибо!