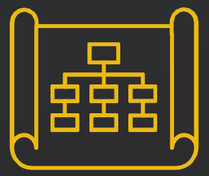
RT Protect SOC

Центр мониторинга
и реагирования на инциденты ИБ

Современные тенденции

PT
Информационная безопасность



Расширение разнообразия используемых для написания вредоносного программного обеспечения языков программирования и технологий, усложнение архитектуры

Всё более сложные социотехнические атаки, что требует повышения осведомленности в информационной безопасности рядовому работнику

Рост активности группировок, связанных с одной из сторон конфликта

Эксплуатация уязвимостей:
- Microsoft Exchange (ProxyNotShell - CVE-2022-41040)
- Apache Tomcat (Log4Shell - CVE-2021-44228)
- Microsoft Outlook Elevation of Privilege (CVE-2023-23397)
- Vmware Spring Framework (Spring4Shell CVE-2022-22965)

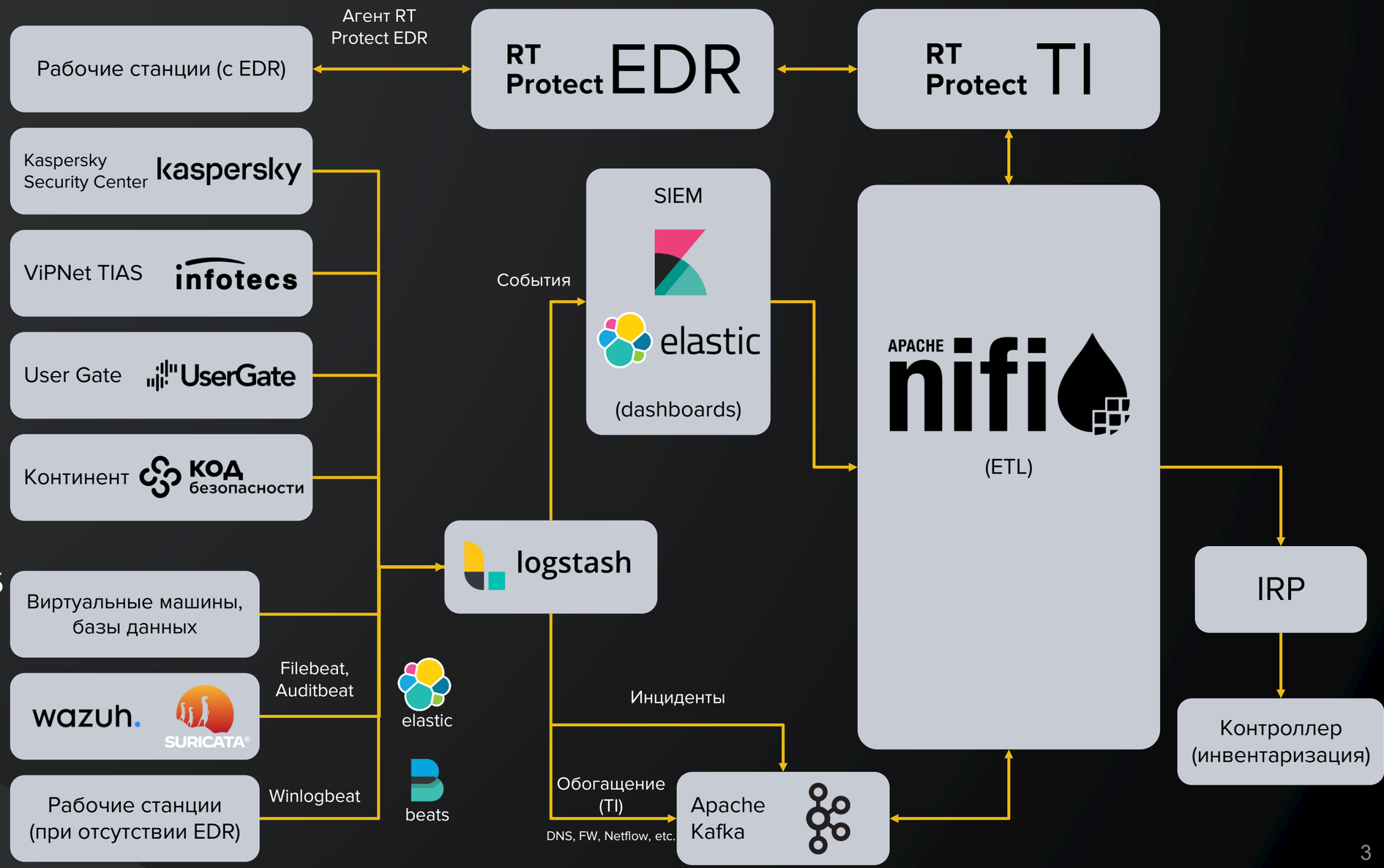
Как следствие, повышение требований к защите конечных точек

RT Protect SOC

PT Информационная безопасность

Задачи:

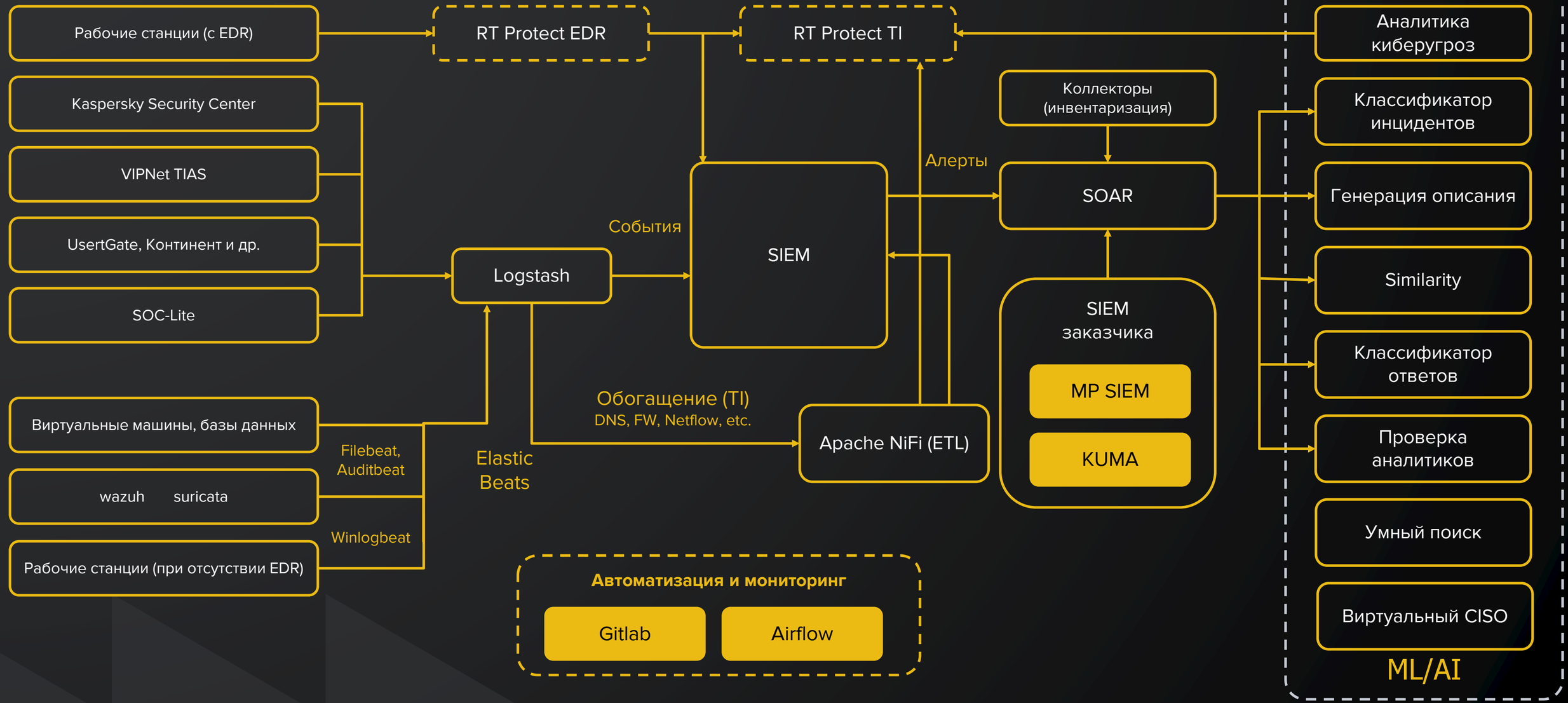
- Круглосуточный мониторинг корпоративной IT-инфраструктуры
- Сокращение времени обнаружения продвинутых атак
- Эффективное противодействие и устранение последствий
- Расследование инцидентов ИБ любого типа сложности
- Обеспечение непрерывности бизнес-процессов



Процессы SOC

PT Информационная безопасность

Архитектура SOC



Архитектура ИИ в SOC

Этапы подключения

PT
Информационная безопасность

Важно! Возможность написания коннекторов для подключения любых источников

1 этап

1. Определение перечня угроз, первичных сценариев для запуска
2. Формирование списка подключаемых источников

2 этап

1. Согласование оборудования и параметров соединения
2. Построение соединения site- to-site между площадками

3 этап

1. Настройка систем сбора/передачи
2. Настройка доступов
3. Предоставление доступа к дашбордам, настройка оповещений

4 этап

1. Контроль работы системы
2. Адаптация к событиям в инфраструктуре заказчика, выявление типичных инцидентов и исключений

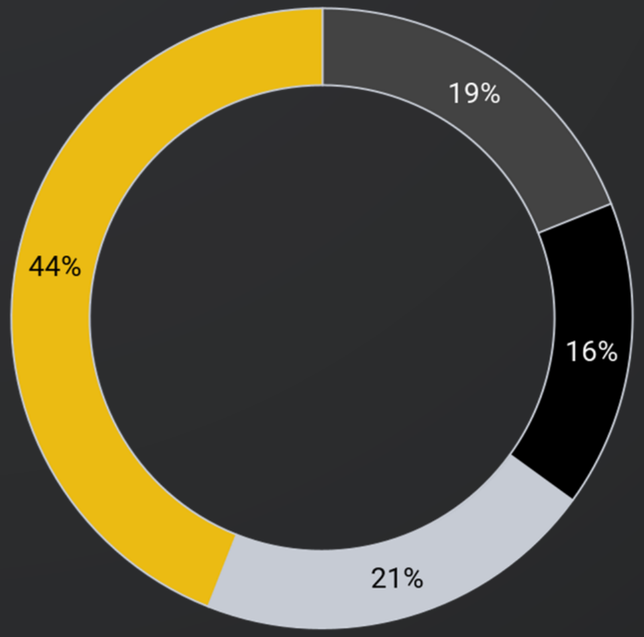
5 этап

1. Запуск мониторинга и реагирования на инциденты
2. Уведомление заказчика об обнаруженных инцидентах с нашими рекомендациями

Тестирование на проникновение

PT Информационная безопасность

Результаты внешнего тестирования (+ комплексного):



- Прошли внешний периметр, попали в локальную сеть
- Захватили ресурсы, но не прошли во внутреннюю сеть
- Получили наивысшие привилегии в ЛВС
- Не захватили ни одного ресурса

Самые популярные векторы атак

ошибки конфигурации (доступна директория .git, LFI)
➔ получение конфигурационных файлов
➔ создание пользователя с правами администратора
➔ проксирование трафика во внутреннюю сеть

устаревшее ПО (RCE)
➔ создание пользователя с правами администратора
➔ проксирование трафика в локальную сеть

ошибки в исходном коде web-приложения (SQLInjection, LFI, RCE)
➔ получение конфигурационных файлов
➔ создание пользователя с правами администратора
➔ проксирование трафика во внутреннюю сеть

социальная инженерия
➔ получение учётной записи пользователя, получение Reverse Shell

Социальная инженерия 10/15 успешно получен Reverse Shell

Самые популярные уязвимости

CVE-2022-27228 (Bitrix vote module RCE),CVE-2021-34473 (MS Exchange RCE ProxyShell)

CVE-2022-41040+CVE-2022-41082 (MS Exchange RCE ProxyNotShell)

Объем обрабатываемых инцидентов

PT Информационная безопасность

Основные характеристики:

Подключение самых разнообразных источников событий ИБ для эффективного мониторинга

более 1000

правил детектирования вредоносной активности

Общий объем обрабатываемых событий в секунду

100 000 EPS

Среднее время обработки инцидента:

12 мин 30 сек

Среднее время расследования:

20 мин 25 сек

Время реагирования на инциденты

PT
Информационная безопасность

Режим обработки инцидентов 24/7

Расследования проводятся опытными аналитиками
(1-е место на киберполигоне SOC-Forum 2022 Blue Team, доклады на PhDays 2023)

Собственная проприетарная архитектура автоматизированного обогащения логов через Apache NiFi

Агенты EDR фиксируют только потенциально опасные события
генерируют меньше FP, указывают на действительно вредоносные действия

Среднее кол-во инцидентов в IRP в час:

21 инцидент
5 (EDR) + 16 (другие источники)

Среднее время обработки инцидента:

12 мин 30 сек

Среднее время расследования:

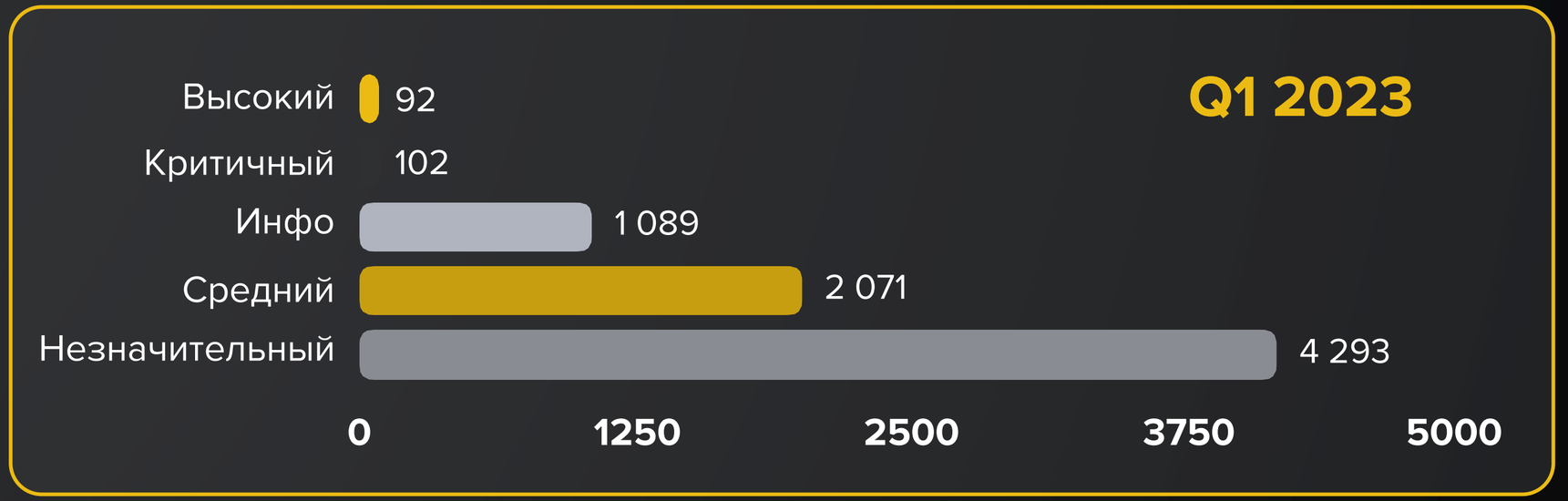
20 мин 25 сек

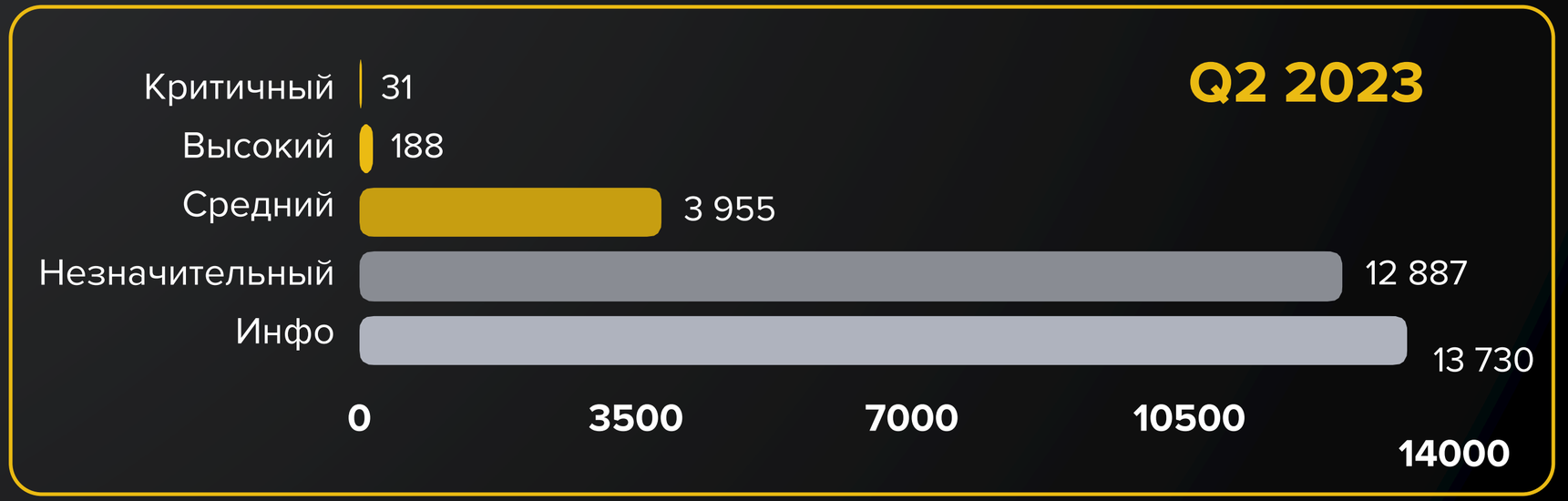
Критичность инцидентов

PT Информационная безопасность

Снижение числа критичных инцидентов:

- удаление ВПО
- расширение системы мониторинга
- совершенствование экспертизы правил

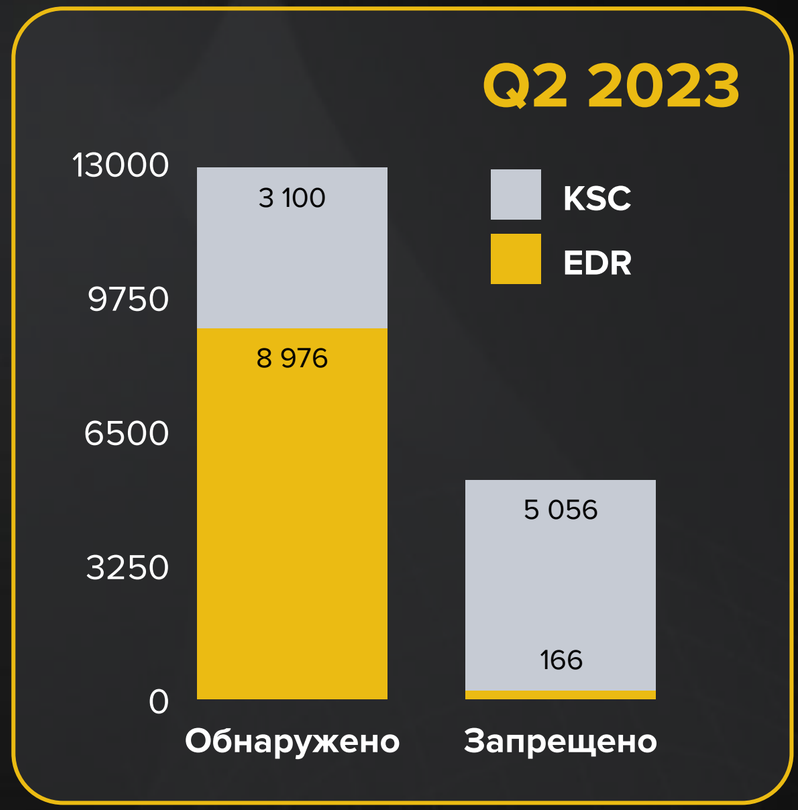




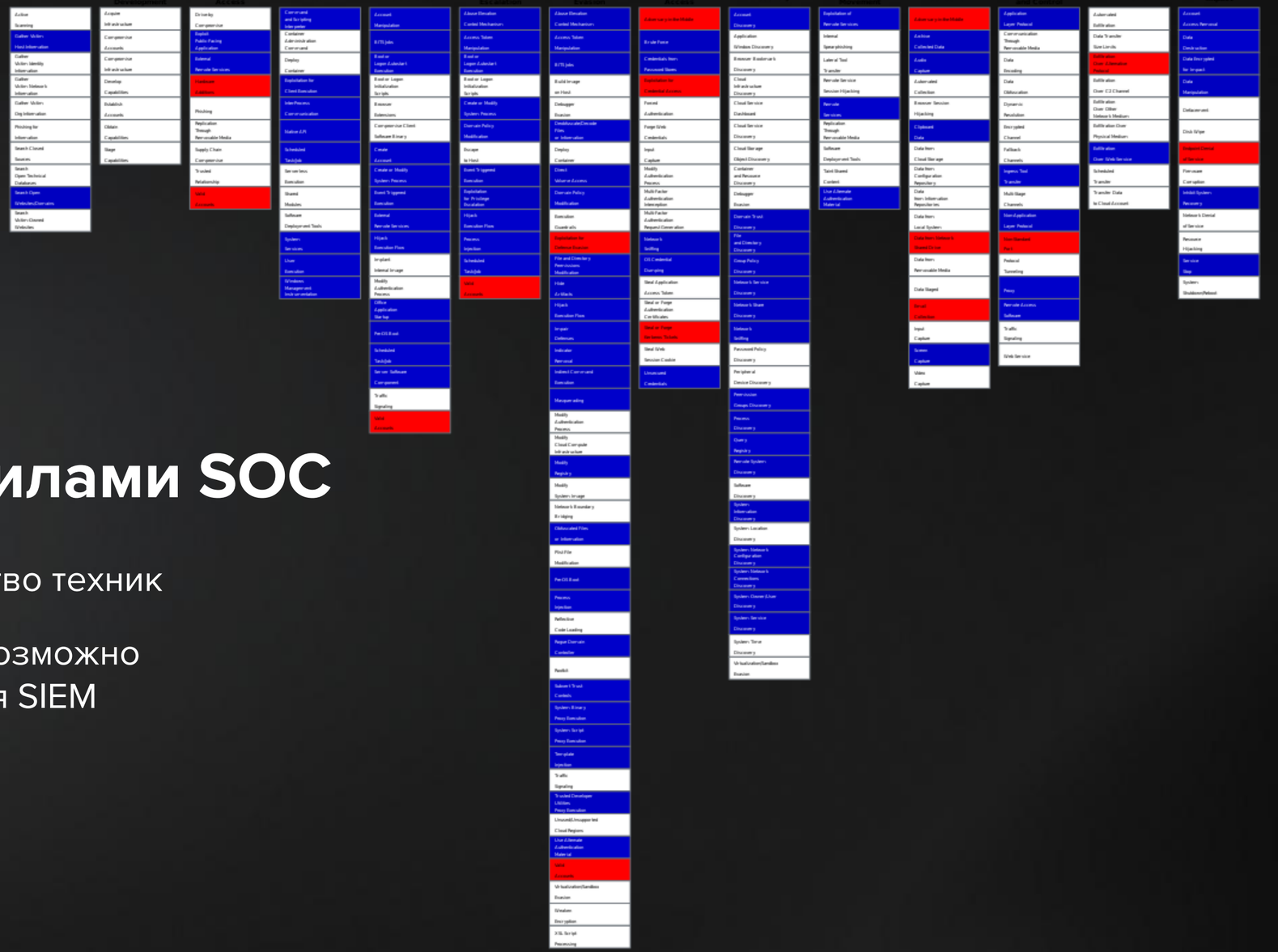
Статистика активного реагирования на конечных точках

PT Информационная безопасность

- Увеличение вклада сработок антивируса в общее число инцидентов после после подключения новых Заказчиков
- EDR блокирует опасные действия, пропущенные антивирусом



Покрытие матрицы MITRE ATT&CK правилами SOC



- RT Protect EDR покрывает множество техник
- Существуют техники, которые невозможно зафиксировать без использования SIEM
- EDR (синий) и SIEM (красный)

PT
Информационная безопасность

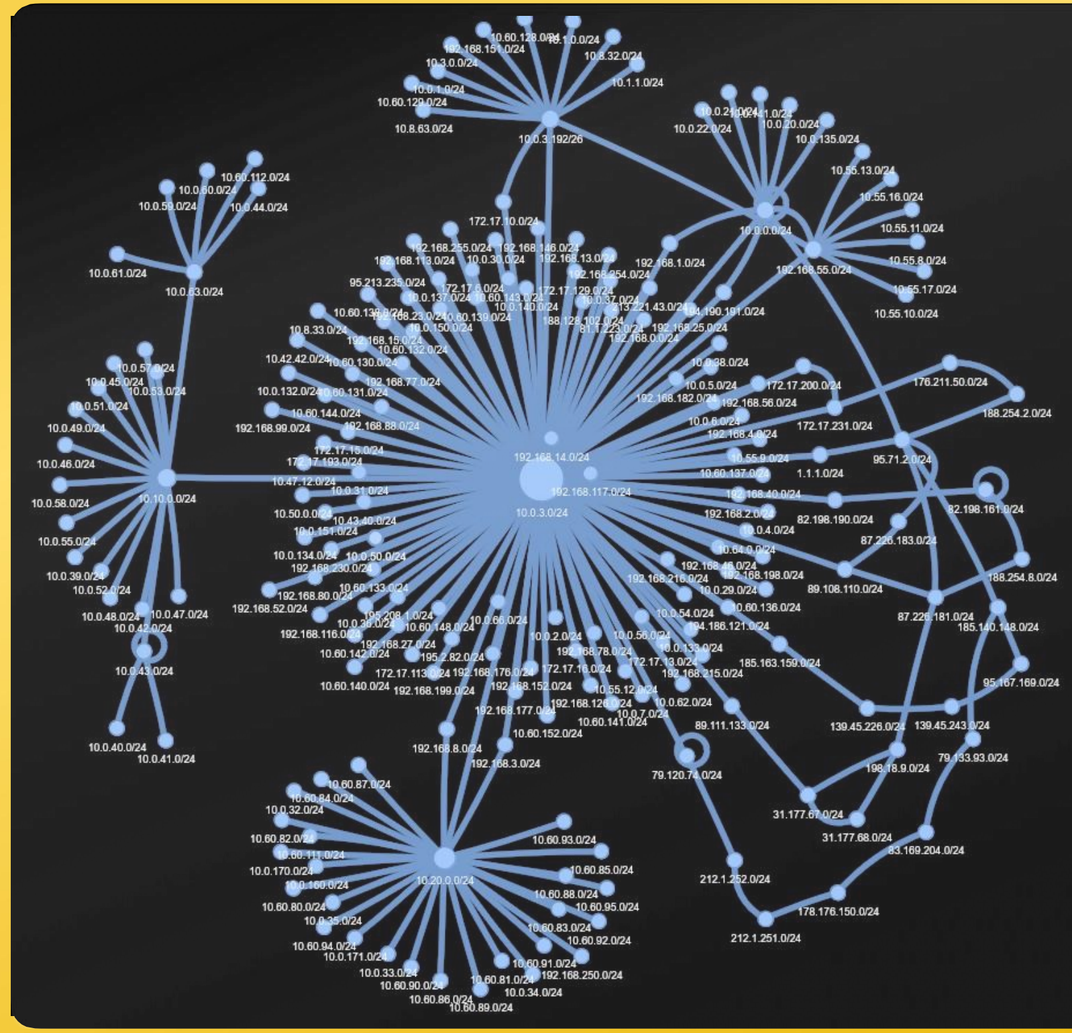
Инвентаризация

Интеграции:

- AD
- KSC
- Veeam
- SNS
- Scan

Другие источники:

- Vulnerability Management
- RT Protect CPT



Threat Intelligence

PT Информационная безопасность

Развитие собственной TI-платформы RT Protect TI:

- Расширение интеграции с источниками данных и платформами
- Централизованное распространение наборов аналитики на серверы EDR
- Углубление аналитики статистики сигнатурных сработок
- Планируется внедрение углубленной аналитики инцидентов с использованием данных Threat Intelligence – переход к верхним элементам “Пирамиды боли”

Подключение новых источников данных (фидов):

- RST Cloud – успешное взаимодействие
- Open Source фиды (более 50 источников)
- Индикаторы компрометации, полученные по результатам расследований SOC

Интеграции для потоковой аналитики:

- VirusTota
- RST Cloud
- Национальный Мультисканер

Прозрачное взаимодействие с AV Soft Athena и PT Sandbox

Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

НОВИКОМБАНК

Контакты

Адрес: 117587, г. Москва, Варшавское шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность