RT Protect SOC

Центр мониторинга
и реагирования на инциденты ИБ

Современные тенденции

Расширение разнообразия используемых для написания ВПО языков программирования и технологий, усложнение архитектуры

Всё более сложные социотехнические атаки, что требует повышения осведомленности об информационной безопасности обычным работникам

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

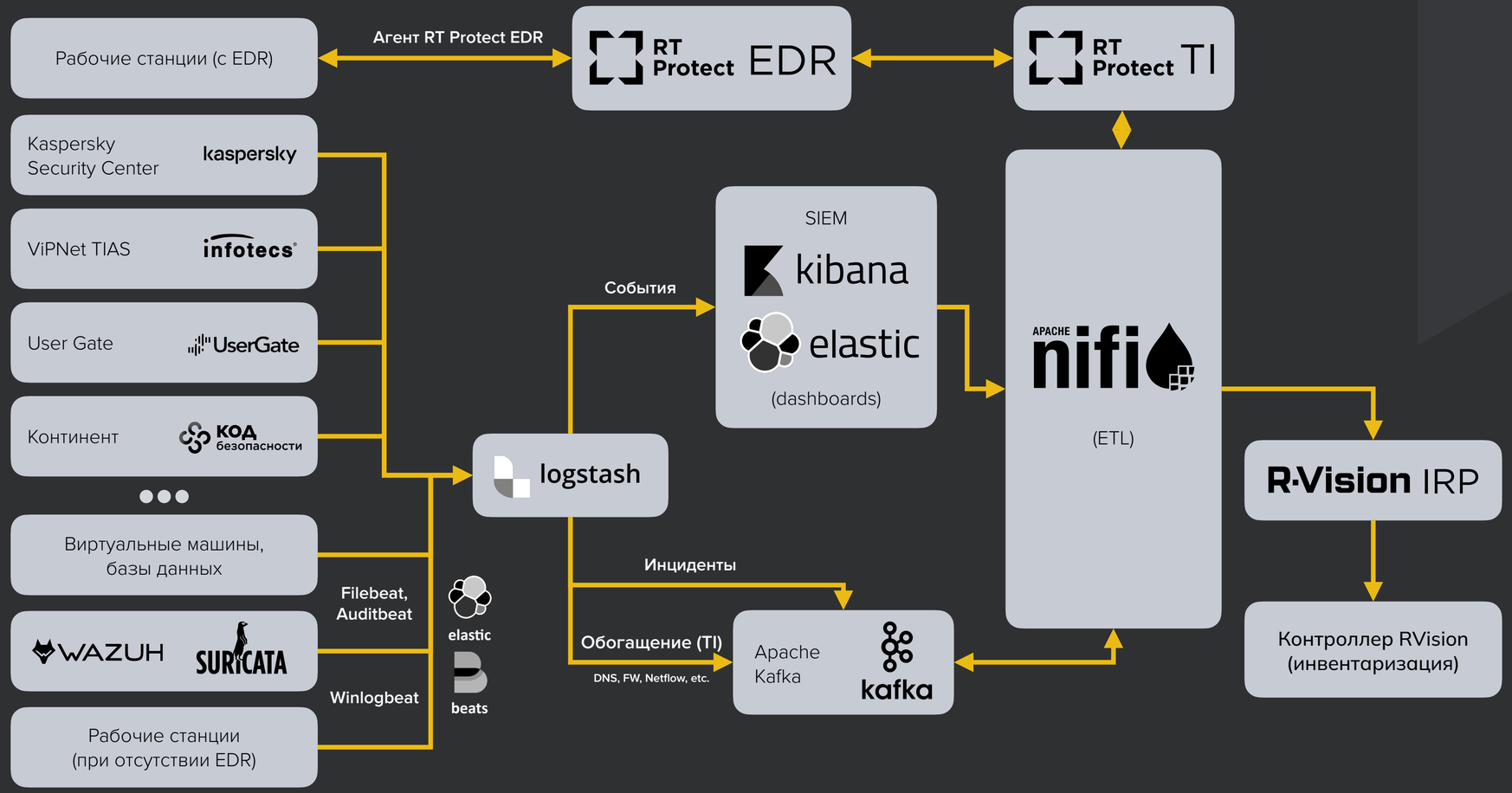
PT
Информационная безопасность

RT Protect SOC

SOC (Операционный центр безопасности)
– это централизованное подразделение (сервис), которое занимается вопросами информационной безопасности на организационном и техническом уровне, в целях нейтрализации угроз информационной безопасности организаций.

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



PT
Информационная безопасность

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

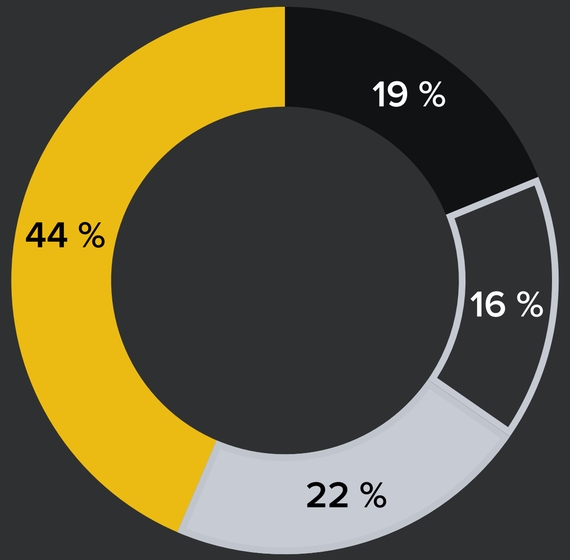
1. Контроль работы системы
2. Адаптация к событиям в инфраструктуре заказчика, выявление типичных инцидентов и исключений

5 этап

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

Тестирование на проникновение

Результаты внешнего тестирования (+ комплексное):



- 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 вектора 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 реверс шелла

Социальная инженерия

10/15

успешно получен шелл

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)

PT
Информационная безопасность

Объем обрабатываемых инцидентов

- Увеличение количества **обрабатываемых инцидентов**
- Снижение количества **ложно-положительных срабатываний**

Q1 2023

Всего 7647

FP 68%

Q2 2023

Всего 30791

FP 60%

Более

50 000 EPS

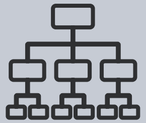
совокупный поток событий, обрабатываемый в SOC

PT
Информационная безопасность

Время реагирования на инциденты

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:

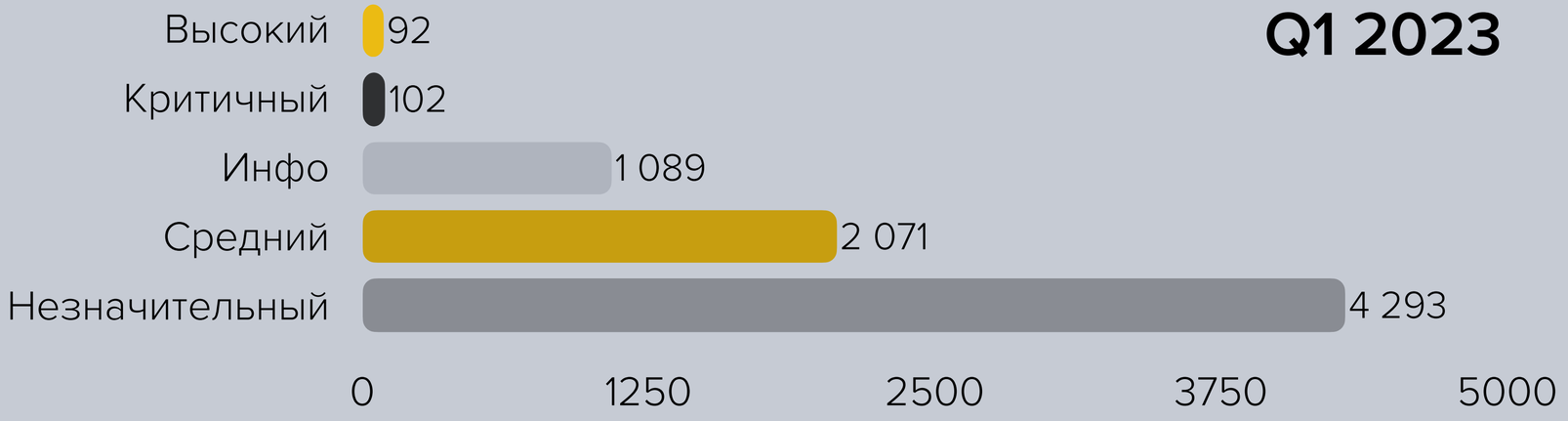
20 мин 25 сек

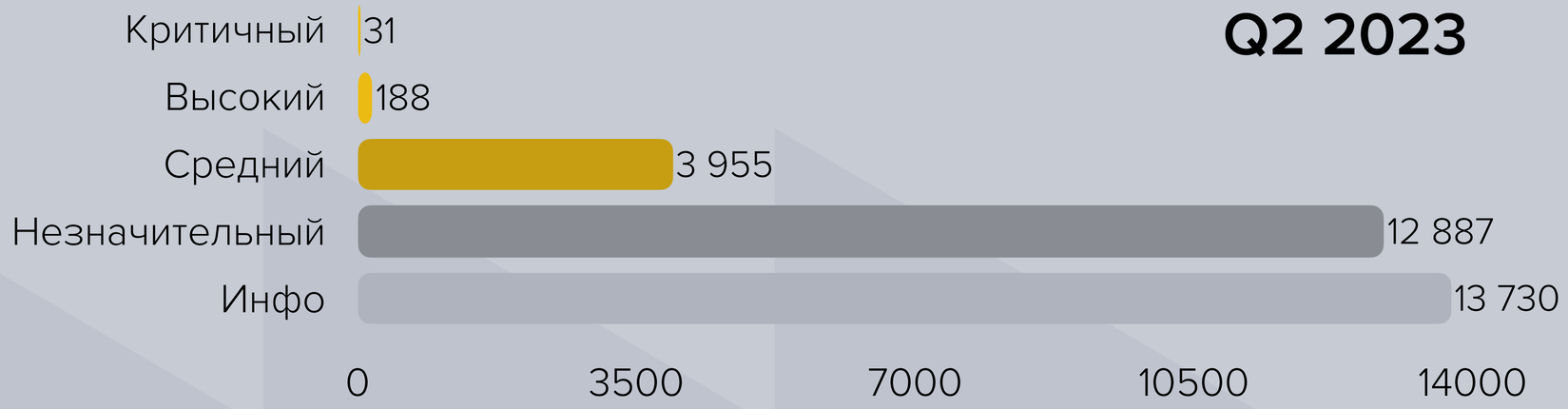
PT
Информационная безопасность

Критичность инцидентов

Снижение числа критичных инцидентов:

- удаление ВПО
- расширение системы мониторинга
- совершенствование экспертизы правил

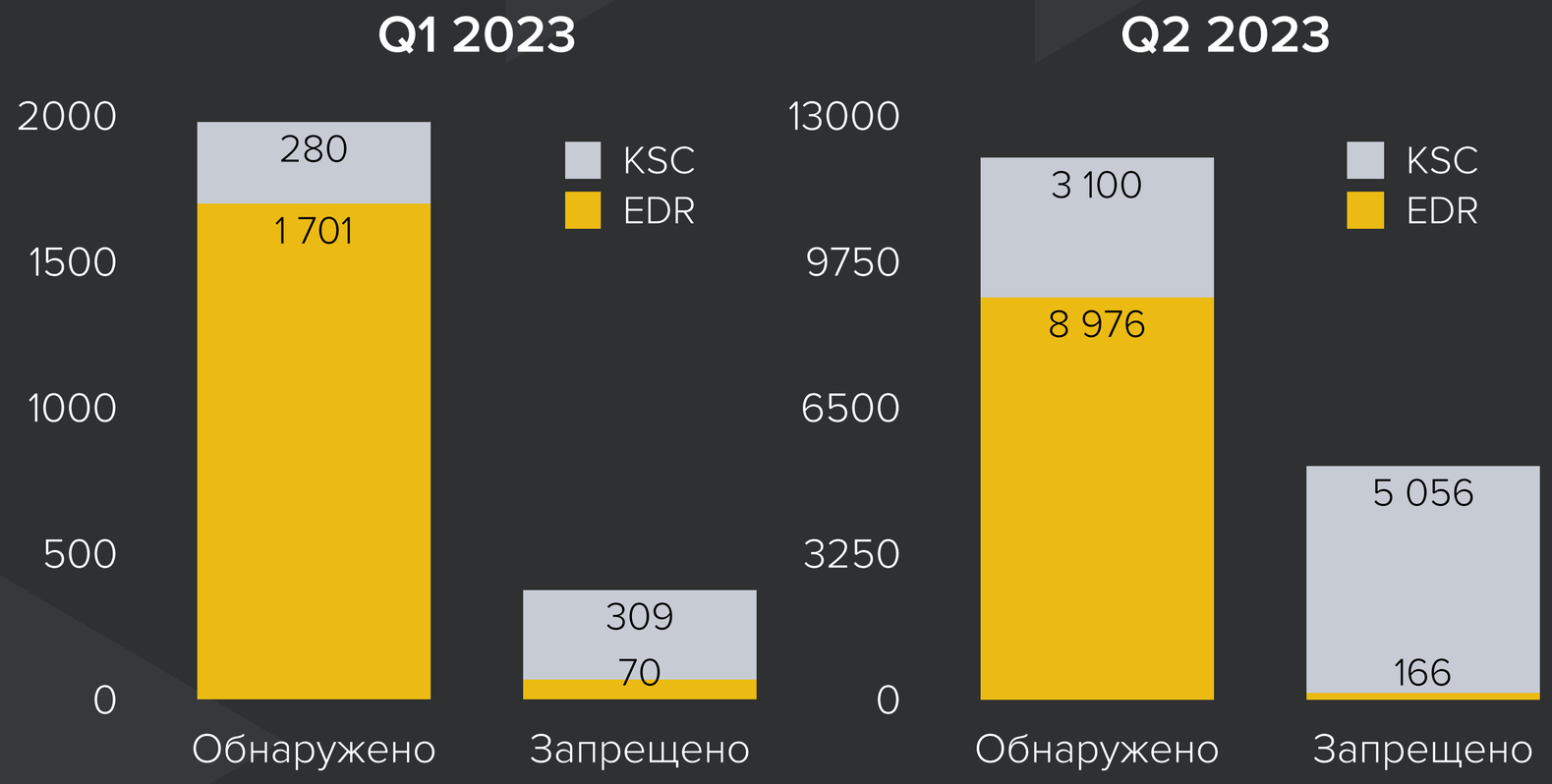




PT
Информационная безопасность

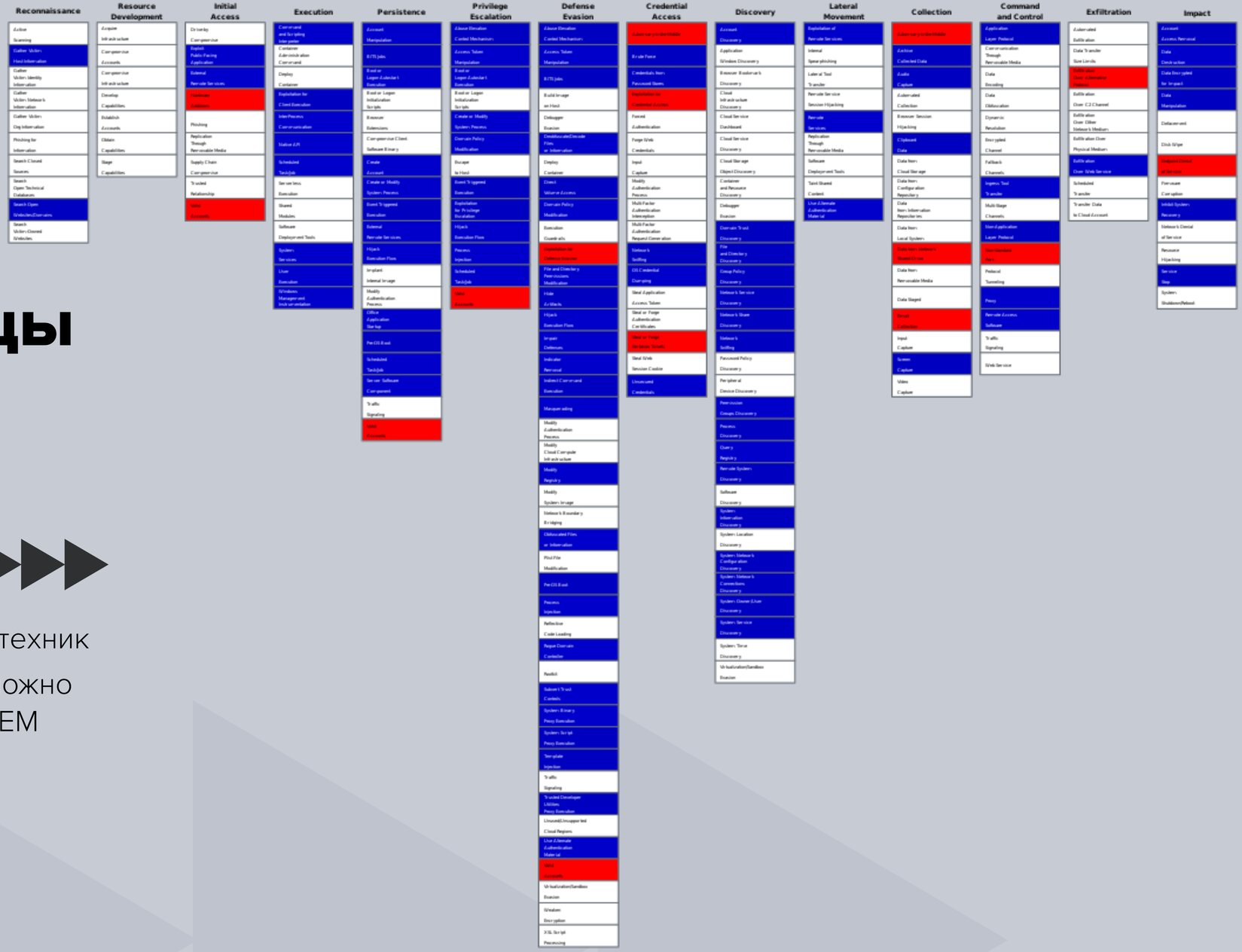
Статистика активного реагирования на конечных точках

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



PT
Информационная безопасность

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

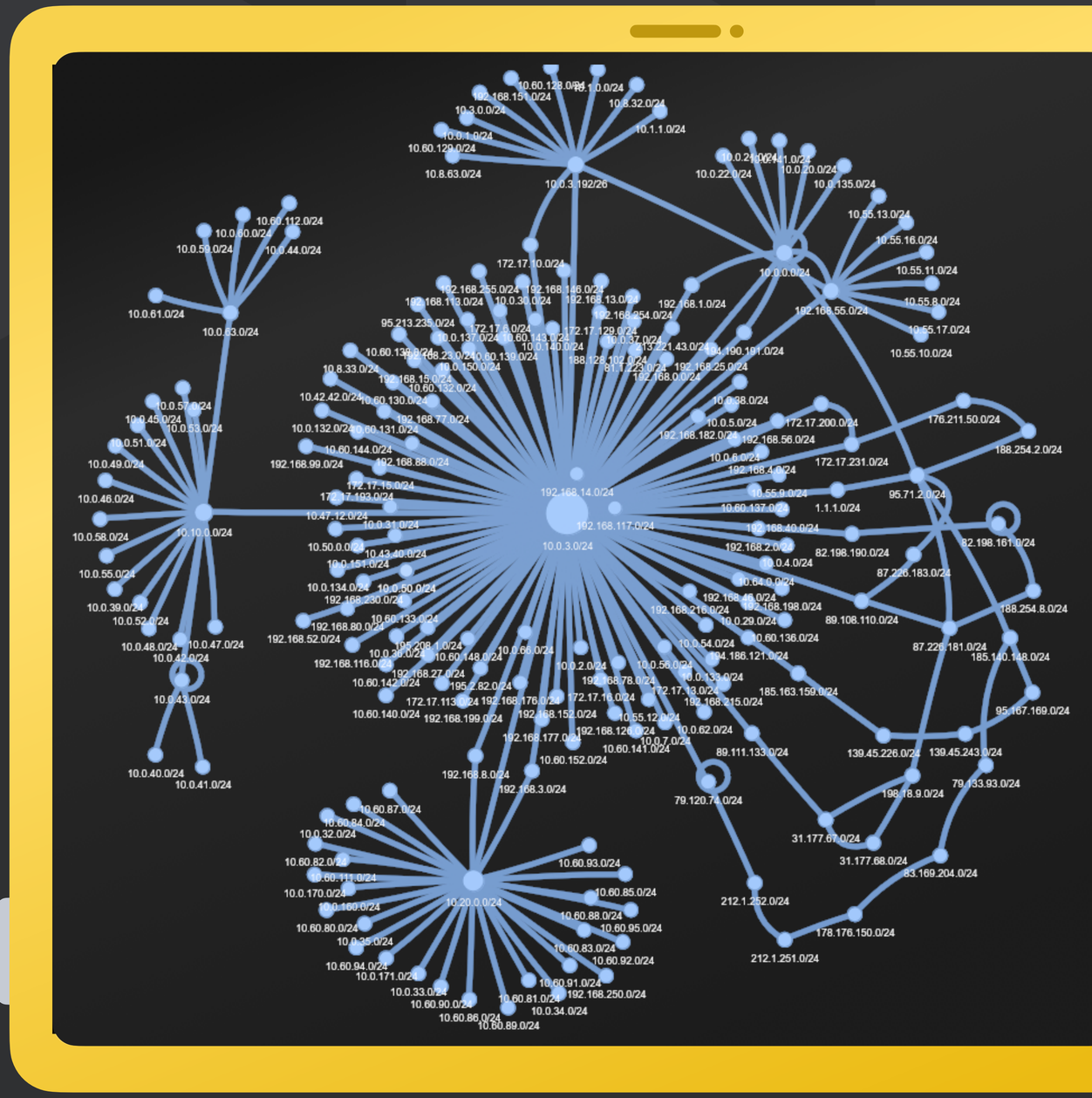
Инвентаризация

Интеграции:

- AD
- KSC
- Veeam
- SNS
- Scan

Другие источники:

- Vulnerability Management
- RT Protect CPT



Расширение покрытия источников

2022

- Windows Logs (RT Protect EDR)
- Linux logs (Wazuh)
- Антивирусы (KSC, Dr.Web)
- Почтовые антивирусы (KSMG)
- IDS/NGFW (UserGate, VipNet TIAS, CheckPoint)
- SIEM (PT MP SIEM)

2023

- Windows Endpoint (RT Protect EDR, WinEvt, DNS и т.д.)
- Linux Endpoint (RT Protect EDR, Auditd, DNS, и т.д.)
- Антивирусы (KSC, Dr.Web, Symantec)
- Почтовые антивирусы (KSMG)
- Сетевое оборудование (Cisco, Huawei – Netflow, Netstream, PortSecurity)
- VPN (OpenVPN, Континент, VipNet)
- IDS/NGFW (UserGate, CheckPoint, VipNet TIAS, WatchGuard)
- PAM (CyberArk, Indeed, Infrascope, SafeInspect, Бастион)
- SIEM (PT MP SIEM, Elastic SIEM, KATA)
- СЗИ от НСД (SecretNet)
- PLM (TeamCenter)
- Бизнес-приложения (1С)
- DLP (Solar Dozor)

PT
Информационная безопасность

Threat Intelligence

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:

- VirusTotal
- RST Cloud
- Национальный Мультисканер

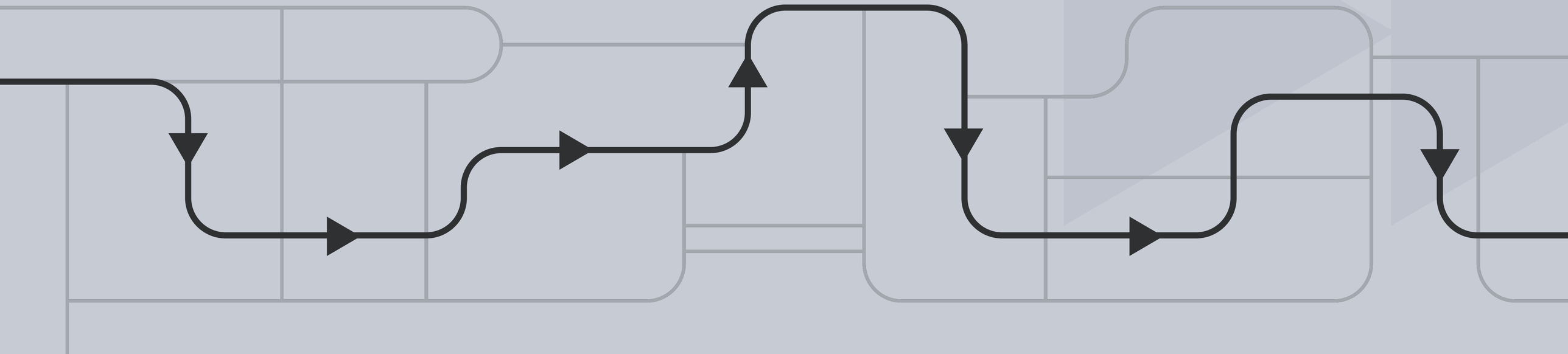
Прозрачное взаимодействие с AV Soft Athena и PT Sandbox

PT
Информационная безопасность

Интеграции

PT
Информационная безопасность

- DCAP/DAG “Спектр” от Cyberpeak – защита от легитимных техник
- Deception XELLO – защита от продвинутых техник
- Sandbox:
  - Athena от АВ Софт
  - PT Sandbox от Positive Technologies



Стратегические достижения

- Увеличение технологического стека SOC-центра
- EDR → XDR
- Detection-as-a-Code
- Аккредитованный центр ГОССОПКА класса А
- КЦОПЛ как один из источников SOC-центра → SOC Lite АО «РТ-Информационная безопасность»
- Прозрачный технологический стек. Прозрачность в качестве сервиса для Заказчиков, поиск улучшений/ автоматизации на постоянной основе

РТ
Информационная безопасность

Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК
УМПО

КБП

СИБЕР

Нацимбио

Янтарный комбинат
акционерное общество

УВЗ

Акционерное общество
Рязанский радиозавод

Контакты

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

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

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность

RT Protect SOC