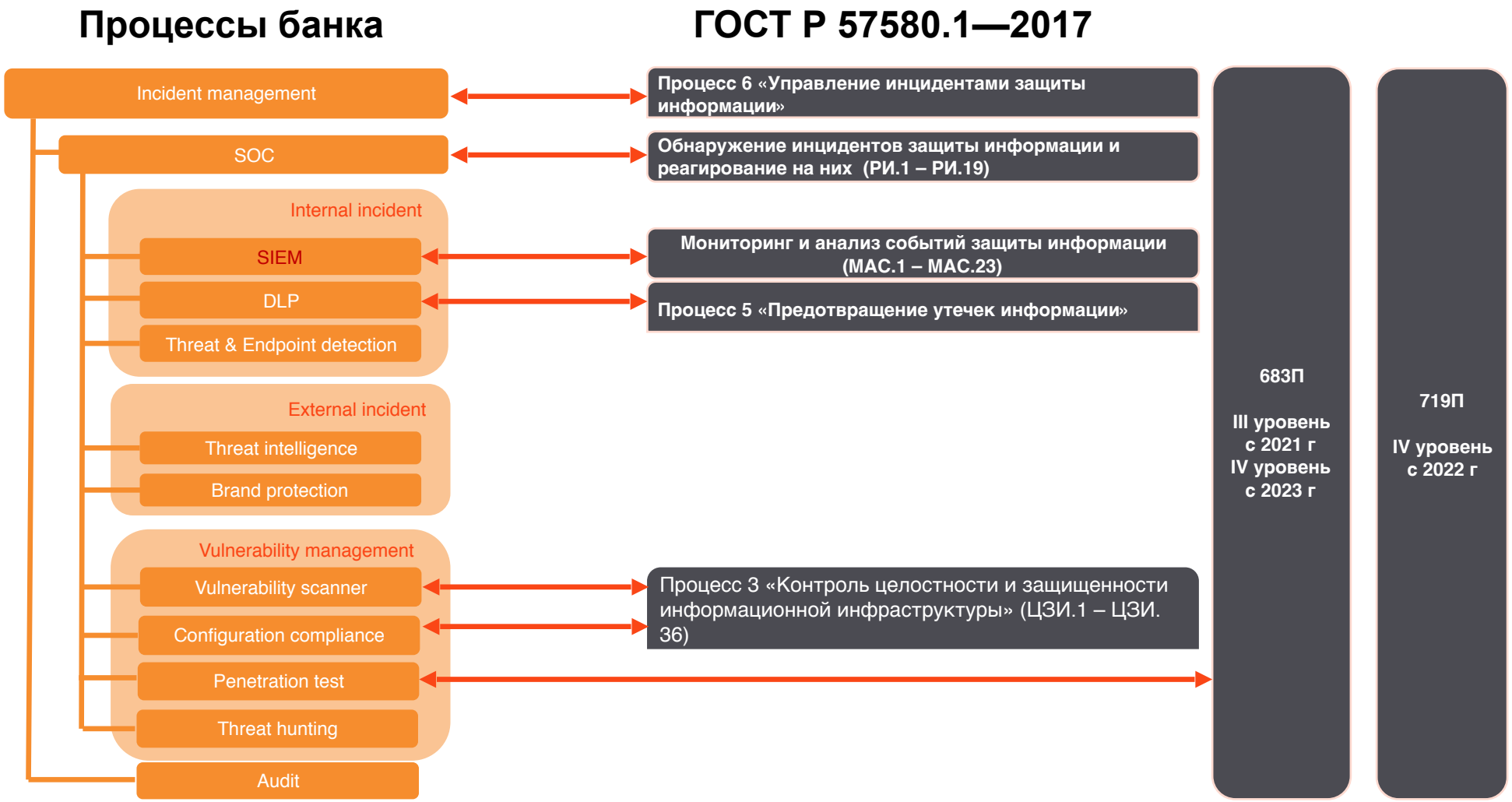
SOC на примере опыта Абсолют банк

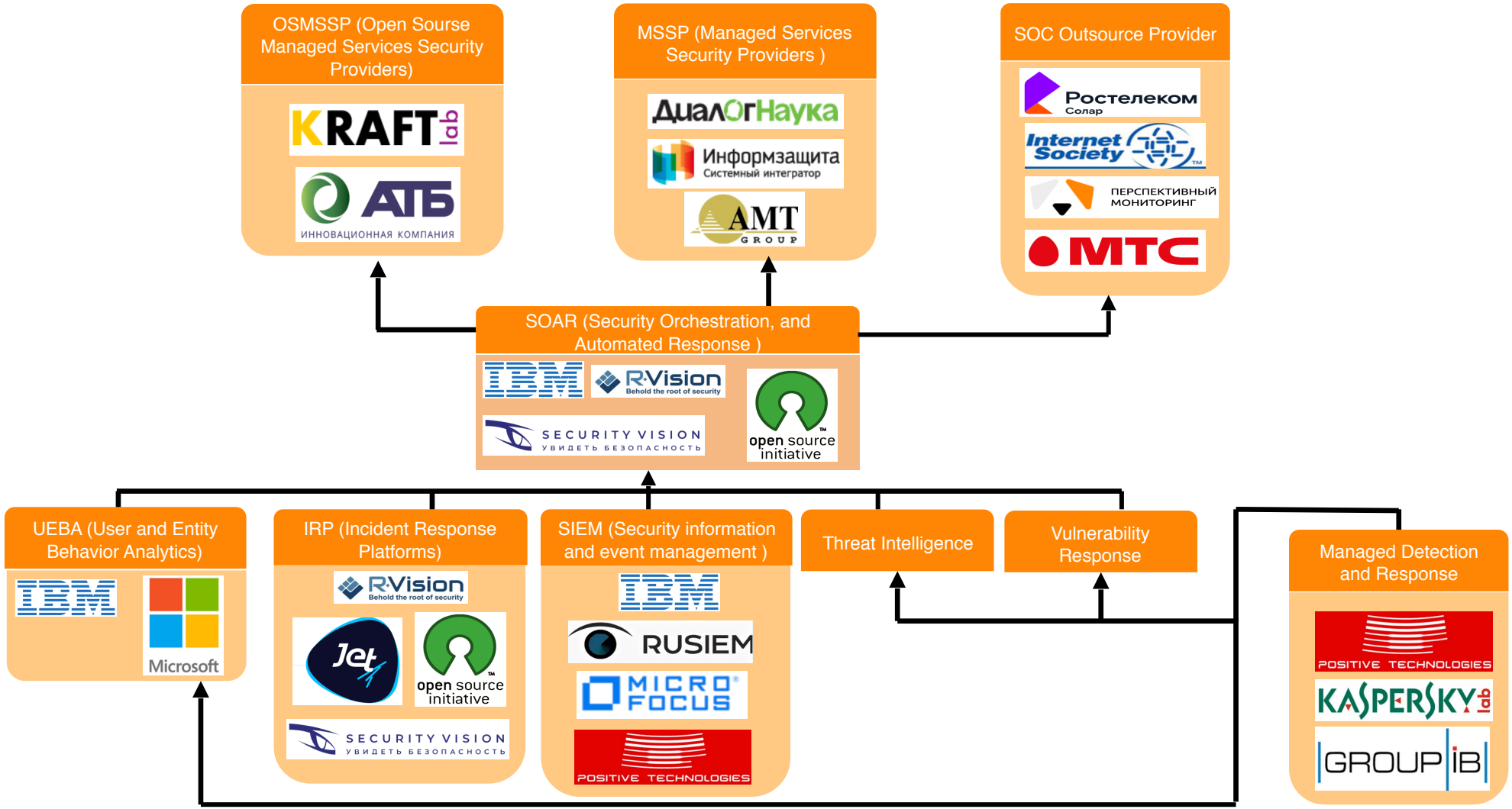
абсолют банк

Управление инцидентами в кредитной организации



Функции SOC на основе классификации MITRE

Поставщики услуг и компонентов SOC



Текущая проблематика

Проблематика

- Множество систем порождает множество консолей (нехватка людей)
- Нет связанности и причинноследственности события (большие ресурсные затраты на анализ)
- Нет возможности реагировать на все инциденты и контролировать устранение (нет физически столько ресурсов)
- Распределенная команда
- Нет прямой связи между ИТ, ИБ, операционными рисками

Предлагаемое решение

- Выполнить регуляторные требования Банка России в части ГОСТ Р 57580.1-2017
- Увеличить процент раскрываемости инцидентов с 30 % до 90 %
- Уменьшить время устранения инцидента до 30 мин
- Реализовать интеграцию средств защиты и контроля в единую экосистему
- Уменьшить сложность реагирования
- Обеспечить интеграцию банка с операционными рисками

Сравнение подходов

Opensource

Плюсы:

- Открытый код и возможность доработки собственными силами
- Гибкость продукта с возможность интеграции любых процессов и систем в том числе систем обрабатывающих конфиденциальную информацию и коммерческую тайну
- Возможность использования различных баз под потребности скорости реагирования
- Встроенные сторонние модули на порядок дешевле стационарного девайса
- Возможность поддержки как собственными силами, так и аутсорсером
- Возможность использования готовых коннекторов

Минусы:

- Необходимость содержания в штате разработчиков
- Возникает зависимость от компании разработчика ядра
- Нет гарантии долгосрочных обязательств компании поставщика ядра на рынке

Коммерческий SOC

Плюсы:

- Основные решения из коробки
- Интеграция с известными системами сбора событий
- IRP/SOAR/SGRC на одной платформе
- Множество готовых плэйбуков
- Интерактивный usability
- Многофункциональный конструктор

Минусы:

- Акцент на информационной безопасности
- Экономическая не целесообразность если не провайдер SOC
- Перегруженность интерфейса
- Большие трудозатраты на внедрение
- Большие трудозатраты на изменение
- Требуется интеграция с со смежными подразделениями

Аутсорсинг

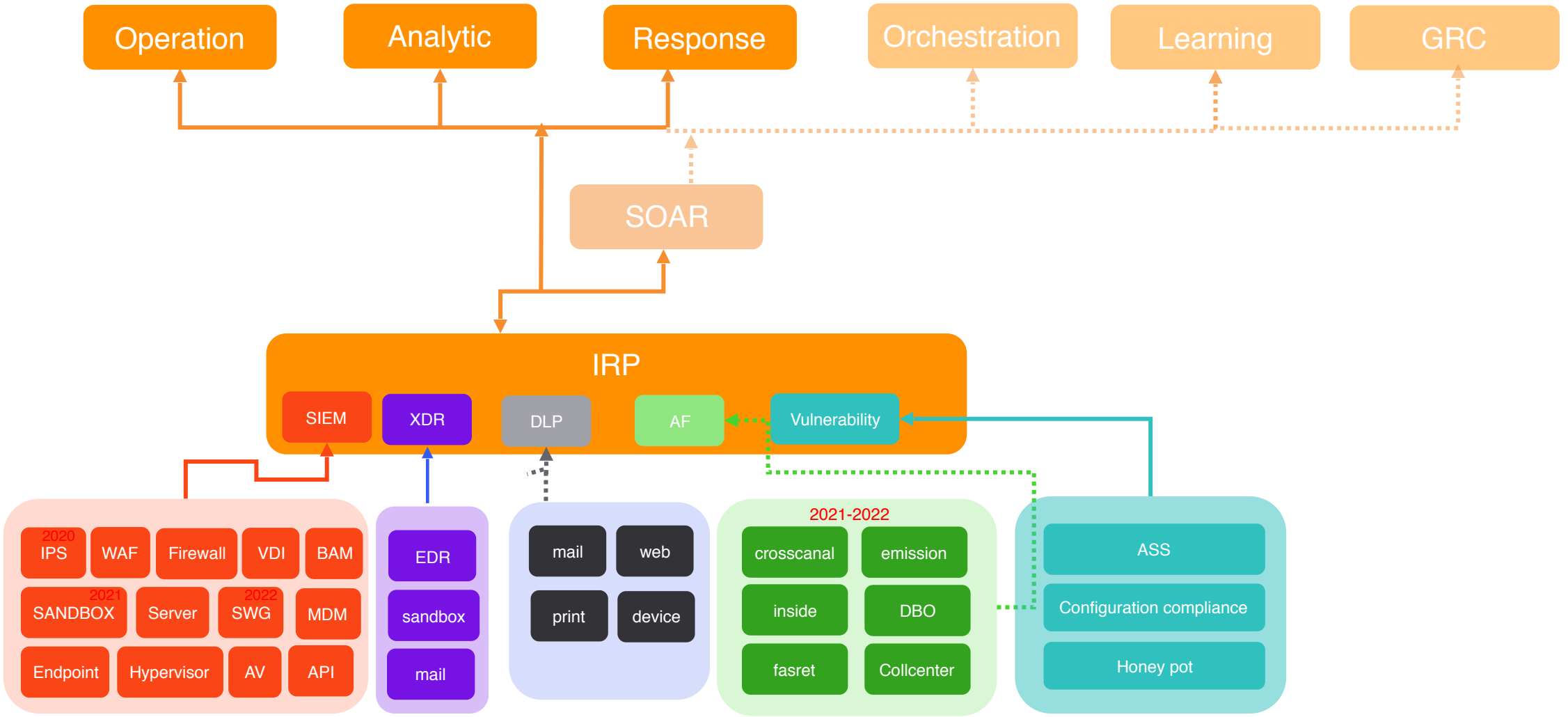
Плюсы:

- Возможность отдавать сырой трафик и получать обработанные события
- Возможность определять SLA в договоре аутсорсинга
- Фактически отдача всего процесса по управлению инцидентами на аутсорсинг – минимизация штата

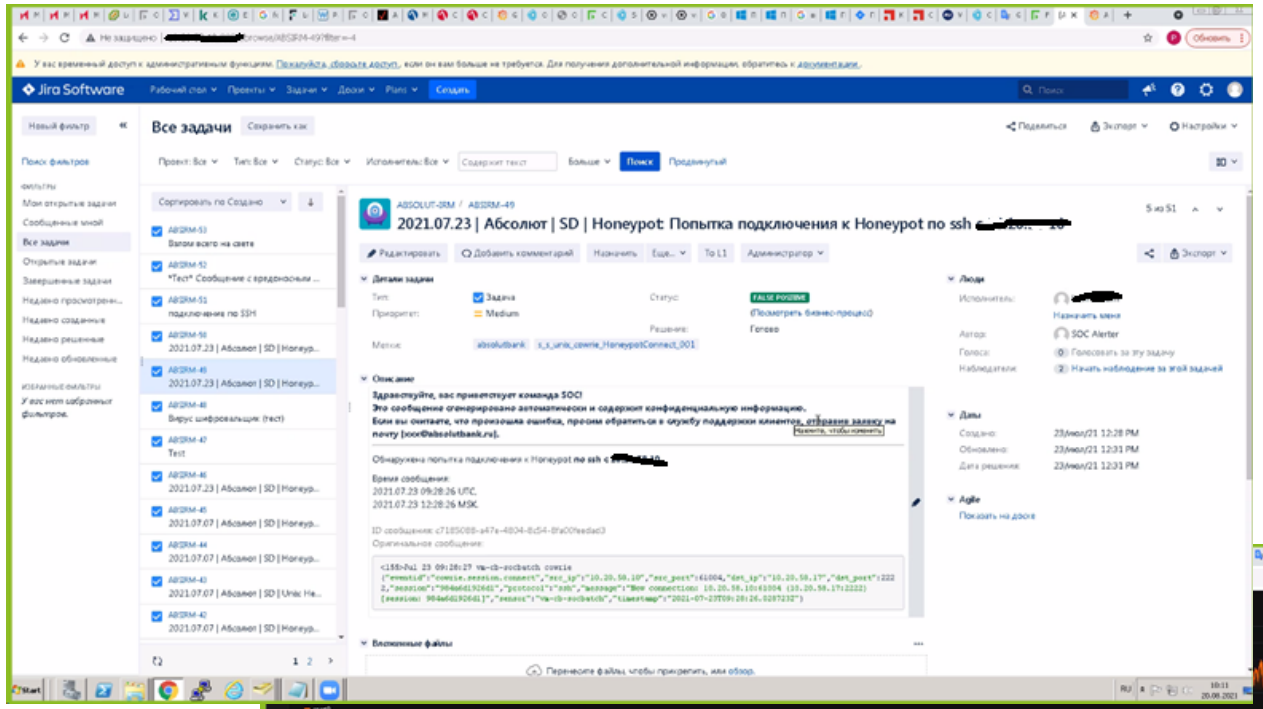
Минусы:

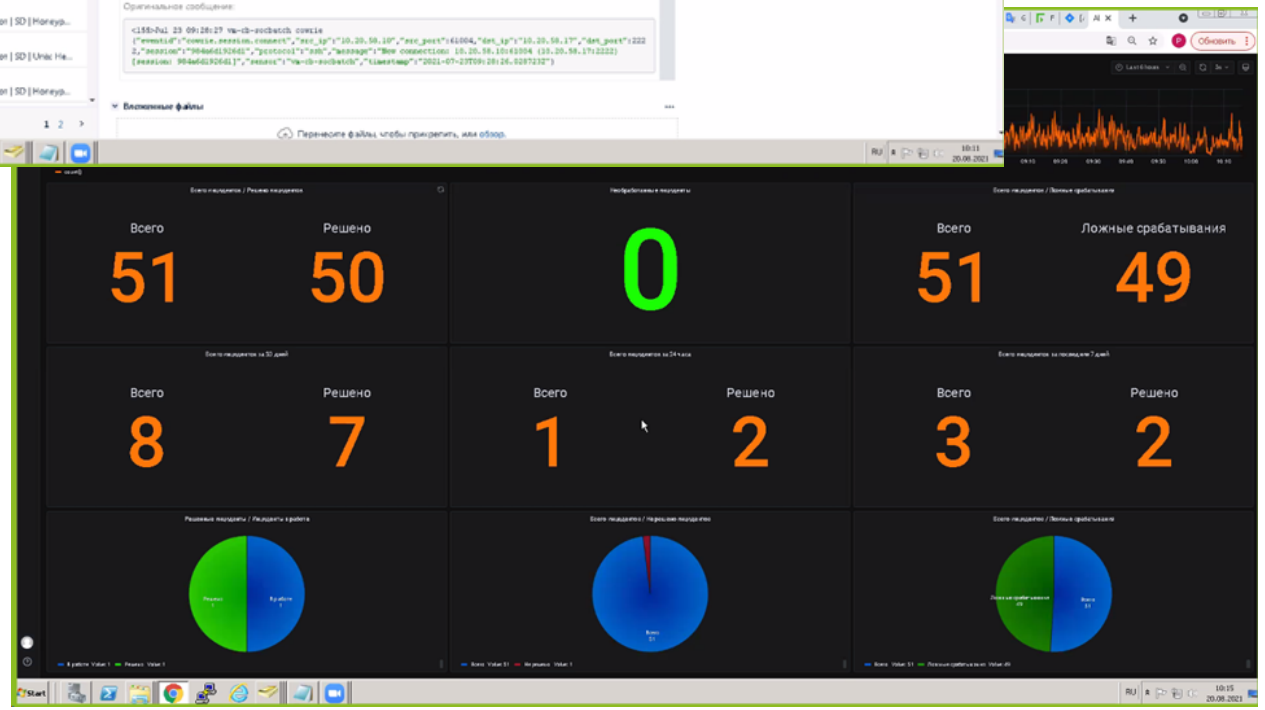
- Не всю информацию возможно отдавать на аутсорсинг (события DLP, фрод)
- Аутсорсер как правила не несет финансовой ответственности
- Как правило отработка события по скрипту прописанному в договоре (ничего больше, ничего меньше)
- Большая сложность в оценке реального сырого трафика (как правило отдают избыточный трафик в несколько раз) из-за чего большая переплата за услуги
- Множество различных подводных камней

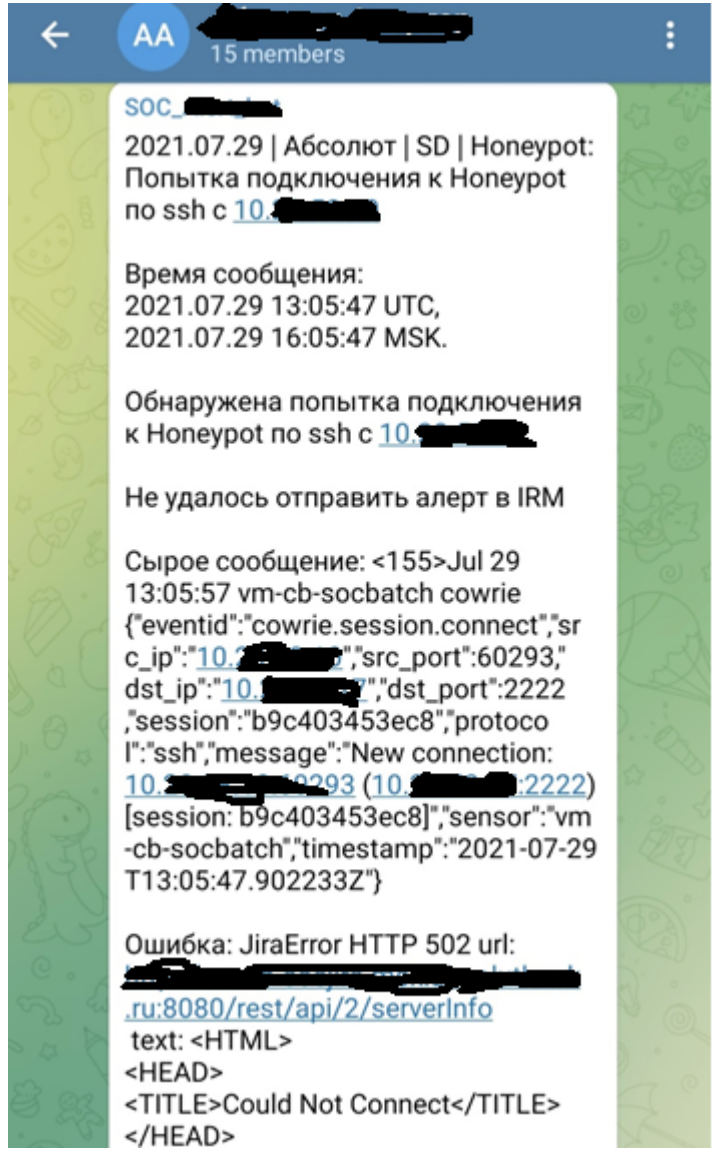
Экосистема SOC



Визуализация







Итого

Спасибо

Ложкин Р.В.

Тел: +79060726191
E-mail: r.lozhkin@absolutbank.ru

АБСОЛЮТ БАНК