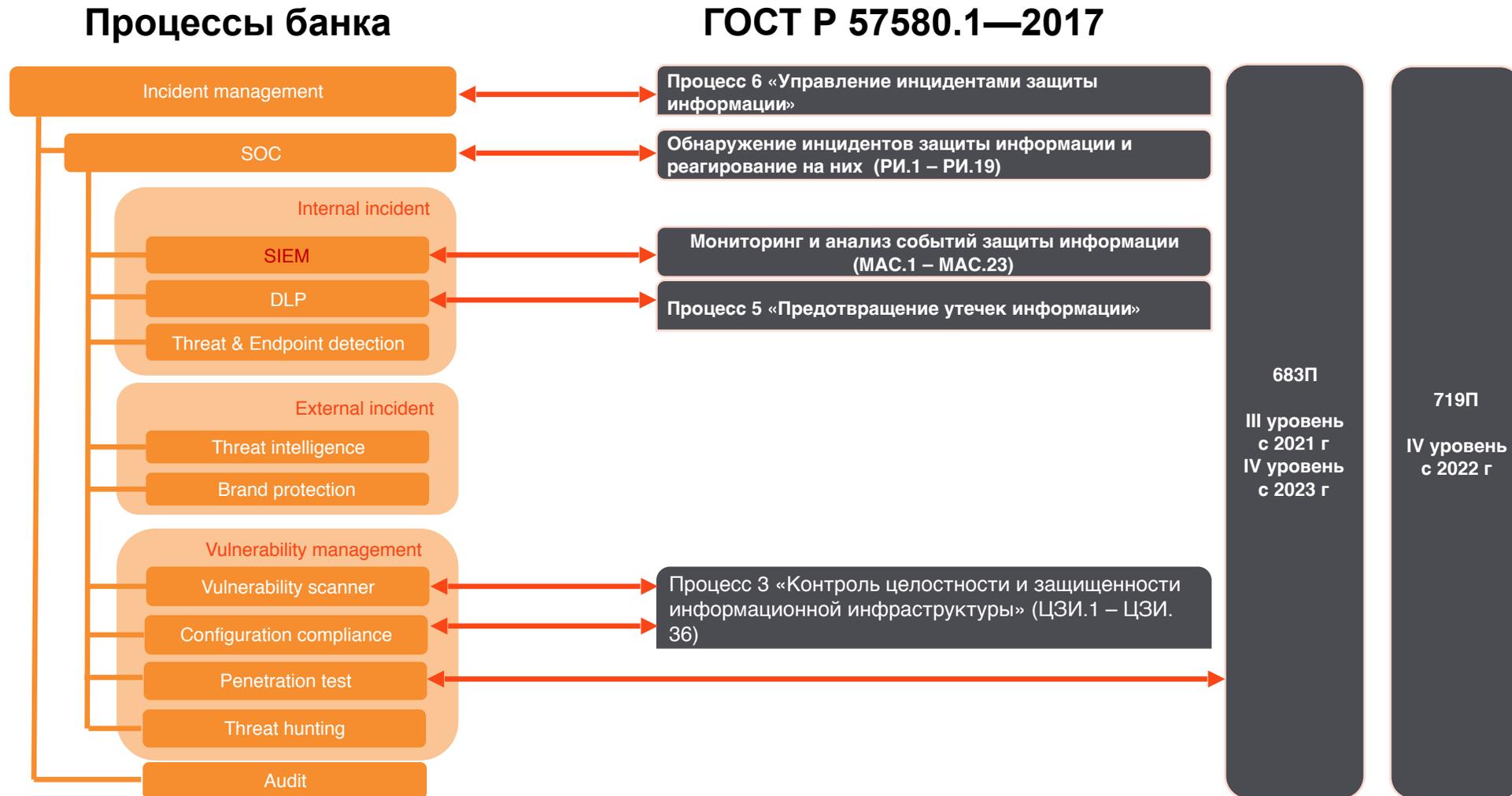


# SOC на примере опыта Абсолют банк

---

**АБСОЛЮТ  
БАНК**

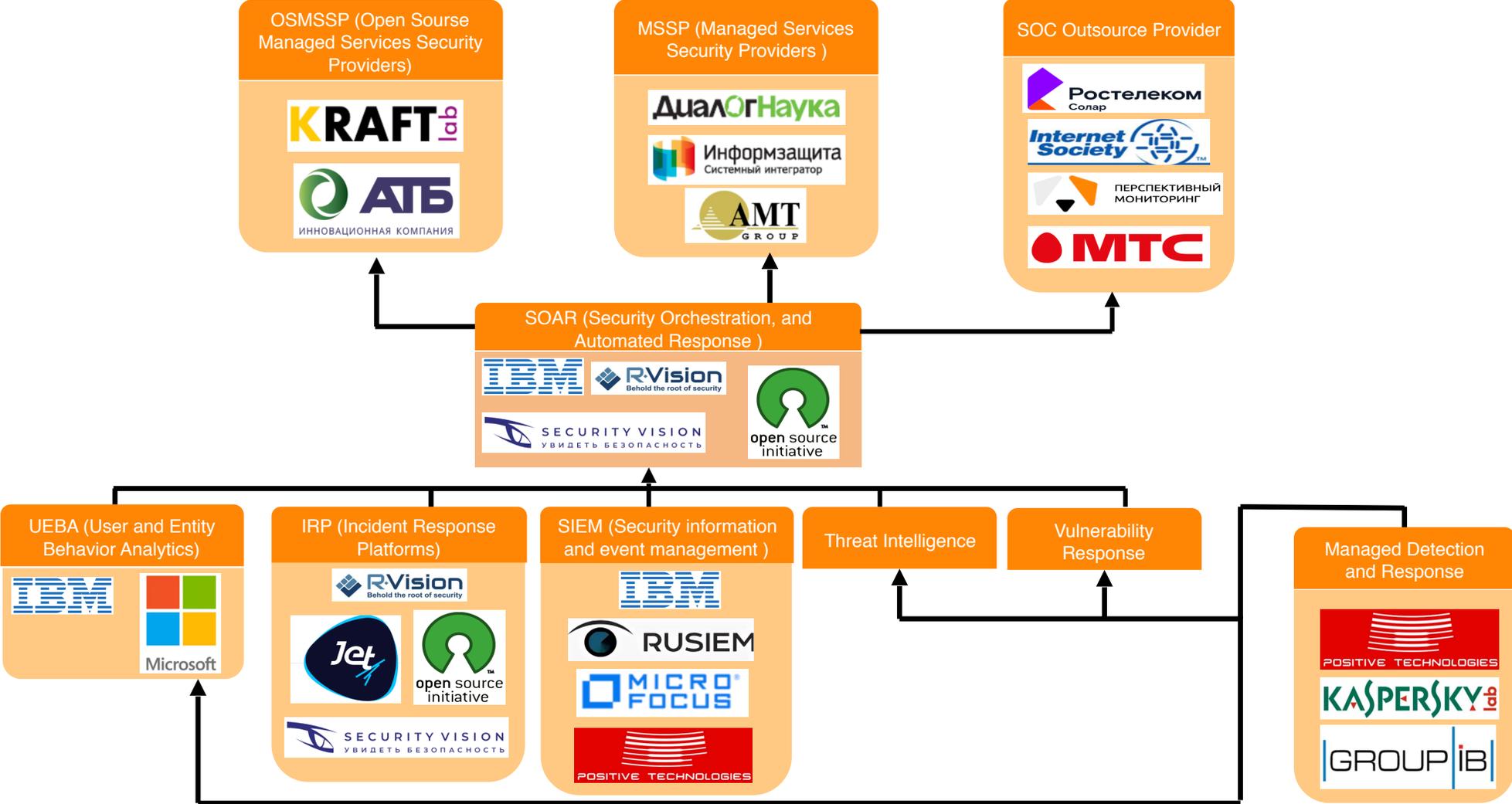
# Управление инцидентами в кредитной организации



# Функции SOC на основе классификации MITRE

Обработка данных в реальном времени	Работа с внешними источниками информации, стратегическое планирование	Анализ и реагирование на инциденты	Анализ цифровых образцов	Обеспечение работоспособности и инструментов SOC	Аудит и отслеживание внутренних угроз	Сканирование и оценка защищенности	Прочее
call-центр	Сбор внешних данных и их анализ	Анализ инцидентов	Сбор цифровых образцов	Поддержка работы граничных систем сетевой безопасности	Сбор и хранение данных аудита	Создание и актуализация карт сети	Оценка средств защиты
	Распространение информации из внешних источников	Слежка за нарушителем		Поддержка работы инфраструктуры SOC			Управление и обработка данных аудита
Мониторинг и разбор данных в режиме real-time	Подготовка материалов для внешнего распространения	Координация реагирования на инциденты	Анализ вредоносного кода	Поддержка работы сенсоров	Поддержка при работе с внутренними угрозами	Сканирование уязвимостей	Повышение осведомленности
	Обогащение правил SOC на основе внешних данных	Внедрение контрмер		Создание собственных правил и сигнатур			Оценка защищенности
	Стратегическое планирование	Работы по реагированию на инцидент на пострадавшей площадке	Анализ прочих цифровых образцов	Подбор и внедрение решений, использующихся в работе SOC	Расследование случаев внутренних нарушений	Тестирование на проникновение	Распространение наработок
	Оценка угроз	Удаленное реагирование на инцидент		Разработка решений, использующихся в работе SOC			Взаимодействие с общественностью и СМИ

# 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

## Open source

### Плюсы:

- Открытый код и возможность доработки собственными силами
- Гибкость продукта с возможностью 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 плейбуков
- 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

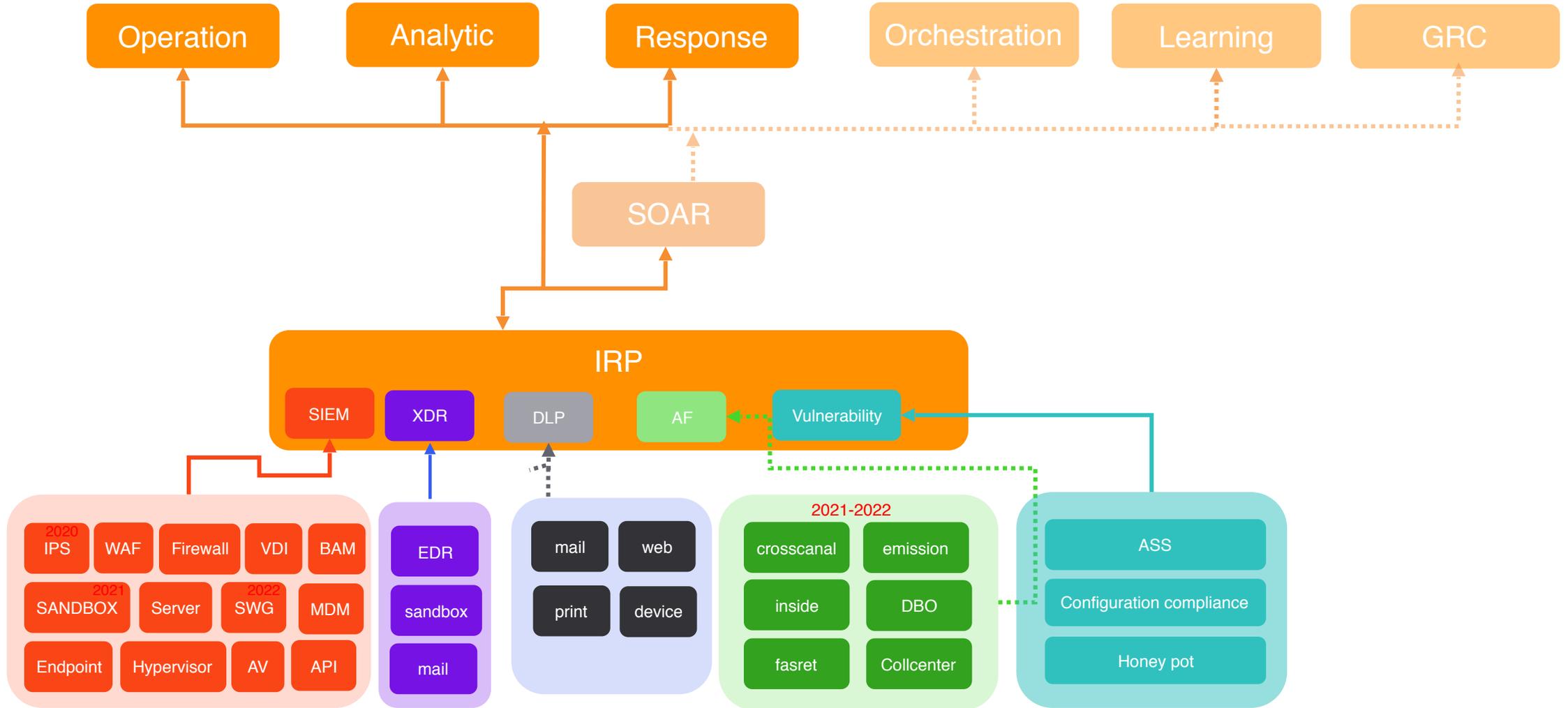
### Плюсы:

- 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

2021.07.23 | Абсолют | SD | HONEypot: Попытка подключения к HONEypot по ssh

Время сообщения:  
2021.07.23 09:28:36 UTC  
2021.07.23 12:28:26 MSK

```
<155>Jul 29 13:05:57 vm-cb-socbatch cowrie
{"eventid":"cowrie.session.connect","src_ip":"10.10.10.10","src_port":60293,"dst_ip":"10.10.10.10","dst_port":2222,"session":"b9c403453ec8","protocol":"ssh","message":"New connection: [session: b9c403453ec8]","sensor":"vm-cb-socbatch","timestamp":"2021-07-29 T13:05:47.902233Z"}
```

← AA [redacted] 15 members

SOC [redacted]  
2021.07.29 | Абсолют | SD | HONEypot: Попытка подключения к HONEypot по ssh с [10.10.10.10](#)

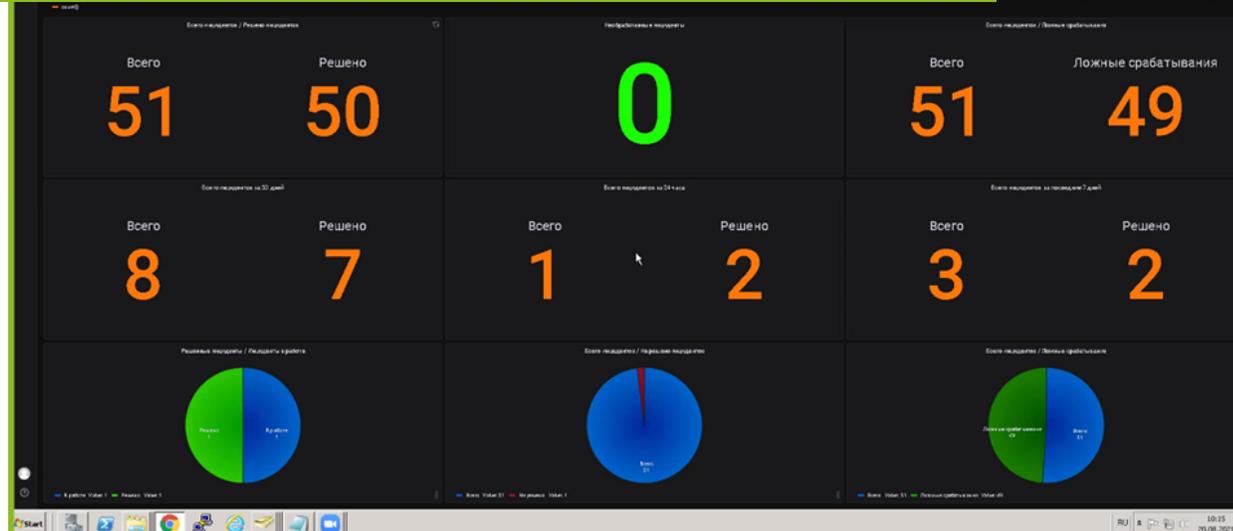
Время сообщения:  
2021.07.29 13:05:47 UTC,  
2021.07.29 16:05:47 MSK.

Обнаружена попытка подключения к HONEypot по ssh с [10.10.10.10](#)

Не удалось отправить алерт в IRM

Сырое сообщение: <155>Jul 29 13:05:57 vm-cb-socbatch cowrie  
{\"eventid\":\"cowrie.session.connect\",\"src\_ip\":\"10.10.10.10\",\"src\_port\":60293,\"dst\_ip\":\"10.10.10.10\",\"dst\_port\":2222,\"session\":\"b9c403453ec8\",\"protocol\":\"ssh\",\"message\":\"New connection: [10.10.10.10:60293 \(10.10.10.10:2222\)](#) [session: b9c403453ec8]\",\"sensor\":\"vm-cb-socbatch\",\"timestamp\":\"2021-07-29 T13:05:47.902233Z\"}

Ошибка: JiraError HTTP 502 url: [\[redacted\].ru:8080/rest/api/2/serverinfo](#)  
text: <HTML>  
<HEAD>  
<TITLE>Could Not Connect</TITLE>  
</HEAD>



Итого



# Спасибо

Ложкин Р.В.

Тел: +79060726191

E-mail: [r.lozhkin@absolutbank.ru](mailto:r.lozhkin@absolutbank.ru)

**АБСОЛЮТ  
БАНК**