SOC
FORUM
2023

Как кибербразведка помогает SOC

SOC
FORUM
2023

Александр Ненахов
Product owner

Руководитель группы киберразведки
«Инфосистемы Джет»

О чем будем говорить

SOC FORUM 2023

1. Что такое киберразведка
2. Как мониторинг теневых ресурсов может сократить время реагирования и последствия
3. Есть ли польза от киберразведки при проведении CA
4. Как интегрировать мониторинг поверхности атаки в процессы SOC
5. Как интегрировать мониторинг фишинговых ресурсов и утечек УЗ в процессы SOC
6. Наш опыт

Что такое киберразведка

SOC FORUM 2023

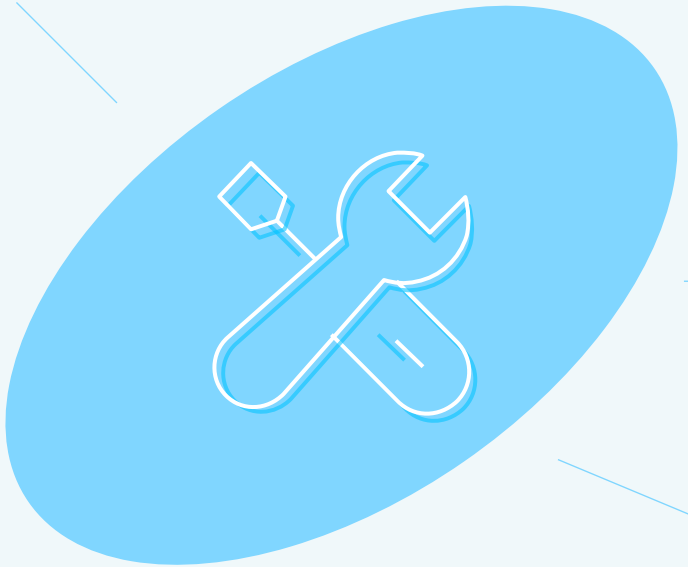
SOC FORUM 2023

Мониторинг утечек

Антифишинг

Мониторинг поверхности атаки

Мониторинг Telegram и DarkNet

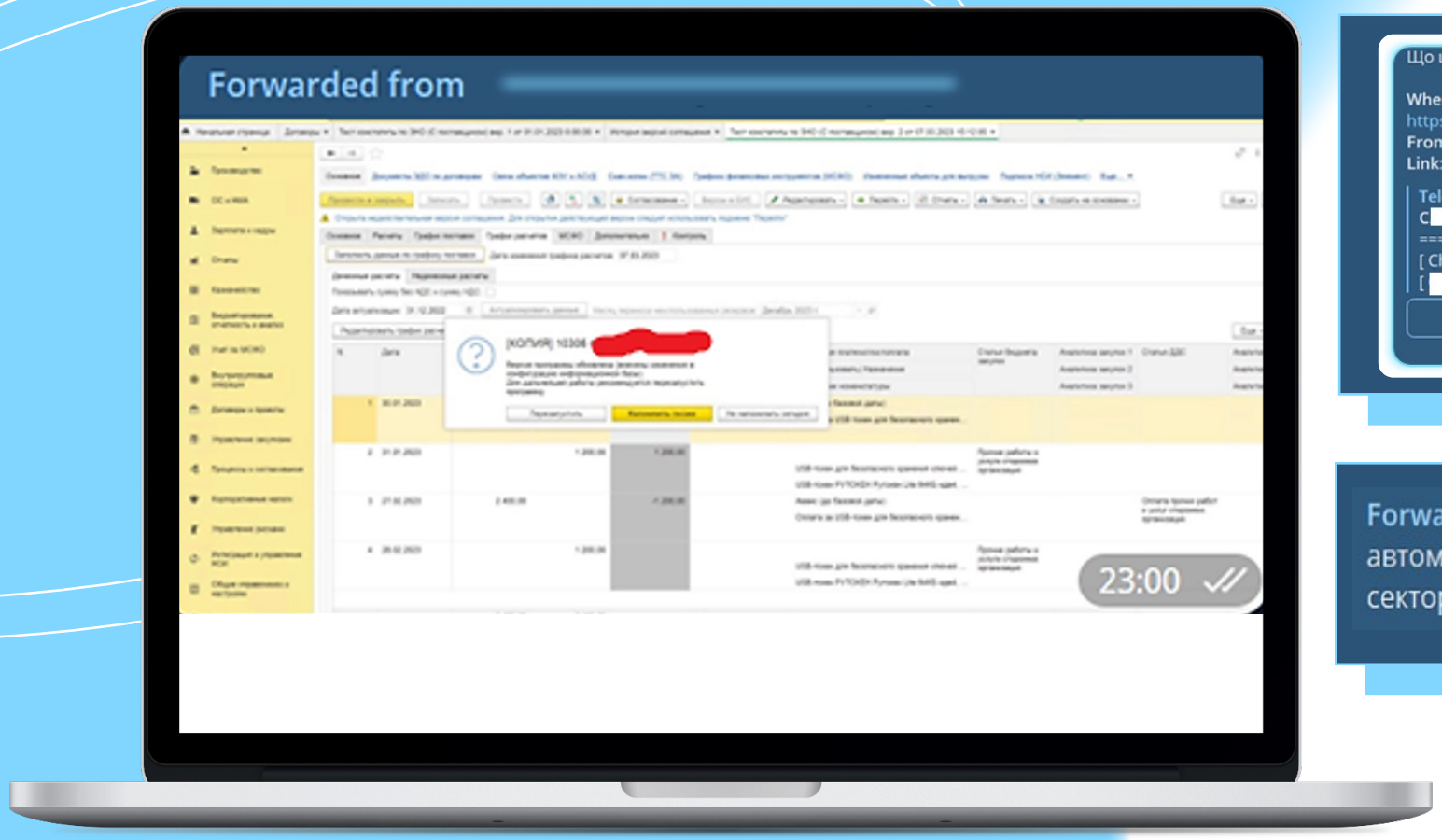


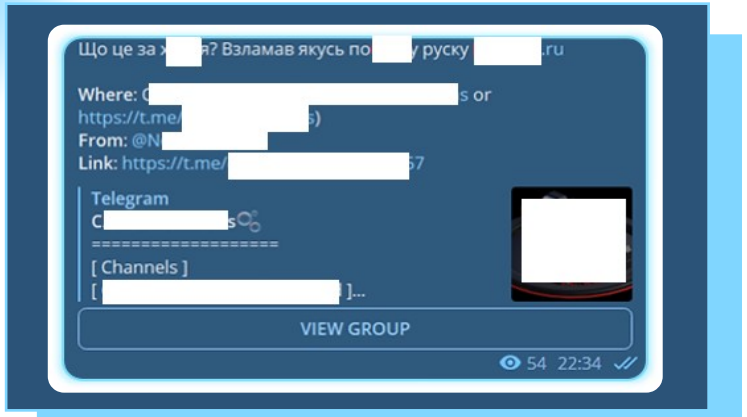
Мониторинг рисков при работе с подрядчиком

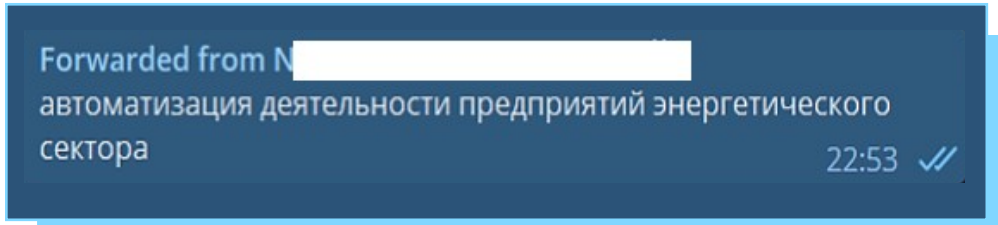
Мониторинг открытых источников и СМИ

Мониторинг теневых ресурсов

SOC FORUM 2023

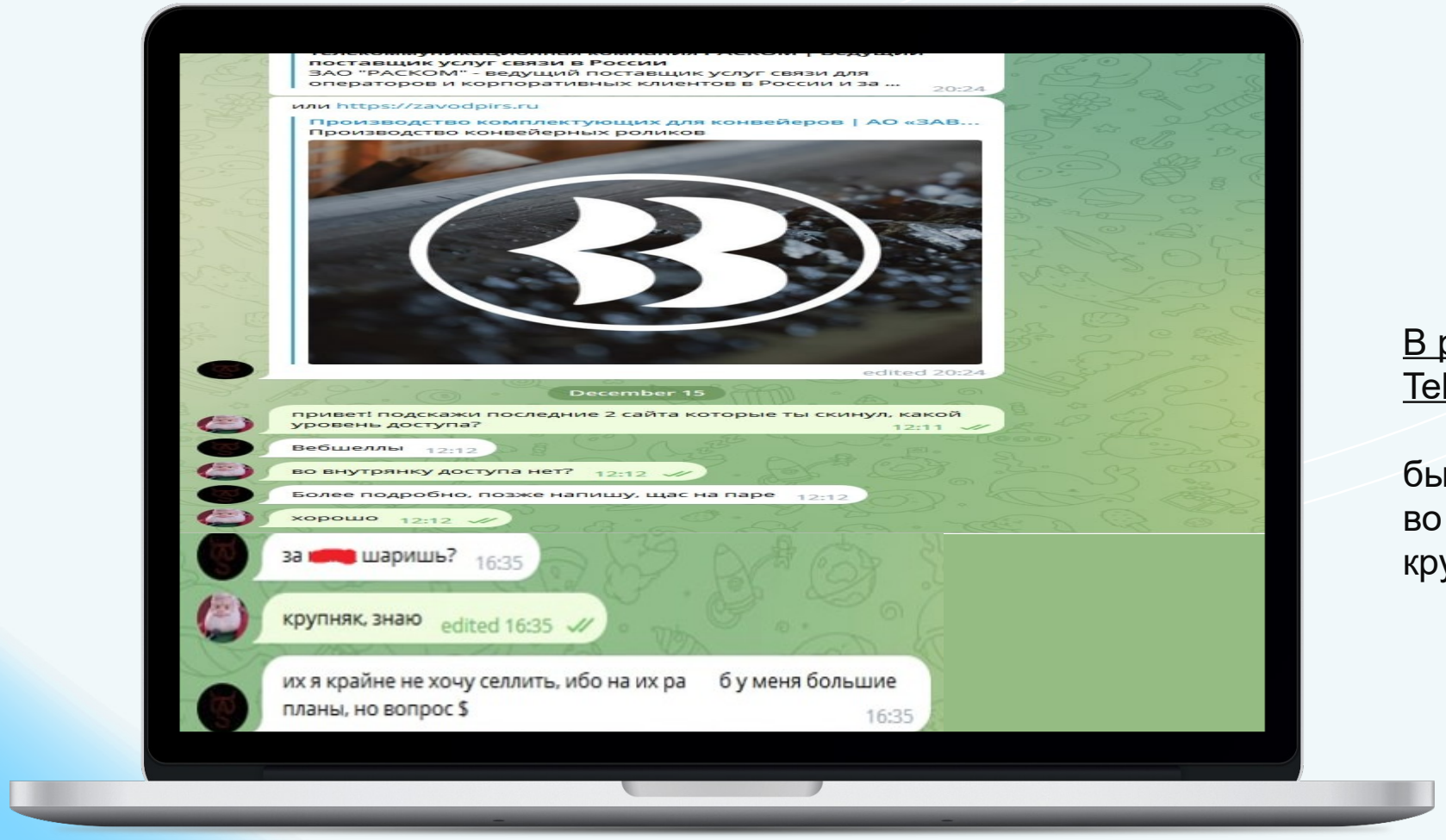






Мониторинг теневых ресурсов

SOC FORUM 2023



[В рамках мониторинга хакерских Telegram-каналов]

был обнаружен факт продажи доступа во внутреннюю инфраструктуру двух крупных организаций

Уязвимости и недостатки

SOC FORUM 2023

Пассивные и активные методы мониторинга поверхности атаки позволяют сфокусировать внимание на потенциальных точках входа

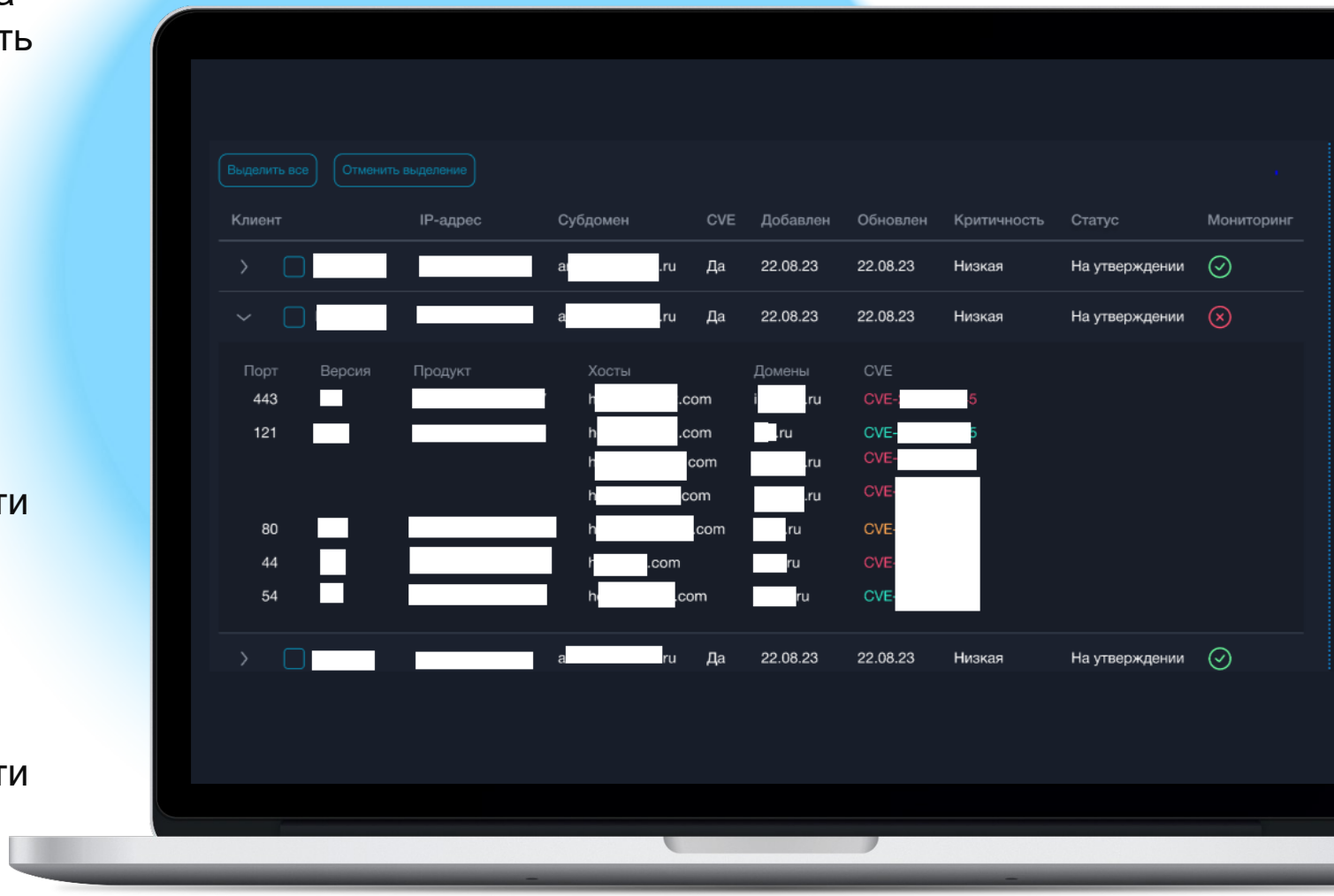
На что обращать внимание:

Скрытые активы:

- Есть ли возможность и необходимость подключения
- Были ли подозрительные активности

Уязвимые сервисы/Формы авторизации:

- Какая критичность
- Нужно ли повышать приоритет реагирования
- Были ли подозрительные активности



Утечки УЗ и фишинг

SOC FORUM 2023

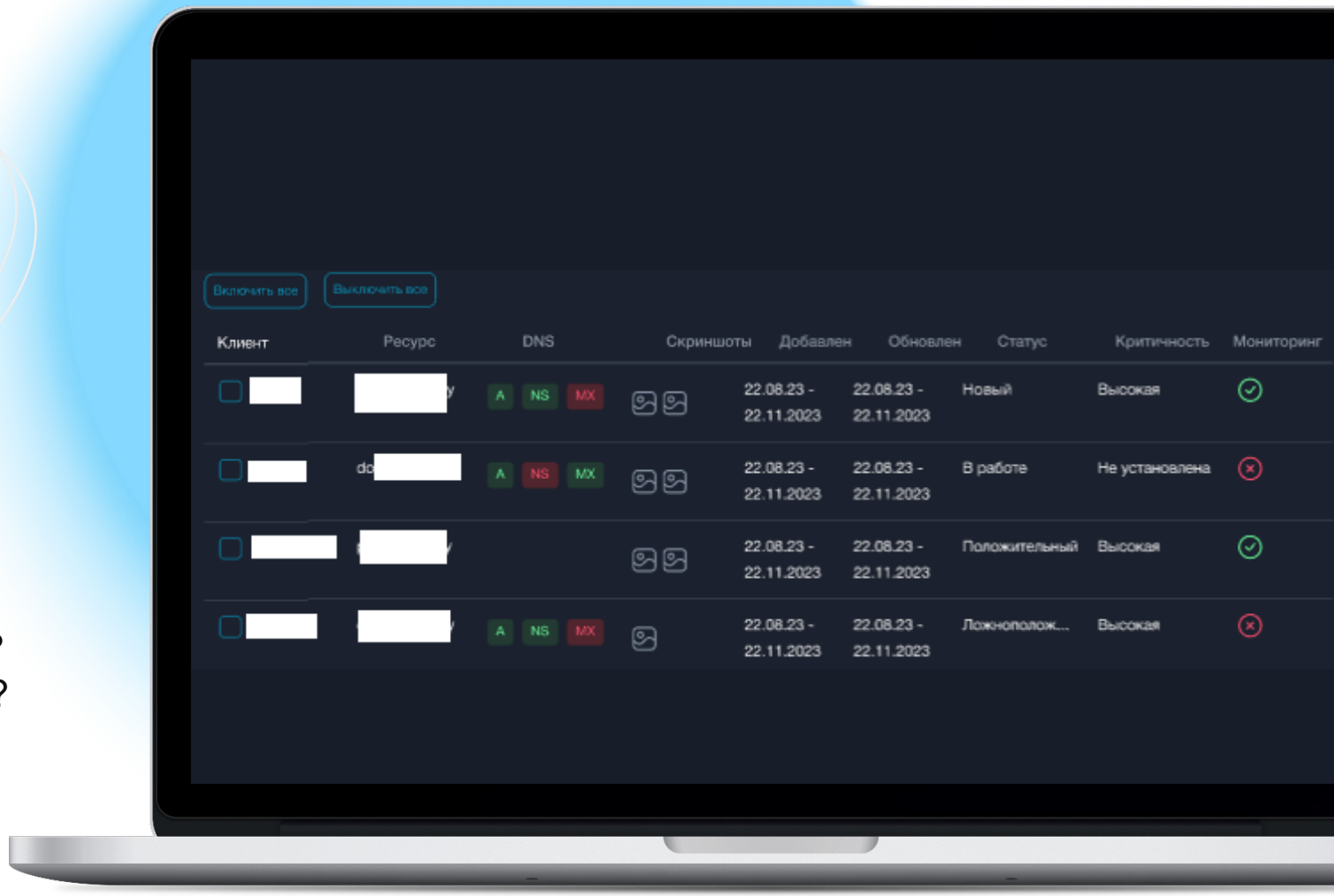
На что обращать внимание:

Утечки УЗ:

- Были ли подозрительные активности, связанные с УЗ

Фишинг:

- Какой тип фишинга: веб-страница или домен под почтовую рассылку?
- Были ли обращения на этот домен?



Compromise Assessment

SOC FORUM 2023

Чем может быть полезна киберразведка для CA?

- Формирование гипотез в условиях неопределенности
- Уточнение скоупа работ
- Сбор информации об инфраструктуре атакующих
- В качестве связки Киберразведка -> Верификация -> CA

Рекомендации

SOC FORUM 2023

Основные тезисы:

- SOC и киберразведка должны «жить» рядом
- Ядро услуги должно формироваться на основании цели и задач
- Без автоматизации интеграция невозможна
- Без аналитики услуга будет сильно фолзить

SOC FORUM 2023