

Как киберразведка помогает SOC



Александр Ненахов
Product owner

Руководитель группы киберразведки
«Инфосистемы Джет»

О чем будем говорить

1

Что такое
киберразведка

2

Как мониторинг теневых ресурсов
может сократить время реагирования
и последствия

3

Есть ли польза от киберразведки
при проведении СА

4

Как интегрировать мониторинг
поверхности атаки в процессы SOC

5

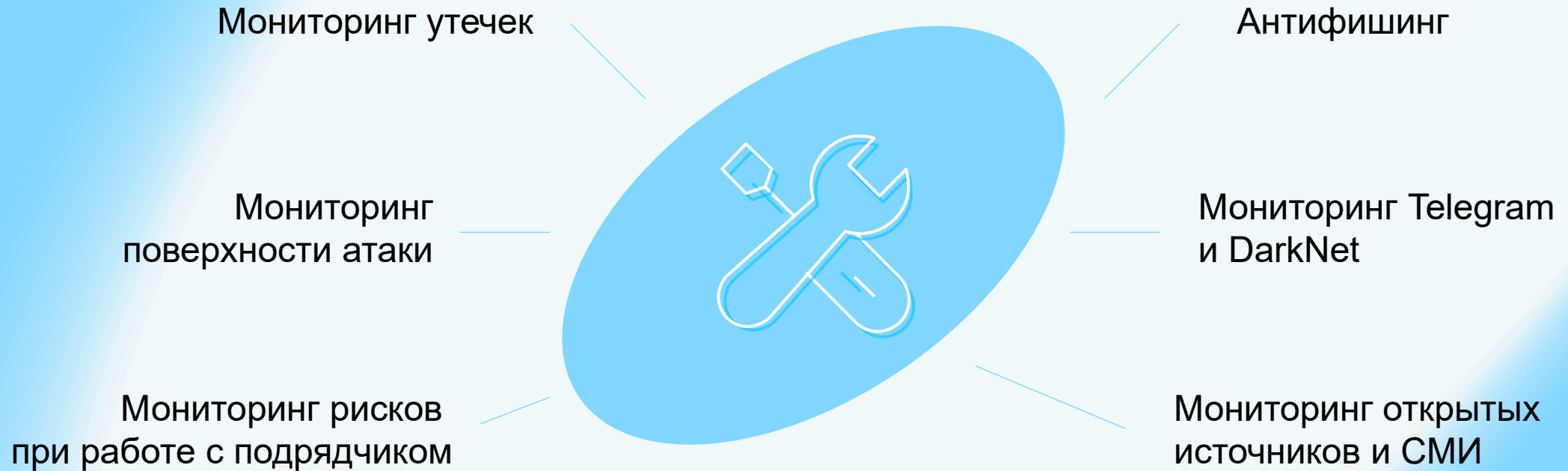
Как интегрировать мониторинг
фишинговых ресурсов и утечек
УЗ в процессы SOC

6

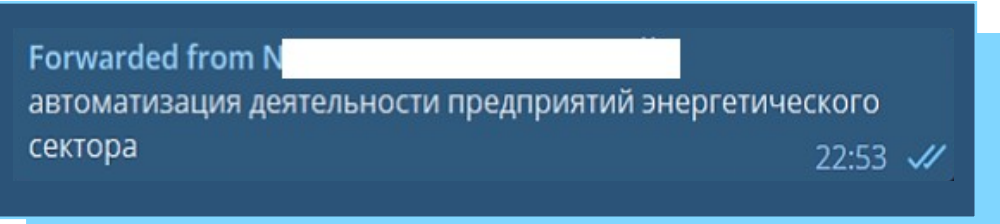
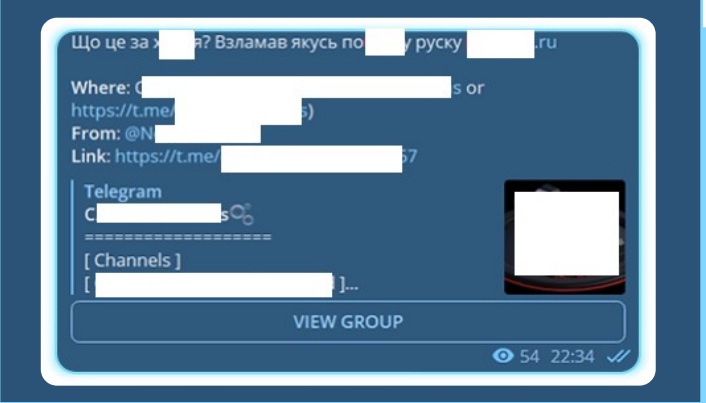
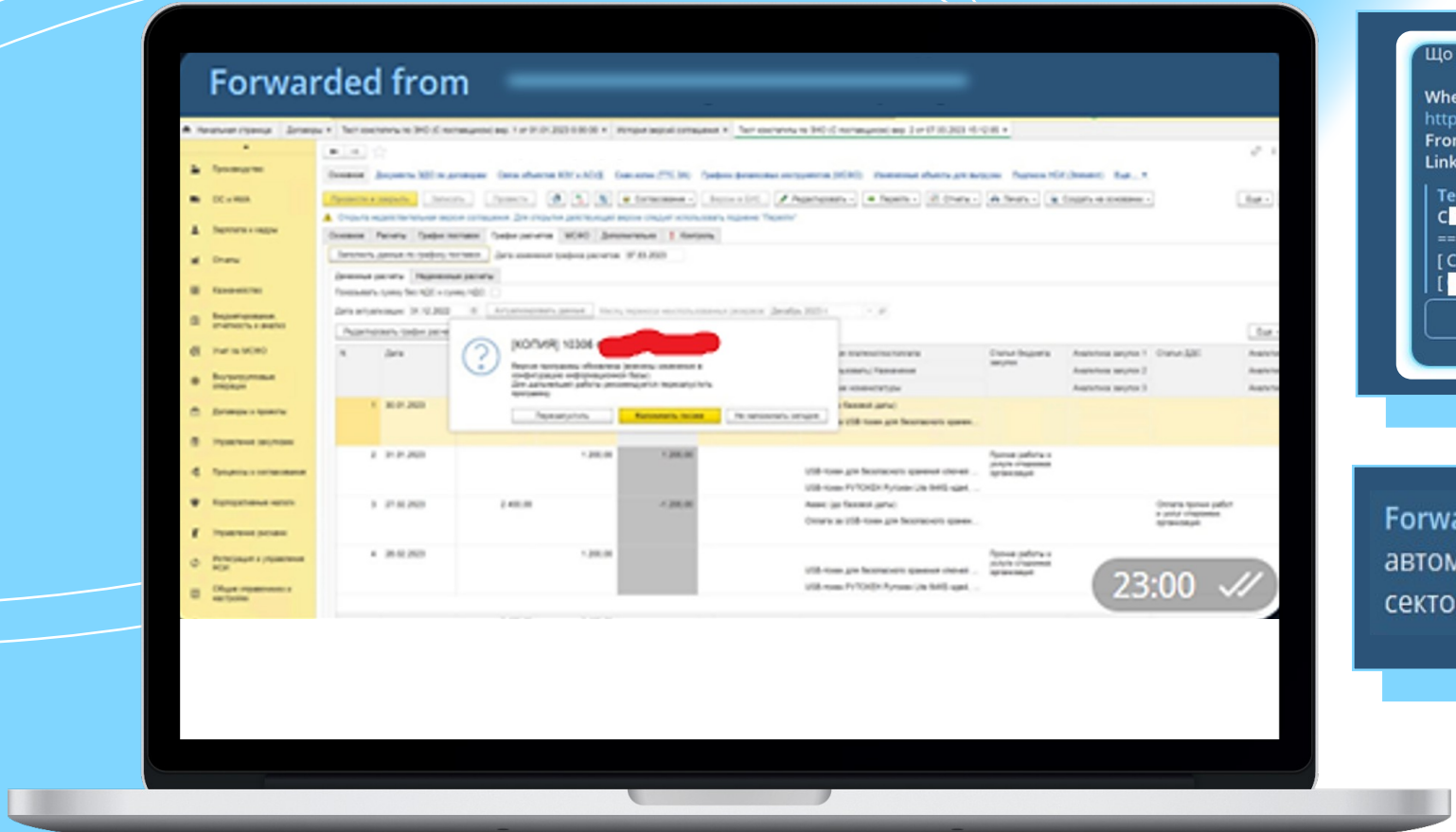
Наш опыт

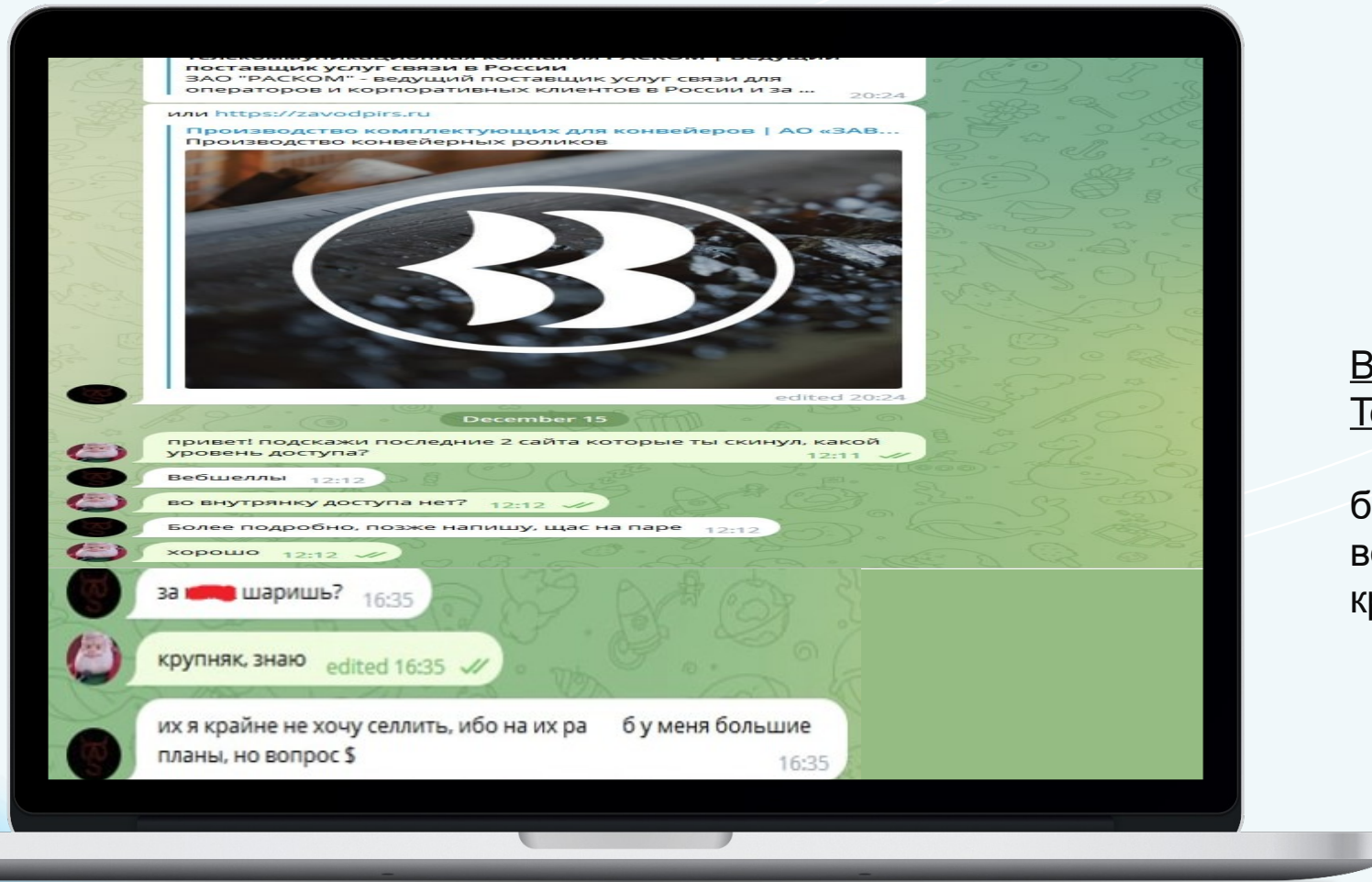
Что такое киберразведка

Humint
DRP OSINT
DRP
Geosint Humint
EASM
Humint
OSINT
CAASM
OSINT
OSINT
EASM



Мониторинг теневых ресурсов





В рамках мониторинга хакерских Telegram-каналов

был обнаружен факт продажи доступа во внутреннюю инфраструктуру двух крупных организаций

Уязвимости и недостатки



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

The screenshot shows a security dashboard with a table of vulnerabilities. At the top, there are two buttons: "Выделить все" (Select all) and "Отменить выделение" (Deselect all). The main table has columns: Клиент (Client), IP-адрес (IP address), Субдомен (Subdomain), CVE, Добавлен (Added), Обновлено (Updated), Критичность (Criticality), Статус (Status), and Мониторинг (Monitoring). There are two rows of data, each with a dropdown arrow and a checkbox on the left. The first row has a green checkmark in the monitoring column, while the second has a red X. Below this is a detailed table of assets with columns: Порт (Port), Версия (Version), Продукт (Product), Хосты (Hosts), Домены (Domains), and CVE. This table lists several entries with their respective ports, versions, products, hosts, domains, and associated CVEs. At the bottom, there is another row of data similar to the top one, with a green checkmark in the monitoring column.

Клиент	IP-адрес	Субдомен	CVE	Добавлен	Обновлен	Критичность	Статус	Мониторинг		
>	<input type="checkbox"/>	[redacted]	[redacted]	а [redacted].ru	Да	22.08.23	22.08.23	Низкая	На утверждении	✓
∨	<input type="checkbox"/>	[redacted]	[redacted]	а [redacted].ru	Да	22.08.23	22.08.23	Низкая	На утверждении	✗
Порт	Версия	Продукт	Хосты	Домены	CVE					
443	[redacted]	[redacted]	h [redacted].com	i [redacted].ru	CVE-[redacted] 5					
121	[redacted]	[redacted]	h [redacted].com	[redacted].ru	CVE-[redacted] 5					
			h [redacted].com	[redacted].ru	CVE-[redacted]					
			h [redacted].com	[redacted].ru	CVE-[redacted]					
80	[redacted]	[redacted]	h [redacted].com	[redacted].ru	CVE-[redacted]					
44	[redacted]	[redacted]	h [redacted].com	[redacted].ru	CVE-[redacted]					
54	[redacted]	[redacted]	h [redacted].com	[redacted].ru	CVE-[redacted]					
>	<input type="checkbox"/>	[redacted]	[redacted]	а [redacted].ru	Да	22.08.23	22.08.23	Низкая	На утверждении	✓

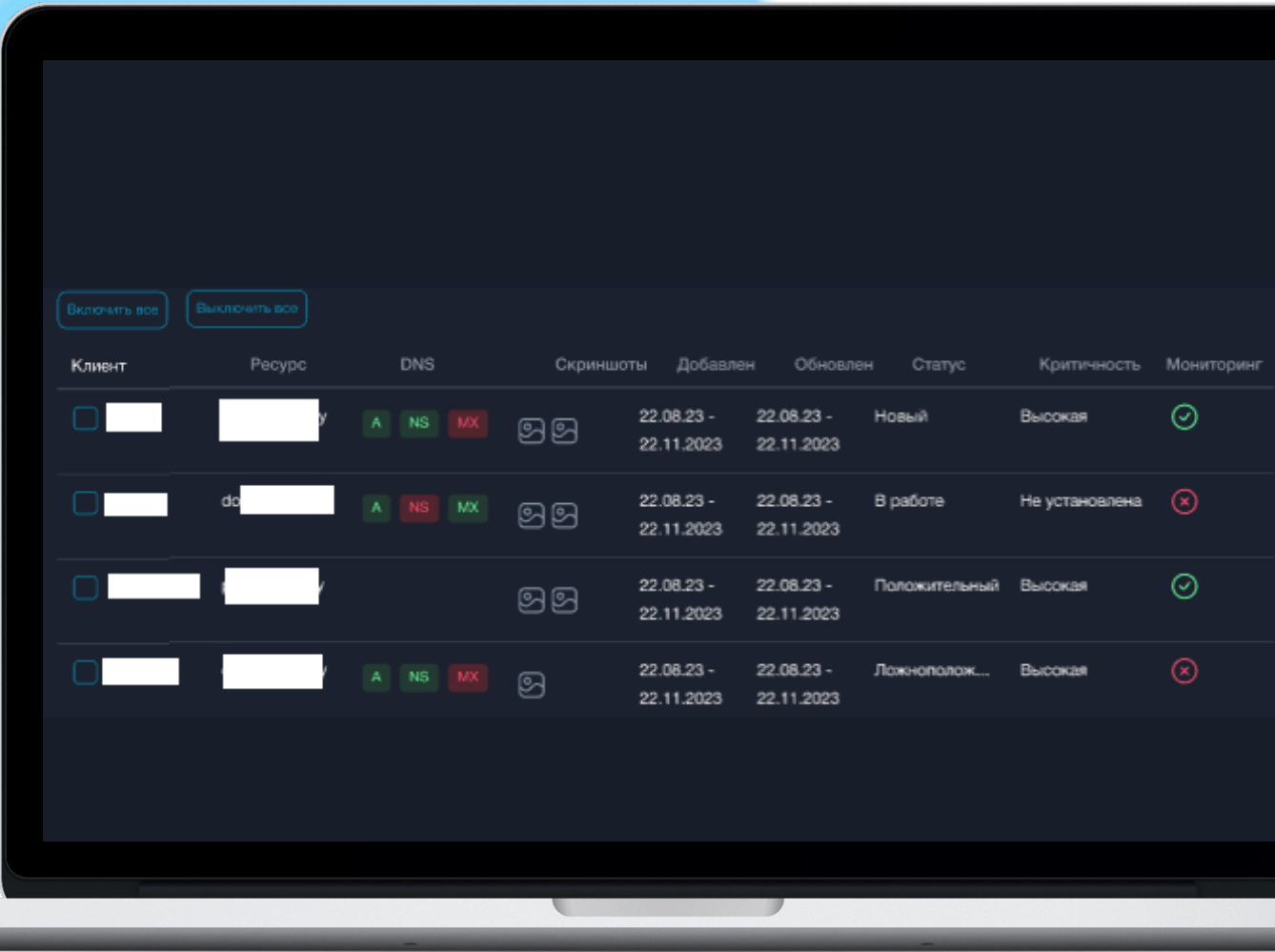
На что обращать внимание:

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?



Клиент	Ресурс	DNS	Скриншоты	Добавлен	Обновлен	Статус	Критичность	Мониторинг
<input type="checkbox"/>	[REDACTED]	A NS MX	[Icons]	22.08.23 - 22.11.2023	22.08.23 - 22.11.2023	Новый	Высокая	✓
<input type="checkbox"/>	dc [REDACTED]	A NS MX	[Icons]	22.08.23 - 22.11.2023	22.08.23 - 22.11.2023	В работе	Не установлена	✗
<input type="checkbox"/>	[REDACTED]		[Icons]	22.08.23 - 22.11.2023	22.08.23 - 22.11.2023	Положительный	Высокая	✓
<input type="checkbox"/>	[REDACTED]	A NS MX	[Icon]	22.08.23 - 22.11.2023	22.08.23 - 22.11.2023	Ложнополож...	Высокая	✗

Чем может быть полезна киберразведка для СА?

✦ Формирование гипотез
в условиях неопределенности

✦ Уточнение скоупа работ

✦ Сбор информации
об инфраструктуре атакующих

✦ В качестве связки Киберразведка ->
Верификация -> СА

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

