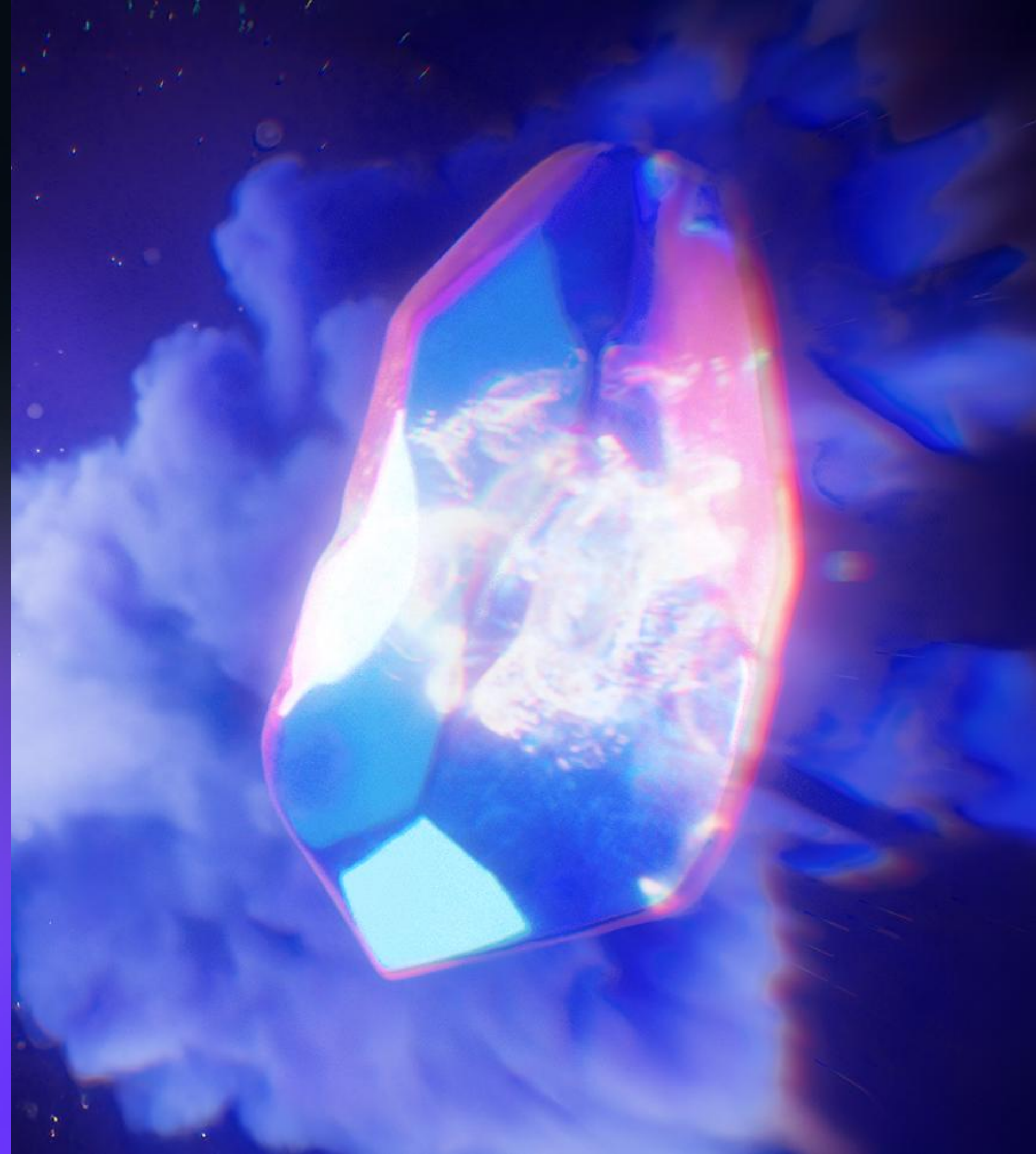


F6

Эффективно отреагировать или эффектно отчитаться?

*Регуляторика и практика
как Инь и Янь реагирования
на киберинциденты*

СЕРГЕЙ ЗОЛОТУХИН
КОНСУЛЬТАНТ ПО КИБЕРБЕЗОПАСНОСТИ
КОМПАНИЯ F6



Счет идет на часы

Тип организации	Куда уведомлять	Основание	Срок уведомления	Санкции
Субъект КИИ (ЗОКИИ)	НКЦКИ	187-ФЗ ст. 9, ФСБ № 547	3 часа	Ч. 2 ст. 13.12.1 КоАП (до 500 000 руб.), ст. 274.1 УК
Субъект КИИ (без категории)	НКЦКИ	187-ФЗ ст. 9, ФСБ № 547	24 часа	Состав ч. 2 ст. 13.12.1 КоАП касается только значимых объектов
Оператор ПДн (утечка)	Роскомнадзор	152-ФЗ ч. 3.1 ст. 21	24 ч. + 72 ч. (расследование)	Ч. 11-18 ст. 13.11 КоАП (до 500 млн руб.)
Банк	ФинЦЕРТ	851-П	3 часа	Меры Банка России
НФО	ФинЦЕРТ	757-П	По 757-П	Меры Банка России
Оператор ГИС	ФСТЭК России + НКЦКИ	приказ ФСТЭК России № 117	по приказу ФСТЭК России № 117	ч. 6 ст. 13.12 КоАП

О чем уведомить регулятора?

F6

← Я ↻ www.cert.gov.ru Форма составления уведомления об атаке или инциденте ...

Добавляйте на эту панель сайты, которые вы часто посещаете. [Импортировать закладки](#)

**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

Форма составления уведомления об атаке или инциденте

Данная форма предназначена для помощи субъектам КИИ и иным владельцам российских информационных ресурсов в составлении уведомления в адрес НКЦКИ. После заполнения формы сформированное уведомление необходимо направить на адрес электронной почты incident@cert.gov.ru

Какую категорию выбрать?

-- Выберите тип --

DDoS-атака

Неудачные попытки авторизации

Попытки внедрения ВПО

Попытки эксплуатации уязвимости

Публикация мошеннической информации

Сетевое сканирование

Социальная инженерия

-- Выберите тип --

Реагирование антивирусом (прошлый век)

F6



Реагирование антивирусом (прошлый век)

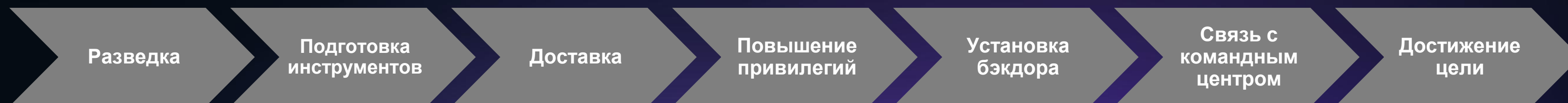
F6



Есть что сказать регулятору?

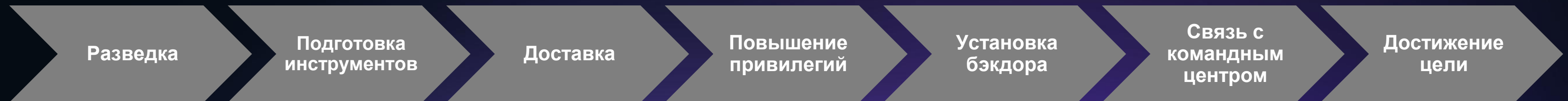
Килл-чейн современной атаки

F6

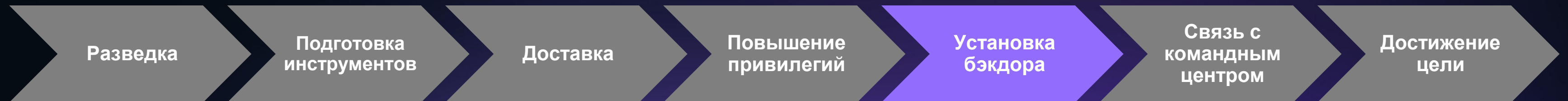


Детект – отправная точка реагирования

F6



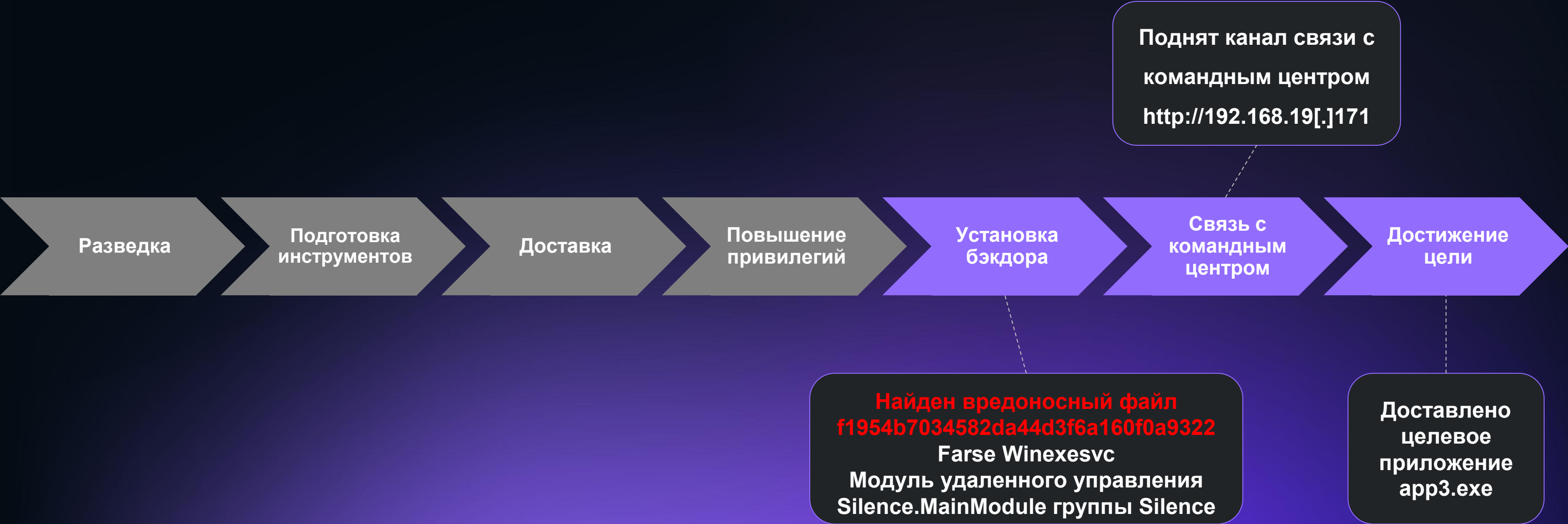
Найден вредоносный файл
f1954b7034582da44d3f6a160f0a9322



Найден вредоносный файл
f1954b7034582da44d3f6a160f0a9322
Farse Winexesvc
Модуль удаленного управления
Silence.MainModule группы Silence

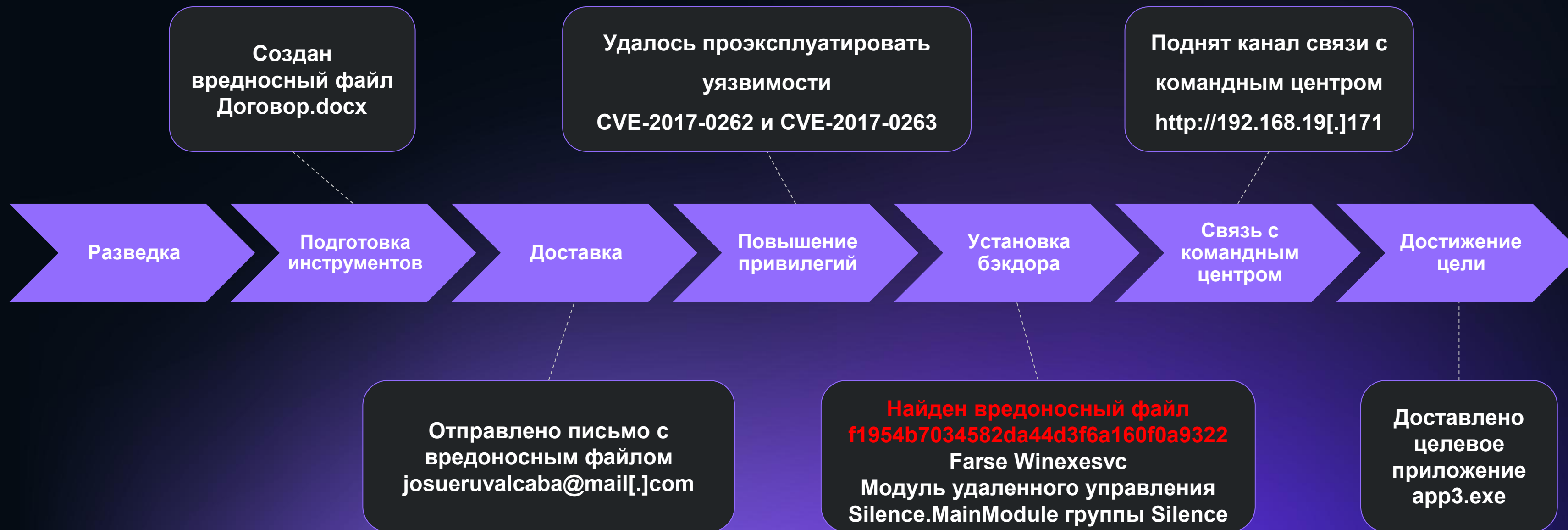
Определение границ инцидента

F6



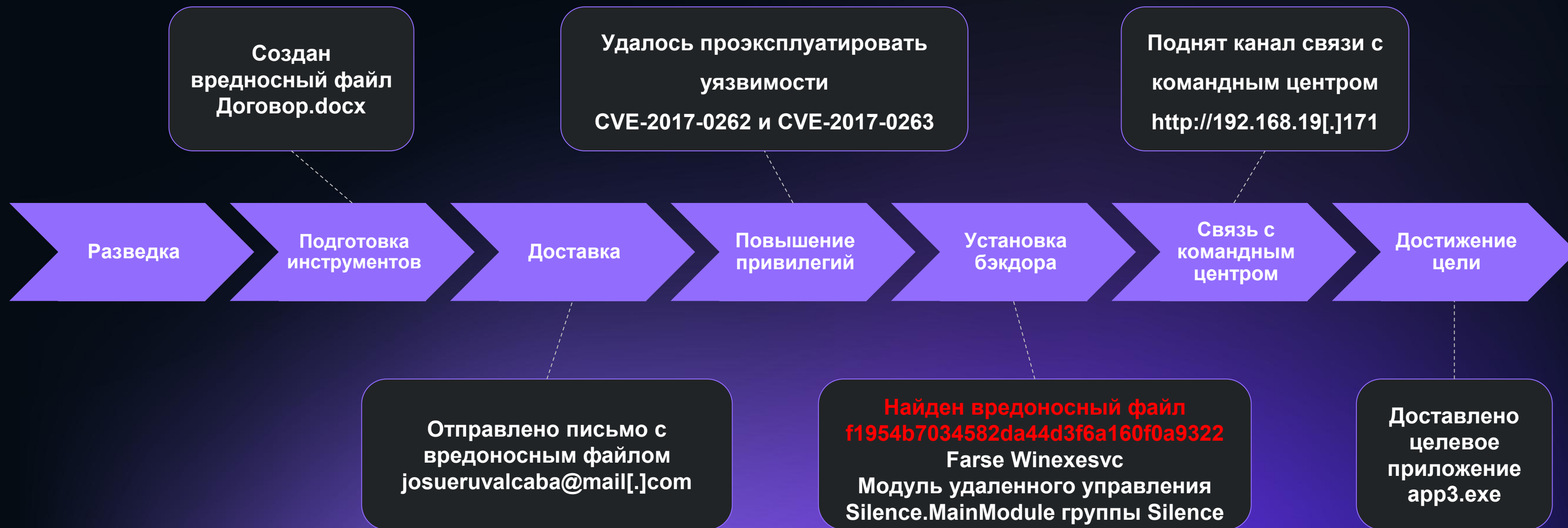
Восстановление цепочки событий

F6



Восстановление цепочки событий

F6



Есть что сказать регулятору!

Как современное реагирование помогает взаимодействию с регуляторами

1. Быстрая оценка ситуации для оперативного и по существу уведомления регулятора.
2. Поиск цифровых следов и корректное оформление артефактов для правоохранительных и регулирующих органов
3. Подтверждение причинно-следственных связей (цепочка событий), возможность анализа механизма преступления и обоснованной правовой оценки в суде
4. Извлечение уроков: конкретика для актуализации защиты (обоснованные патчинг, харденинг, внедрение классов решений, организация контролей, обучение и т.д.)

Практика



Регуляторика

Гармоничное взаимодействие двух противоположных, но взаимодополняющих начал, благодаря которому возникает движение, развитие и равновесие в мире

Благодарим за внимание!

F6



Решения для предотвращения
кибератак, борьбы с мошенничеством
и защиты брендов

На связи 24/7

f6.ru team@f6.ru

Контактные данные

+7 906 093 3517

@zolutukhinsg

zolutukhin@f6.ru