

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Инцидент без паники: как ГБР переводит хаос в управляемое расследование

От хаотичного реагирования — к управляемому
процессу принятия решений

Софья Карева
менеджер продукта

Марат Лантаев
ведущий специалист по реагированию
на компьютерные инциденты

Перспективный мониторинг





Инцидент быстро выходит за рамки ИТ

Бизнесу нужны ответы!

- ▶ Что произошло?
- ▶ Насколько это критично?
- ▶ Какие системы затронуты?
- ▶ Есть ли риск простоя?
- ▶ Есть ли признаки утечки данных?
- ▶ Безопасно ли восстанавливать системы?
- ▶ Нужно ли уведомлять клиентов и регуляторов?
- ▶ Как избежать повторения инцидента?

01

Технический сигнал

подозрительный вход, скрипт, неизвестная служба

02

Операционный сбой

недоступность сервисов, зашифрованные узлы

03

Риск данных

утечка, потеря доступа, неопределённый масштаб

04

Бизнес-ущерб

простои, репутация, финансы, регуляторика

Первые часы инцидента: разные команды — разные KPI

Проблема: конфликт целей в первые часы инцидента

Команда	Основная цель
Бизнес	Минимизировать простой Быстрое восстановление рабочих процессов, сохранение работоспособности пользовательских систем
IT	Восстановить сервисы Перезагрузка серверов, переустановка и обновление систем
ИБ	Определить критичность атаки Масштаб компрометации, наличие злоумышленника в сети
Юристы	Снизить регуляторные риски Уведомление регулятора, договорные риски с Заказчиками, неустойки
PR	Контролировать информационный фон Уведомление Заказчиков и Партнёров
ГБР	Сохранить артефакты и локализовать угрозу

ГБР вызывают, когда последствия уже могут влиять на бизнес



Шифровальщики и массовое заражение

остановить распространение, проверить чистые бэкапы, проанализировать ransomware



Компрометация инфраструктуры

подозрительные входы, привилегии, lateral movement, закрепление



Недоступность критичных сервисов

понять связь с инцидентом и условия безопасного запуска



Непонятный масштаб атаки

проверить ключевые узлы, учётные записи, журналы и сетевые признаки

При шифровальщике важны одновременно сдерживание, чистое восстановление и проверка возврата

Сдерживание

- ▶ остановить распространение
- ▶ изолировать активный контур
- ▶ сохранить артефакты

Чистое восстановление

- ▶ проверить резервные копии
- ▶ исключить сохранённый доступ
- ▶ вернуть критичные сервисы

Разбор ransomware

- ▶ механизм запуска
- ▶ IoC и артефакты
- ▶ ключевой материал / декриптор, если применимо

Работа стартует удалённо, а выезд подключается там, где это ускоряет разбор

Ampire ЭБЗ^о

Удалённо

первые часы без ожидания выезда, приоритеты, доступы, первичный сбор

На площадке

закрытые контуры, изолированные сегменты, критичные системы и большой объём данных

Комбинированно

часть команды уже работает удалённо, часть организует очный сбор и коммуникацию

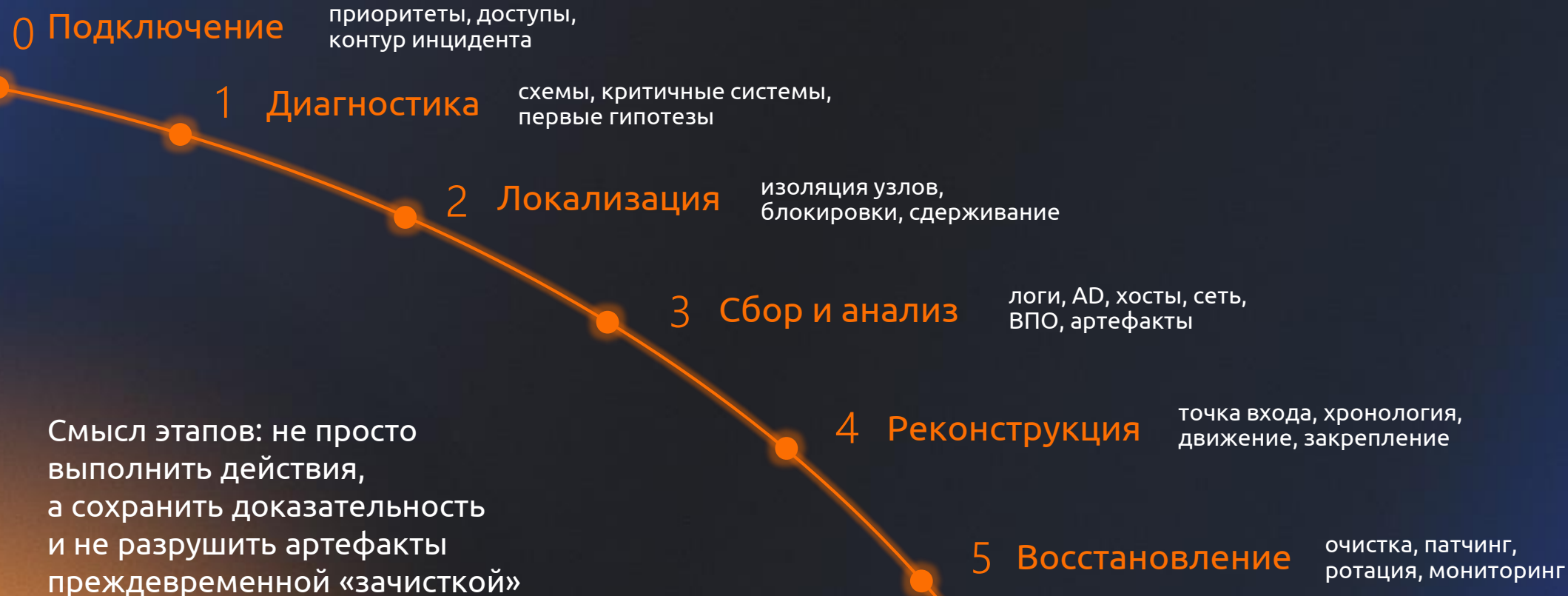
Есть опыт: ВПК

Банковский сектор

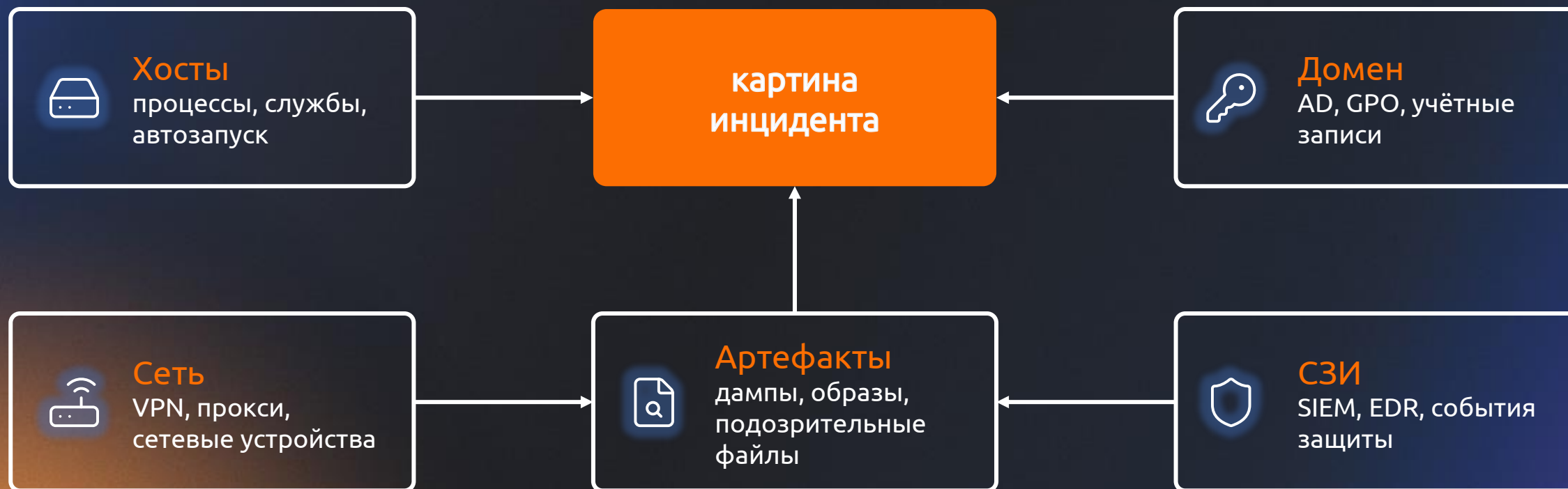
Органы власти

Очно и удалённо

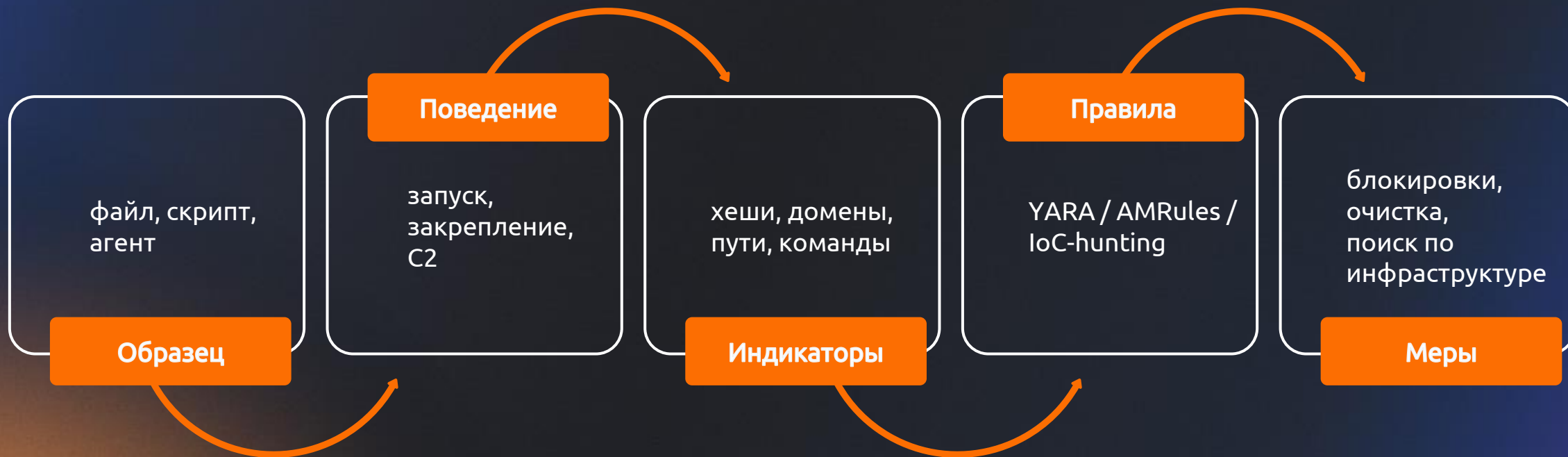
Процесс переводит хаос в последовательность решений



Картина атаки собирается из нескольких независимых источников

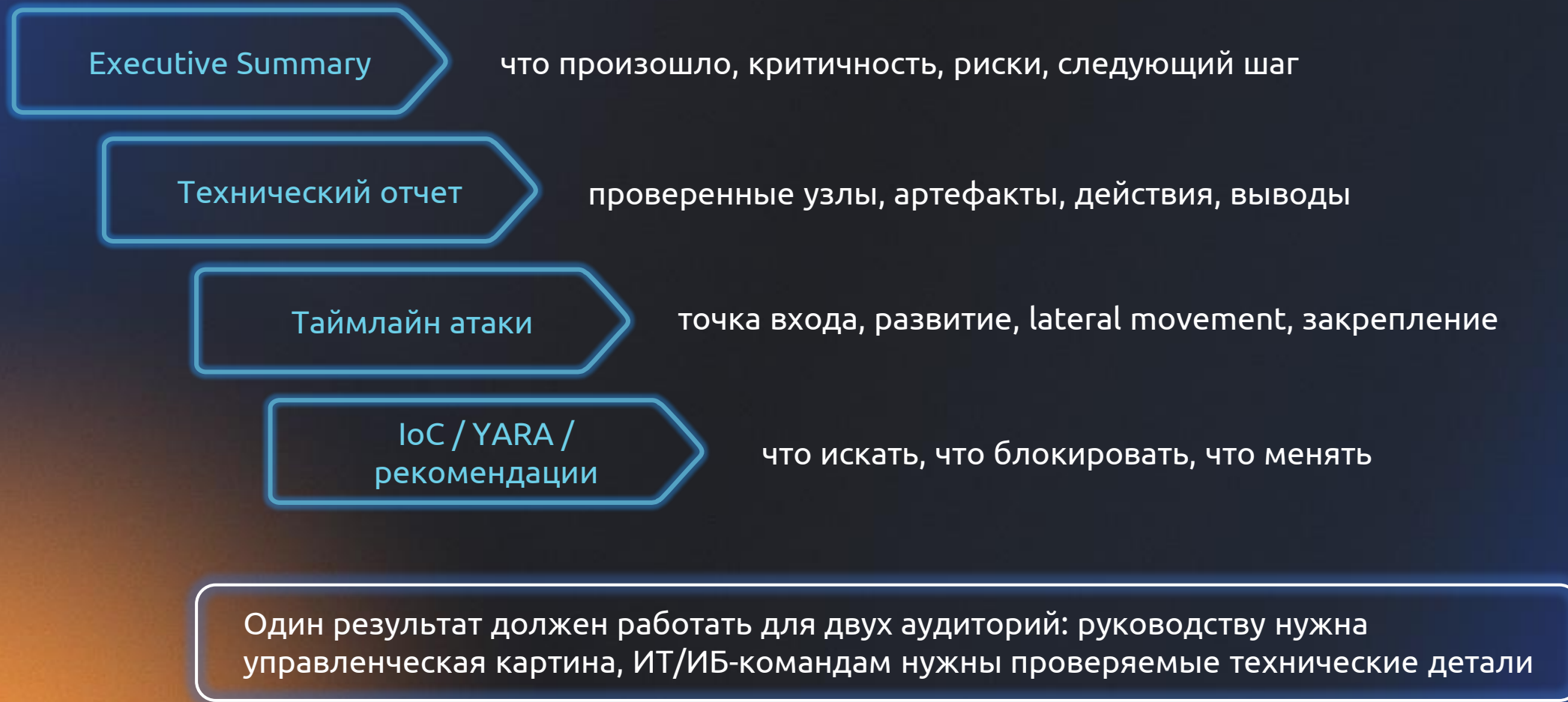


Анализ ВПО превращает файл в индикаторы, правила и меры



При сложных или обфусцированных образцах подключается углублённый реверс-инжиниринг; объём зависит от характера инцидента и доступных материалов

Заказчик получает картину инцидента, а не набор разрозненных находок

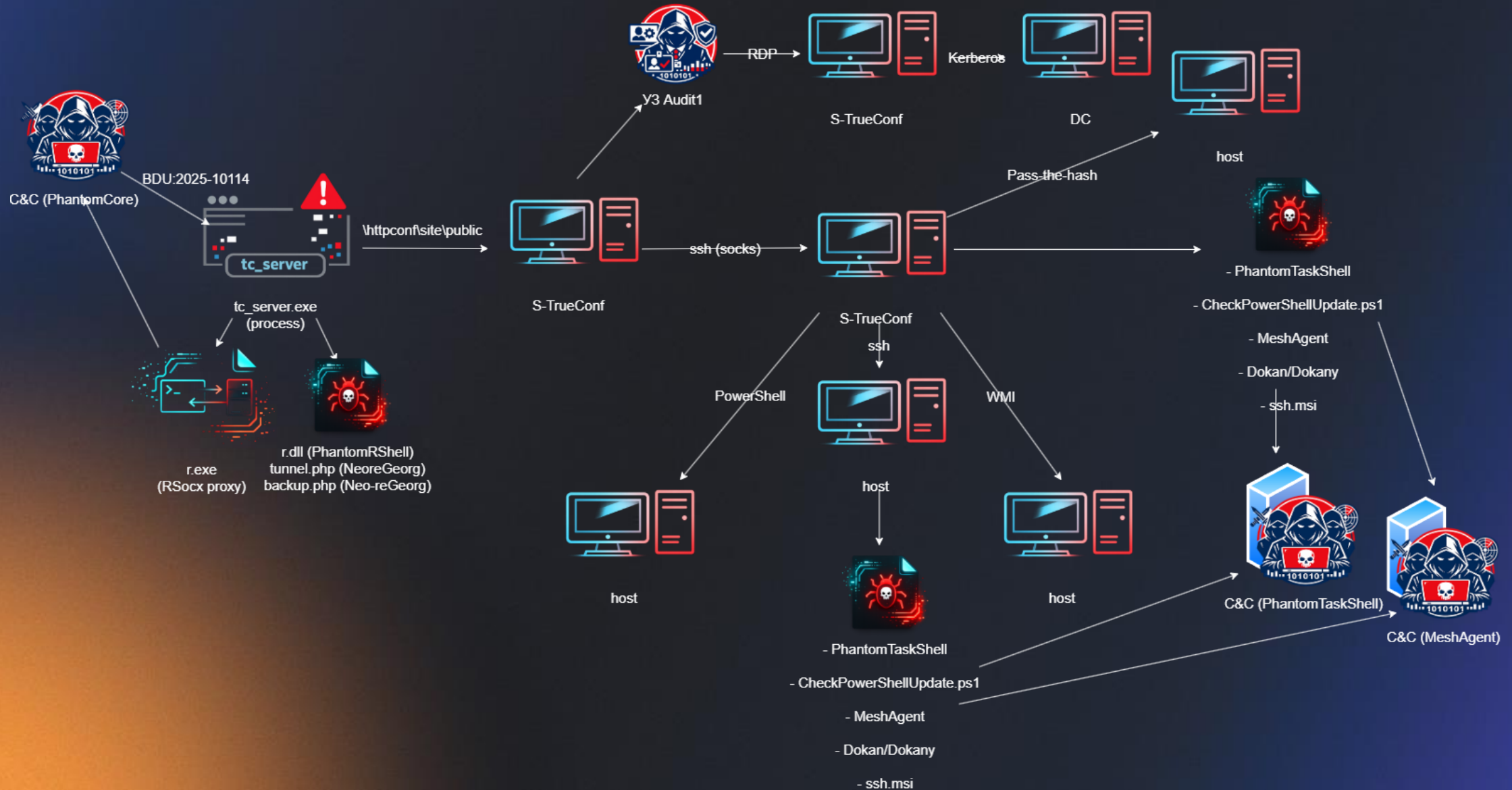




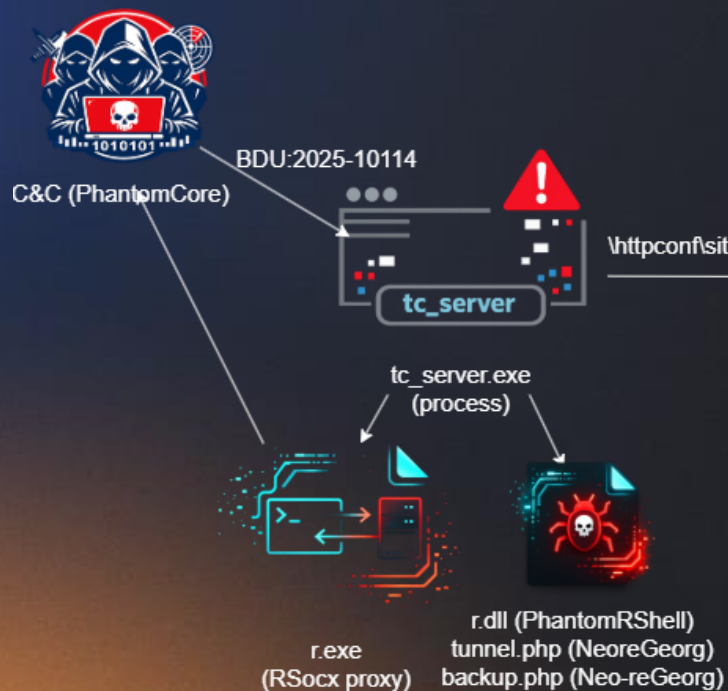
Внешний узел может оказаться началом цепочки атаки



Цепочка атаки IV квартал 2025 – I квартал 2026



Цепочка атаки IV квартал 2025 – I квартал 2026



```
[rsocx] connect to  
5.252.178.171:8080 success"
```

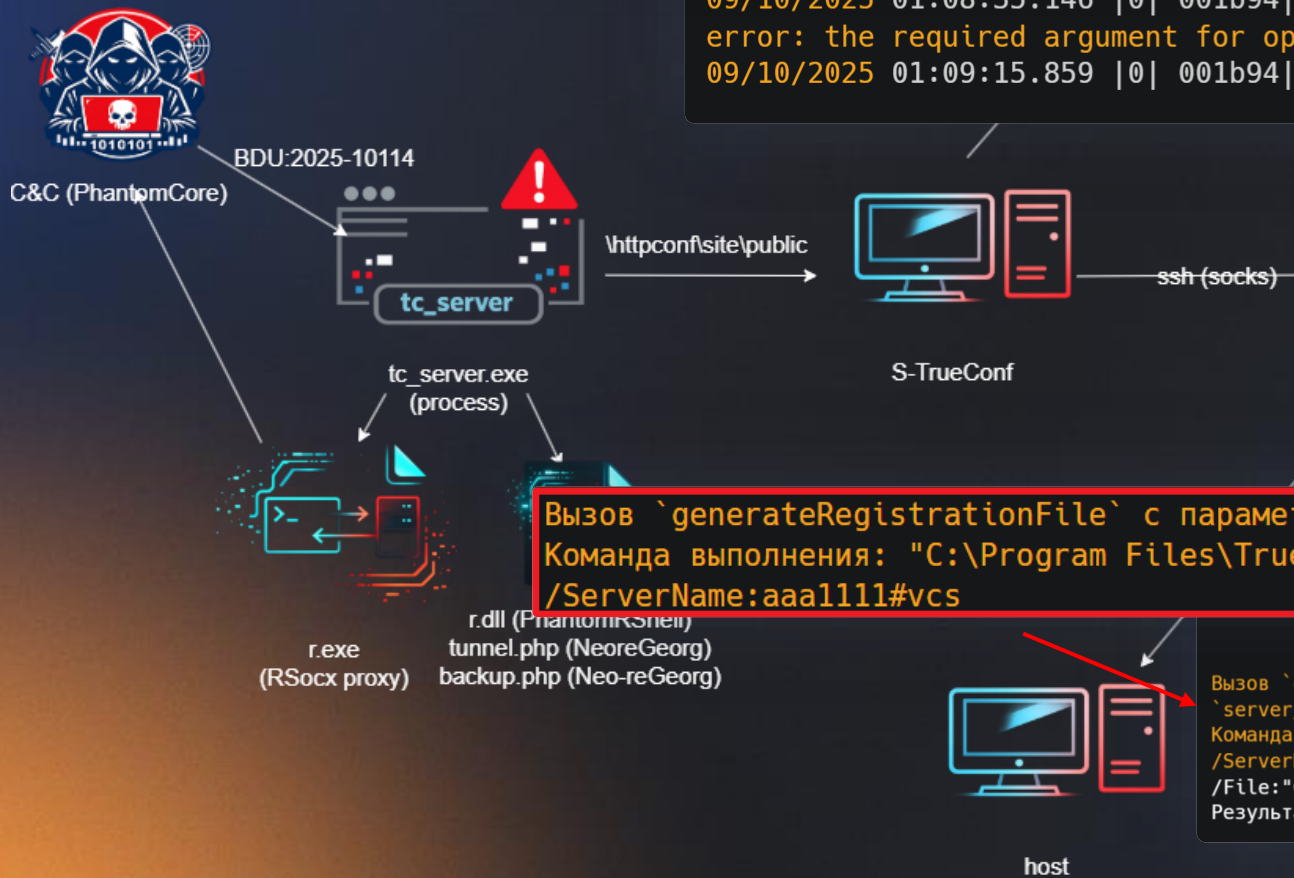
```
[2025-10-09T20:53:57.663739+00:00] WebManager.INFO: output: ["2025-10-09T17:37:59.693Z INFO  
[rsocx] connect to  
5.252.178.171:8080 success", "2025-10-09T17:39:41.492Z INFO [rsocx::socks] Proxy connecting to  
127.0.0.1:445", "2025-10-09T17:39:43.097Z INFO [rsocx::socks] Proxy connecting to  
127.0.0.1:135", "2025-10-  
09T17:39:44.253Z INFO [rsocx::socks] Proxy connecting to 127.0.0.1:445", "2025-10-09T17:39:45.213Z  
INFO  
[rsocx::socks] Proxy connecting to 127.0.0.1:445", "2025-10-09T17:45:28.826Z INFO [rsocx::  
INFO [rsocx::socks] Proxy connecting to 127.0.0.1:445", "2025-10-09T17:39:43.097Z INFO  
[rsocx::socks] Proxy  
connecting to 127.0.0.1:135", "2025-10-09T17:39:44.253Z INFO [rsocx::socks] Proxy connecting to  
127.0.0.1:445", "2025-10-09T17:39:45.213Z INFO [rsocx::socks] Proxy connecting to  
127.0.0.1:445", "2025-10-  
09T17:45:28.826Z INFO [rsocx::socks] Proxy connecting to 10.100.253.0:445", "2025-10-  
09T17:45:28.937Z INFO  
[rsocx::socks] Proxy connecting to 10.100.253.2:445", "2025-10-09T17:45:29.138Z INFO [rsocx::  
[2025-10-09T20:53:57.663739+00:00] WebManager.INFO: output: ["2025-10-09T17:37:59.693Z INFO  
[rsocx] connect to  
5.252.178.171:8080 success", ...]
```

```
C:\Program Files\TrueConf Server\httpconf\site\public\r.exe,
```

```
16.10.2025 19:24:57 Сбой работы программы r.exe C:\Program Files\TrueConf  
Server\httpconf\site\public\r.exe  
r.exe, 0.0.0.0, 669e9995, r.exe, 0.0.0.0, 669e9995, c0000409, 000000000004d745, 3658,  
01dc3eb9694386e5,  
C:\Program Files\TrueConf Server\httpconf\site\public\r.exe, C:\Program Files\TrueConf  
Server\httpconf\site\public\r.exe, 63c41ce3-7c0b-4502-8125-b8ddb225fe17
```

Цепочка атаки IV квартал 2025 – I квартал 2026

LDAP connect failed to



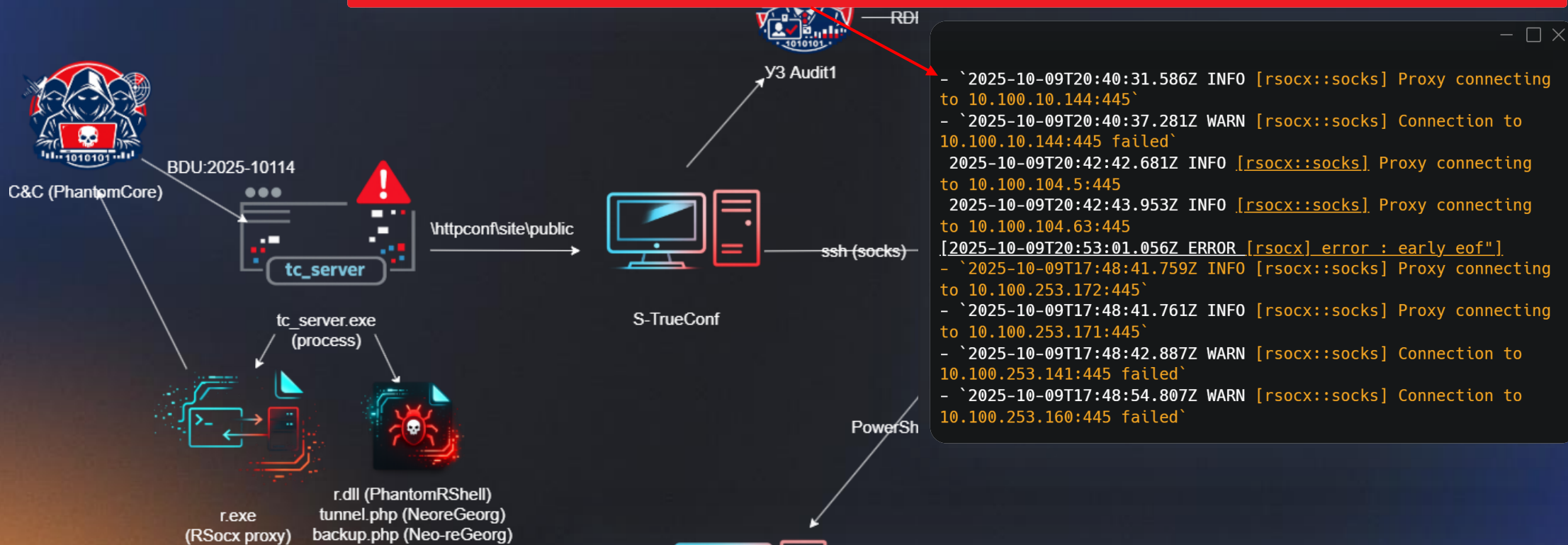
```
09/10/2025 01:08:35.146 |0| 001b94| STORAGE| LDAP connect failed to ██████████.ru:389:  
error: the required argument for option '--Serial' is missing  
09/10/2025 01:09:15.859 |0| 001b94| STORAGE| LDAP connect failed to ██████████.local:389:
```

```
Вызов `generateRegistrationFile` с параметрами сервера `server_id=a`, `server_name=aaa1111#vcs`.
Команда выполнения: "C:\Program Files\TrueConf Server\tc_server.exe/mode:1 /ServerID:a
/ServerName:aaa1111#vcs
```

```
Вызов `generateRegistrationFile` с параметрами сервера `server_id=a`,  
`server_name=aaa1111#vcs`.  
Команда выполнения: "C:\Program Files\TrueConf Server\tc_server.exe/mode:1 /ServerID:a  
/ServerName:aaa1111#vcs  
/File:"C:\TrueConf\activation\offlinereg.vrg".  
Результаты выполнения: `result:1` или `result:0`.
```

Цепочка атаки IV квартал 2025 – I квартал 2026

```
- `2025-10-09T20:40:31.586Z INFO [rsocx::socks] Proxy connecting to 10.100.10.144:445`
```

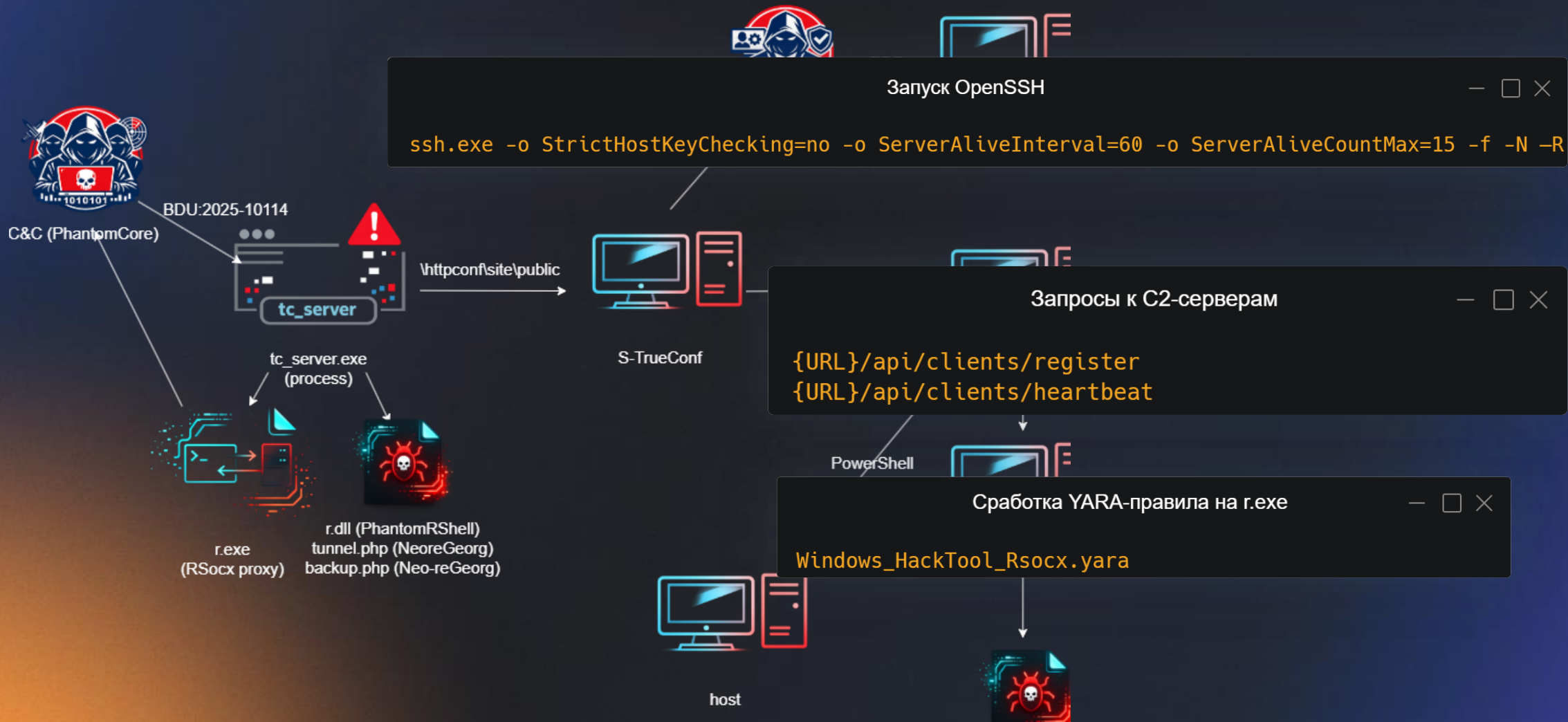


```
- `2025-10-09T20:40:31.586Z INFO [rsocx::socks] Proxy connecting to 10.100.10.144:445`  
- `2025-10-09T20:40:37.281Z WARN [rsocx::socks] Connection to 10.100.10.144:445 failed`  
2025-10-09T20:42:42.681Z INFO [rsocx::socks] Proxy connecting to 10.100.104.5:445  
2025-10-09T20:42:43.953Z INFO [rsocx::socks] Proxy connecting to 10.100.104.63:445  
[2025-10-09T20:53:01.056Z ERROR [rsocx] _error : early eof"]  
- `2025-10-09T17:48:41.759Z INFO [rsocx::socks] Proxy connecting to 10.100.253.172:445`  
- `2025-10-09T17:48:41.761Z INFO [rsocx::socks] Proxy connecting to 10.100.253.171:445`  
- `2025-10-09T17:48:42.887Z WARN [rsocx::socks] Connection to 10.100.253.141:445 failed`  
- `2025-10-09T17:48:54.807Z WARN [rsocx::socks] Connection to 10.100.253.160:445 failed`
```

Зафиксирован факт модификации:

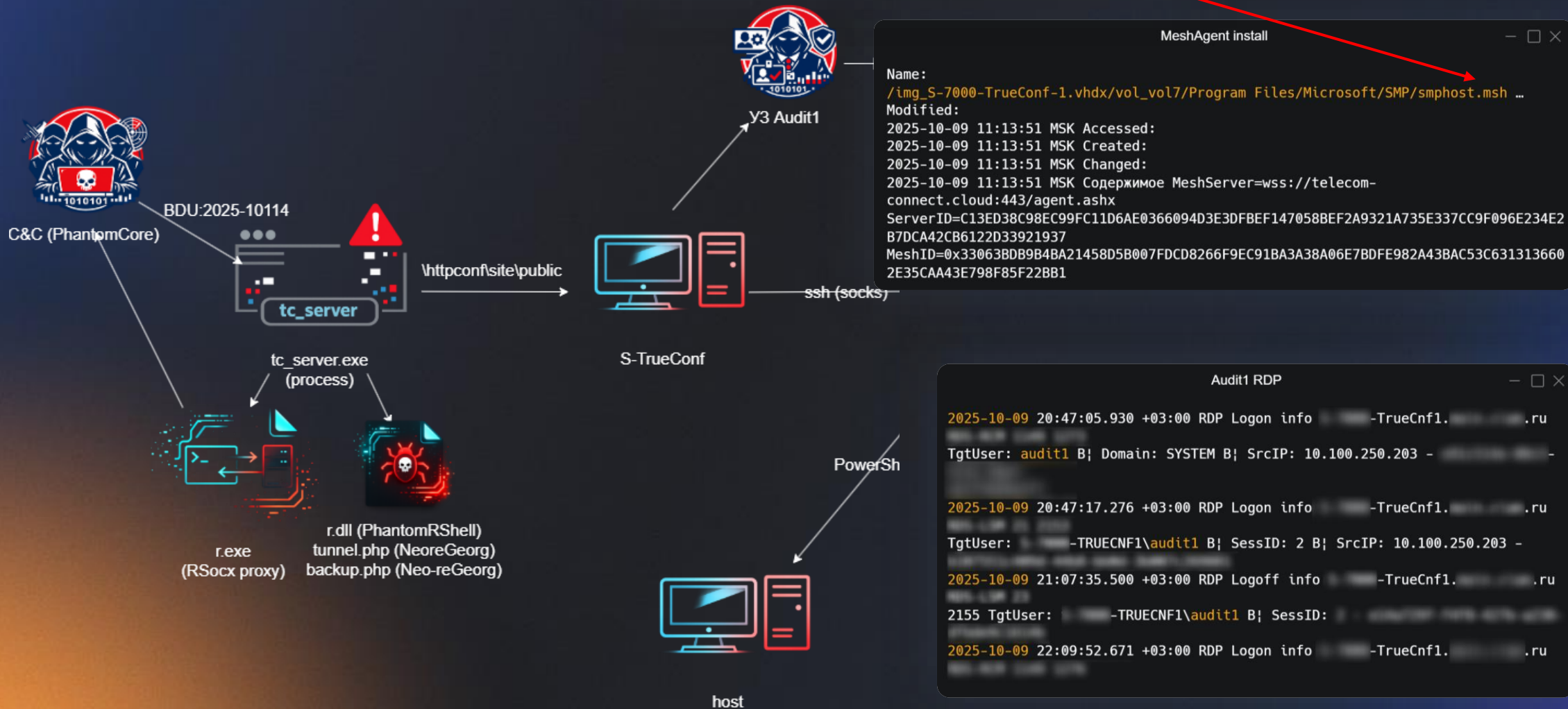
C:\Program Files\TrueConf Server\httpconf\site\private\css\c.css

Цепочка атаки IV квартал 2025 – I квартал 2026



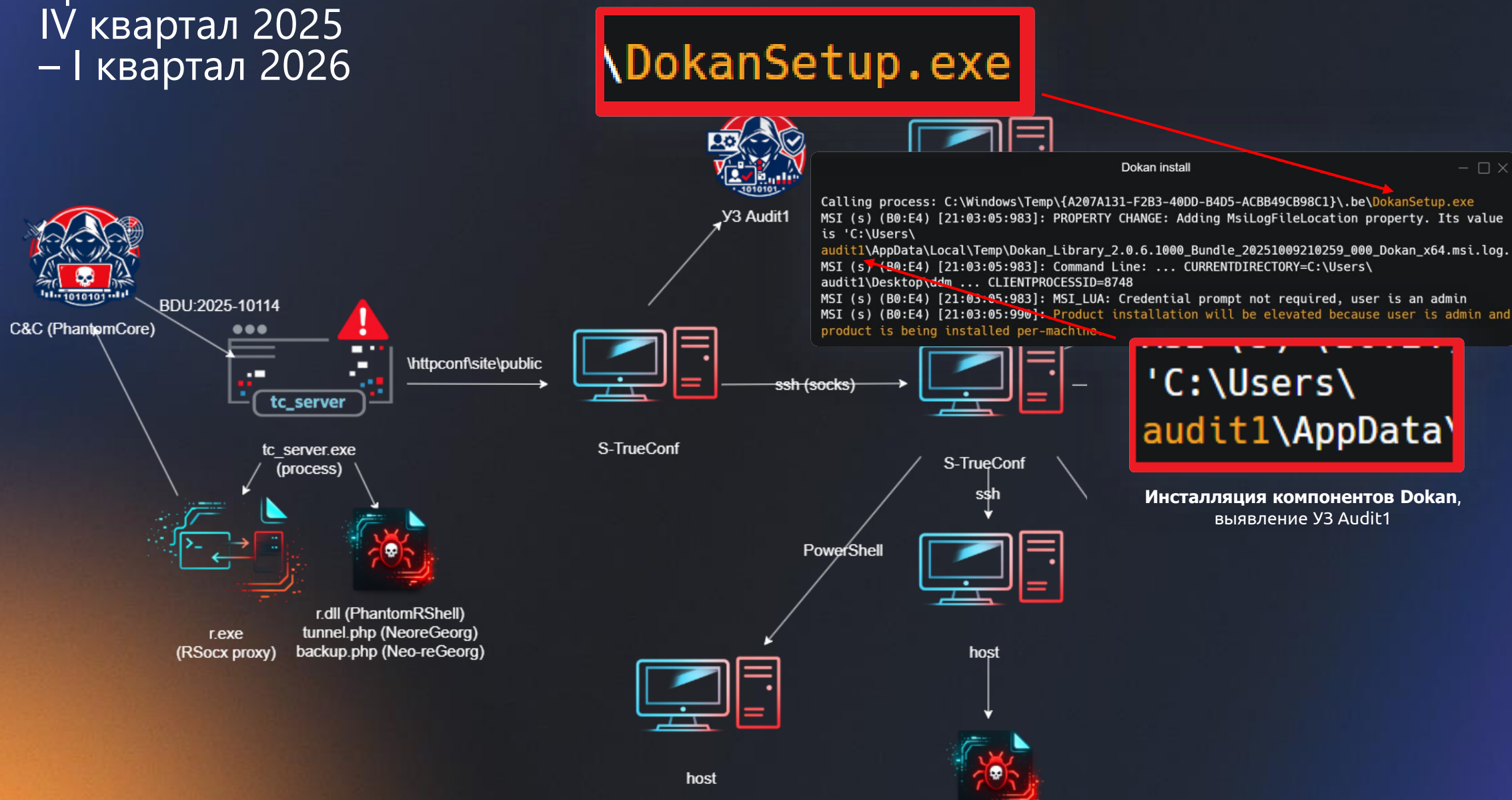
Цепочка атаки IV квартал 2025 – I квартал 2026

/Microsoft/SMP/smphost.msh

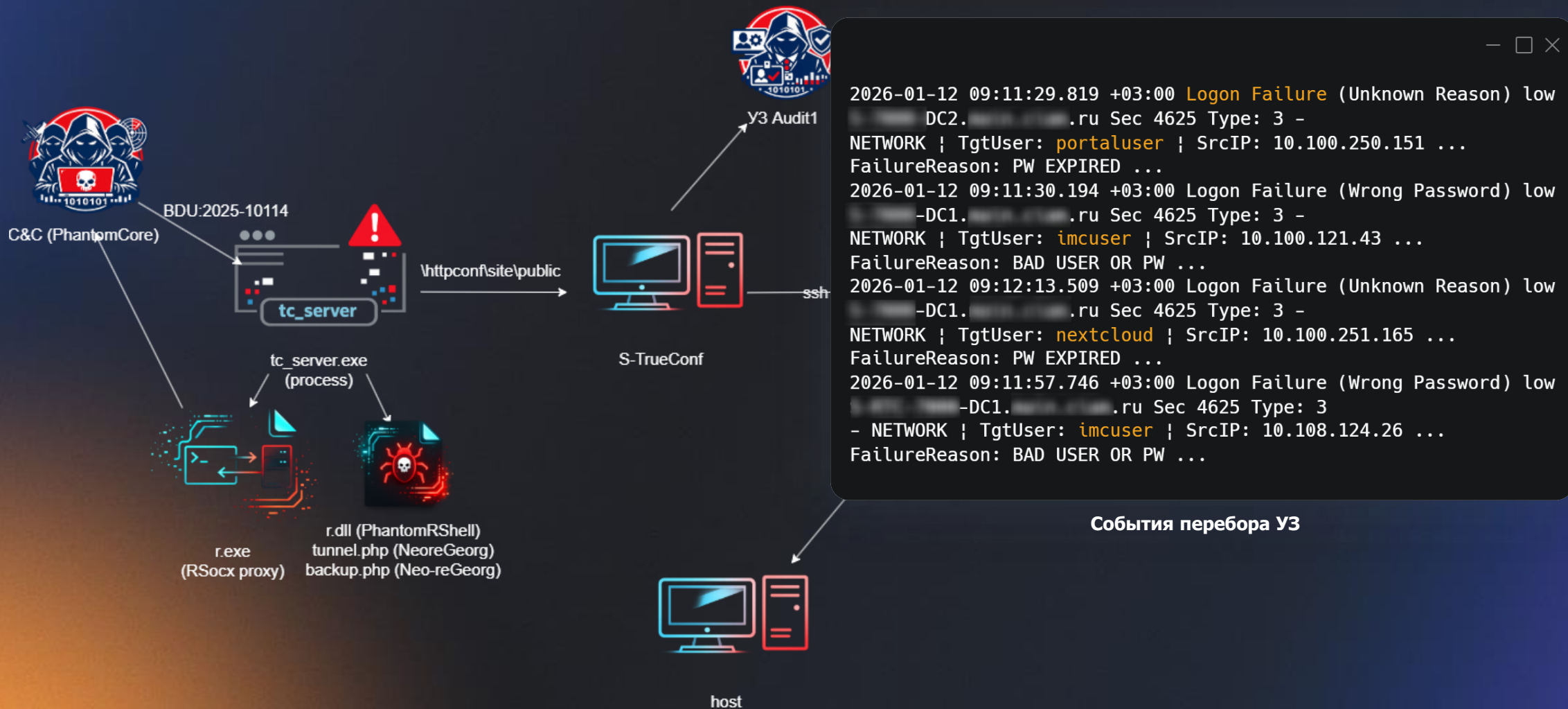


Активное латеральное перемещение УЗ Audit1 по RDP

Цепочка атаки IV квартал 2025 – I квартал 2026

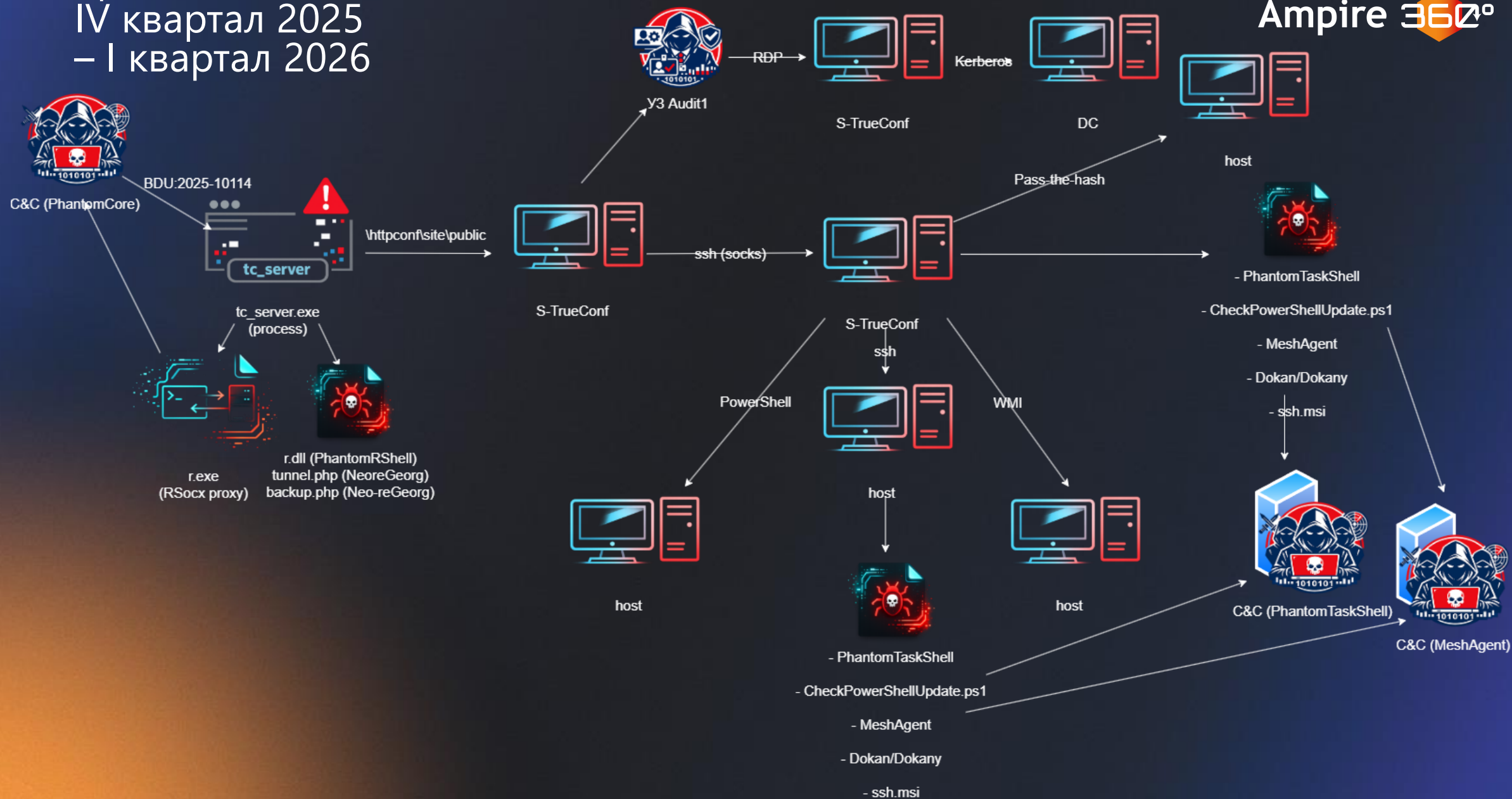


Цепочка атаки IV квартал 2025 – I квартал 2026



Цепочка атаки IV квартал 2025 – I квартал 2026

Ampire 360°



Шаги по реагированию

Поиск следов

Ampire 360°

vitalock[.]space

optivault[.]space

fortisec[.]online

infoseon[.]online

Особенности инфраструктуры

ASN 56971

Российские и иранские IP – адреса

401 Authorization Required: Www-Authenticate:
Basic realm="Restricted Content"

SSH на 80/443 порту

Маскировка наименований доменов под сферу
ИБ

.space/.online/.store домены только второго
уровня

nexaguard[.]space

cyberposi[.]space

> 30 ресурсов

astrasec[.]online

tech-infosec[.]store



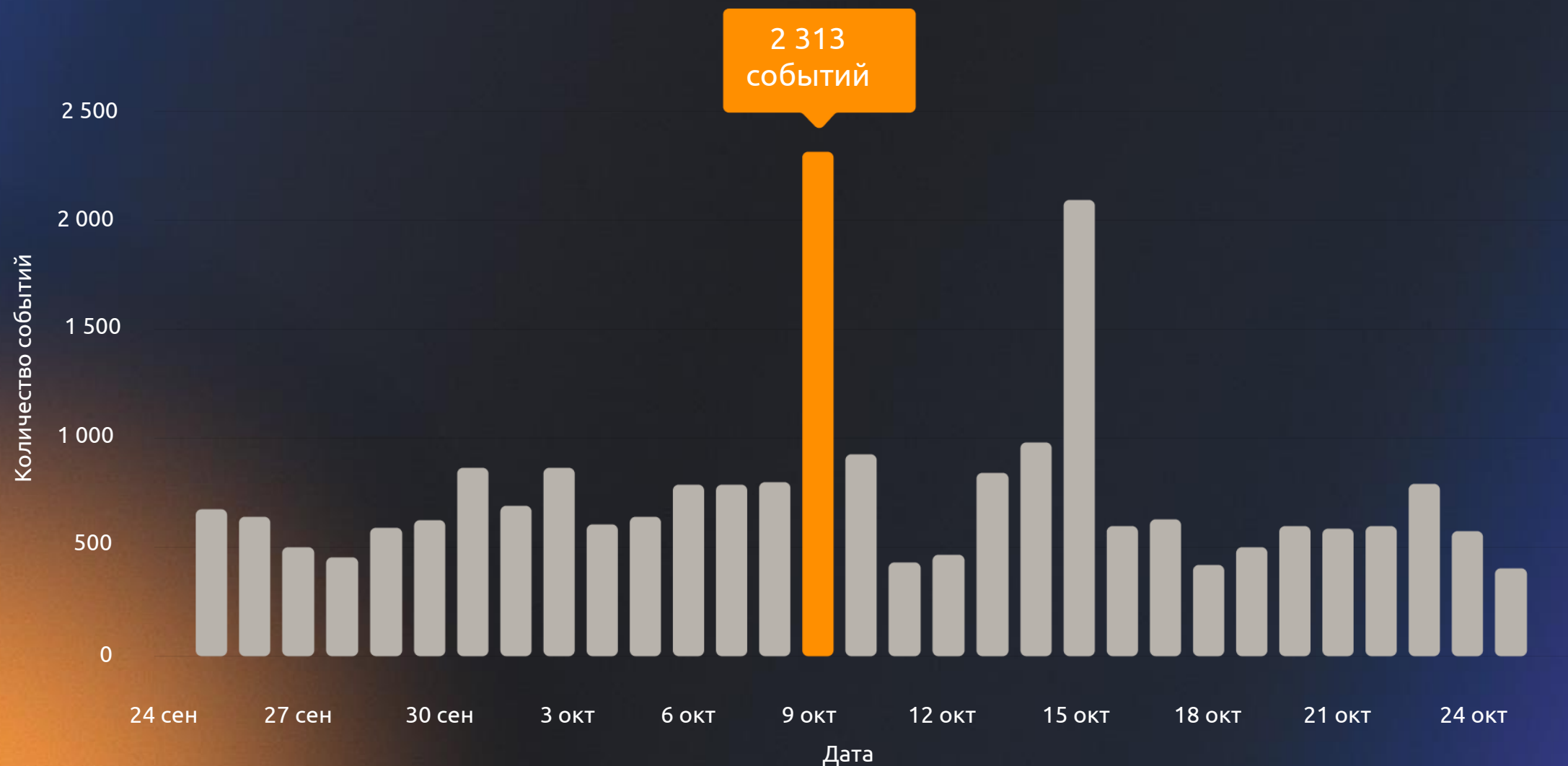
MeshAgent



Шаги по реагированию

Таймлайн активности

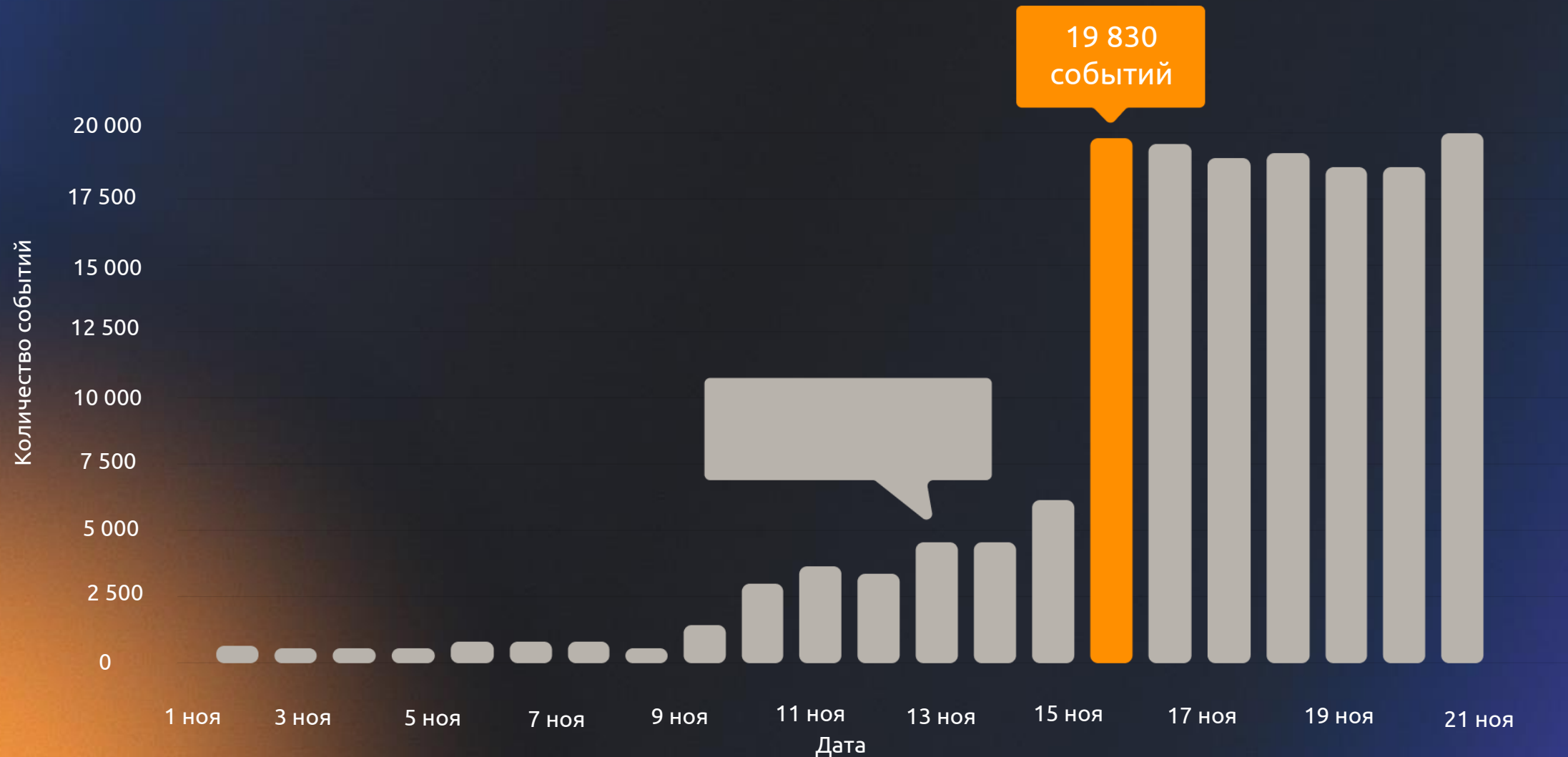
Ampire 360°



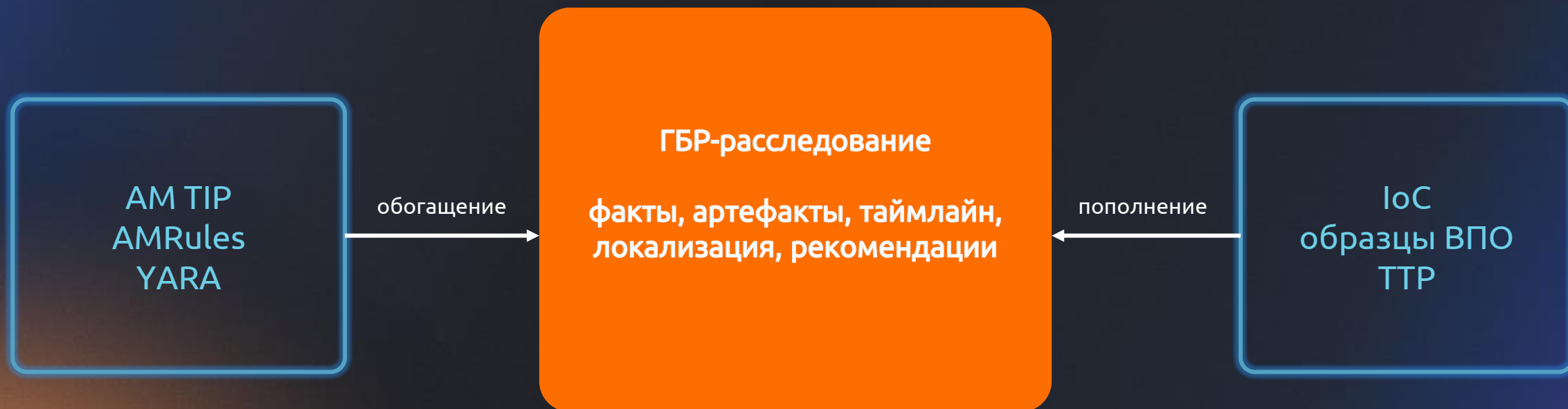
Шаги по реагированию

Таймлайн активности

Ampire 360°



Экспертная база работает в две стороны: помогает расследованию и пополняется им



Смысл контура: расследование быстрее за счёт экспертных данных, а каждый реальный инцидент усиливает будущую детектирующую логику

Благодарим за внимание!

Софья Карева
менеджер продукта

Марат Лантаев
ведущий специалист по реагированию
на компьютерные инциденты



Ampire 360°