20.04.2023

Возможности Xello Deception для детектирования APT-атак и расследования киберинцидентов

Щетинин Александр

Генеральный директор Xello

Соловьев Владимир

Руководитель направления внедрения средств защиты отдела технических решений АО "ДиалогНаука"

О компании

Xello — первый российский разработчик решения класса Distributed Deception Platform (DDP)

2018 год

Дата основания

2019 год

Релиз продукта

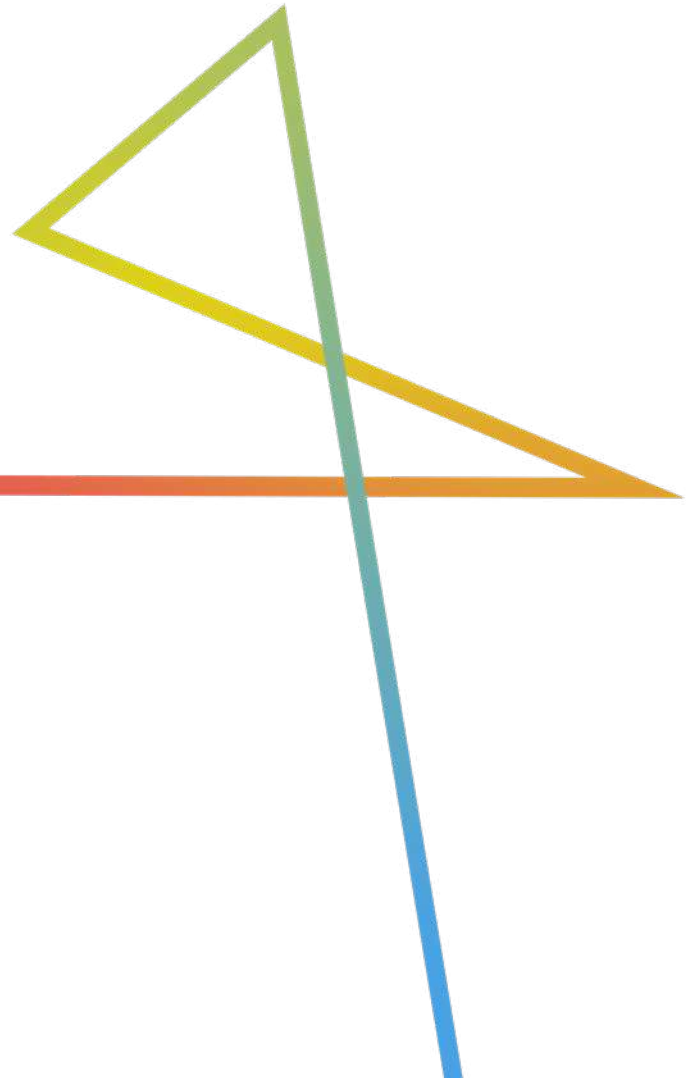
25+

Реализованных проектов (Enterprise)

20+

Разработчиков платформы

Анатомия APT-атак



Особенности APT-атаки

xello

Финансовые и технические возможности

Организация подготовленной группой: APT-группировкой

Долгосрочное и тщательное планирование: закупка инструментов, анализ инфраструктуры и другое

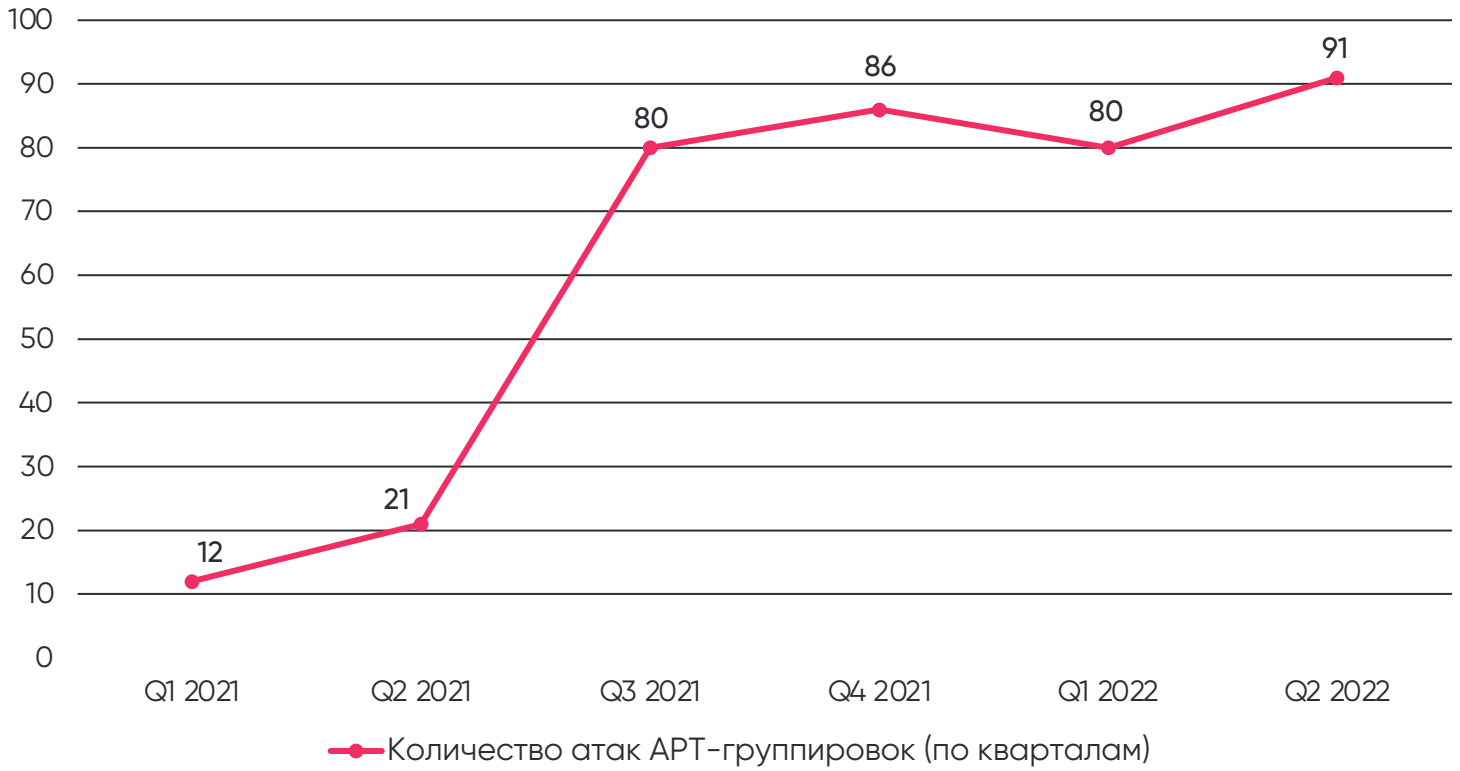
Сложности обнаружения: чистка логов и других следов

Нацеленность на конкретный объект: корпоративные секреты, исходники кода, топ-менеджмент

Длительности атаки: реализуется до конечного результата

Актуальность

Рост атак, исходящих от квалифицированных и хорошо организованных групп (APT)



Актуальные киберугрозы: II квартал 2022 года // Positive Technologies

Чем компании сегодня защищаются

xello

- Антивирус
- IPS/IDS
- SIEM-система
- Next generation firewall (NGFW)
- Песочница (Sandbox)
- Network traffic analysis (NTA)
- Web application firewall (WAF)
- Privileged access management (PAM)
- Data loss prevention (DLP)
- Endpoint detection and response (EDR)

xello

Возможностей проникнуть в корпоративную сеть множество

Уязвимости
в Open Source
компонентах

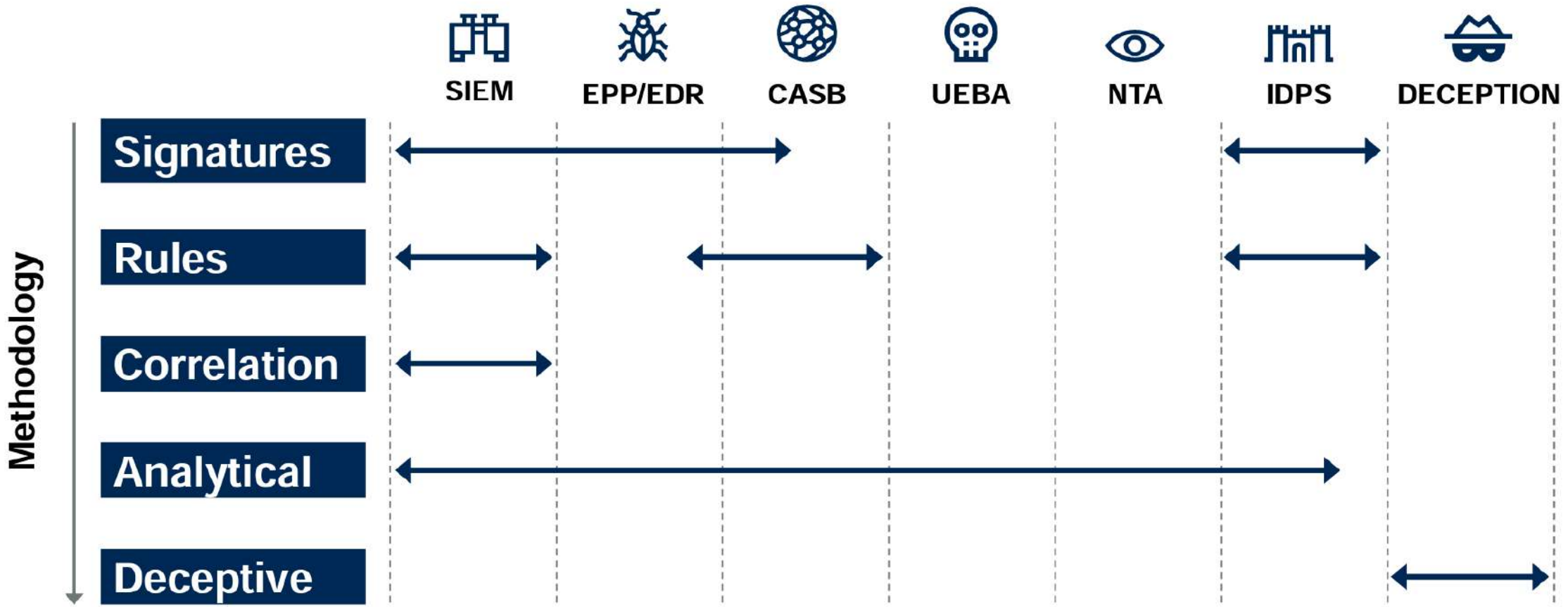
Снижение уровня
защищённости

Компрометация менее
защищённых
компаний-подрядчиков

Использование
методов социальной
инженерии

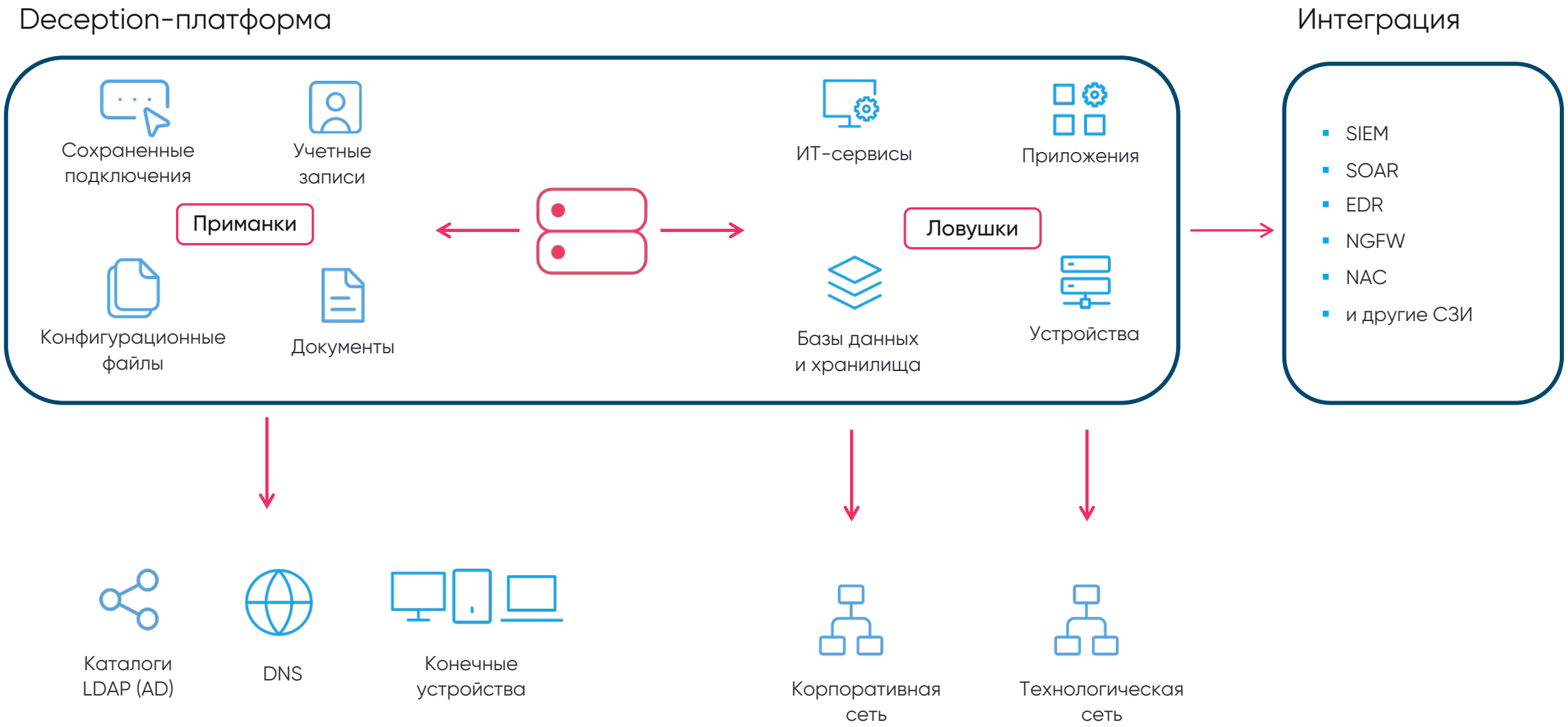
Другой подход выявления киберугроз

xello



Gartner

Как это работает



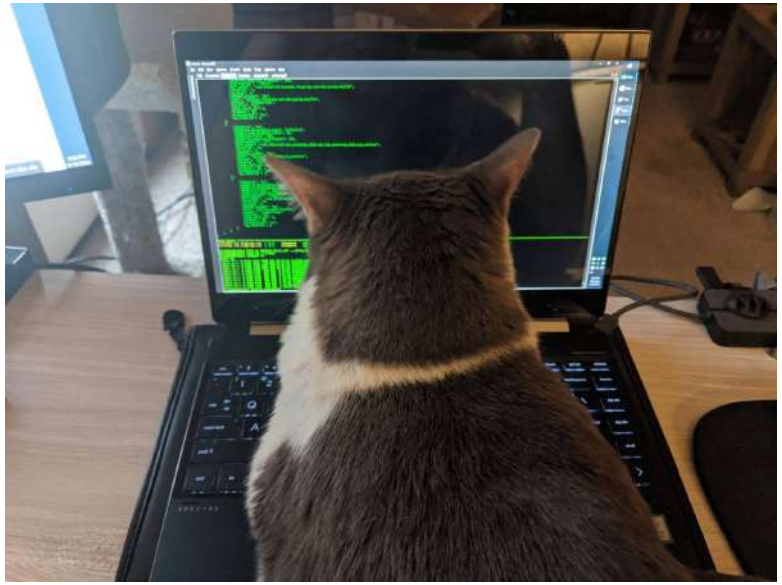
Deception при Detect, Response и Attribution

Дисклеймер: вся представленная информация предназначена исключительно для ознакомительного изучения

1 этап: подготовка

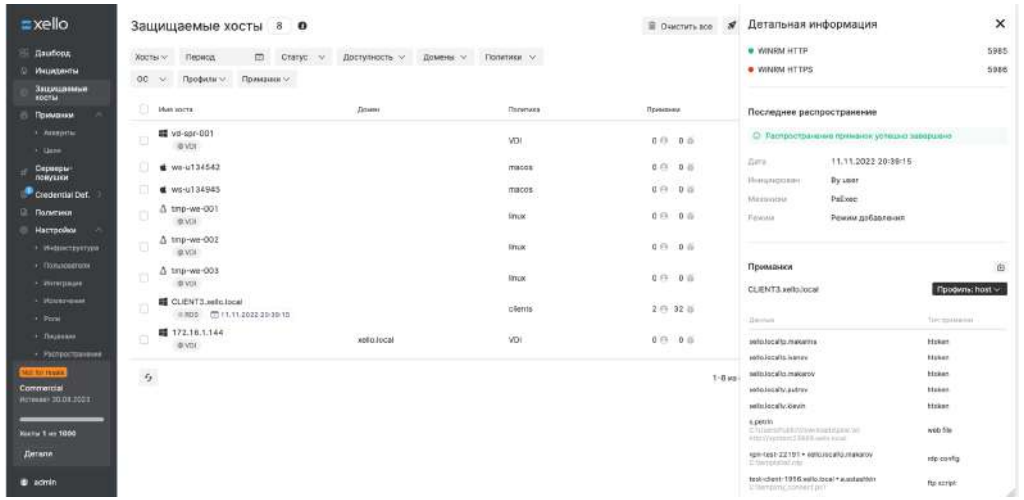
Злодеи

- Изучение цели
- Разработка концепции атаки
- Подготовка инструментария



Безопасники

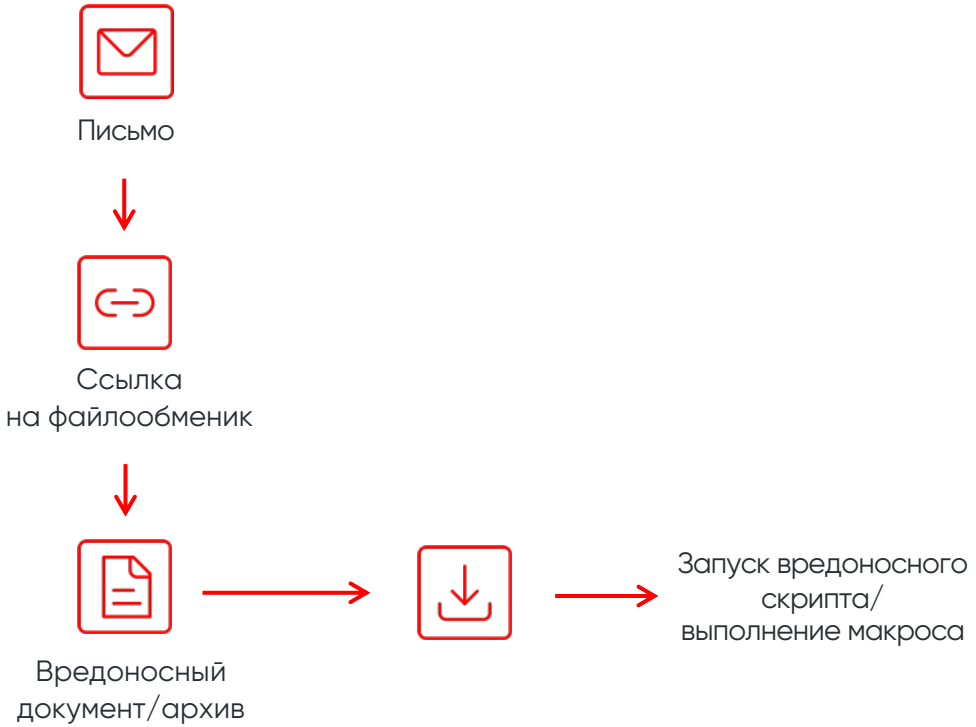
- Внедрение DDP (в добавок к существующему стеку технологий)
- Распространение приманок и ловушек



2 этап: старт атаки

Злодеи

- Рассылка фишинга



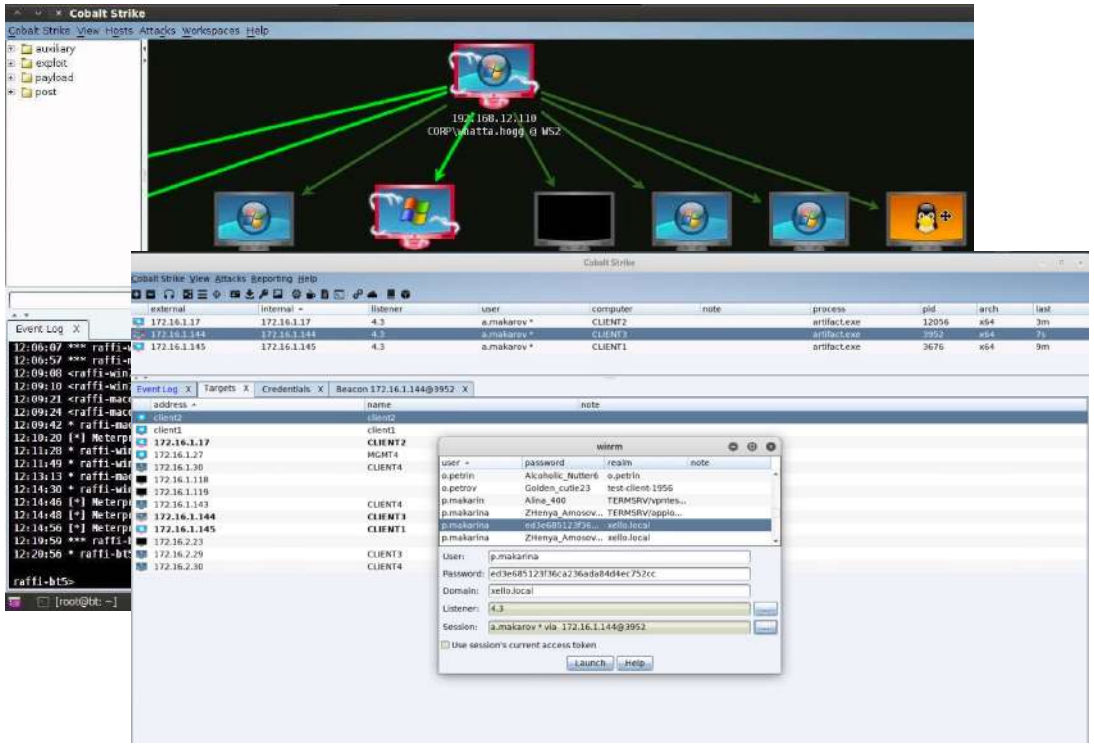
Безопасники

Изображение: Namennayo

3 этап: активная фаза

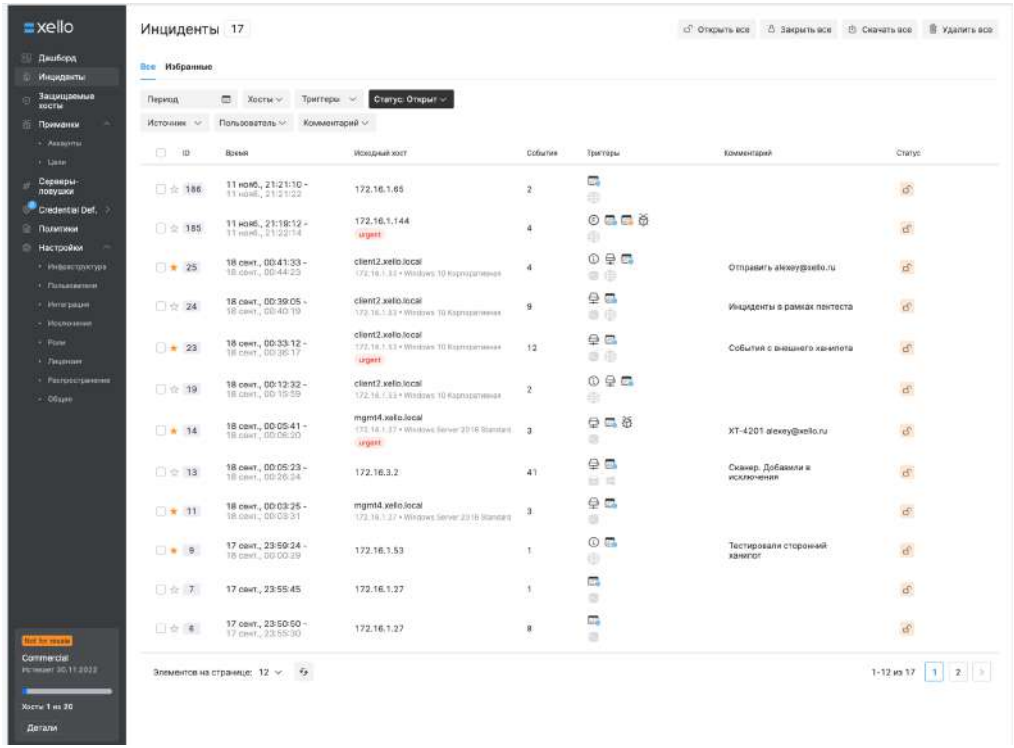
Злодеи

- Закрепление
- Нахождение приманок или ловушек
- Попытки распространения



Безопасники

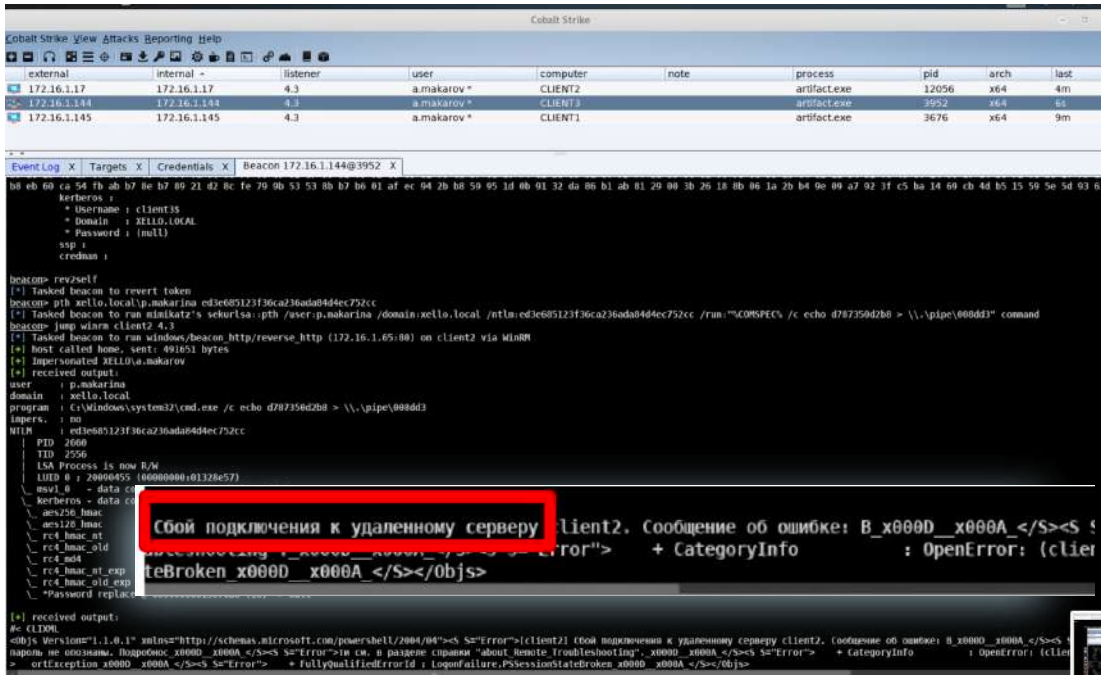
- Получение инцидентов



4 этап: перелом

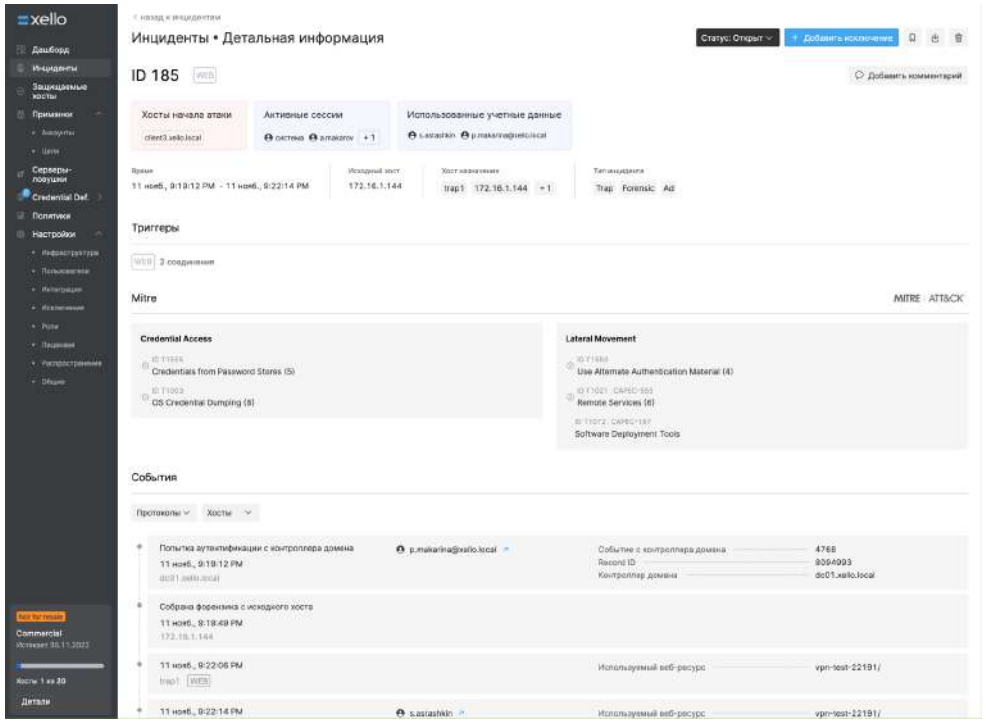
Злодеи

- Отсутствие доступа



Безопасники

- Анализ форензики
- Отправка заражённых хостов в карантин

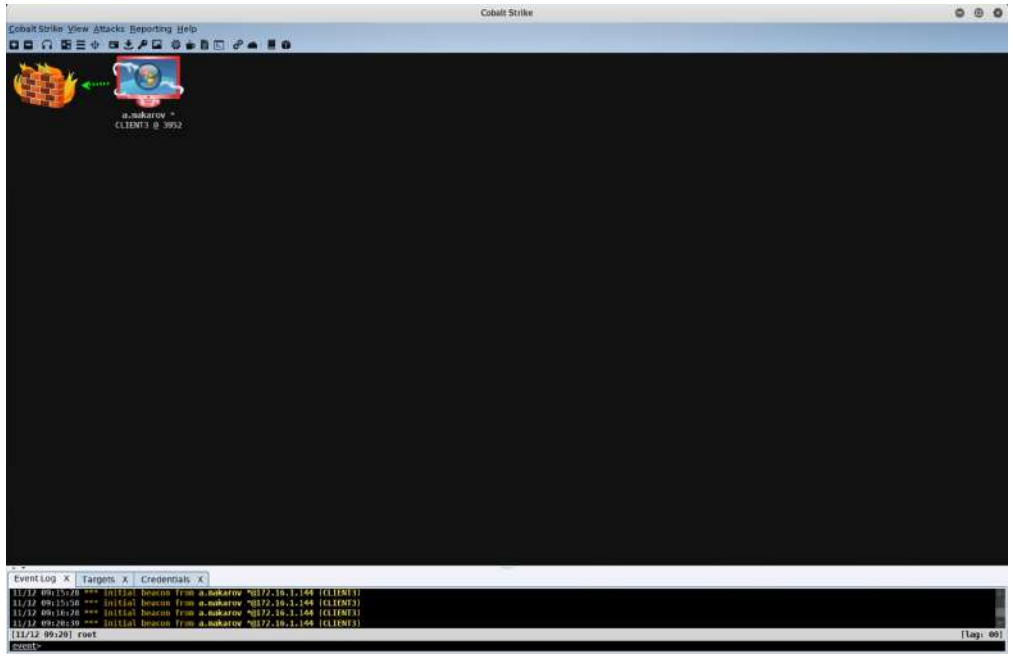


Этап 5: лечение

xello

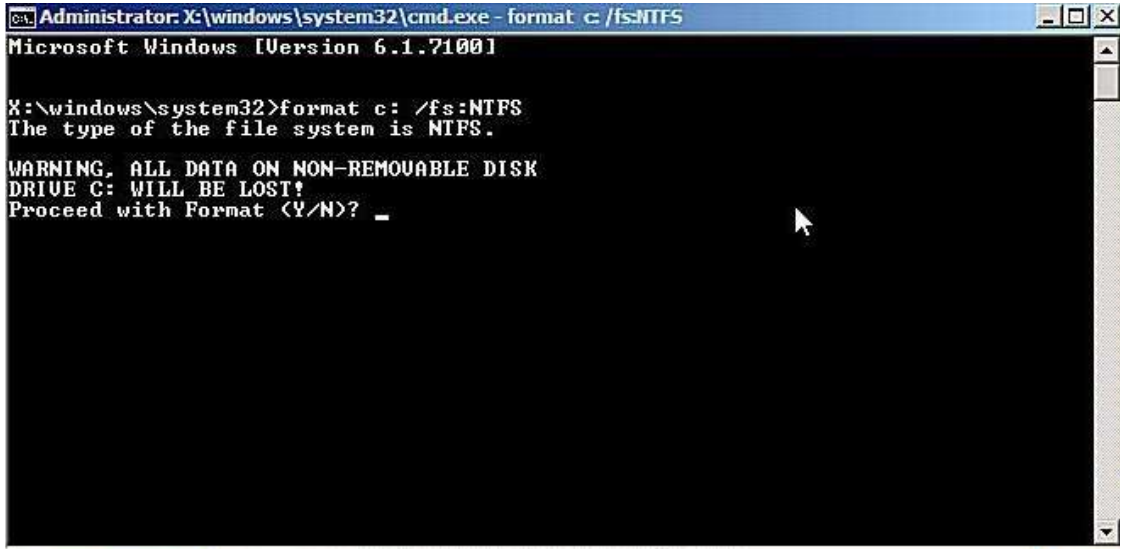
Злодеи

- Потеря контроля



Безопасники

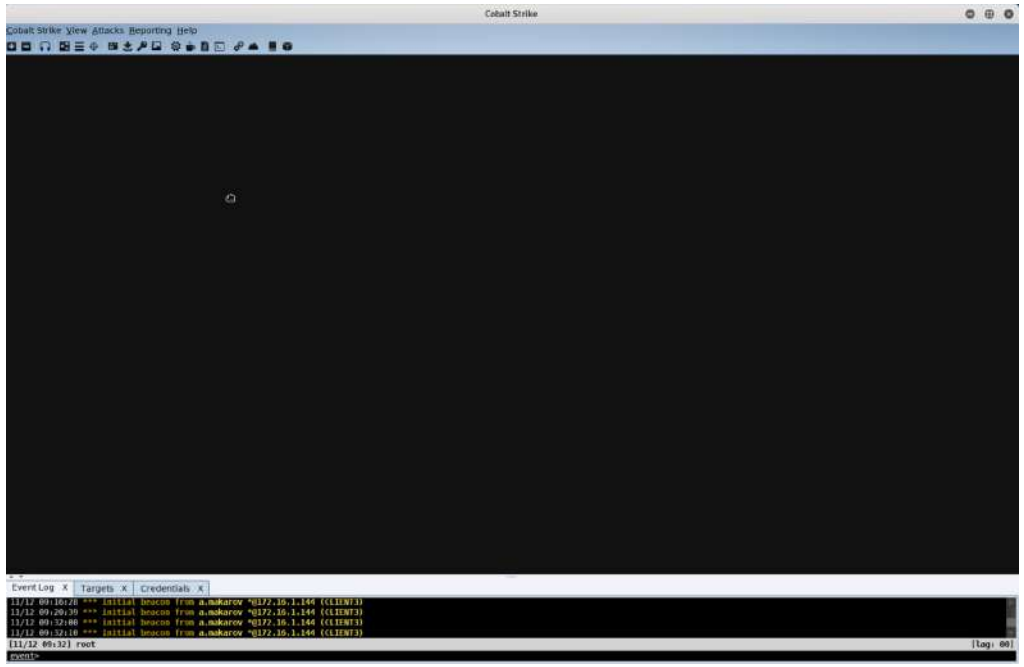
- Сбор дополнительной форензики
- Очистка заражённых хостов



Этап 6: уроки

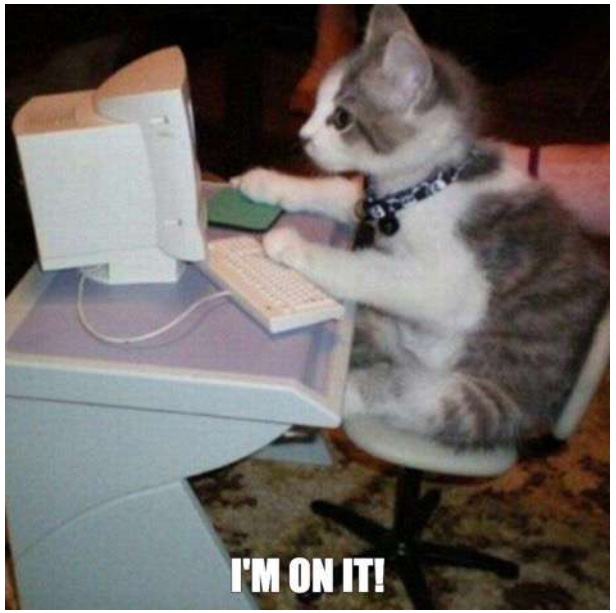
Злодеи

- Потеря контроля



Безопасники

- Анализ инцидента
- Тюнинг средств защиты информации
- Формирование компенсирующих мер



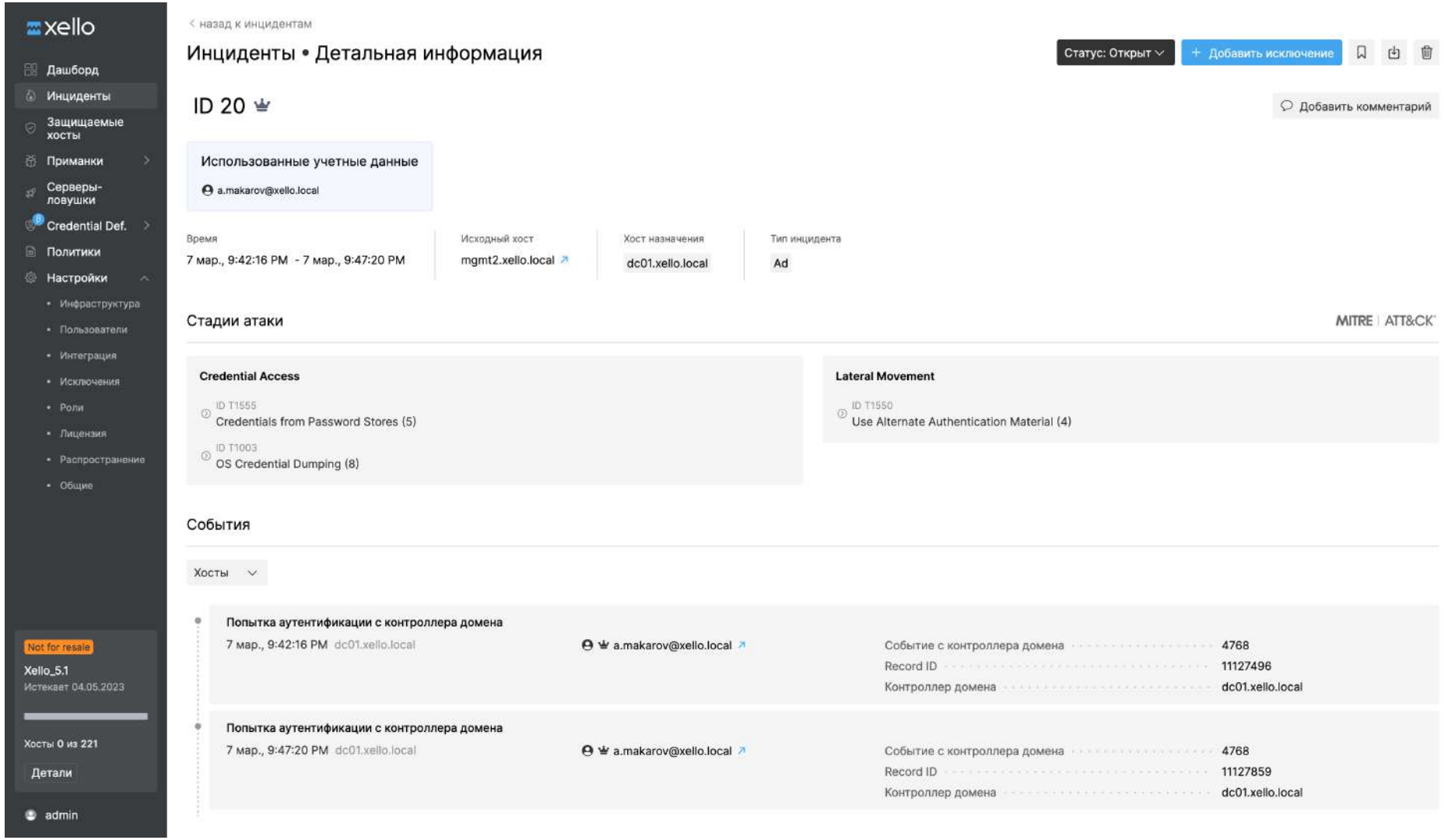
Соответствие Xello Deception матрице MITRE ATT&CK

xello

Credential Access	Discovery	Lateral Movement	Collection
Adversary-in-the-Middle	Account Discovery	Remote Services	Adversary-in-the-Middle
Brute Force	File and Directory Discovery	Software Deployment Tools	Automated Collection
Credentials from Password Stores	Network Service Discovery	Taint Shared Content	Data from Information Repositories
Network Sniffing	Network Share Discovery	Use Alternate Authentication Material	Data from Local System
OS Credential Dumping	Network Sniffing		Data from Network Shared Drive
Unsecured Credentials	Permission Groups Discovery		
	Query Registry		
	Remote System Discovery		
	System Network Configuration Discovery		
	System Network Connections Discovery		
	System Owner/User Discovery		

● Детектирование ● Обман

Карточка инцидента



Open Source-системы

xello

Достоинства

- Относительно низкая стоимость внедрения на старте
- Возможность сократить капитальные затраты
- Гибкая доработка при наличии ресурсов

Недостатки

- Возможны непредвиденные расходы на обучение, доработку
- Отсутствие тех.поддержки
- Риск приостановки деятельности проекта
- Отсутствие централизованного управления ловушками и приманками (приманки могут отсутствовать в принципе)

Open Source по дефолту

xello

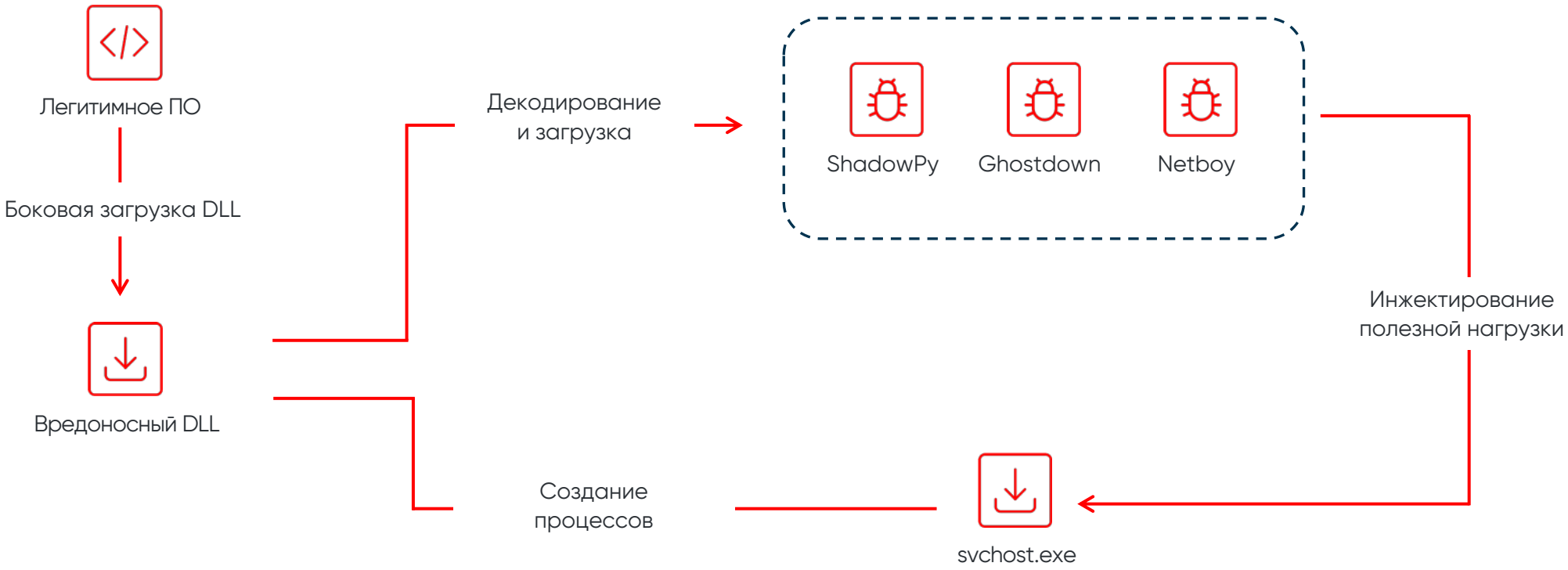
```
root@adhd:~# nmap -sV -Pn 192.168.0.103

Starting Nmap 6.01 ( http://nmap.org ) at 2016-11-07 19:23 CST
Nmap scan report for 192.168.0.103
Host is up (0.00024s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Dionaea honeypot ftpd
42/tcp   open  nameserver?
80/tcp   open  http         Apache httpd 2.2.22
135/tcp  open  msrpc?
443/tcp  open  ssl/https?
445/tcp  open  microsoft-ds Dionaea honeypot smbd
1433/tcp open  ms-sql-s     Dionaea honeypot MS-SQL server
5060/tcp open  sip          (SIP end point; Status: 200 OK)
5061/tcp open  ssl/sip      (SIP end point; Status: 200 OK)
```

Кейсы

Кейс. Атака на цепочку поставки

Схема доставки вредоносного ПО

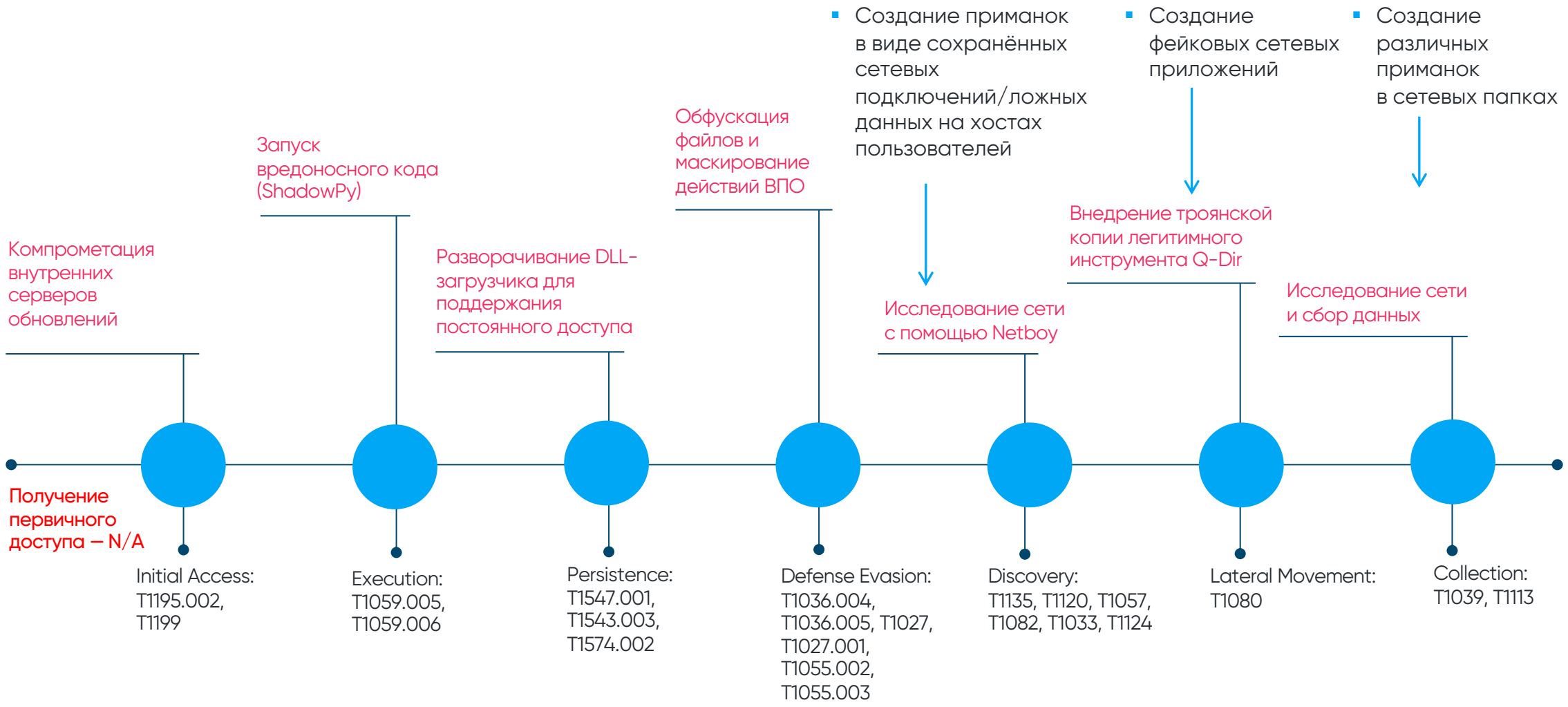


The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia // ESET

Кейс. Атака на цепочку поставки

xello

Если бы был внедрен киберобман



The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia // ESET

Технологическая ценность

xello

Обогащение

Сбор и передача данных об инцидентах в SIEM, расследование

Видимость

Контроль использования приманок в пределах доменной инфраструктуры, создание ложных целей каталоге, обслуживание всех компонентов платформы из единой консоли

Гибкость

Распространение приманок различными механизмами без применения агентов (PsExec, MS GPO, SCCM, Puppet, Ansible и т.д.)

Интеграция

Взаимодействие с другими системами, построение процесса реагирования (двусторонний API, syslog).
Сценарии работы с NAC, AV, BAS, Path Attack Management, NGFW и пр.

Решаемые задачи

Стратегический уровень

- Повышение эффективности SOC
- Оптимизация стратегии кибербезопасности

Тактический уровень

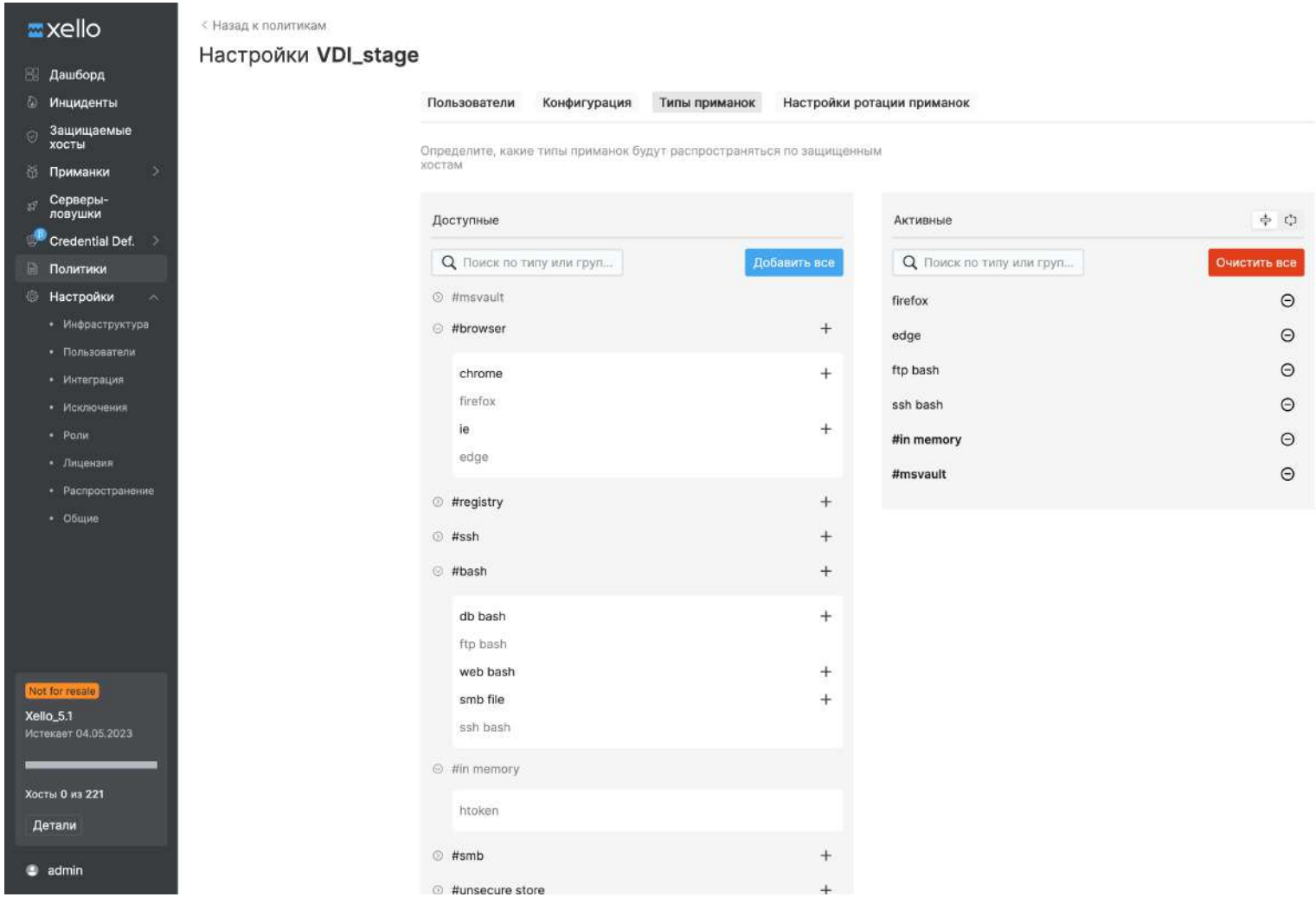
- Ускорение процесса реагирования с помощью выявления только реальных инцидентов
- Сокращение времени разбора инцидента благодаря непрерывному сбору и хранению форензики
- Автоматизация процесса реагирования

Операционный уровень

- Снижение нагрузки на специалистов кибербезопасности за счёт минимизации количества ложных срабатываний

Преимущества Xello Deception

Наибольшее количество типов приманок и безагентский способ их распространения



Типы приманок и ловушек

xello

30+ различных типов ловушек

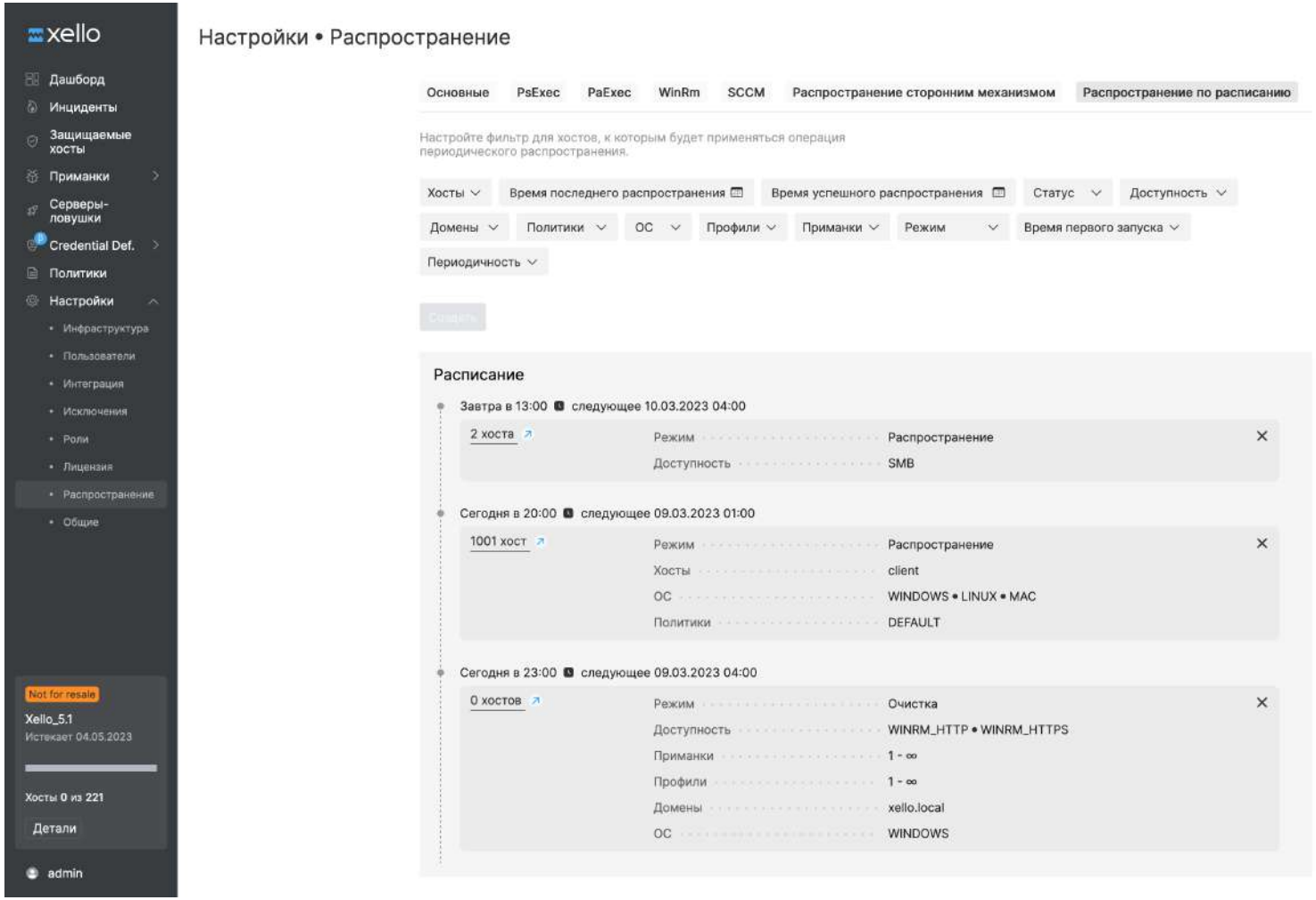
Триггер	Порт
FTP	TCP/21
SSH	TCP/22
Web	TCP/80, 443
SMB	TCP/445
RDP	TCP/3389
Database (MongoDB, MYSQL, MSSQL, PostreSQL, Memcache)	–
ICMP Detector	–
Scan Detector	–
LLMNR/NBT-NS Poisoning Detector	UDP/5355
SFTP	TCP/27017
Telnet	TCP/23, 2323
MQTT	TCP/1883
SNMP	UDP/161, 162
DNS	TCP/53
И другие	

30+ различных типов приманок

Протокол	Тип приманки
Приманки для ОС Windows	
Web credentials	Chrome
	Internet Explorer
	Mozilla Firefox
RDP saved credentials	Configs
	Scripts
	Microsoft Credential Manager
Приманки для ОС Linux	
SSH	Files
	Bash history
	Known hosts
Приманки для ОС Mac	
FTP	Bash history
	Configs
	Scripts
И другие	

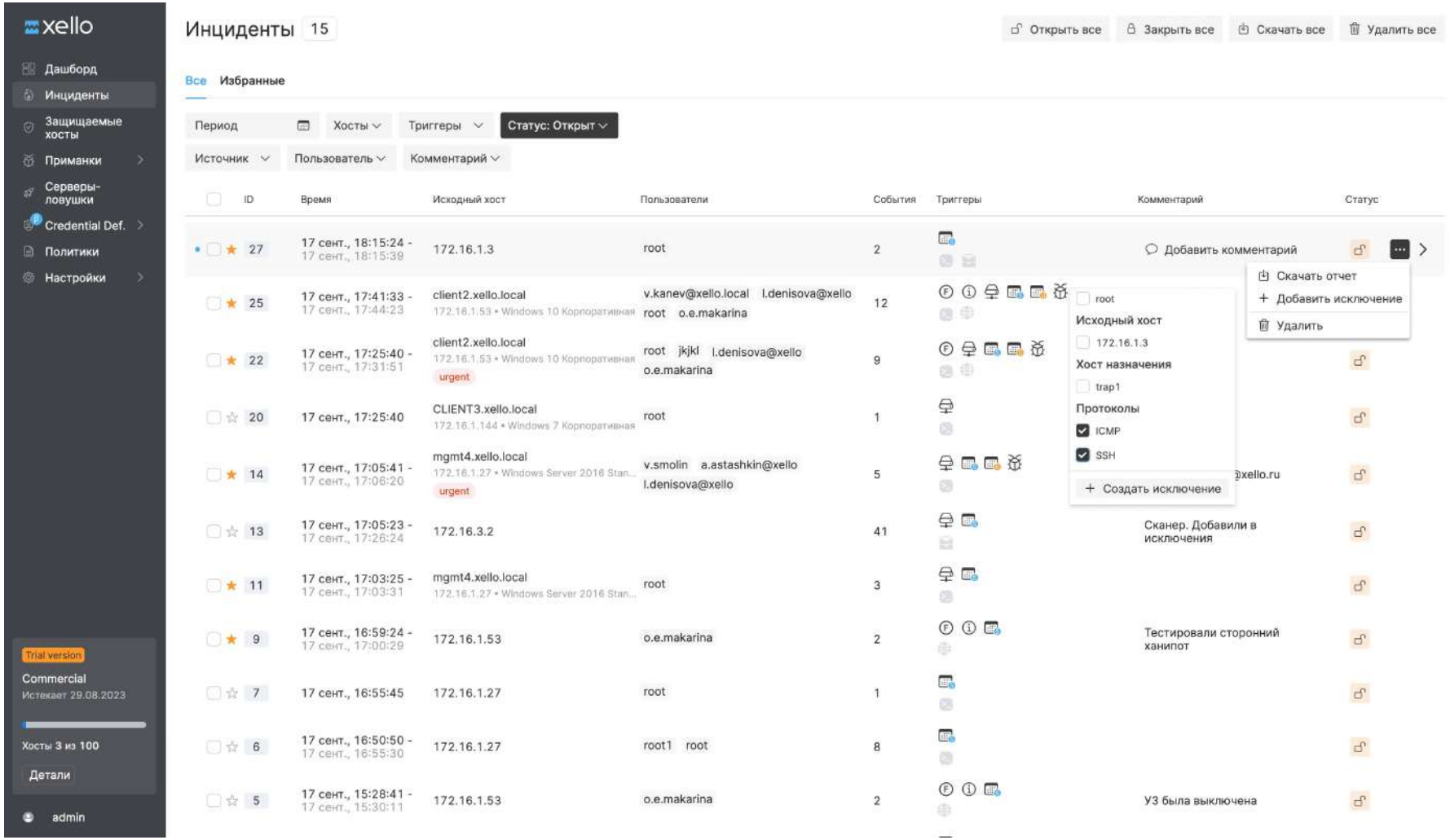
! На слайде указана часть из всех типов приманок и ловушек.
Полный перечень доступен по запросу: sales@xello.ru

Наибольшее количество способов распространения



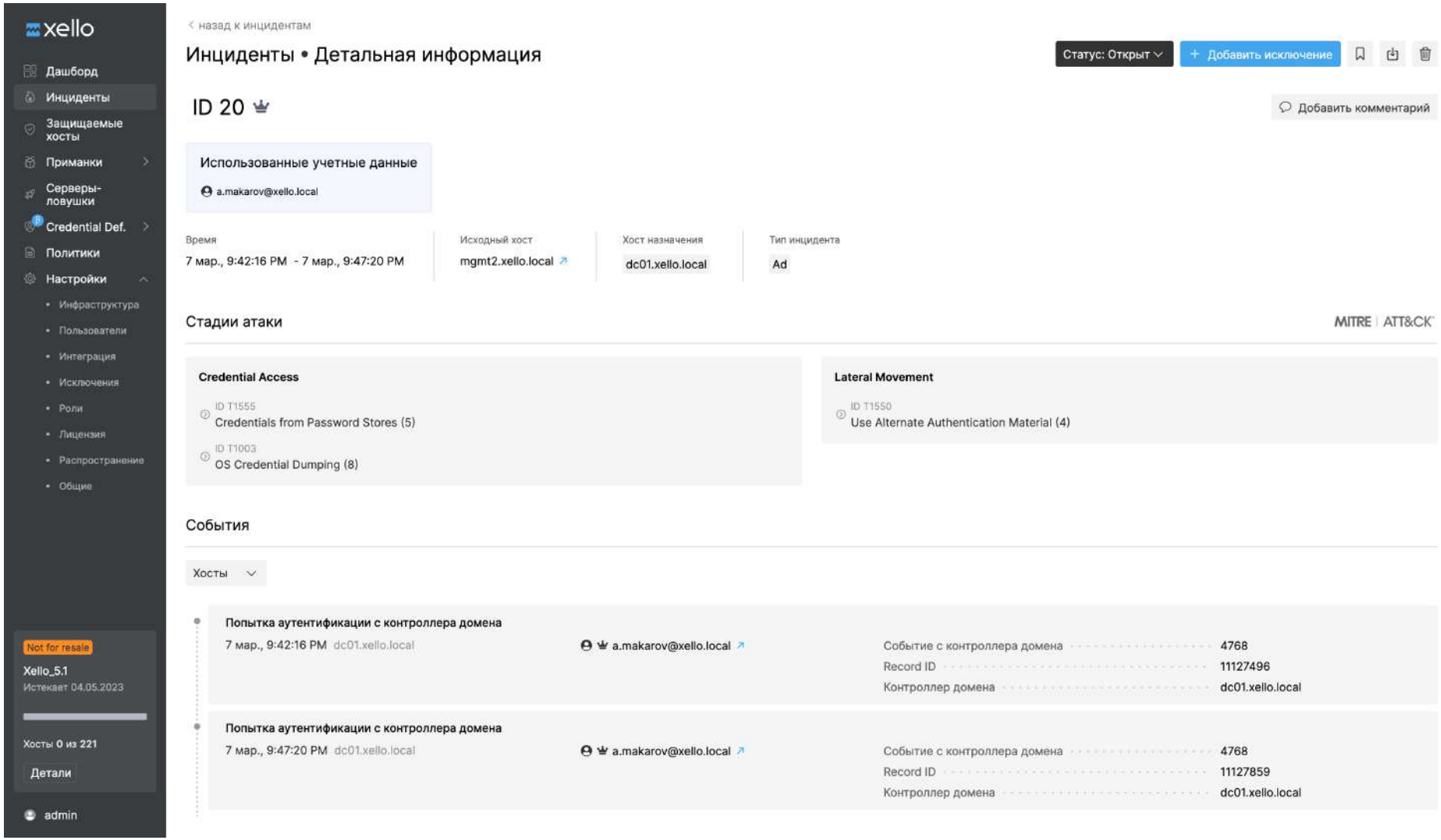
Флоу работы с инцидентами

xello



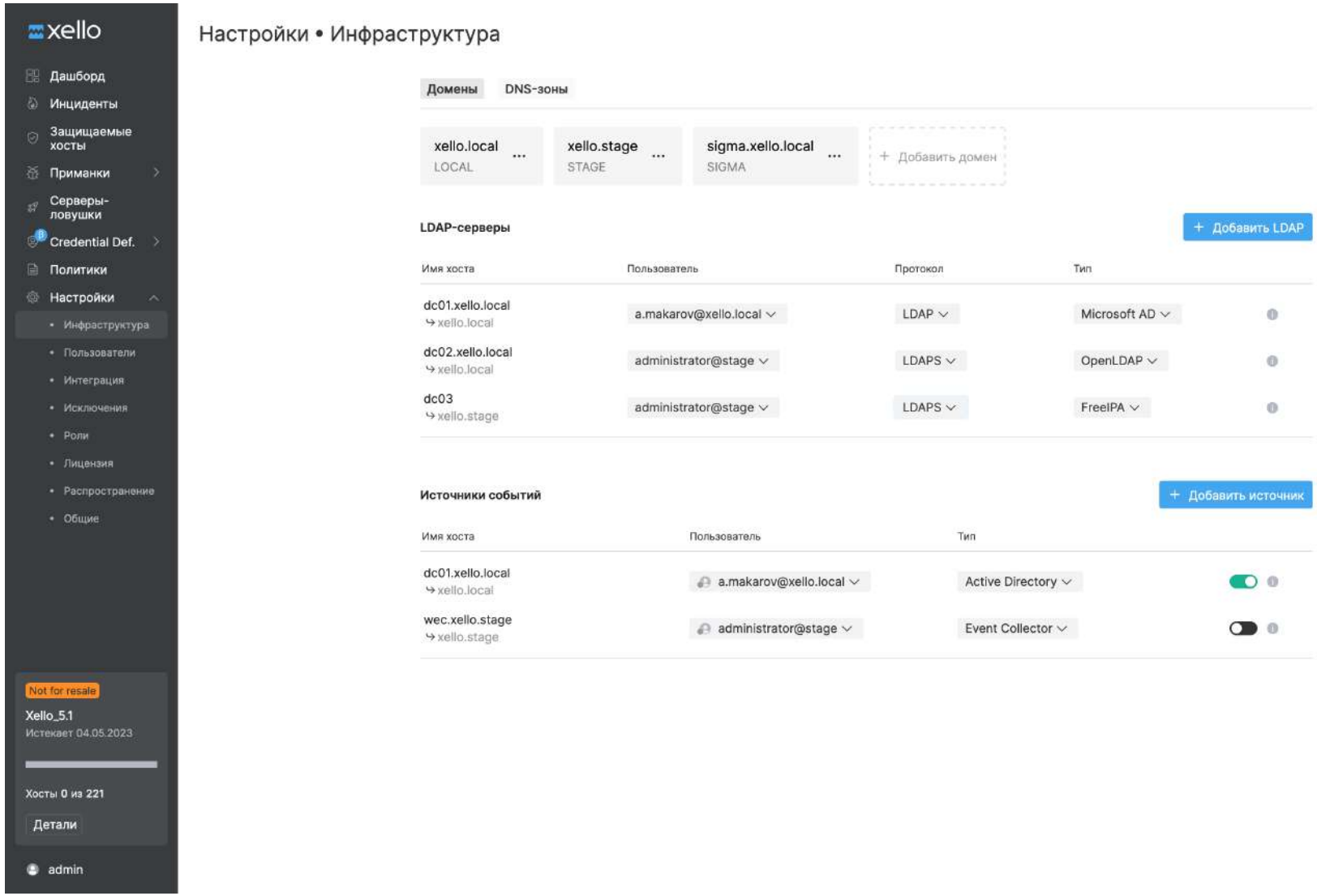
Сбор и хранение форензики

xello



Гибкая встраиваемость в инфраструктуру

xello



Демонстрация

xello

Ответим
на ваши вопросы!

info@xello.ru
+7 (495) 786 03 35