24.10.2023

Xello Deception 5.3: защита от целевых атак для распределённых площадок

Черников Дмитрий

Руководитель направления пресейла Xello

Соловьев Владимир

Руководитель направления внедрения средств защиты отдела технических решений АО «ДиалогНаука»

Спикеры

Черников Дмитрий

Руководитель направления пресейла Xello

Соловьев Владимир

Руководитель направления внедрения средств защиты отдела технических решений АО «ДиалогНаука»

О компании

Xello — лидер сегмента решений класса Distributed Deception Platform (DDP) на российском рынке информационной безопасности

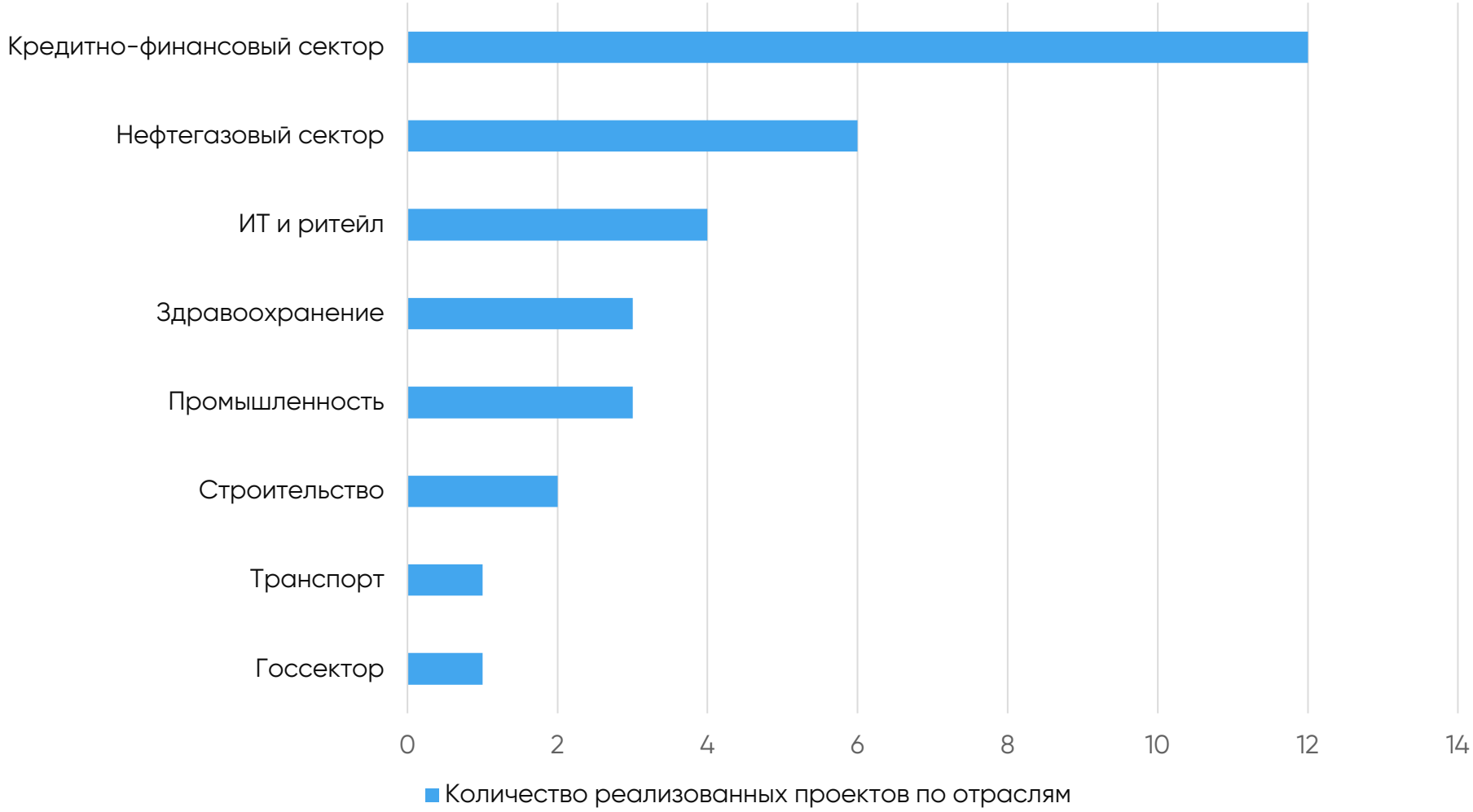
30+

проектов реализовали в различных сферах к сентябрю 2023 года

5+

лет разрабатываем первую российскую платформу кибероброманa

Реализованные проекты



Xello Deception

Защита от целевых атак с помощью ложного слоя данных и активов

xello

Сеть

- Разной степени интерактивности ловушки, позволяющие эмулировать корпоративные системы, приложения, базы данных и другие ИТ-активы
- Сетевой трафик
- Уязвимости в сетевых устройствах (маршрутизаторы, коммутаторы и т.п)

Конечные устройства

- Учётные записи
- Сохранённые пароли в браузерах
- История команд в BASH и PowerShell
- Сохранённые SSH-ключи в хранилищах
- Ветки реестра ОС и стороннего ПО

Технологический сегмент

- Промышленное оборудование
- Программируемые логические контроллеры (ПЛК)
- АРМ-сервера
- Уязвимости в оборудовании, ПО
- Умные устройства

Xello Deception

Xello Deception Industrial

2024 г.

Выявление целевых атак

SIEM | IPS/IDS | PAM | DLP | NGFW

Sandbox | NTA | Threat Intelligence | EDR

- Опираются на описанную логику и правила
- Используют поведенческий анализ
- Быстро принимают решение

Выявление целевых атак

xello

Deception

Distributed Deception Platform

DDP

Приманки

Ловушки

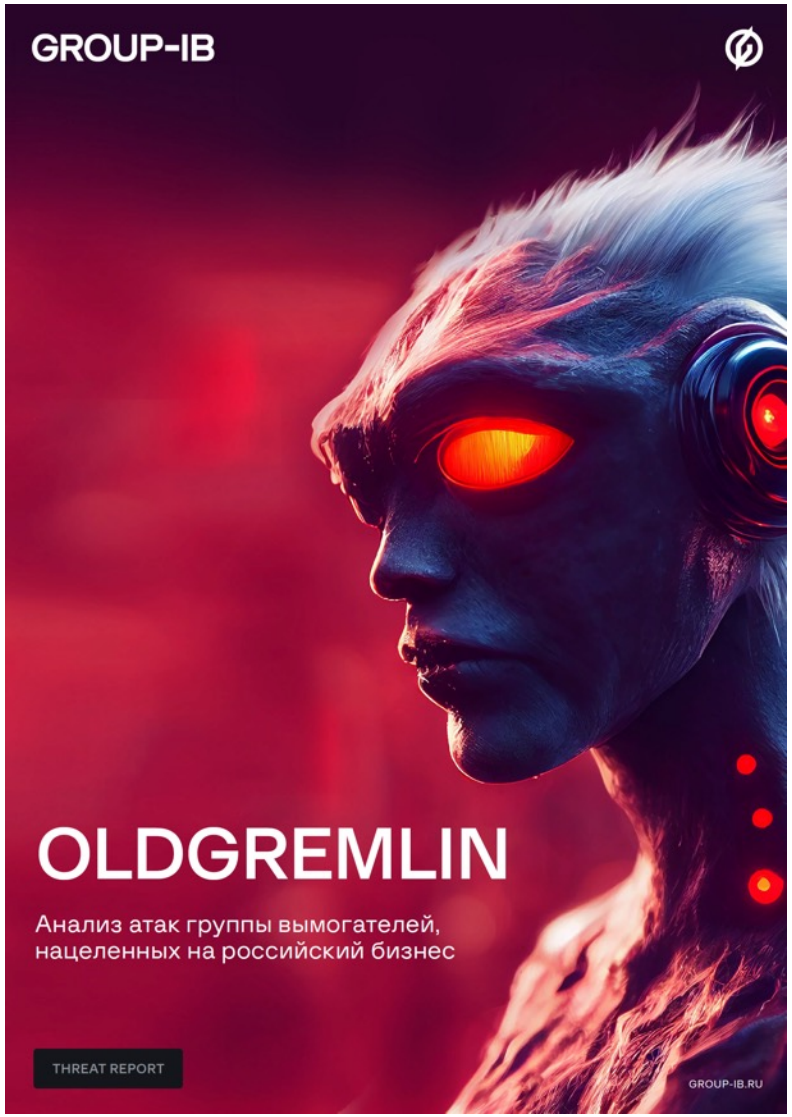
Киберобман

Xello Deception

- Не зависит от предварительных знаний об угрозе (индикаторы компрометации, сигнатуры, правила корреляции)
- Анализирует особенности инфраструктуры отдельной компании и создаёт релевантные ложные данные и активы
- Ориентируется на психологию злоумышленника и теорию вероятности

APT-атаки в 2022 году

xello



positive technologies

Летающие в «облаках»: APT31 вновь использует облачное хранилище, атакуя российские компании

Дата публикации 4 августа 2022

Введение

В апреле 2022 года специалисты PT Expert Security Center в ходе ежедневного мониторинга угроз выявили атаку на ряд российских организаций сферы медиа и ТЭК, в которой использовался вредоносный документ с именем «список.docx», извлекающий из себя вредоносную нагрузку, упакованную VMProtect. Мы проанализировали пакет сетевой коммуникации и выяснили, что он идентичен тому, который мы рассматривали в отчете по исследованию инструментов группировки APT31, что позволило предположить, что и эти инструменты могут принадлежать этой же

BI.ZONE | Eng

Группировка Red Wolf вновь шпионит за коммерческими организациями на территории России

Эксперты BI.ZONE обнаружили новую волну атак группировки Red Wolf (также известна как RedCurl), которая не проявляла себя с 2022 года

Рост количества APT-атак

xello

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

68 %

Успешных атак **в первом квартале 2023** года имели целенаправленный характер

78 %

Успешных атак **во втором квартале 2023** года имели целенаправленный характер

Актуальные киберугрозы: I квартал 2023 года // Positive Technologies
Актуальные киберугрозы: II квартал 2023 года // Positive Technologies

Актуальность

xello

84 минуты

среднее время
проникновения
злоумышленника
в инфраструктуру компании

16 дней

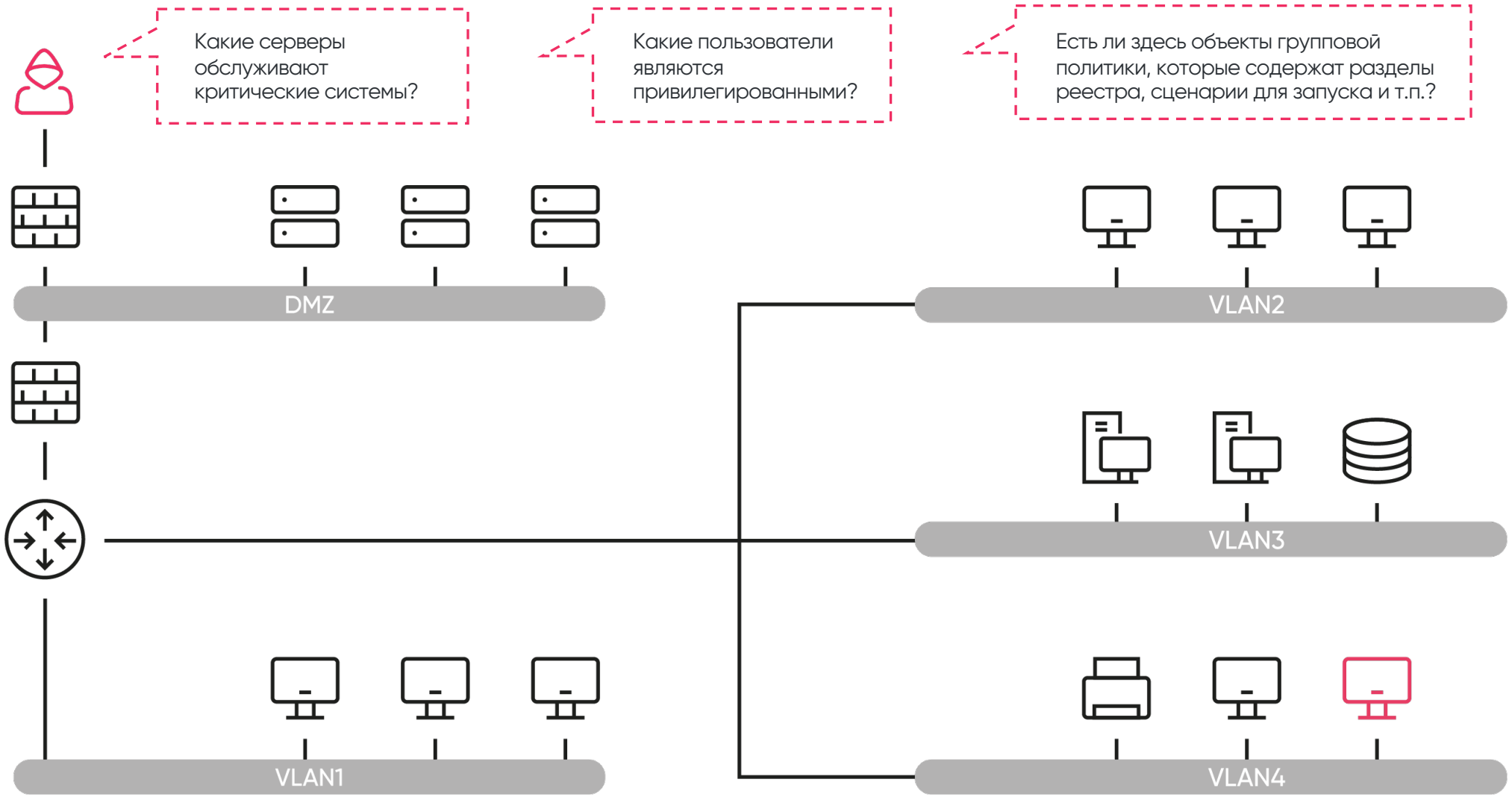
медианное время
незаметного присутствия
злоумышленника
в инфраструктуре

2023 Global Threat Report // CrowdStrike

M-Trends 2023 // Mandiant (Google Cloud)

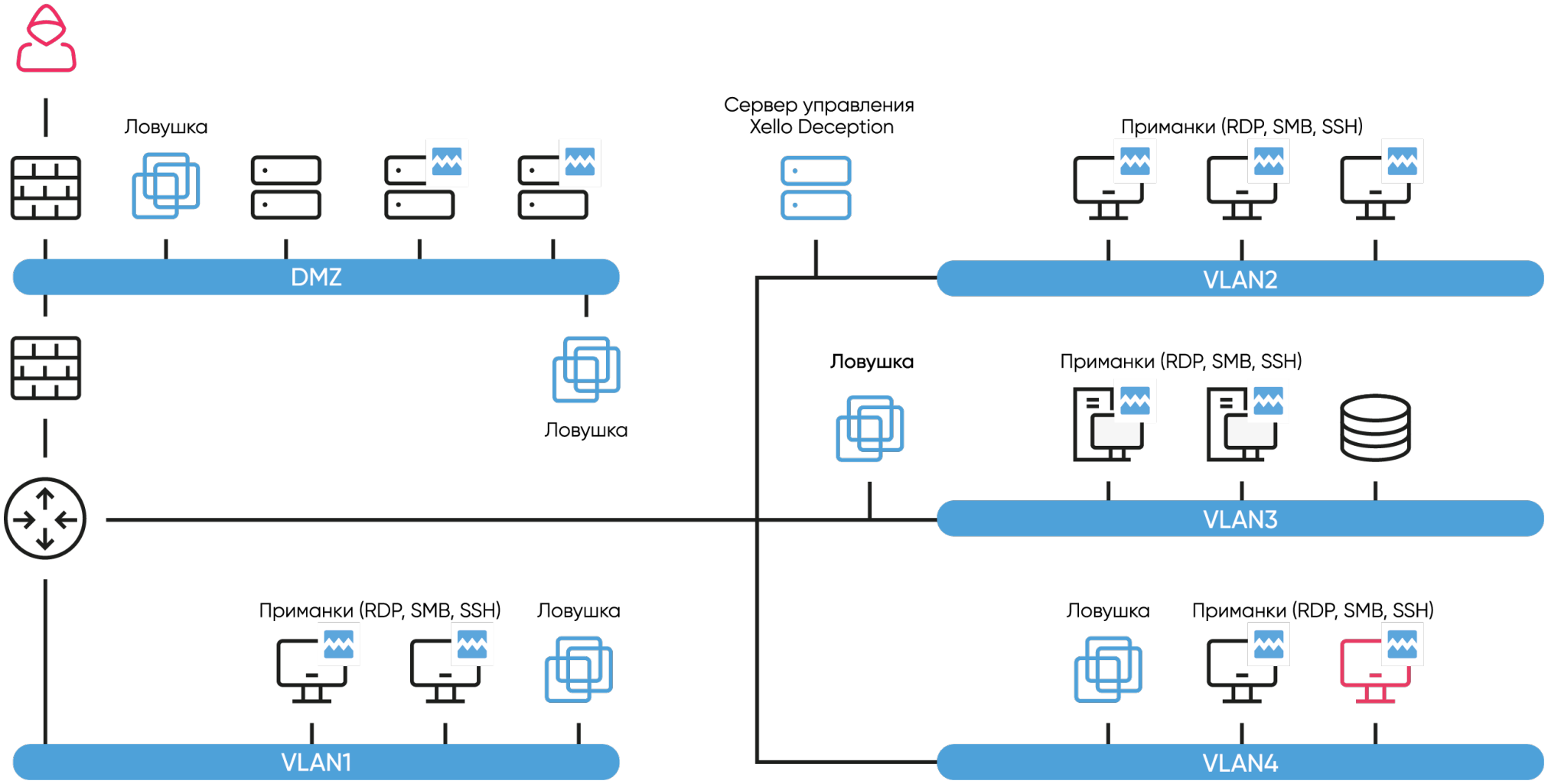
Горизонтальное передвижение — наиболее критический этап атаки

xello



Периметровые средства защиты пропустили хакера и у него появляется возможность использовать легитимные протоколы и учётные записи для дальнейшей реализации кибератаки

Ложный слой данных, который невозможно избежать



Модульная архитектура

xello

1. Xello Lures

Модуль генерации приманок и их распространения на конечные устройства пользователей

2. Xello RealOS Traps

Модуль генерации ловушек и их распространения в сети

NEW

3. Xello Decoy Traps

Модуль гибридной эмуляции (протоколы, сервисы, ОС, устройства)

NEW

4. Xello Trapless

Модуль получения событий аутентификации из внешних систем

NEW

5. Xello Satellites

Модуль управления ложным слоем данных на распределённых площадках

6. Xello Identity Protection*

Модуль цифровой гигиены

*(ранее – Credential Defender)

Модульная архитектура

xello

7. Xello VDI RDS

Модуль распространения приманок в сегменты VDI и RDS

NEW

8. Xello MITM

Модуль выявления MITM-атак («человек посередине», Man-in-the-Middle)

9. Xello API

Модуль для интеграции с внешними системы

2024 г.

10. Xello Industrial

Модуль защиты АСУ ТП с помощью распределённых ловушек

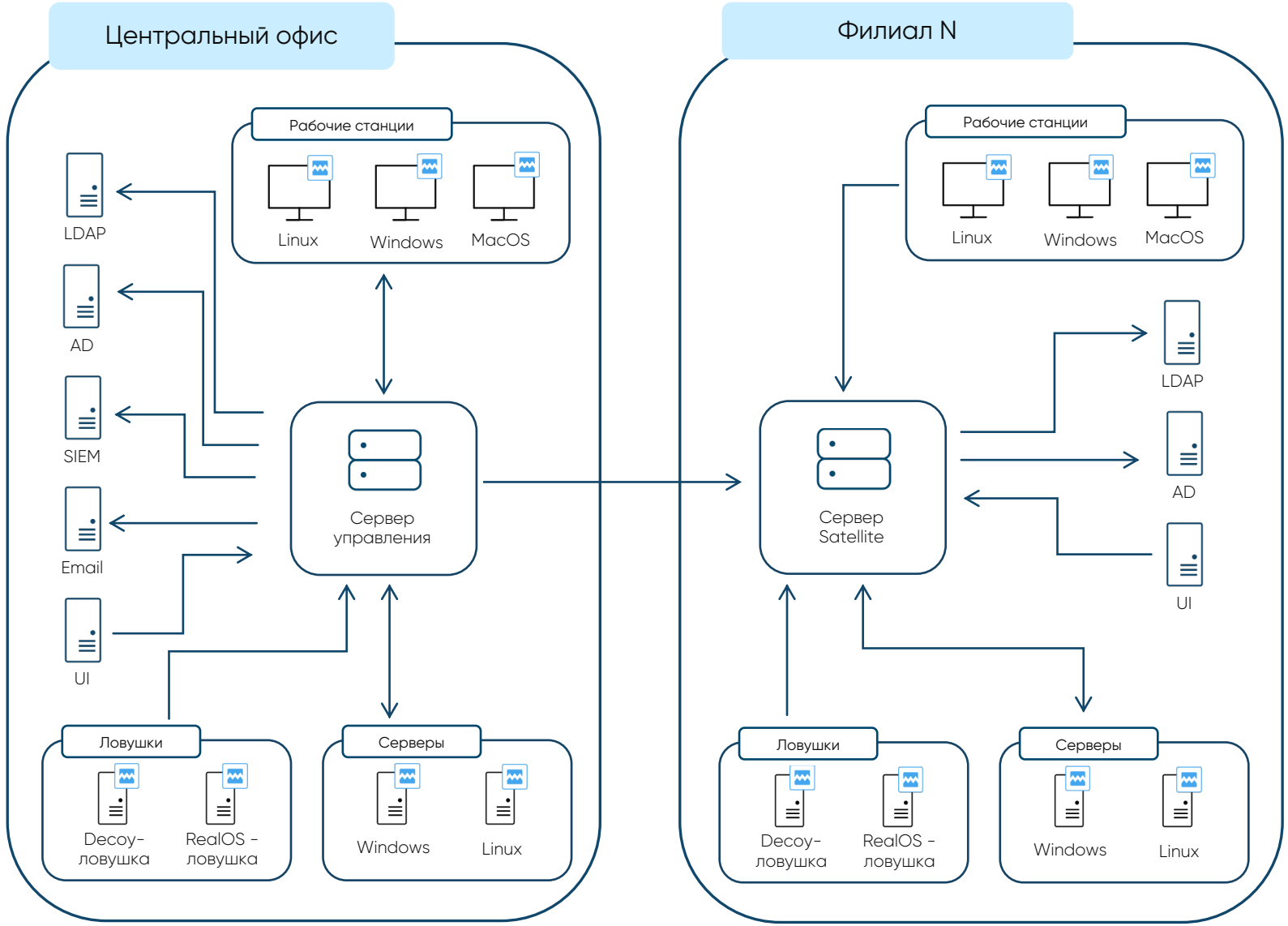
2024 г.

11. Xello HoneyCloud

Модуль эмуляции приманок в облачной инфраструктуре

Xello Satellites

Модуль позволяет централизованно подключать к платформе географически распределённые площадки и гибко управлять ложным слоем данных на них.



Xello Decoy Traps

Модуль позволяет создавать ловушки на уровне протоколов, операционных систем, сервисов и устройств.

ЭМУЛИРУЕМЫЕ АКТИВЫ

Сетевые

- Коммутаторы
- Маршрутизаторы
- Межсетевые экраны (Fortinet, Check Point, Huawei, Cisco)

Рабочие станции и серверы

- Windows OS 7, 8, 10
- Windows Server 2012, 2016
- Debian
- Ubuntu
- CentOS

Специализированные

- Медицинское оборудование
- Финансовые терминалы

Мобильные

- Android 4.4–7.0

Интернет вещей (IoT)

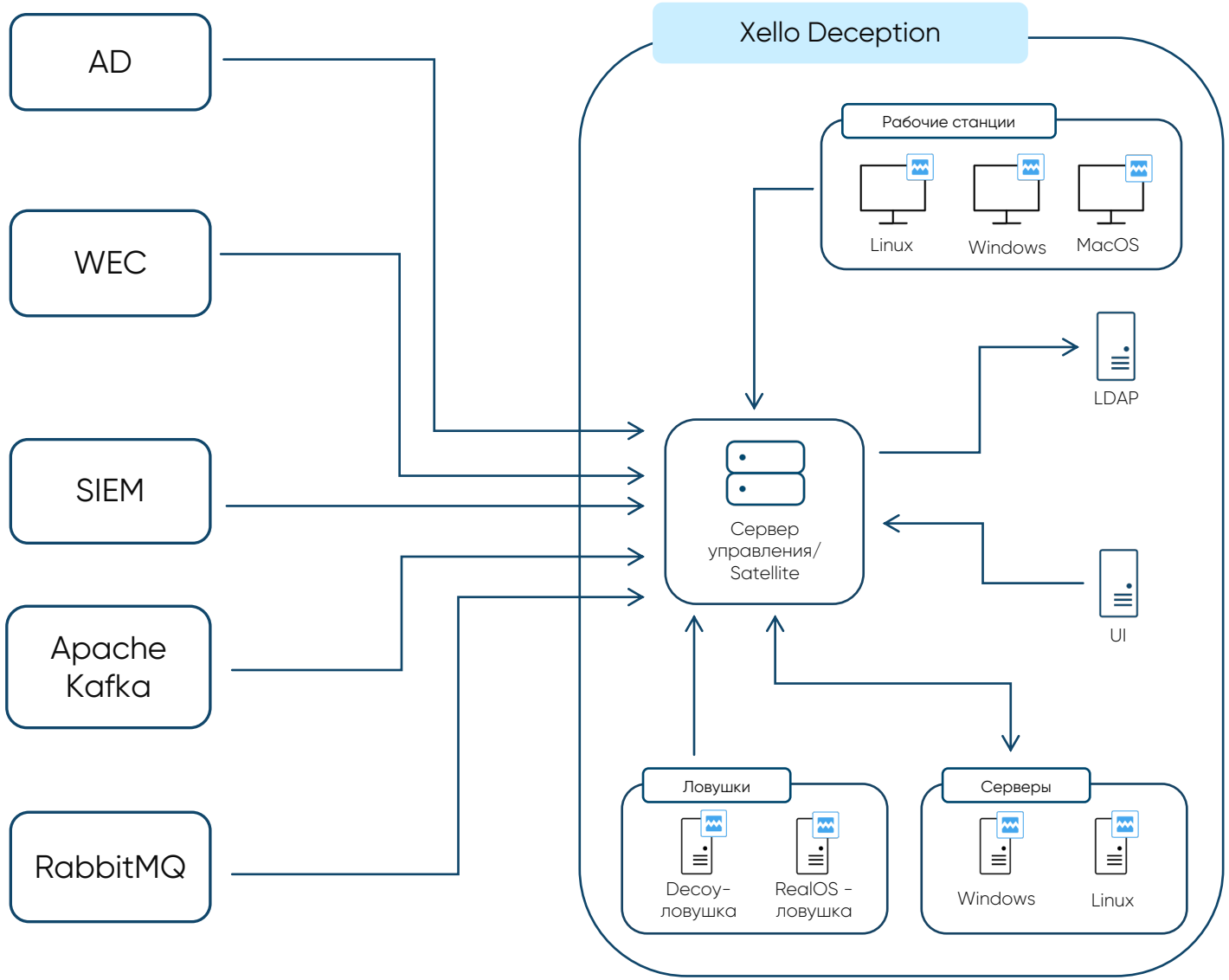
- IP-камеры
- Видеорегистраторы
- Принтеры

Уязвимости в устройствах

Xello Decoy Trapless

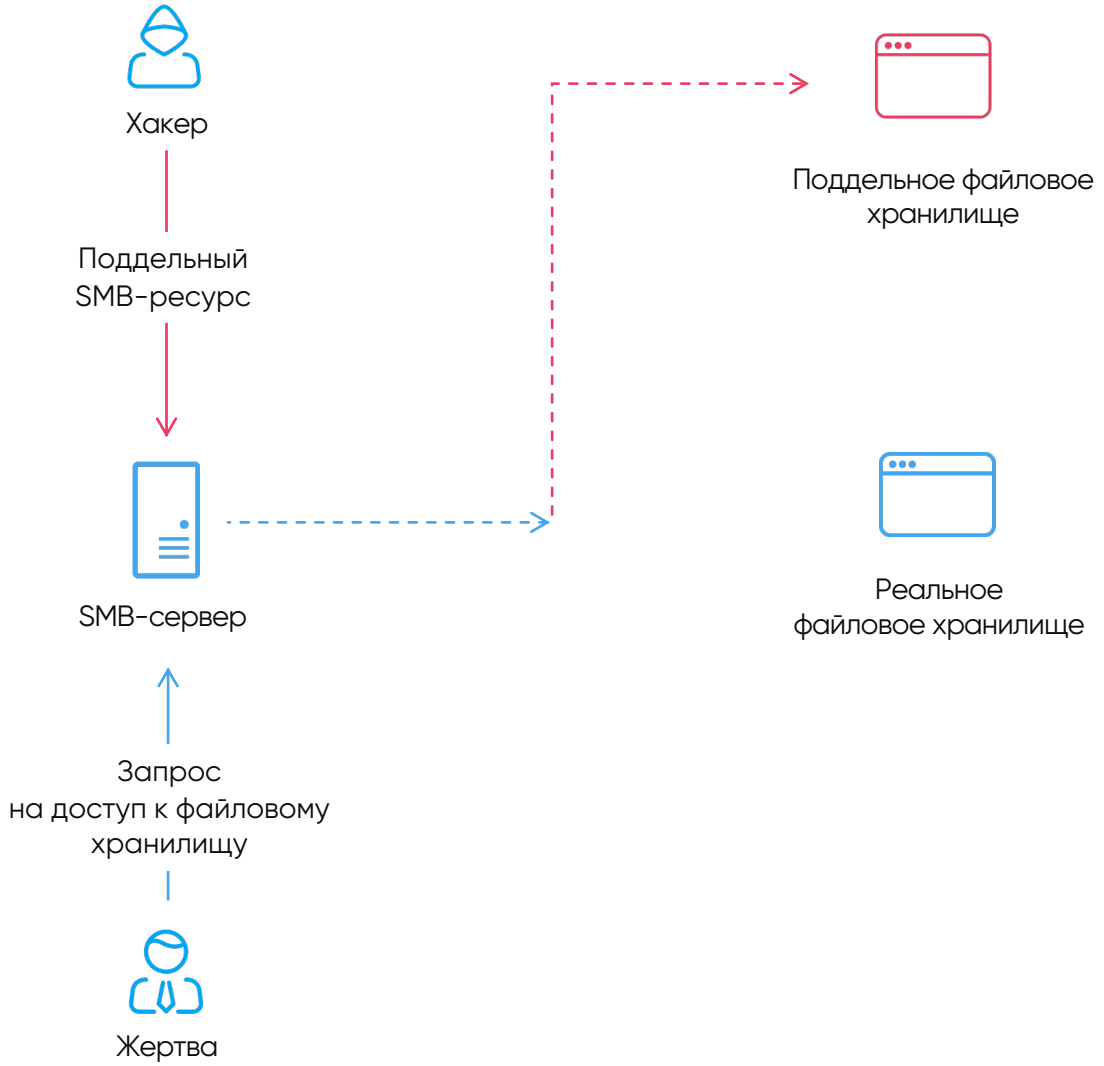
Модуль позволяет подписываться на сообщения из сторонних систем — Apache Kafka, RabbitMQ, SIEM, AD, Windows Event Collector.
И искать события, связанные с ложными активами.

Для интеграции не требуются дополнительные мощности — сервер управления.



Xello MITM

Модуль в режиме реального времени выявляет вредоносную активность, связанную с протоколами LLMNR, mDNS, NBT-NS.



Демонстрация

Условия лицензирования

Параметры ценообразования

Учитывается
количество защищаемых хостов

Срок
1 год или бессрочная лицензия

При истечении лицензии
все продолжает работать,
но отсутствует возможность
добавления новых хостов

Как протестировать бесплатно

Напишите нам: marketing@dialognauka.ru

И мы предоставим тестовый период

1 месяц

длительность тестового периода
без ограничений функциональности

1-2 виртуальных сервера

потребуется для установки Xello Deception

xello

Ответим на ваши вопросы!

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