xello

11.10.2022

Новые возможности для предотвращения APT-атак с Xello Deception

Александр Щетинин

Генеральный директор, Xello

alexander@xello.ru

О компании

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

2018 год

Дата основания

2019 год

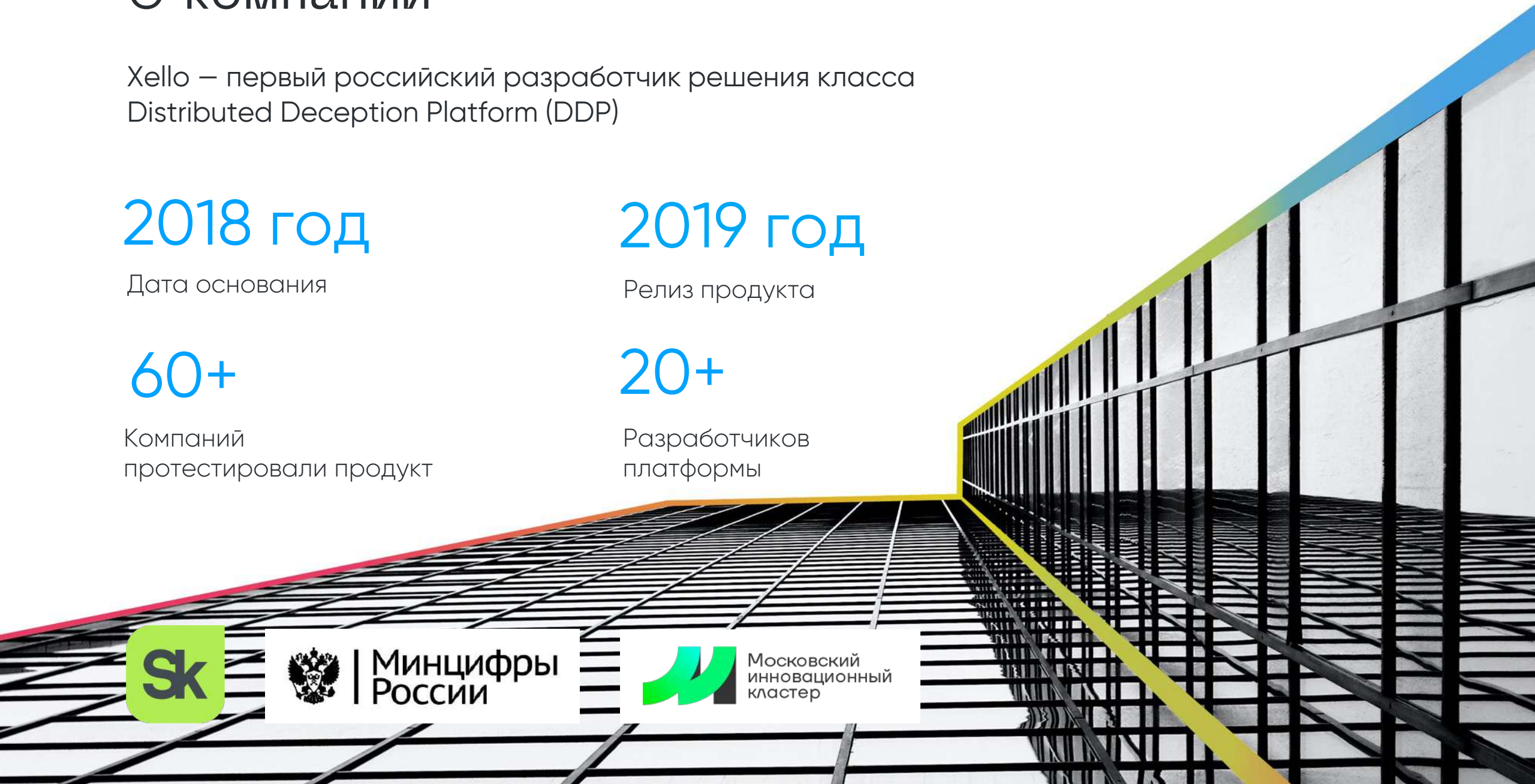
Релиз продукта

60+

Компаний протестировали продукт

20+

Разработчиков платформы



Злоумышленники используют Deception (обман)

- Фишинг
- IP-спуфинг
- Покупка и аренда инфраструктуры (облачные и веб сервисы, домены, DNS)
- Социальная инженерия

APT32 Tactics

In their current campaign, APT32 has leveraged ActiveMime files that employ social engineering methods to entice the victim into enabling macros. Upon execution, the initialized file downloads multiple malicious payloads from remote servers. APT32 actors continue to deliver the malicious attachments via spear-phishing emails.

APT32 actors designed multilingual lure documents which were tailored to specific victims. Although the files had ".doc" file extensions, the recovered phishing lures were ActiveMime ".mht" web page archives that contained text and images. These files were likely created by exporting Word documents into single file web pages.

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

Дата публикации 4 августа 2022

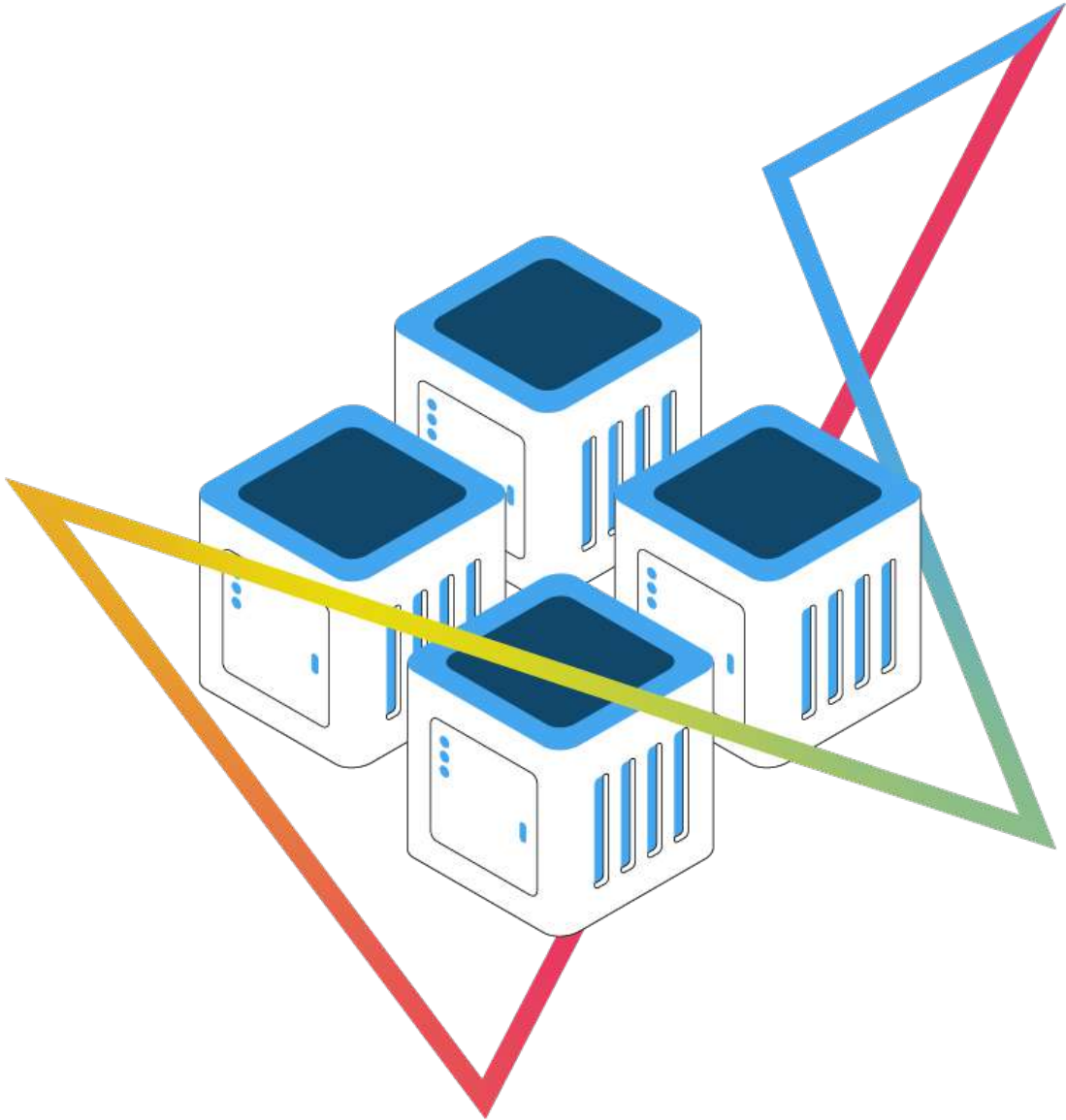
Our initial discovery was a scheduled task, masquerading with the name `GoogleUpdater` that ran a VBScript script `qwert.vbs`. This is a commonly used technique (MITRE ATT&CK T1035.005) to blend in and avoid detection by sounding like something legitimate—in this case, Google. Using a legitimate file (`wscript.exe`) to run the malicious script further helps to avoid detection that is based on scanning of the binary that is running.

Это позволяет обходить «классические» СЗИ

- Антивирус
- IPS/IDS
- SIEM-система
- Next generation firewall (NGFW)
- Песочница (Sandbox)
- Решения класса network traffic analysis (NTA)
- Web application firewall (WAF)
- DLP-система
- Решения класса endpoint detection and response (EDR)

21 день

медианное время незаметного присутствия злоумышленника в инфраструктуре



Последние инциденты

Бизнес, 28 мар, 23:59 | 23 529 | Поделиться

Росавиация из-за возможной кибератаки перешла на бумажный документооборот

Возможная кибератака на системы Росавиации привела к сбою электронного документооборота и потере документов в электронном виде, сообщили источники РБК. Глава ведомства Александр Нерадько заявил, что документооборот в порядке

«Объединённая Авиастроительная Корпорация» подверглась «шпионской» кибератаке 66.9 т

Коммерсантъ

15.03.2022, 18:29 обновлено 21:22

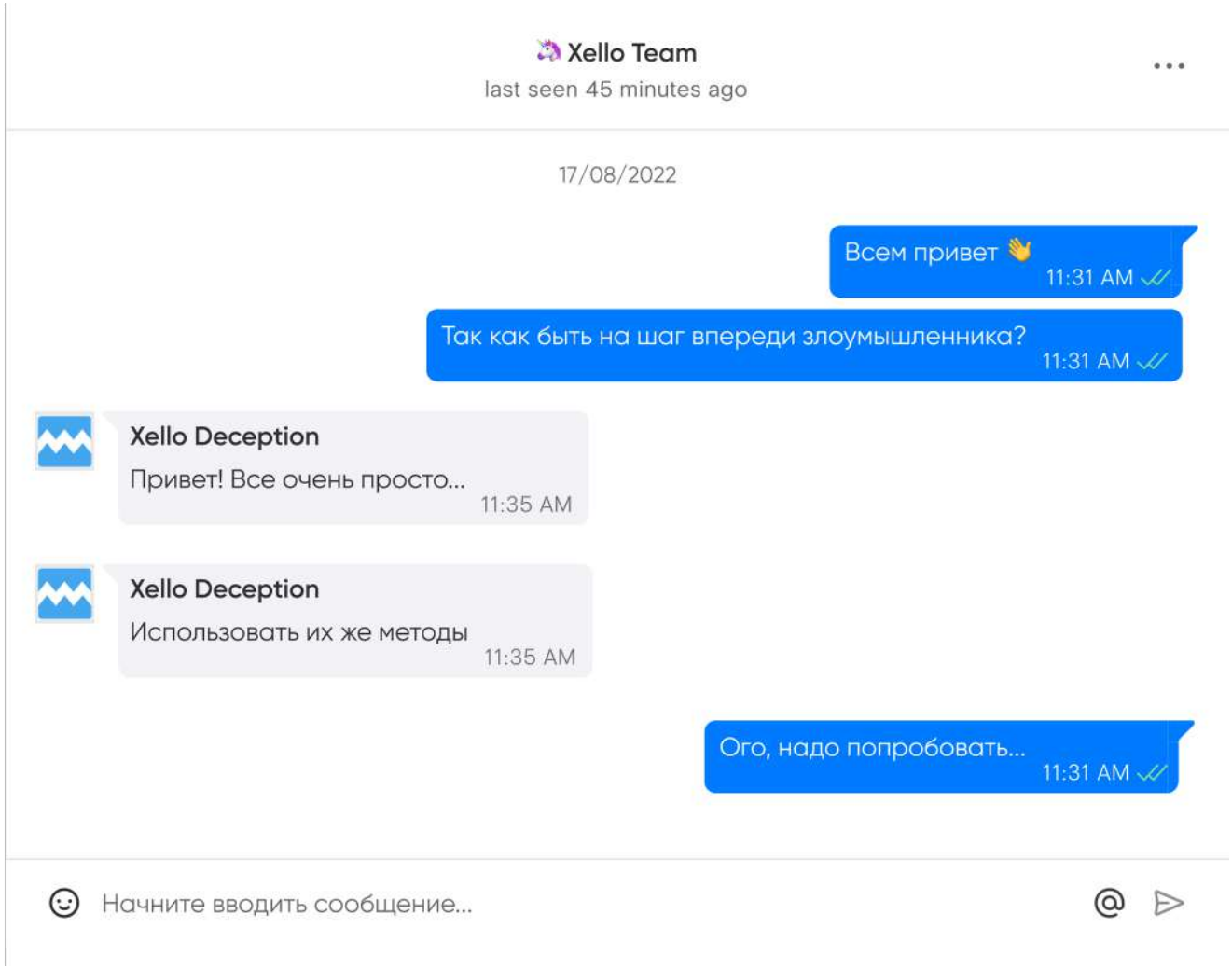
Хакеры пошли за покупками

Wildberries подвергся масштабной атаке

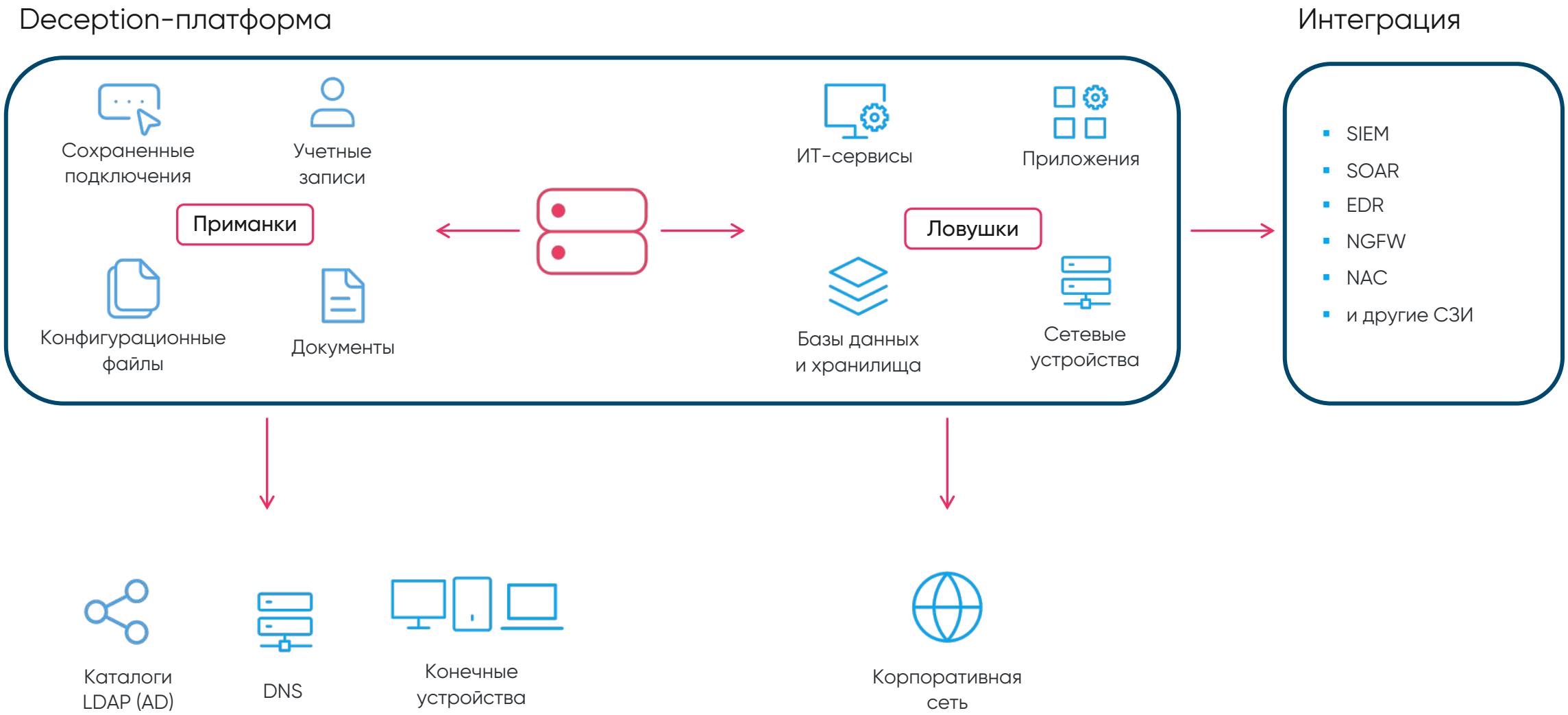
В работе маркетплейса Wildberries второй день наблюдаются проблемы: около половины пользователей заявляют о сложностях с доступом в приложение и с отслеживанием заказов. В самой компании заверяют, что более 70% ошибок исправлены, заказы выдаются, персональные данные не пострадали. По мнению экспертов, маркетплейс стал жертвой атаки вируса-шифровальщика, в подготовке которой могли участвовать сотрудники Wildberries.

Как быть на шаг впереди?

– Использовать киберобман на своей стороне



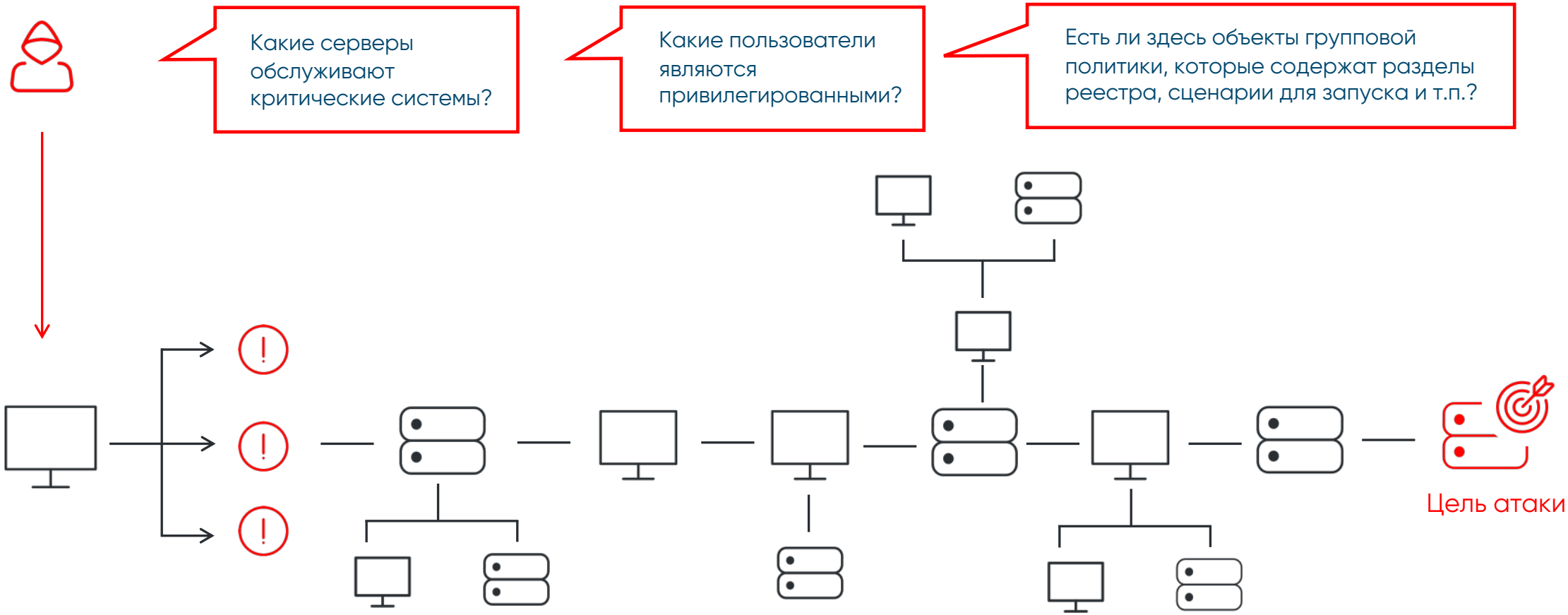
Как это работает



Место DDP-систем при APT-атаке

Горизонтальное передвижение

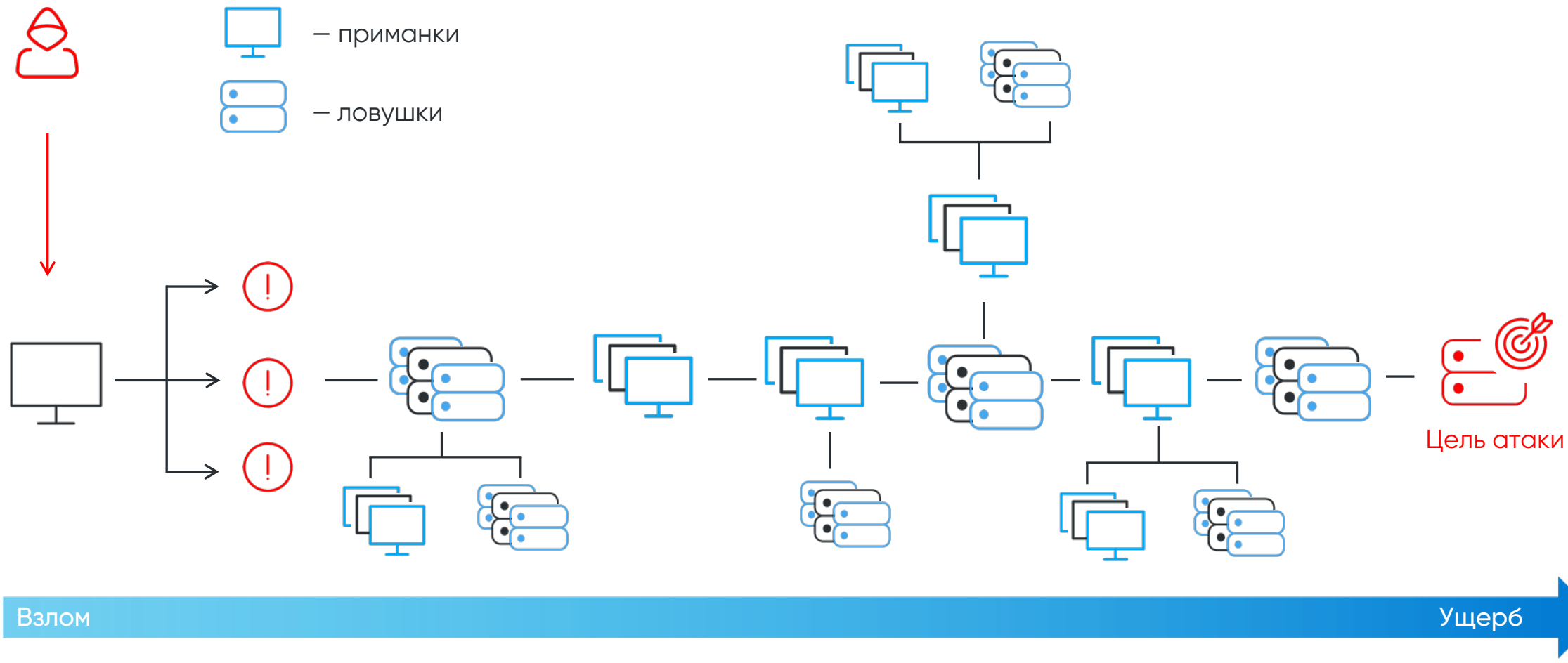
Наиболее критический этап атаки



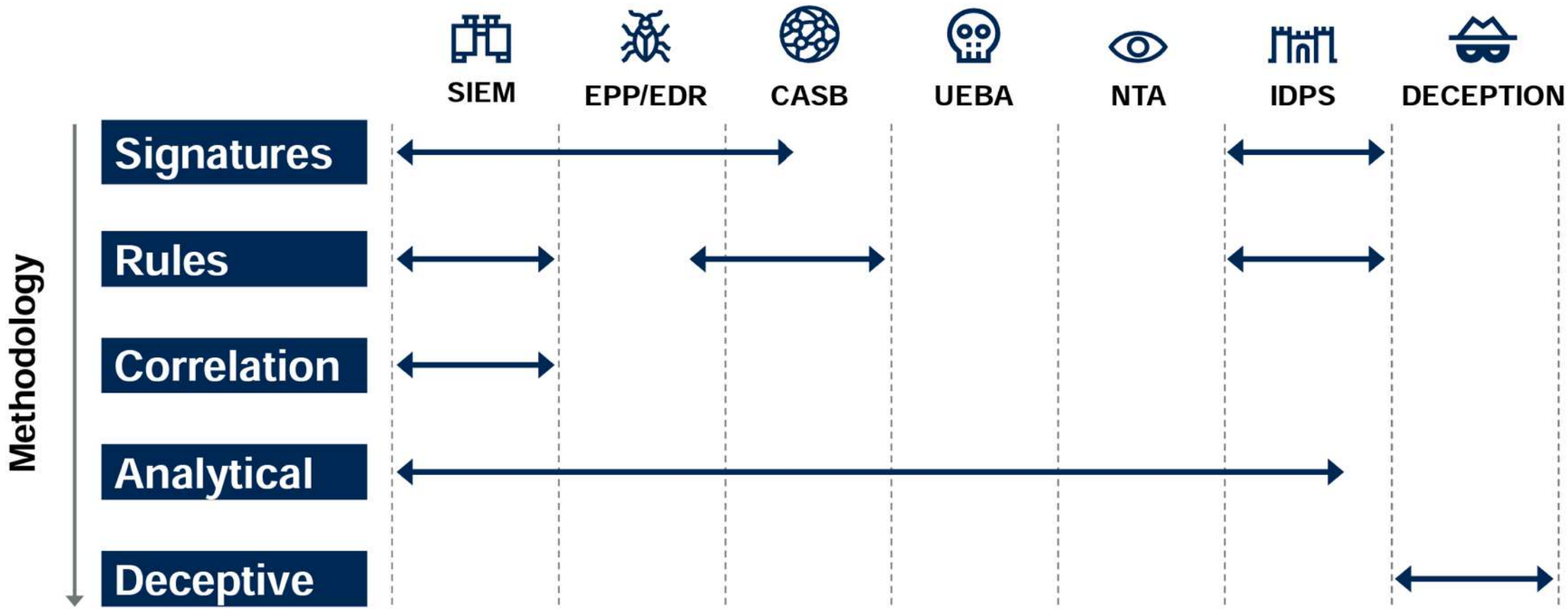
Взлом → Ущерб

Горизонтальное передвижение

Распределенные приманки и ловушки создают ложный слой инфраструктуры, который невозможно избежать



Deception — другой подход выявления киберугроз



Gartner

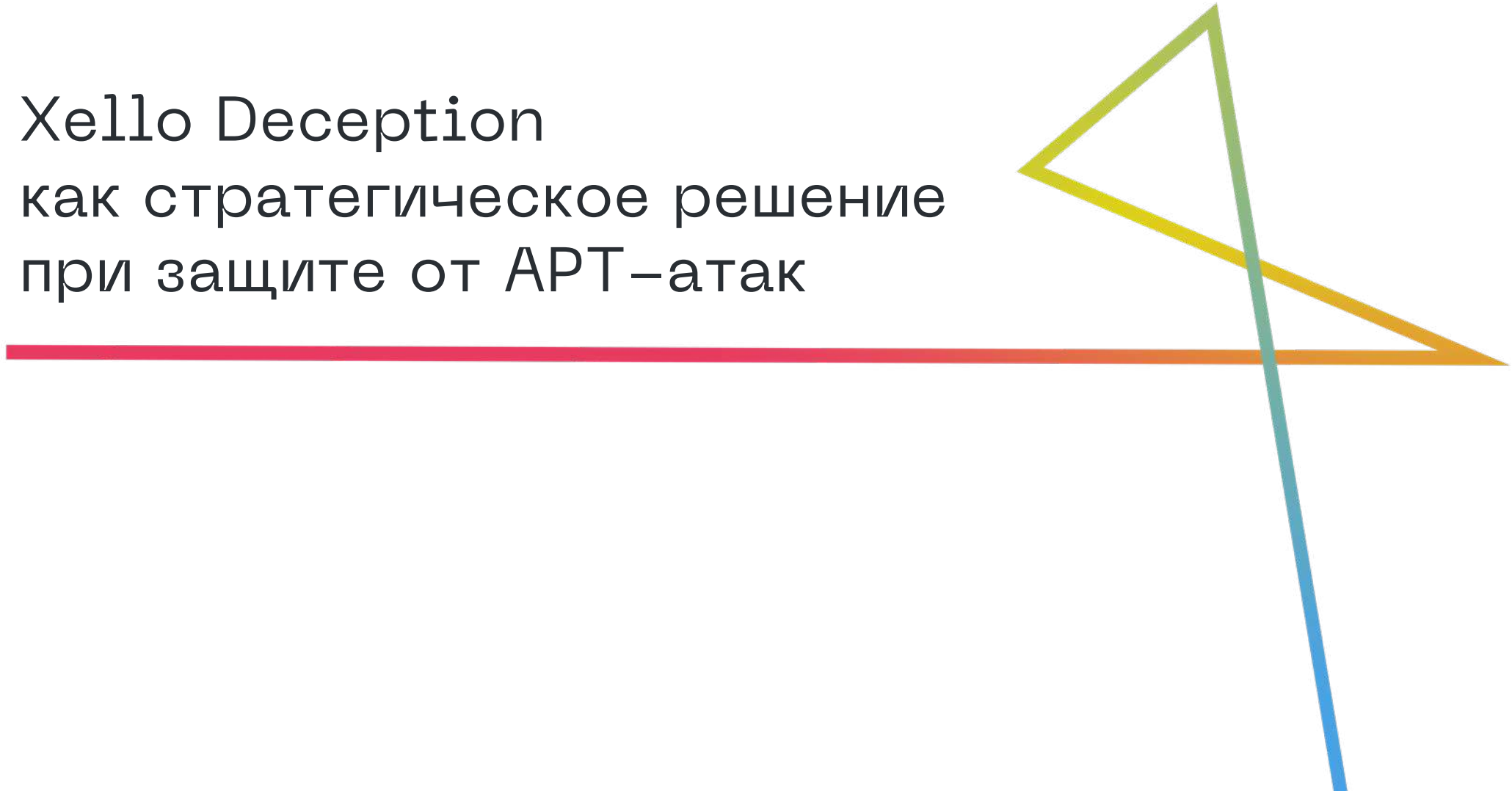
Особенности технологии

Не зависит
от предварительных
знаний о конкретной
кибератаке
или злоумышленнике
(не использует
IoC/IoA/сигнатуры/
эвристику и т.д)

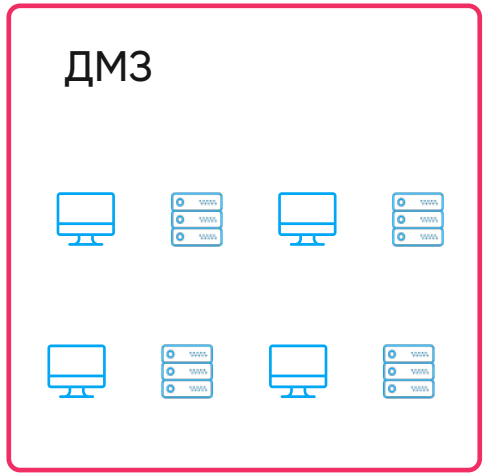
Невозможно
отключить или обойти

Минимальное количество
ложных срабатываний

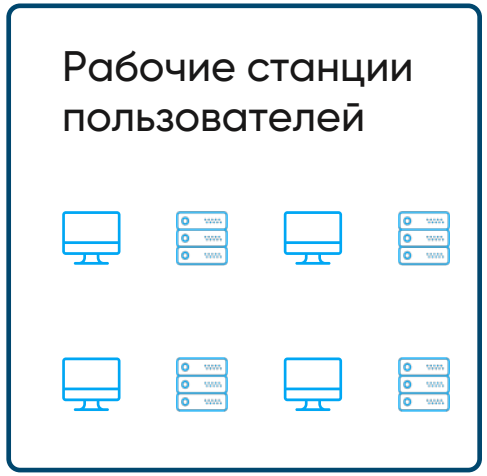
Xello Deception
как стратегическое решение при защите от APT-атак



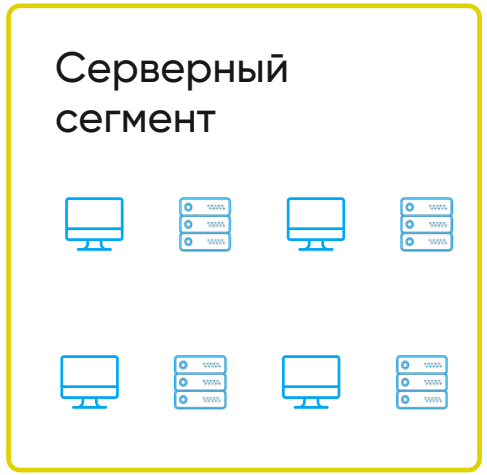
Где размещают ложную инфраструктуру?



Область
высоких рисков



Отправная точка
APT-атаки



Ядро
инфраструктуры

Опора
бизнеса

Как работает платформа?

Решаемые задачи

Стратегический уровень

- Повышение эффективности существующих систем защиты – NGFW, EDR, Sandbox, SIEM и другие
- 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 счет минимизации количества ложных срабатываний

Ключевые преимущества

1. Адаптивная генерация приманок

2. Первая Deception-платформа в мире, поддерживающая VDI

3. Не создает дополнительной нагрузки на инфраструктуру – безагентский способ распространения приманок

4. Простое внедрение и отсутствие необходимости в квалифицированных специалистах для дальнейшей эксплуатации

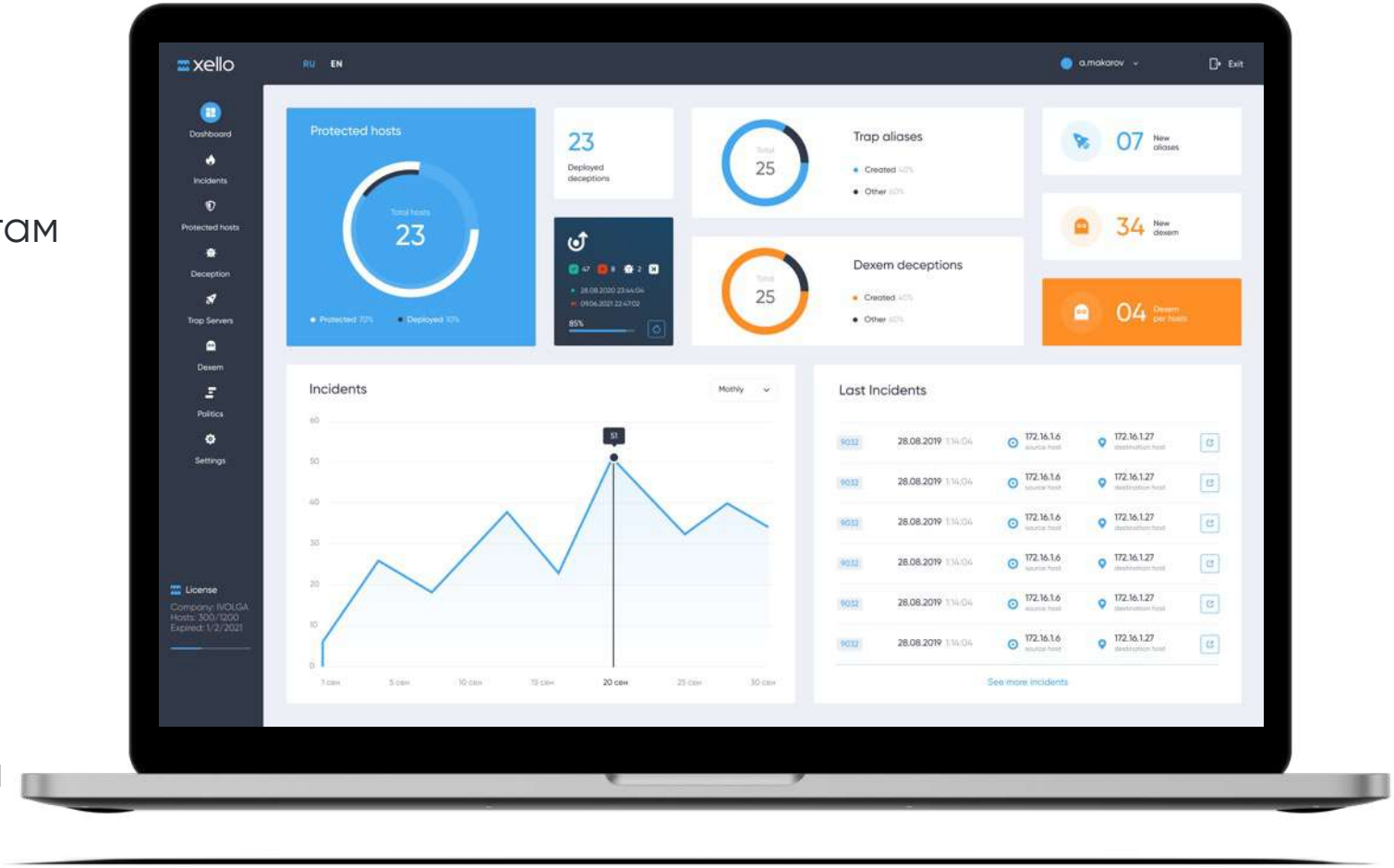
5. Учитывает особенности архитектуры

6. Открытый API для интеграции с различными средствами защиты

Единая консоль управления

Возможности

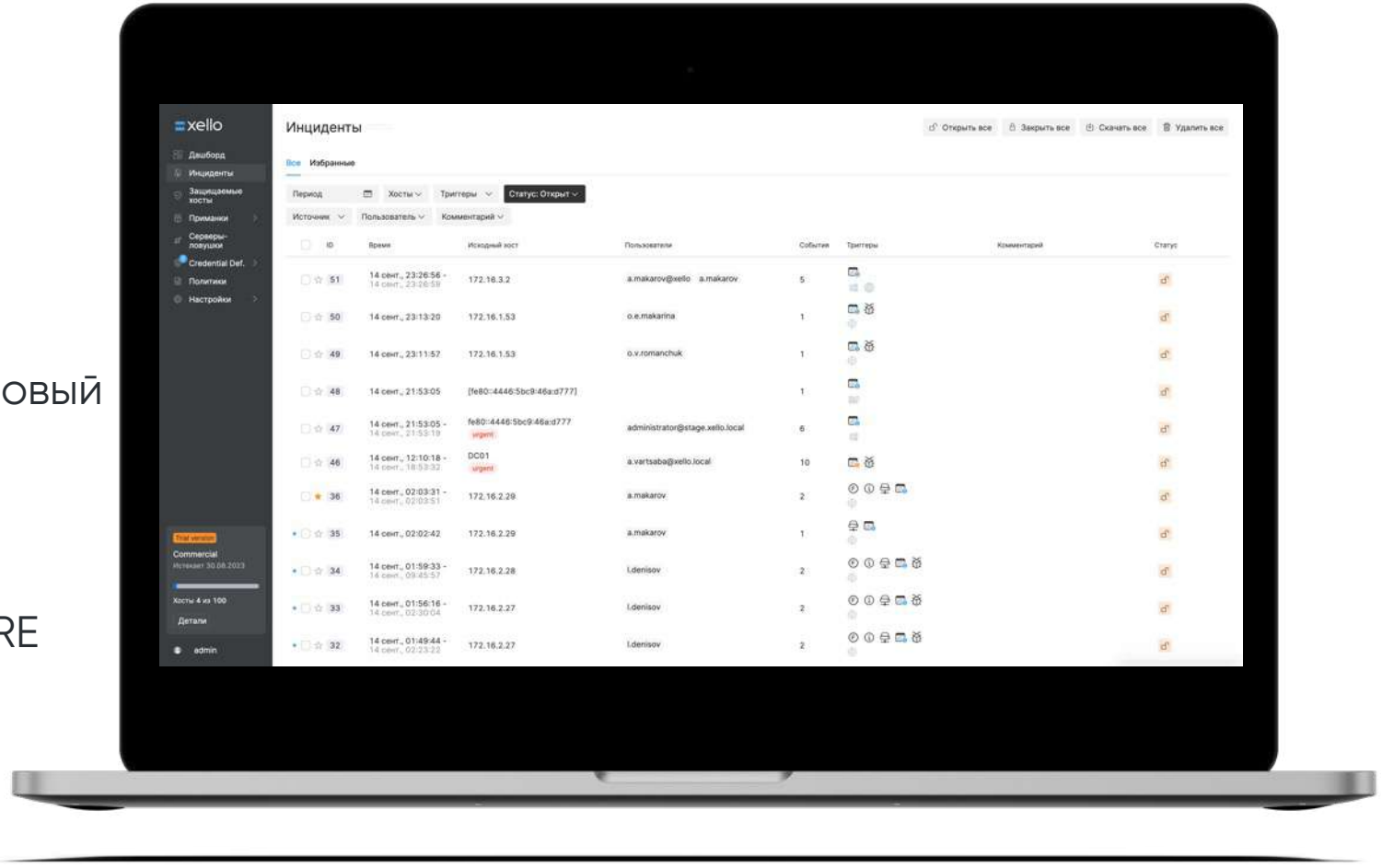
- Управление ложным слоем
- Генерация приманок и распространение их по хостам
- Настройка политик защиты
- Очистка кэшированных паролей и учетных данных с помощью модуля Credential Defender
- Мониторинг и анализ инцидентов безопасности
- Хранение данных форензики
- И другие



Новая версия

Что будет:

- Новые возможности встраиваемости — гибкая интеграция в внешними сервисами и внутренней инфраструктурой.
- Улучшенное юзабилити — новый удобный интерфейс.
- Работа с инциденты — таймлайн событий внутри инцидента, маппинг на MITRE ATT&CK и другие



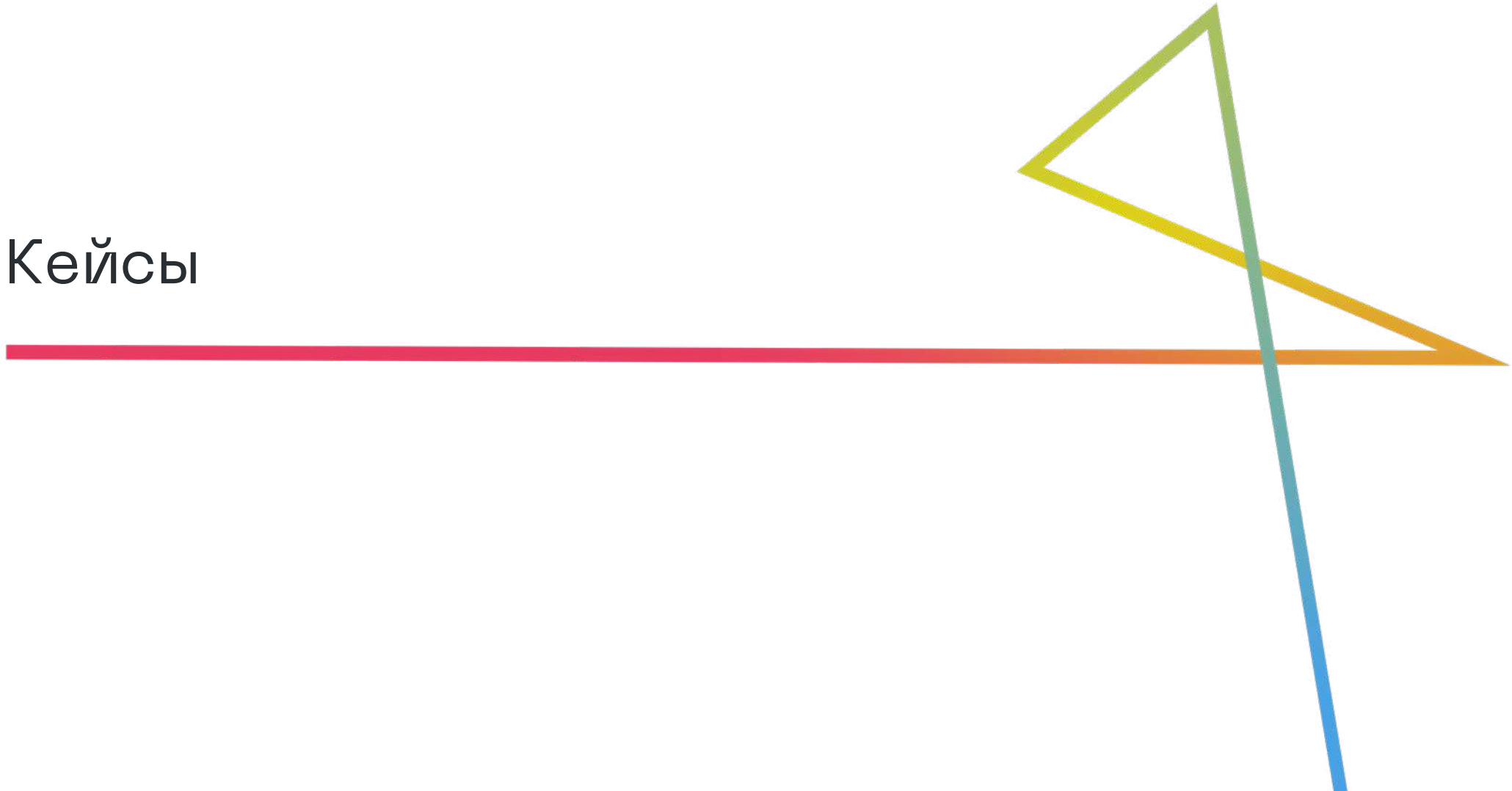
Зарегистрируйтесь
и получите ссылку
на онлайн-трансляцию.

Чтобы увидеть
все возможности новой
версии платформы.

18 октября 14:00

promo.xello.ru

Кейсы



Кейс 1

Несогласованный пентест компании

- Промышленность
- 2000+ хостов
- ДЗО холдинга из ТОП-5
- Единый домен холдинга

Задача

Выявление неправомерных действий
с информационными активами компании

Решение

Платформа Xello Deception позволила выявить несогласованный пентест от другого дочернего общества, когда существующие средства защиты не смогли выявить его.

Кейс 2

Выявление реальных событий безопасности и их расследование

- Банк
- 10 000 хостов
- 20 филиалов
- Большой сегмент VDI

Задача

Повысить эффективность работы специалистов SOCa, т.к. огромный поток алертов значительно увеличивает нагрузку. Кроме того, на выявление реальных инцидентов уходит большой объем трудозатрат.

Решение

Платформа Xello Deception позволила добавить в корреляцию высокодоверенный индикатор компрометации учетных данных, тем самым сократить количество алертов.

Как протестировать бесплатно

Напишите нам: sales@xello.ru

И мы предоставим тестовый период

1 месяц

длительность тестового периода
без ограничений функциональности

1-2 виртуальных сервера

потребуется для установки Xello Deception

Ответим
на ваши вопросы!

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