xello

Повышение эффективности SOC с помощью Xello Deception

Xello Deception позволяет выявлять нелегитимные действия злоумышленника в корпоративной сети и предотвращать целевые атаки. Платформа повышает эффективность и качество процессов мониторинга киберинцидентов и реагирования на них.

более

11 000

алертов ежедневно в среднем обрабатывают внутренние службы кибербезопасности*

ВОЗМОЖНОСТИ ДЛЯ SOC

Выявление киберугроз на ранних стадиях

- Предоставляет сведения о вредоносной активности в корпоративной сети, которая может быть невидима для других средств защиты

Снижение количества ложных срабатываний

- Оповещает только о подозрительных или вредоносных действиях в сети

Автоматизация процесса реагирования

- Предоставляет надёжные триггеры, которые позволяют автоматизировать процесс реагирования на киберинциденты
- Блокирует действия злоумышленника при интеграции с другими системами кибербезопасности

Расследование киберинцидентов

- Собирает и хранит данные форензики: техники и тактики, инструменты и методы, применяемые при реализации кибератаки
- Коррелирует разрозненные события в единую цепочку атаки

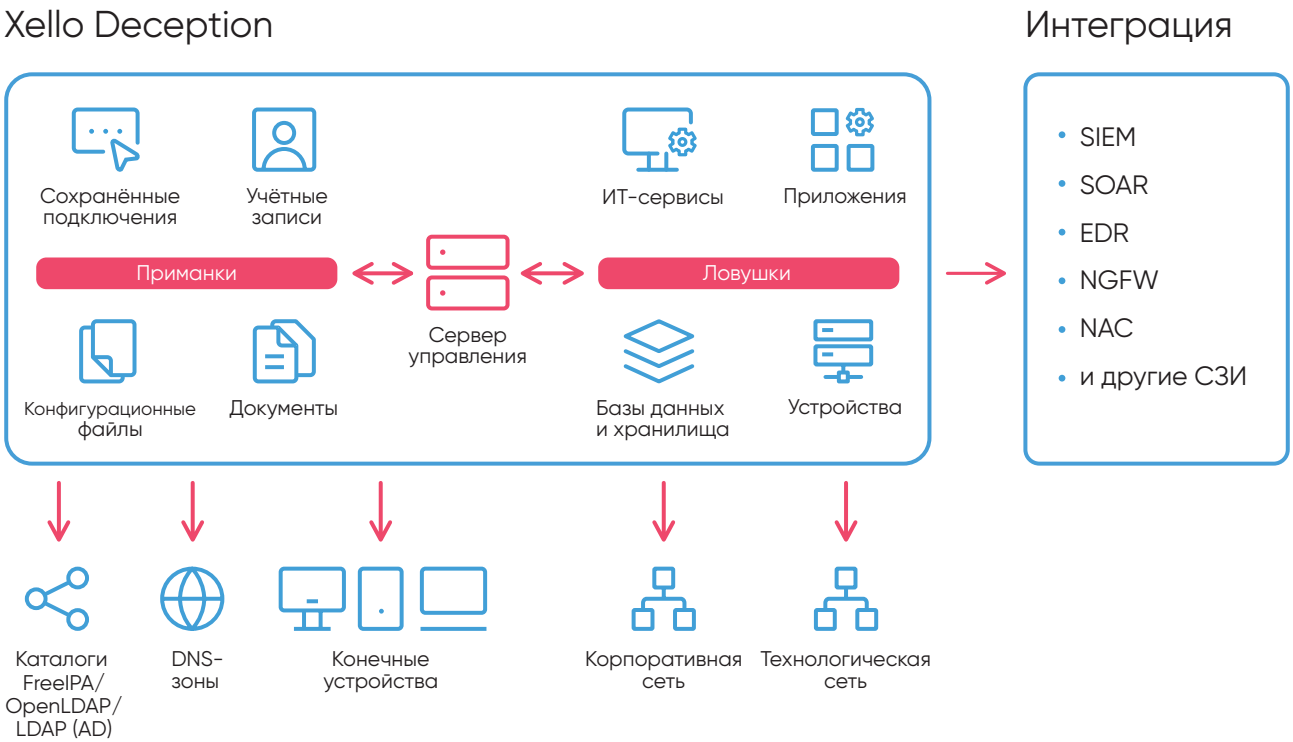
*The 2020 State of Security Operations // Forrester

СХЕМА РАБОТЫ XELLO DECEPTION

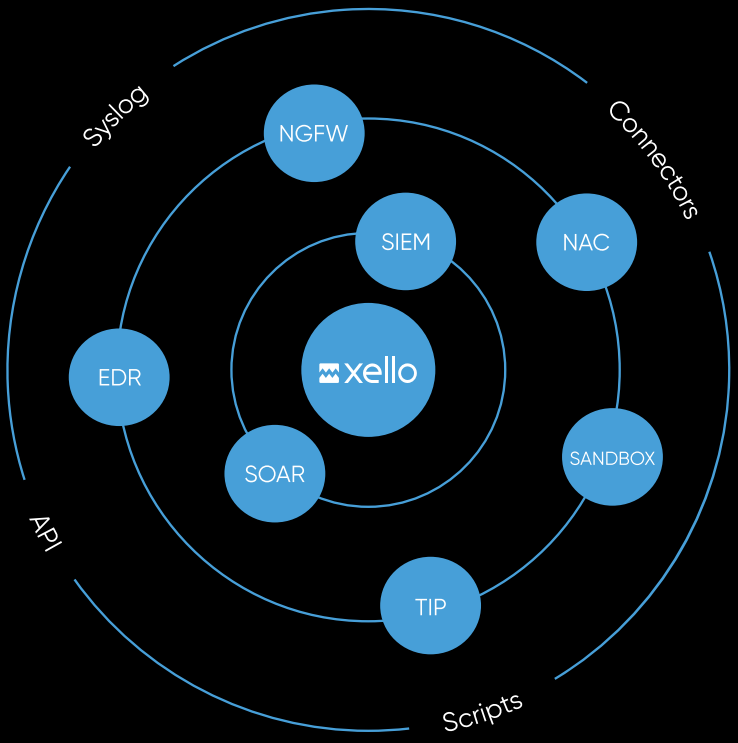
Xello Deception создаёт инфраструктуру из ложных информационных активов и данных (серверов, учётных записей, конфигурационных файлов, сетевых устройств, ИТ-сервисов) с помощью приманок и ловушек.

Если конечная точка попытается получить доступ к ним, то с большой вероятностью она скомпрометирована, поскольку для такой деятельности нет легитимных бизнес-процессов. Приманки и ловушки направлены исключительно на злоумышленника.

СХЕМА РАБОТЫ



ПРОСТАЯ ИНТЕГРАЦИЯ С СИСТЕМАМИ КИБЕРБЕЗОПАСНОСТИ



- **Инсталляция занимает от нескольких дней до двух недель**
- **Внедрение не требует значительных вычислительных ресурсов**
- **Безагентный способ распространения не создаёт дополнительной нагрузки на инфраструктуру**

Если вы используете нестандартную систему, подключение к ней мы возьмём на себя

ВОЗМОЖНЫЕ СЦЕНАРИИ

DECEPTION + SIEM

- Оперативные оповещения о взломанных машинах в SIEM
- Автоматический поиск заражённых систем с помощью настроенных политик
- Автоматизация процесса реагирования при помощи надёжных алертов от системы

DECEPTION + NGFW

- Возможность отправки запросов на блокировку или карантин заражённых конечных устройств
- Ручное и автоматическое управление

DECEPTION + EDR

- Блокировка и отправка заражённых конечных устройств в карантин
- Автоматическое реагирование на инциденты с помощью политик изоляции

DECEPTION + SANDBOX

- Отправка подозрительных исполняемых файлов в песочницу для анализа
- Формирование отчётов по итогам анализа вредоносных программ с информацией об индикаторах компрометации

DECEPTION + NAC

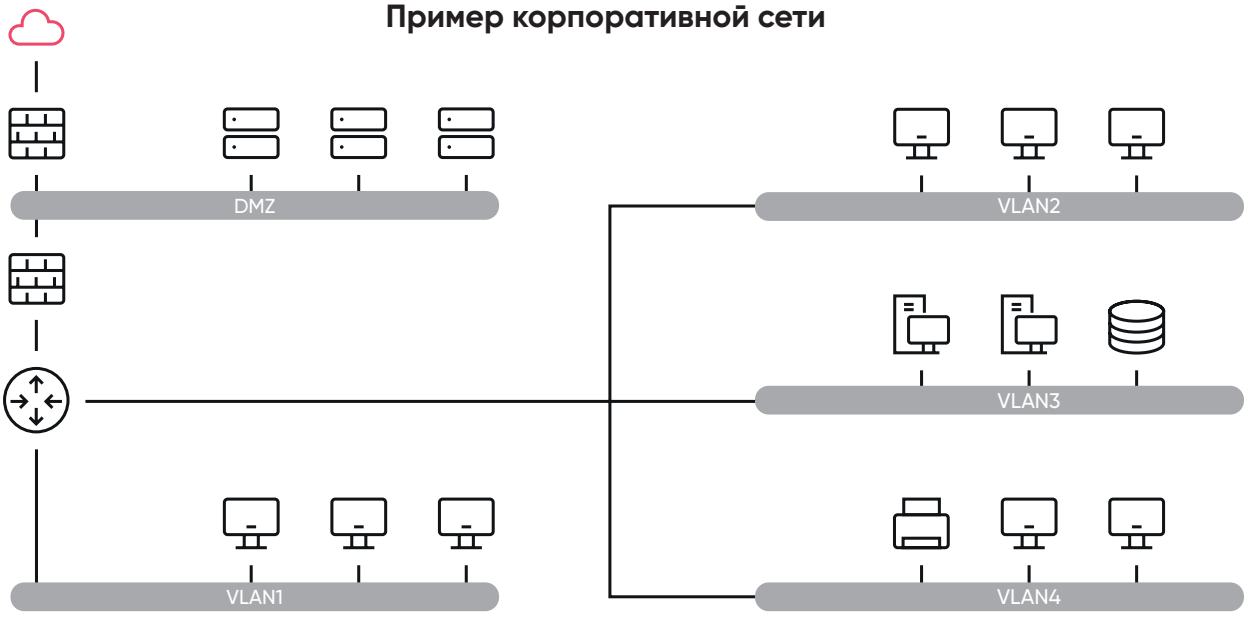
- Отправка вредоносных активностей в NAC-систему для внесения в чёрный список
- Удобное извлечение данных о вредоносных активах и действиях через единую консоль управления

ЗАЩИТА ОТ ЦЕЛЕВЫХ АТАК

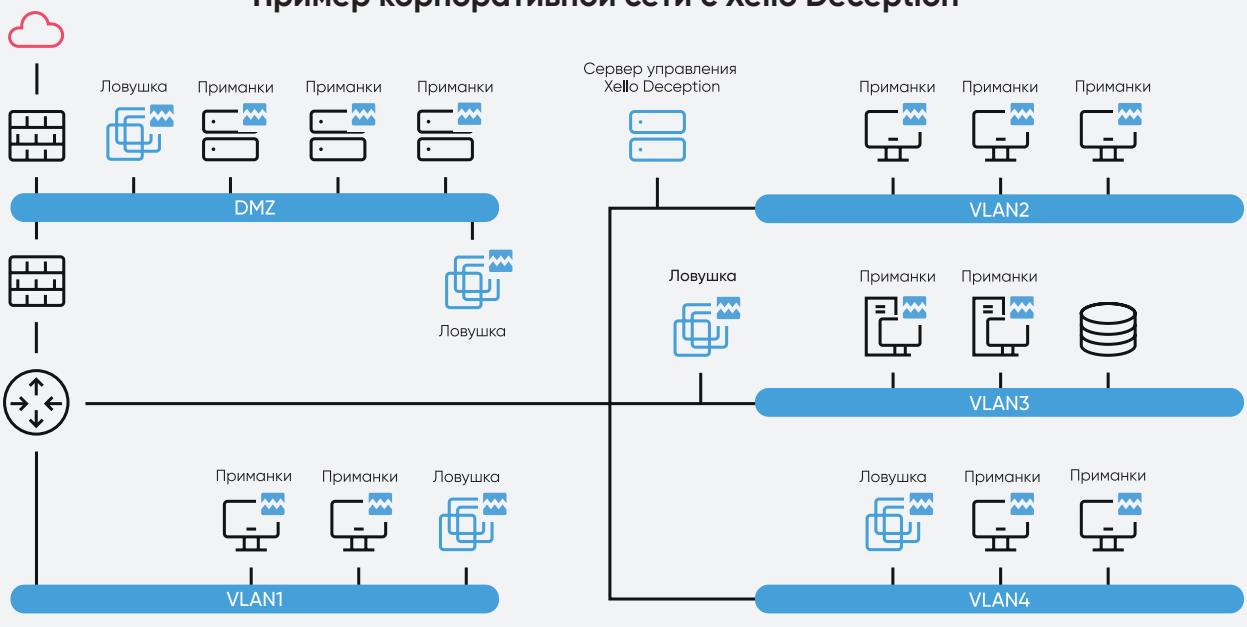
Сегодня, в условиях размытого периметра, уязвимостей в Open Source-компонентах, а также неограниченных возможностей использования методов социальной инженерии, получение первичного доступа к инфраструктуре компании — вопрос времени.

Xello Deception позволяет детектировать нелегитимные действия злоумышленника даже на самом критическом этапе атаки — горизонтальном передвижении (lateral movement), создавая инфраструктуру из ложных активов и данных по всей сети компании.

Пример корпоративной сети



Пример корпоративной сети с Xello Deception



xello

Разработчик первой российской платформы киберобмана

ПРОТЕСТИРУЙТЕ XELLO DECEPTION БЕСПЛАТНО

Оцените возможности платформы, заполнив заявку на сайте или написав нам на почту: sales@xello.ru

+7 (495) 842-90-90
info@xello.ru