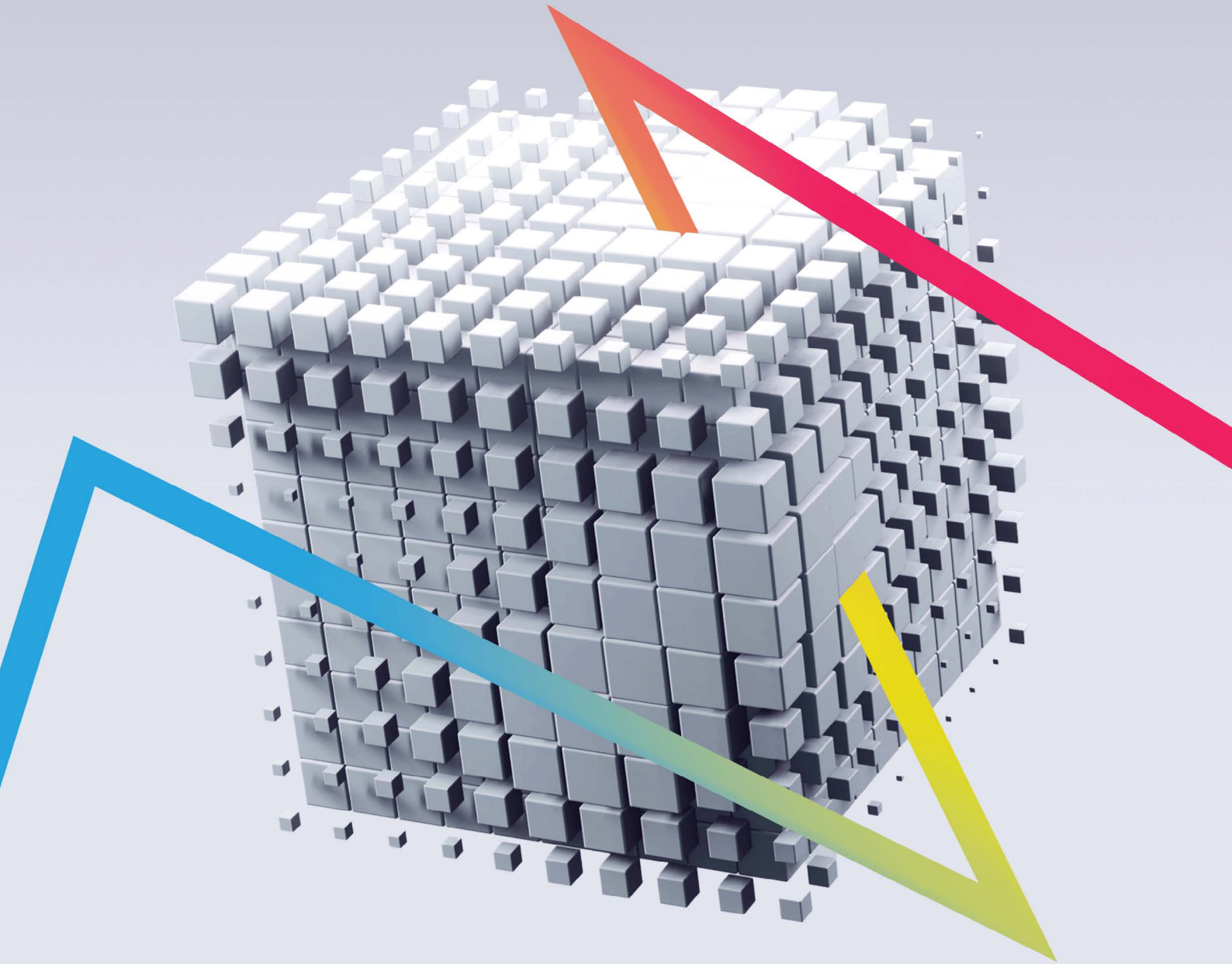
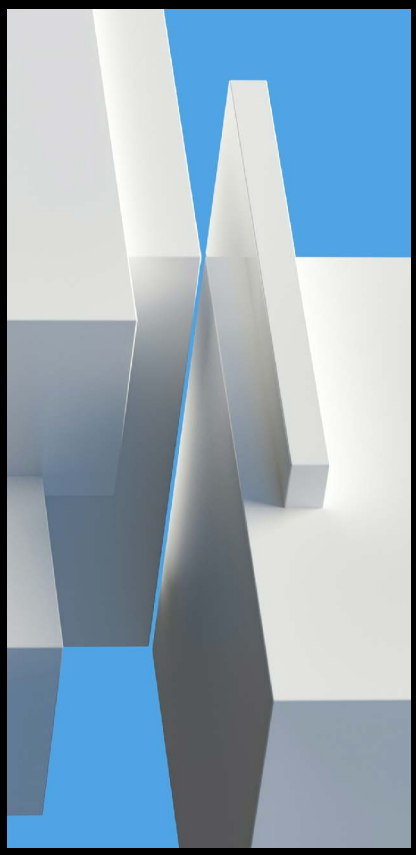
xello

Xello Deception: платформа для предотвращения целевых атак с помощью технологии киберобмана



ПРОНИКНОВЕНИЕ ЗЛОУМЫШЛЕННИКА В ИНФРАСТРУКТУРУ — ВОПРОС ВРЕМЕНИ



Чтобы успешно реализовать кибератаку, злоумышленнику достаточно найти одно уязвимое место во всей инфраструктуре. В то время как специалистам по кибербезопасности необходимо контролировать весь периметр в условиях постоянных изменений и ограниченности ресурсов.

Вероятность проникновения злоумышленника в инфраструктуру компании не исключена даже при наличии обширного стека различных средств защиты и систем кибербезопасности.

84 минуты

среднее время проникновения злоумышленника в инфраструктуру компании в 2022 г. [1]

16 дней

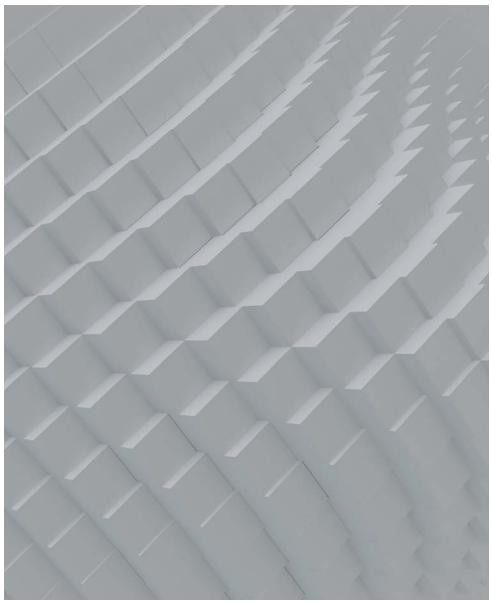
медианное время незаметного присутствия злоумышленника в инфраструктуре в 2022 г. [2]

[1] 2023 Global Threat Report // CrowdStrike

[2] M-Trends 2023 // Mandiant (Google Cloud)

НОВЫЙ ПОДХОД ВЫЯВЛЕНИЯ КИБЕРУГРОЗ В СЕТИ

Большинство кибератак начинается с конечных устройств пользователей: случайно открытое фишинговое письмо, эксплуатация уязвимостей на внешнем периметре (в том числе нулевого дня), компрометация веб-ресурсов компании. Попадая на хост, злоумышленники стараются повысить свои привилегии для дальнейшего продвижения по сети к критическим активам бизнеса различными способами:



- эксплуатируют уязвимости программного обеспечения и приложений;
- пытаются получить привилегированные учётные данные пользователей через подбор паролей на максимально возможном количестве учётных данных (Password Spraying), перебор учётных данных из украденных баз данных (Credential stuffing), компрометацию механизмов смены и сброса паролей (Password changes and resets);
- ищут некорректные конфигурации систем, сервисов и файлов.

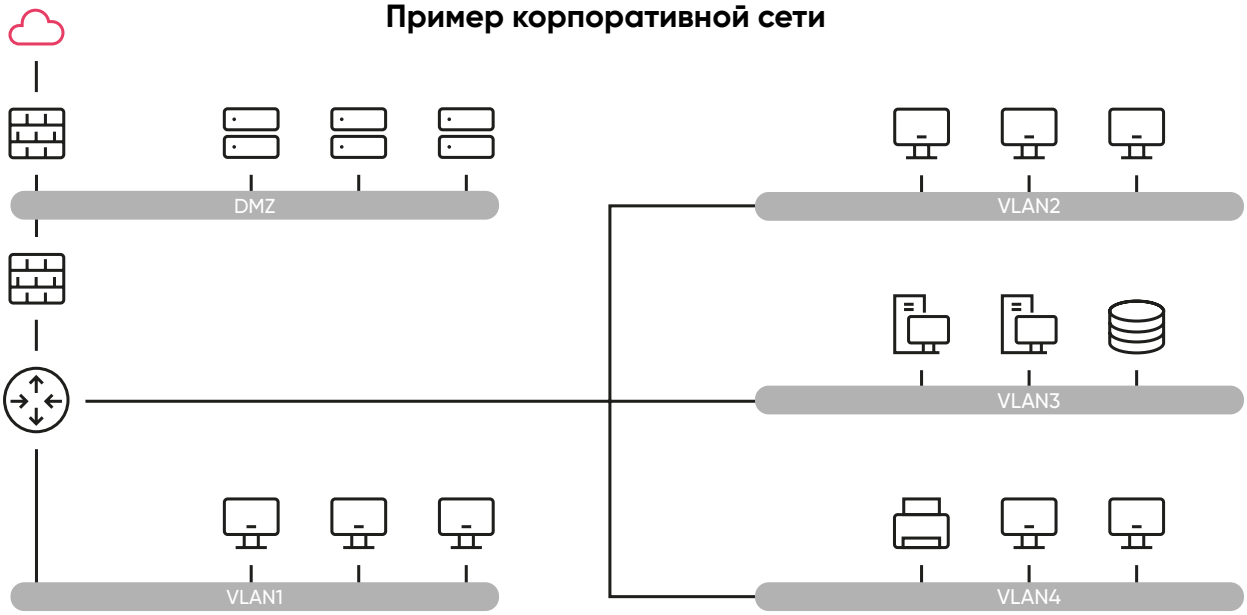
Повышение привилегий обычно выполняется злоумышленником, использующим скомпрометированные идентификационные данные сотрудников компании. Такие атаки достаточно сложно обнаружить обычными сигнатурами и правилами.

Xello Deception не зависит от предварительных знаний об угрозе (индикаторы компрометации или атак, сигнатуры, репутационные списки, правила корреляции) для выявления нелегитимных действий в сети. Решение предоставляет злоумышленникам недостоверную информацию об ИТ-инфраструктуре компании (в том числе идентификационные данные) и перенаправляет их на ловушки, что обеспечивает защиту критически важных информационных активов.

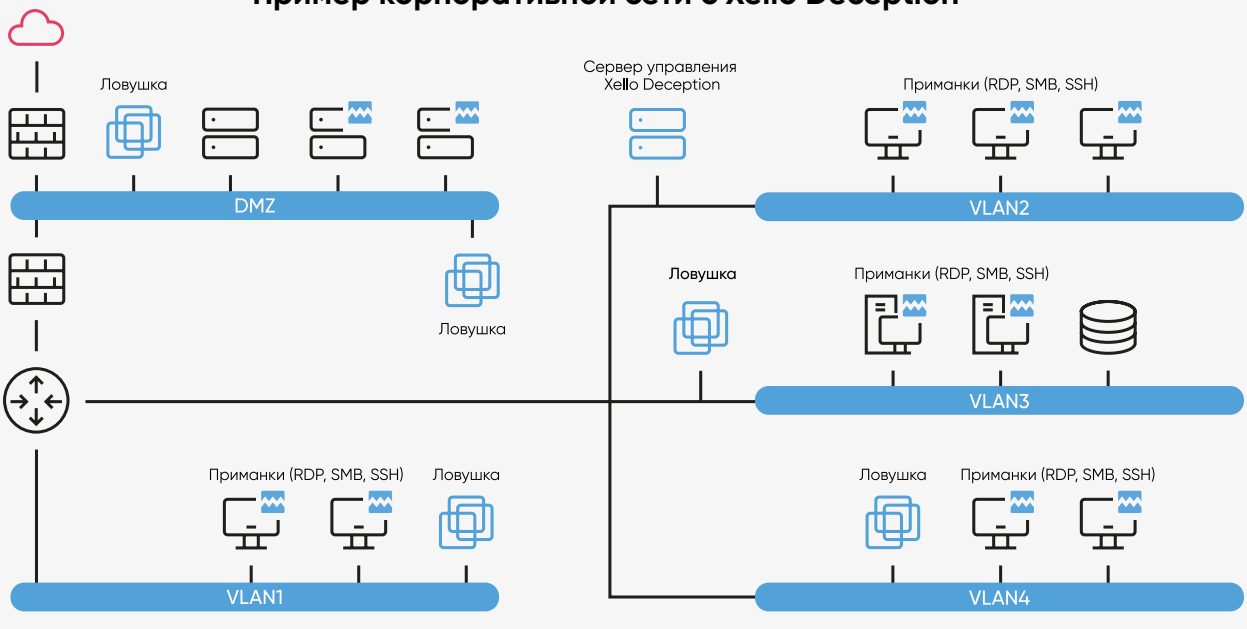
ЗАЩИТА ОТ ЦЕЛЕВЫХ АТАК

Xello Deception создаёт инфраструктуру из ложных активов и данных по всей сети компании. Это возможно благодаря приманкам и ловушкам. Приманки — ложные артефакты на конечных устройствах реальных пользователей компании, которые злоумышленники обычно используют для развития кибератаки и повышения своих привилегий (учётные записи, сохранённые пароли, конфигурационные файлы в памяти операционных систем, файловых систем или браузерах и другие). Если злоумышленник попытается их использовать в процессе реализации кибератаки, система его перенаправит на ловушку — ложный сервис, ресурс ИТ-инфраструктуры, базу данных или сервер.

Пример корпоративной сети



Пример корпоративной сети с Xello Deception

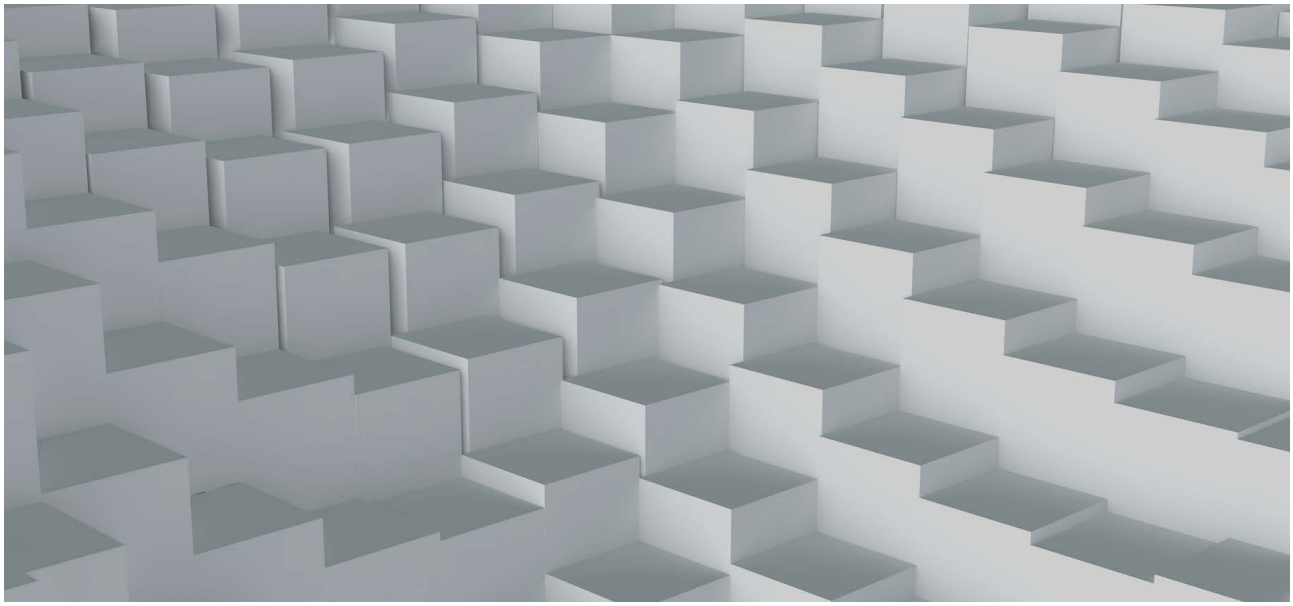


РАСПРЕДЕЛЁННЫЕ ПРИМАНКИ И ЛОВУШКИ ПО ВСЕЙ СЕТИ КОМПАНИИ СОЗДАЮТ ЛОЖНЫЙ СЛОЙ ИНФРАСТРУКТУРЫ, КОТОРЫЙ НЕВОЗМОЖНО ИЗБЕЖАТЬ

Полностью автоматизированные системы киберобмана дают представление о вредоносной активности в корпоративной сети, которая может быть невидима для других средств защиты.

Приманки и ловушки невидимы для авторизованных пользователей и направлены исключительно на злоумышленника, поэтому уведомление от Xello Deception с высокой долей вероятности будет считаться инцидентом безопасности, а не ложным срабатыванием.

Они грамотно распределяются среди рабочих ИТ-активов компании, покрывая всю сеть так, что злоумышленник не имеет шанса избежать их.



Примеры эмулируемых активов и данных:

Сетевые устройства | Хранилища и базы данных | ИТ-сервисы

Ключи от ИТ-систем | Учётные записи | Операционные системы

МЕСТО XELLO DECEPTION ПРИ ЦЕЛЕВОЙ АТАКЕ

> Xello Deception может использоваться для прерывания цепочки атаки, истощения ресурсов злоумышленника и выявления деталей (инструментов) реализации атаки.

Решаемые задачи

- Предотвращение целевых атак (APT) с помощью грамотно распределённых приманок и ловушек по всей сети компании
- Ускорение процесса реагирования за счёт выявления только реальных киберинцидентов
- Сокращение времени расследования инцидента благодаря непрерывному сбору и хранению данных форензики
- Снижение нагрузки на специалистов кибербезопасности за счёт минимизации количества ложных срабатываний
- Повышение эффективности существующих систем кибербезопасности (SIEM, IRP, EDR, Sandbox)
- Закрытие слепых зон классических систем защиты

ВОЗМОЖНОСТИ XELLO DECEPTION

1 | Адаптивная генерация приманок

Современные сети отличаются быстрой изменчивостью и динамичным развитием. Именно поэтому Xello Deception регулярно обновляет приманки с учётом текущих особенностей инфраструктуры компании. Система тщательно анализирует модель поведения каждого пользователя. Независимо от конфигурации и предназначения защищаемого хоста (компьютер бухгалтера, сервер базы данных или ноутбук разработчика) она подбирает приманки такого типа, программное обеспечение которого используется на этом хосте. Ложный слой данных уникален для конкретной корпоративной сети.

2 | Простое внедрение и отсутствие дополнительной нагрузки на инфраструктуру

Xello Deception не использует агенты для распространения приманок и поддержания связи с сервером управления, поэтому не оказывает дополнительной нагрузки на реальную инфраструктуру компании. Приманки распространяются с помощью различных протоколов удалённого управления (WMI, WinRM, SSH) и другими сторонними механизмами. Вся информация о распространённых по сети приманках хранится в системе. Их удаление не влияет на ИТ-инфраструктуру.

3 | Единая консоль управления

Результаты работы платформы отражены в единой консоли управления. С её помощью можно управлять приманками на защищаемых хостах и настраивать индивидуальные политики защиты, генерировать и управлять ловушками в ИТ-инфраструктуре. Все события от системы отображаются в карточке инцидента, где они коррелируются в единую цепочку атаки и классифицируются по модели MITRE ATT&CK.

4 | Поддержка операционных систем

Xello Deception устанавливается на операционные системы Linux, Windows. Приманки распространяются на ОС Linux, Windows, MacOS.

ГИБКАЯ АДАПТАЦИЯ ПОД РАЗЛИЧНЫЕ ИНФРАСТРУКТУРЫ

Платформа Xello Deception имеет модульную архитектуру. Это позволяет гибко адаптироваться под модель угроз информационной безопасности конкретной компании.

01 Xello Lures

Модуль для генерации приманок и их распространения на конечные устройства пользователей

Модуль анализирует инфраструктуру конкретной компании, гибко интегрируясь с ней (LDAP-серверами, DNS-зонами, сторонними системами). На основе полученных данных создаёт максимально реалистичные приманки и распространяет их на конечные устройства пользователей при помощи:

- групповых политик (Group Policy, GPO);
- систем управления конфигурациями (SCM), например, Ansible или Puppet;
- диспетчера конфигурации системного центра (Microsoft Endpoint Configuration Manager, ранее SCCM);
- инструментов управления удалёнными устройств (Mobile Device Management, MDM);
- агента стороннего решения;
- предоставления прав локального администратора.

02 Xello RealOS Traps

Модуль для генерации ловушек и их распространения по сети

Модуль эмулирует ложные сервисы в сети, которые работают в среде реальной операционной системы, на которой они развернуты.
Это дает возможность на данный тип ловушек устанавливать любое ПО. Таким образом, любая продакшн-система превращается в ловушку, при попадании на которую система оповестит специалистов информационной безопасности об инциденте.

03 Xello Decoy Traps

Модуль гибридной эмуляции

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

Это обеспечивает максимальное покрытие всех сегментов сети различными ложными сервисами, службами, системами.

Типы эмулируемых активов:

- сетевые: коммутаторы, маршрутизаторы, межсетевые экраны различных производителей (Fortinet, Check Point, Cisco, Huawei);
- рабочие станции и серверы: Windows OS (7, 8, 10), Windows Server (2012, 2016), Debian, Ubuntu, CentOS;
- специализированные: медицинское оборудование, финансовые терминалы;
- мобильные устройства на базе ОС Android;
- интернет вещей (IoT): IP-камеры, видеорегистраторы, принтеры и МФУ.

На прикладном уровне устройство может быть связано с интерактивным сервисом, когда злоумышленнику предоставляется возможность, например, ввода реальных команд в терминале SSH или учётных данных в брендированной веб-форме авторизации устройства.

04 Xello Satellites

Модуль управления ложным слоем инфраструктуры на распределённых площадках

Модуль централизованно подключает к платформе географически распределённые площадки и гибко управляет на них ложным слоем инфраструктуры (распространяет приманки и ловушки, собирает события аутентификации и информацию о сети).

Модуль также позволяет распространять ловушки в демилитаризованной зоне сети (DMZ).

05 Xello Trapless

Модуль получения событий аутентификации из внешних систем

Модуль позволяет подписываться на сообщения из сторонних систем (Apache Kafka, RabbitMQ, SIEM, Active Directory, Windows Event Collector) и искать события, связанные с ложными активами. Это позволяет использовать решение в инфраструктурах без доменов.

Для интеграции не требуются дополнительные мощности — сервер управления.

06 Xello VDI RDS

Модуль защиты виртуальных рабочих мест (VDI) и терминальных серверов (RDS) с помощью распределённых приманок

Модуль интегрируется с инфраструктурой виртуальных рабочих мест и терминальными серверами, распространяя в них различные типы приманок.

07 Xello Identity Protection

Модуль цифровой гигиены для сокращения поверхности атаки

Модуль уменьшает поверхность атаки, удаляя различные артефакты работы пользователей на конечных устройствах (сохранённые учётные записи, SSH-соединения, открытые RDP-сессии, нелегитимных пользователей из групп безопасности/Security Group), которые хакер использует для дальнейшего незаметного передвижения по сети.

08 Xello MITM

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

Модуль выявляет нелегитимные действия с перехватом пользовательских данных на сетевом уровне. В режиме реального времени выявляет вредоносную активность, связанную с протоколами LLMNR, mDNS, NBT-NS, которые злоумышленники эксплуатируют в ходе реализации кибератак.

09 Xello API

Модуль для интеграции со сторонними системами и сервисами

Модуль позволяет интегрировать Xello Deception с внешними системами и обрабатывать инциденты от них в рамках единого процесса в консоли управления. Например, если в компании уже используются собственные или Open Source-ловушки, то при интеграции Xello Deception будет работать с ними, как с собственными (каждое событие будет проходить весь процесс обработки внутри платформы). Благодаря модулю платформу можно интегрировать с внутренними системами мониторинга (для отправки всех получаемых инцидентов) или любыми другими системами и средствами защиты (IRP, NAC, NGFW, Sandbox и другими).

10 Xello Industrial

2024 г.

Модуль защиты АСУ ТП с помощью распределённых ловушек

Модуль позволяет распространять ловушки, эмулирующие специальное программное обеспечение, устройства ICS/SCADA, ПЛК в сети. Они устанавливаются вокруг существующих системных компонентов и ограничивают риск негативного влияния на доступность и целостность технологических процессов.

Распределённые по всей сети ловушки позволяют выявить нелегитимное взаимодействие с ними. Например, вредоносные программы в ИТ-среде ищут уязвимые версии сетевых служб, а в промышленном сегменте — типы устройств, которые взаимодействуют с интересующими их процессами. Если злоумышленник попытается использовать ловушки в процессе реализации атаки, специалисты сразу же будут оповещены системой киберобмана о потенциальном инциденте безопасности.

11 Xello Honey Cloud

2024 г.

Модуль эмуляции приманок в облачной инфраструктуре

Модуль позволяет распространять различные типы приманок и ловушек в облачные инфраструктуры.

Протестируйте все возможности платформы Xello Deception на бесплатном пилотном проекте. Свяжитесь с нами удобным для вас способом — написав на почту sales@xello.ru или оставив заявку на сайте xello.ru.

О КОМПАНИИ

Xello (Кселло) — разработчик первой российской платформы для предотвращения целевых атак с помощью технологии киберобмана. Решение относится к классу Distributed Deception Platform, DDP. Включено в реестр Отечественного ПО.

Компания пять лет на рынке информационной безопасности. За это время реализовано более тридцати проектов в различных отраслях экономики: кредитно-финансовом, нефтегазовом секторе, промышленности, топливно-энергетическом комплексе, ИТ и телекоме, ритейле, государственном.