xello

Повышение эффективности SOC с помощью Xello Deception

Sk Участник

Московский инновационный кластер

Xello Deception позволяет выявлять нелегитимные действия злоумышленника в корпоративной сети и предотвращать целенаправленные атаки. Кроме этого, при помощи платформы решаются задачи по повышению эффективности, качества мониторинга и реагирования на инциденты безопасности.

Согласно совместному исследованию Forrester и Palo Alto Networks, внутренние службы кибербезопасности в среднем обрабатывают более **11 000** алертов ежедневно*

ВОЗМОЖНОСТИ ДЛЯ SOC

Снижение количества ложных срабатываний

Предоставляет высокодоверенные индикаторы компрометации информационных активов

Оповещает только о подозрительных или вредоносных действиях

Оперативное реагирование

Предоставляет надежные триггеры, которые не нужно проверять администратору системы

Интегрируется со всеми системами для реагирования на инциденты безопасности

Расследование инцидентов

Собирает и хранит данные форензики: техники и тактики, инструменты и методы, применяемые при реализации кибератаки

Формирует корреляцию между разрозненными событиями в единую цепочку атаки

Проактивная защита

Обнаруживает угрозы до того, как они нанесут ущерб организации

Предоставляет возможность блокировки действий злоумышленника при интеграции с другими системами безопасности

* The 2020 State of Security Operations // Forrester

Технология кибероbмана

ПОЗВОЛЯЕТ СОКРАТИТЬ СРЕДНЕЕ ВРЕМЯ ОБНАРУЖЕНИЯ ЗЛОУМЫШЛЕННИКА В СЕТИ ДО 5,5 ДНЕЙ*

Xello Deception создает инфраструктуру из ложных информационных активов (серверов, сайтов, учетных данных, конфигурационных файлов и других) с помощью приманок и ловушек. Если конечная точка попытается получить доступ к ним, то с большой вероятностью она скомпрометирована, поскольку для такой деятельности нет законных оснований. Приманки и ловушки направлены исключительно на злоумышленника.

ПРОСТАЯ ИНТЕГРАЦИЯ С СИСТЕМАМИ КИБЕРБЕЗОПАСНОСТИ

- Перенаправление событий в SIEM
- Сдерживание угроз через брандмауэры и другие средства защиты
- Предоставление широких возможностей для интеграции благодаря открытому API

* Mandiant Security Effectiveness Report: DEEP DIVE INTO CYBER REALITY 2020 // Mandiant

ВОЗМОЖНЫЕ СЦЕНАРИИ ИНТЕГРАЦИИ

01 DECEPTION + SIEM

Оперативные оповещения
о взломанных машинах в SIEM

Автоматический поиск машин
систем с помощью настроенных политик

Организация реагирования
при помощи надежных Deception–алертов

02 DECEPTION + EDR

Блокировка и отправка зараженных
конечных станций в карантин

Автоматическое реагирование
на инциденты с помощью политик изоляции

03 DECEPTION + NGFW

Возможность отправки запросов
на блокировку или карантин зараженных
конечных устройств

Ручное и автоматическое управление

04 DECEPTION + SANDBOX

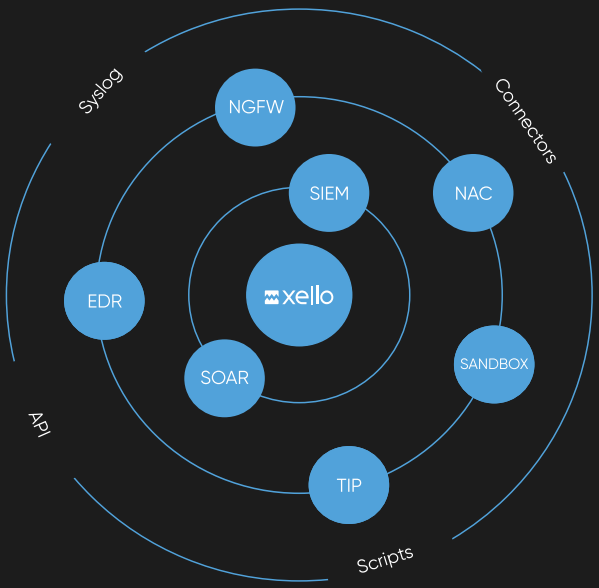
Отправка подозрительных исполняемых
файлов в песочницу для анализа

Формирование отчета об анализе
вредоносных программ с оперативными IOC

05 DECEPTION + NAC

Отправка вредоносных активностей
в NAC-систему для внесения в черный список

Удобное извлечение данных о вредоносных
активах и действиях через единую консоль
управления Xello Deception

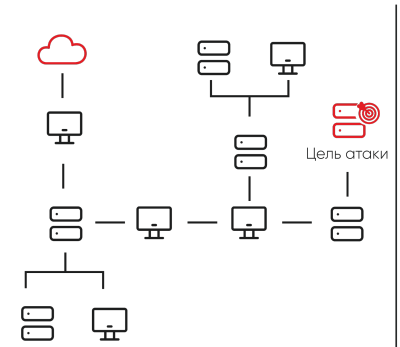


Если вы используете нестандартную систему,
подключение к ней мы возьмем на себя

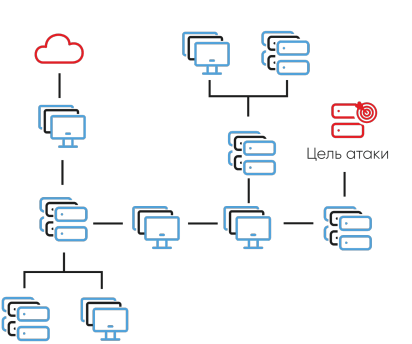
КАК ТЕХНОЛОГИЯ КИБЕРОБМАНА ЗАЩИЩАЕТ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК?

Сегодня в условиях размытого периметра, уязвимости в OpenSource-компонентах, а также неограниченных возможностей использования методов социальной инженерии, получение первичного доступа к инфраструктуре остается вопросом времени.

Xello Deception позволяет предотвращать сложные кибератаки даже при условии проникновения в корпоративную сеть организации, создавая инфраструктуру из ложных активов.



Пример корпоративной сети



Пример корпоративной сети с Xello Deception

— приманки

ЗАКАЖИТЕ ПИЛОТ XELLO DECEPTION

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

xello

Xello – первый разработчик российской Deception-платформы

Контакты:

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