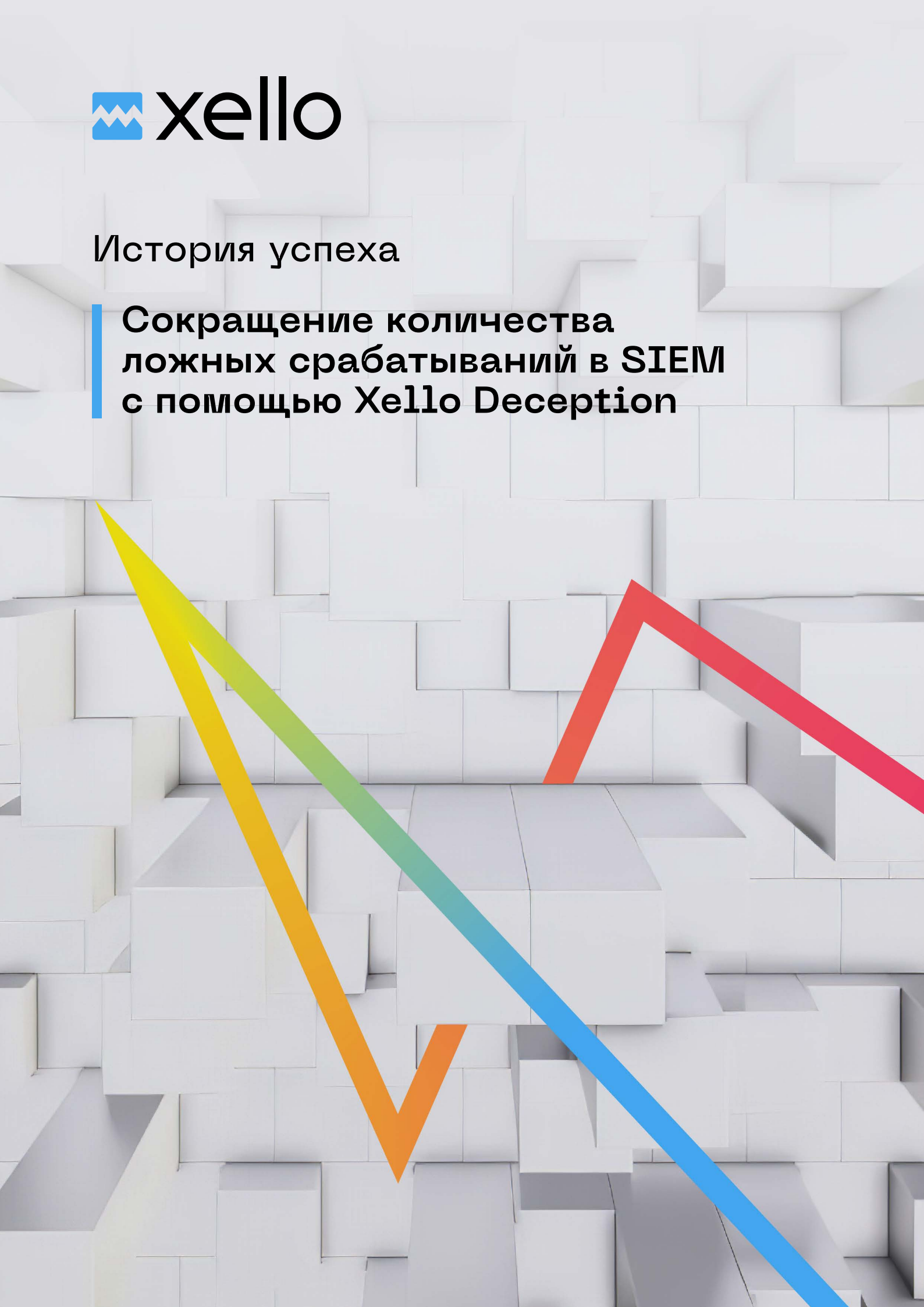
xello

История успеха

Сокращение количества ложных срабатываний в SIEM с помощью Xello Deception



ПРОФИЛЬ КОМПАНИИ

Заказчик	строительная компания РФ из ТОП-5
Количество АРМ	+ 1500
Количество серверов	+ 3000
Год внедрения	конец 2020 — начало 2021 гг.

Компания осуществляет строительство жилых комплексов на рынке недвижимости более десяти лет. За это время была сформирована значительная распределенная филиальная сеть с офисами по всей стране. Множество подрядчиков помогают осуществлять проектирование и возведение зданий. Ориентация на потребителей требует от компании использования технологий и систем, позволяющих организовывать гибкую работу с ними: CRM и ERP-порталы, контакт-центр, ЭДО для взаимодействия с подрядчиками.

ЗАДАЧА

На каждом этапе строительства объектов недвижимости участвуют контрагенты, которые могут иметь разный уровень доступа к информационным системам компании для работы с технической документацией проекта, базами знаний, финансовыми отчетам и другой конфиденциальной информацией.

В компании уже реализован мониторинг событий безопасности и обмен данными об инцидентах между самостоятельными дочерними структурами. Автоматизированы процессы по управлению инцидентами и уязвимостями. И несмотря на регулярные ИТ и ИБ-аудиты, предоставление доступа сторонним исполнителям к инфраструктуре создает большой поток ложных срабатываний в Центр мониторинга инцидентов безопасности и реагирования на них (SOC), а отсутствие актуальных знаний об активах компании — риски несанкционированного доступа к данным и системам компании.

Команда информационной безопасности в рамках обеспечения целостности, доступности и сохранности данных и информационных систем компании регулярно тестирует новые продукты и технологии. Так, было принято решение о пилотировании нового на тот момент класса решений Distributed Deception Platform (DDP). Выбор пал на российское решение Xello Deception.

Ключевыми требованиями при выборе решения были:

01

отсутствие дополнительной нагрузки на эксплуатирующий персонал в процессе управления

02

возможность гибкой интеграции с существующими системами защиты

03

отсутствие ложных срабатываний

ПИЛОТИРОВАНИЕ

6 месяцев
длился пилотный проект

80%
пул хостов от всей инфраструктуры компании, сформированные сотрудниками ИБ-департамента. Они были добавлены в систему для дальнейших действий: их анализа и автоматической генерации необходимых приманок.

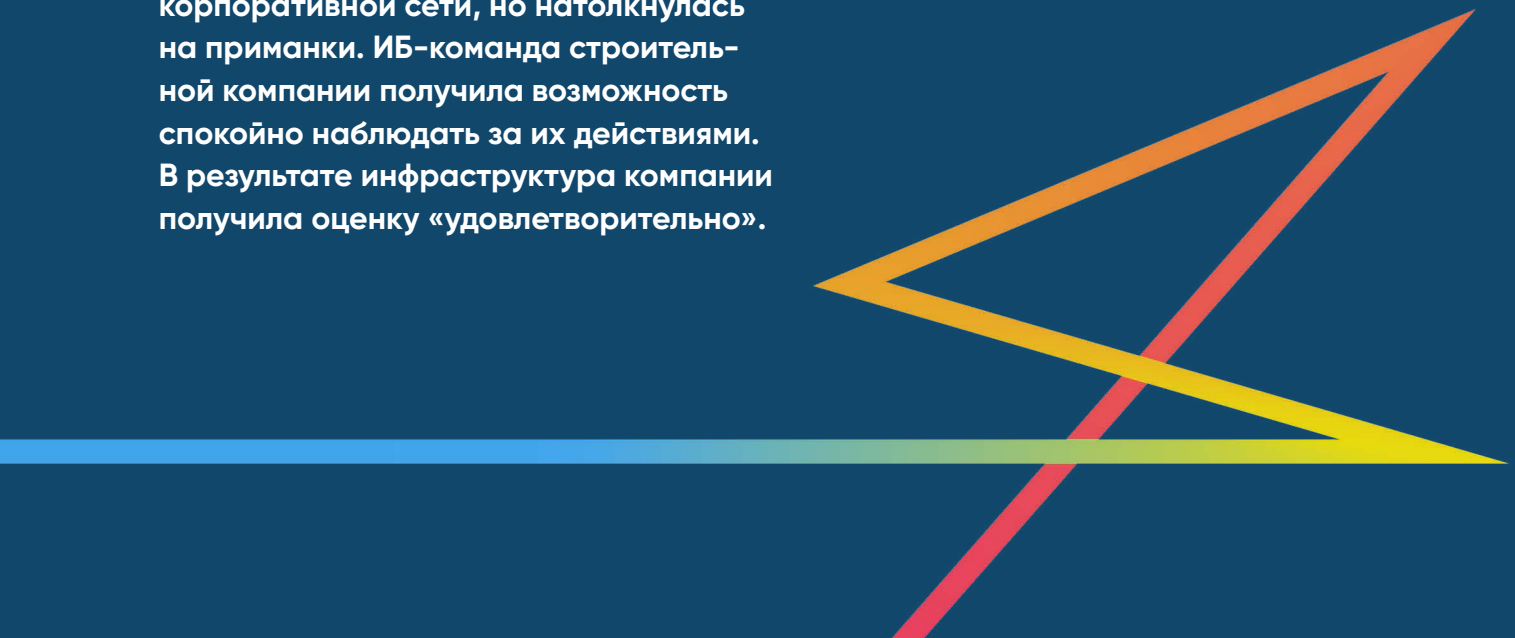
Также в организации были выбраны наиболее уязвимые группы пользователей (бухгалтерия, секретариат, ИТ-департамент), и на основании их атрибутов системой были созданы ложные учетные записи в Active Directory (AD) с целью введения в заблуждение злоумышленника при попытке их использования в рамках кибератаки.

В короткие сроки настроили отправку событий безопасности в SIEM-систему по протоколу Syslog в формате CEF.

ИТОГИ

В первом полугодии 2021 года, в процессе пилотирования решения был проведен внешний пентест. Xello Deception успешно выявила действия команды пентестеров, которая пыталась заполучить в своё распоряжение аутентификационные данные привилегированных пользователей, обладающих правами на множестве хостов корпоративной сети, но натолкнулась на приманки. ИБ-команда строительной компании получила возможность спокойно наблюдать за их действиями. В результате инфраструктура компании получила оценку «удовлетворительно».

Благодаря добавлению в корреляцию высокодоверенного идентификатора компрометации сократились количество алертов и нагрузка на аналитиков. Уведомления от Xello Deception были приоритизированы в рамках процесса управления инцидентами безопасности в SIEM-системе.



О КОМПАНИИ

Xello (Кселло) — разработчик первой российской платформы для предотвращения целенаправленных атак с помощью технологии киберобмана. Решение относится к классу Distributed Deception Platform, DDP.

Компания основана в 2018 году. Первый коммерческий релиз Xello Deception состоялся в 2019 году.

Сегодня клиентами компании являются крупнейшие представители различных отраслей экономики: промышленность, ТЭК, кредитно-финансовый сектор, ИТ и телеком, ритейл, а также государственные организации.

Чтобы получить консультацию или бесплатно протестировать платформу Xello Deception, свяжитесь с нами удобным для вас способом

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

xello.ru