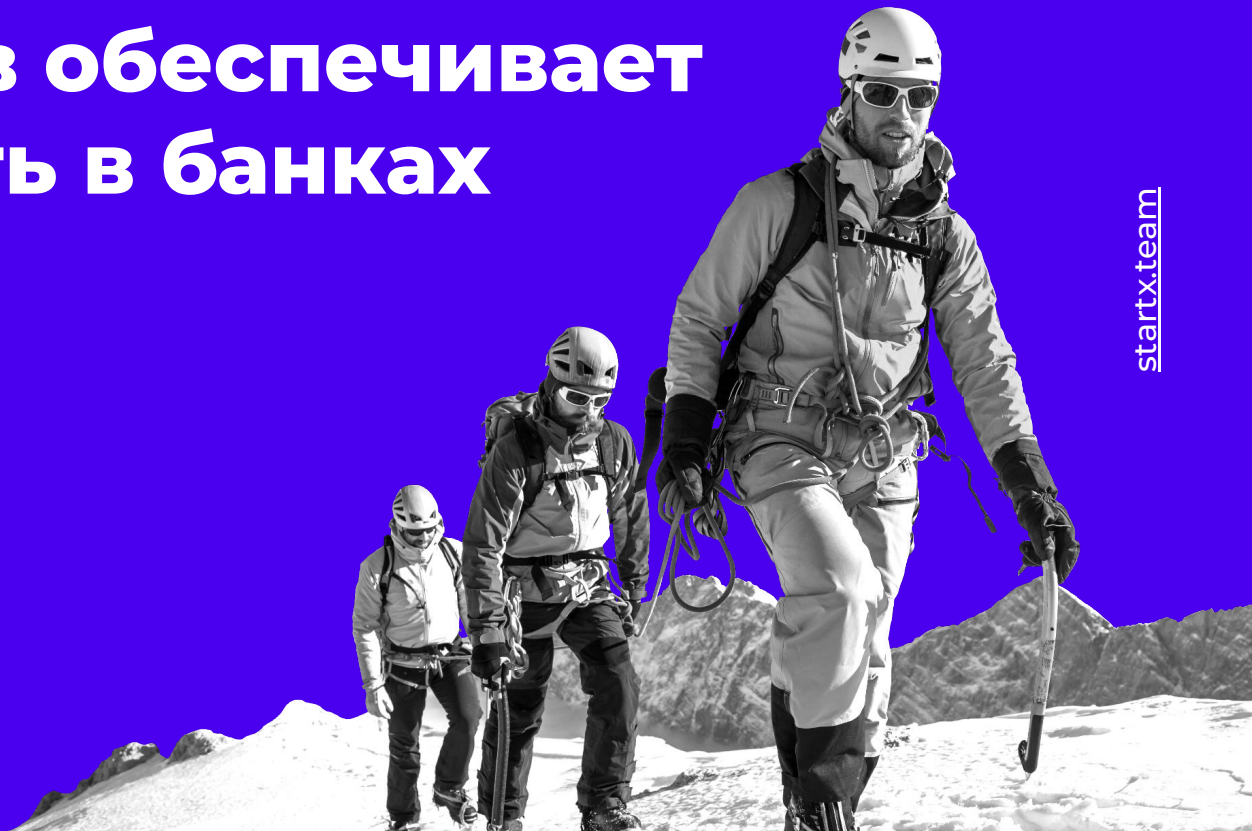
Start AWR:
Как киберграмотность сотрудников обеспечивает безопасность в банках

2023

startx.team



Start X

Об экосистеме Start X

Мы — российская исследовательская компания и разработчик программного обеспечения ООО «Антифишинг».

Разрабатываем экосистему продуктов **Start X**, которая помогает снизить риски человеческого фактора и повысить эффективность работы людей во всех ключевых бизнес-процессах, включая разработку, поддержку и эксплуатацию систем и приложений.

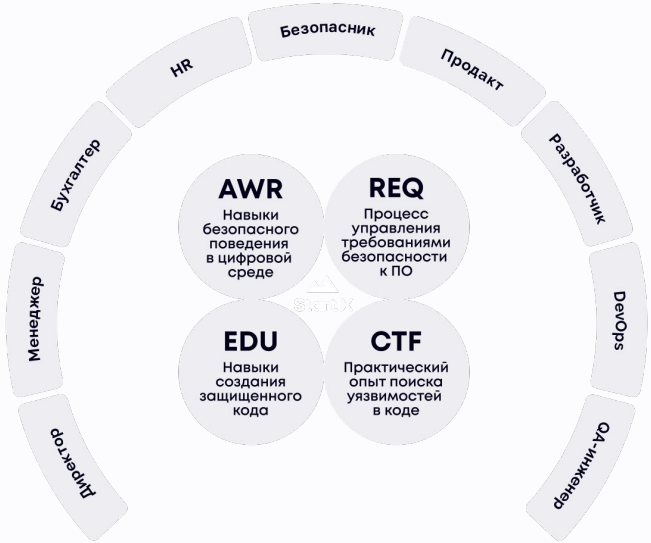
Продукты входят в реестр Минцифры

Компания — лицензиат ФСТЭК

Start X

Даём цифровой иммунитет людям и компаниям

Экосистема продуктов для защиты всех сотрудников и процессов компании



Снизить риск инцидента через атаки на сотрудников	Управлять требованиями ИБ к ПО и наладить контакт с разработкой	Писать код с нуля без уязвимостей	Вовлечь команду разработки в процесс SSDLC

Продукты экосистемы Start X:

Учат сотрудников распознавать и предотвращать цифровые атаки, сохранять бюджет и имидж компании.

Помогают сформировать требования по безопасности к ПО компании и улучшить коммуникацию с продуктовыми командами, чтобы уменьшить Time-to-Market и снизить затраты на проектную команду.

Налаживают контакт между безопасностью и сотрудниками, вовлекают их в защиту компании от цифровых атак.

Делают безопасность частью культуры компании, а человеческий фактор — управляемым параметром безопасности.

Ключевые заказчики

OZK
ОБЪЕДИНЕННАЯ ЗЕРНОВАЯ КОМПАНИЯ

М.ВидеоЭльдорадо

ПРОМОМЕД

QIWI

Райффайзен БАНК

БАНК САНКТ-ПЕТЕРБУРГ

Применение Start AWR в банкинге

Start X

QIWI внедрили Start AWR: сотрудники реже переходят по ссылкам и в 3 раза чаще сообщают об атаках в службу ИБ

Цели проекта и внедрения продукта

- Эффективно и регулярно обучать и тренировать сотрудников вопросам ИБ, научить распознавать фишинг
- Сократить количество возможных инцидентов

Инструменты, которые применялись для решения задачи

Платформа Start AWR (ранее Антифишинг для сотрудников) для регулярной тренировки навыков сотрудников вопросам ИБ, и организации эффективного непрерывного процесса повышения осведомленности с помощью нее.

Результаты проекта

- ✓ Лояльность сотрудников QIWI к отделу информационной безопасности повысилась.
- ✓ Количество сообщений от сотрудников о спаме/подозрительных письмах выросло в 3 раза.
- ✓ Пользователи стали реже переходить по фишинговым ссылкам и вводить логины и пароли на фишинговых сайтах.

Start AWR

Крупный российский региональный банк из топ-20 внедрил Start AWR: сотрудники на 35% реже совершают опасные действия в письмах

Цели проекта и внедрения продукта экосистемы

- Снизить число сотрудников, которые открывают фишинговые письма и становятся жертвами злоумышленников.
- Вывести систему обучения сотрудников на новый уровень, в том числе, организовать отработку навыков отражения атак.
- Организовать мониторинг опасных действий сотрудников и уровня защищенности.

Инструменты, которые применялись для решения задачи

Платформа Start AWR (ранее Антифишинг для сотрудников) для регулярной тренировки навыков сотрудников вопросам ИБ, и организации эффективного непрерывного процесса повышения осведомленности с помощью нее.

Результаты проекта

- ✓ За год число опасных действий в письмах снизилось с 45% до 10%
- ✓ Число сообщений о фишинговых атаках выросло на 20%
- ✓ У службы безопасности есть точные данные об уровне защищенности каждого сотрудника и компании в целом.

Start AWR

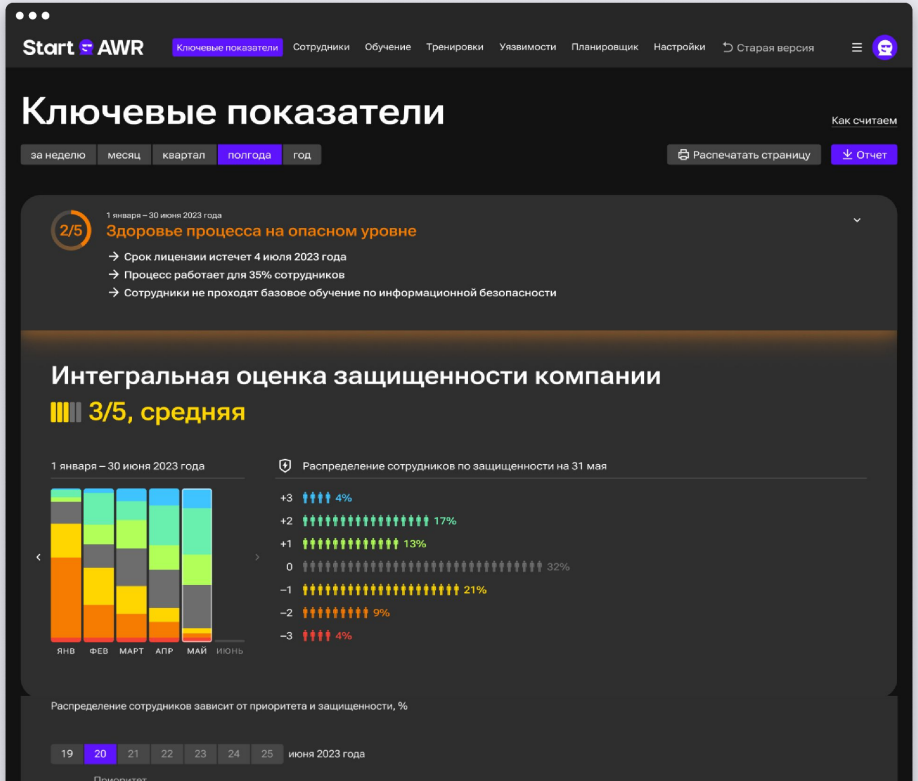
Start AWR — решение для защиты организаций от цифровых атак через сотрудников

Платформа **Start AWR** (ранее Антифишинг для сотрудников) содержит электронные курсы и тесты, а также сценарии и шаблоны имитированных атак.

Компания участвует в информационном обмене с Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере («ФинЦЕРТ») Банка России.

Продукты входят в реестр Минцифры

Компания — лицензиат ФСТЭК



Ключевые преимущества

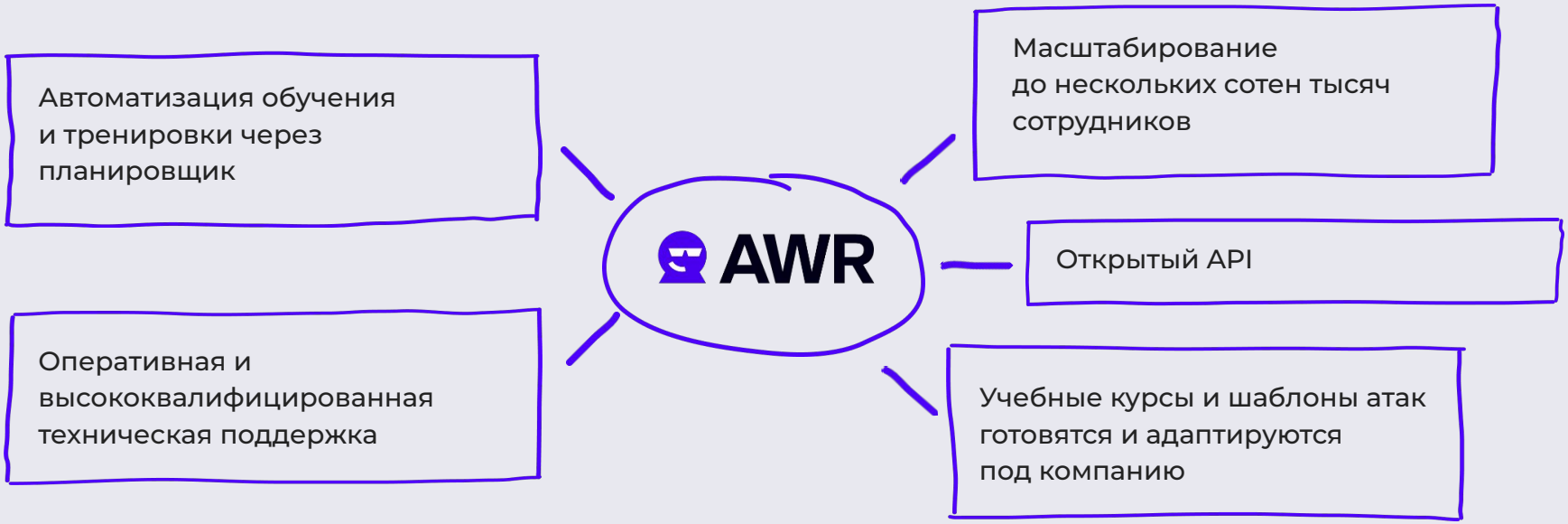
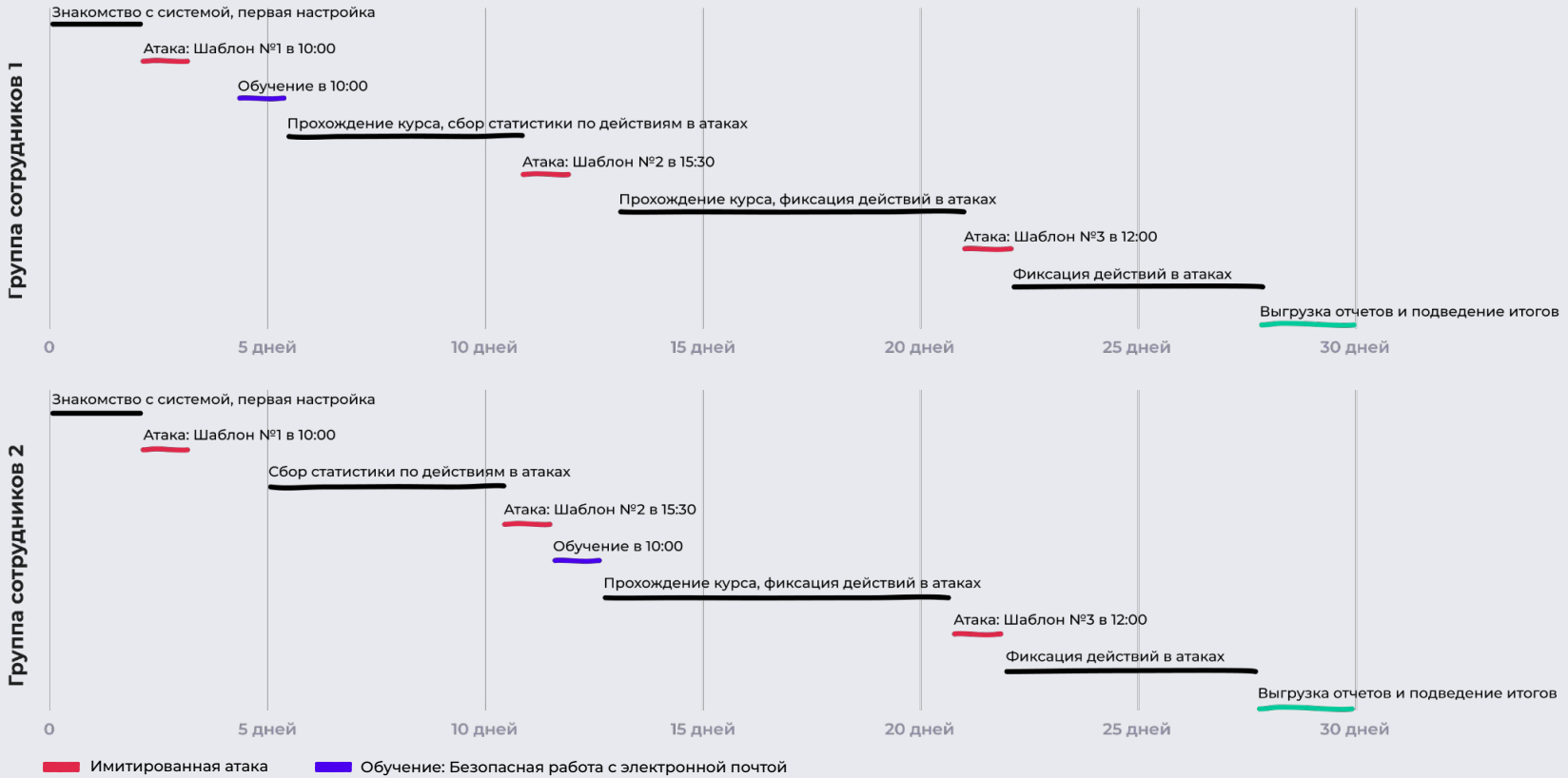


График пилотного проекта



Start @ AWR

Основной проект

SaaS

Start X продлевает лицензию для заказчика, расширяя её до промышленной.

С компанией-заказчиком согласовываются целевые сценарии имитированных атак, далее сотрудники Start X разрабатывают сценарии и загружают их в аккаунт заказчика.

On-Premise

Если инфраструктура не изменяется, то заказчик применяет промышленную лицензию обновлением и продолжает работу.

С компанией-заказчиком согласовываются целевые сценарии имитированных атак, команда Start X разрабатывает их и выдаёт обновление заказчику.

Сложная инсталляция On-Premise

С заказчиком согласовываются технические детали размещения инсталляции на одной или нескольких машинах, в зависимости от объёма лицензии.

Start X разрабатывает архитектуру и поставляет нужное количество виртуальных машин для разворачивания в инфраструктуре заказчика.

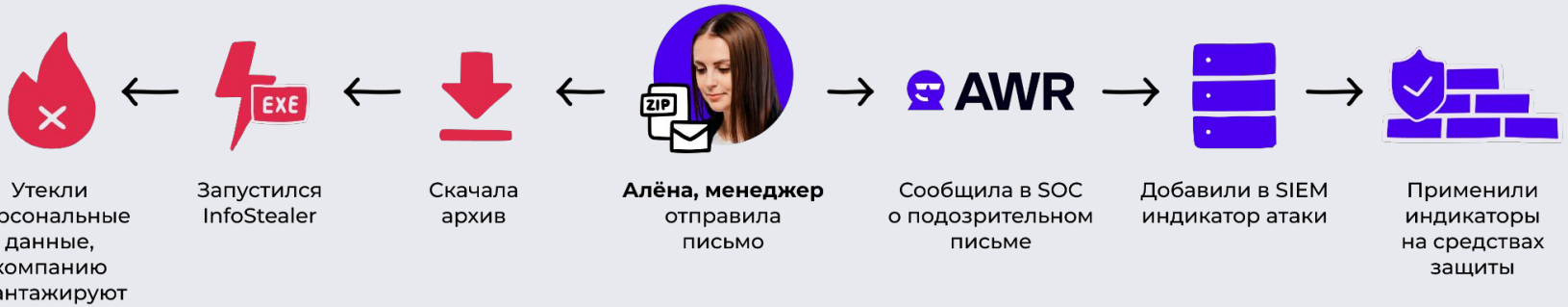
Согласовываются целевые сценарии имитированных атак. Команда Start X разрабатывает сценарии и выдаёт их обновление заказчику.

Как Start AWR повышает защищённость компании

Start X

Человек — причина 74%* инцидентов информационной безопасности в 2022 году

Start AWR позволяет снижать уровень риска инцидентов для компании и управлять человеческим фактором в безопасности.

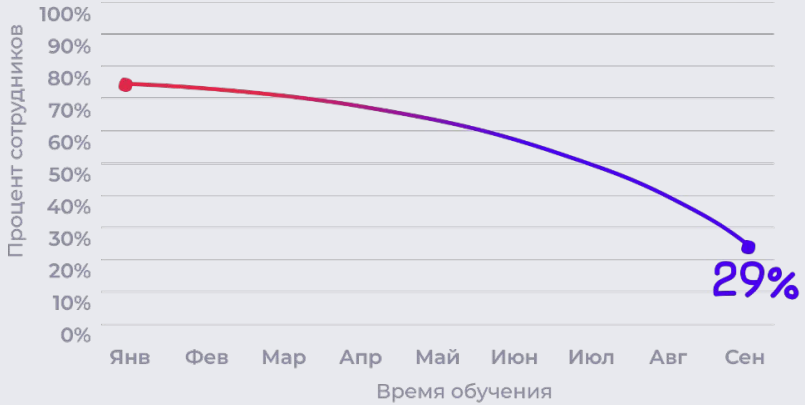


Источник: Verizon Data Breach Investigations Report

Как Start AWR повышает защищенность компании

При применении Start AWR сотрудники начинают вести себя безопасно в рабочих процессах

Доля открытых писем



в 3 раза
сокращается % открытий фишинговых писем

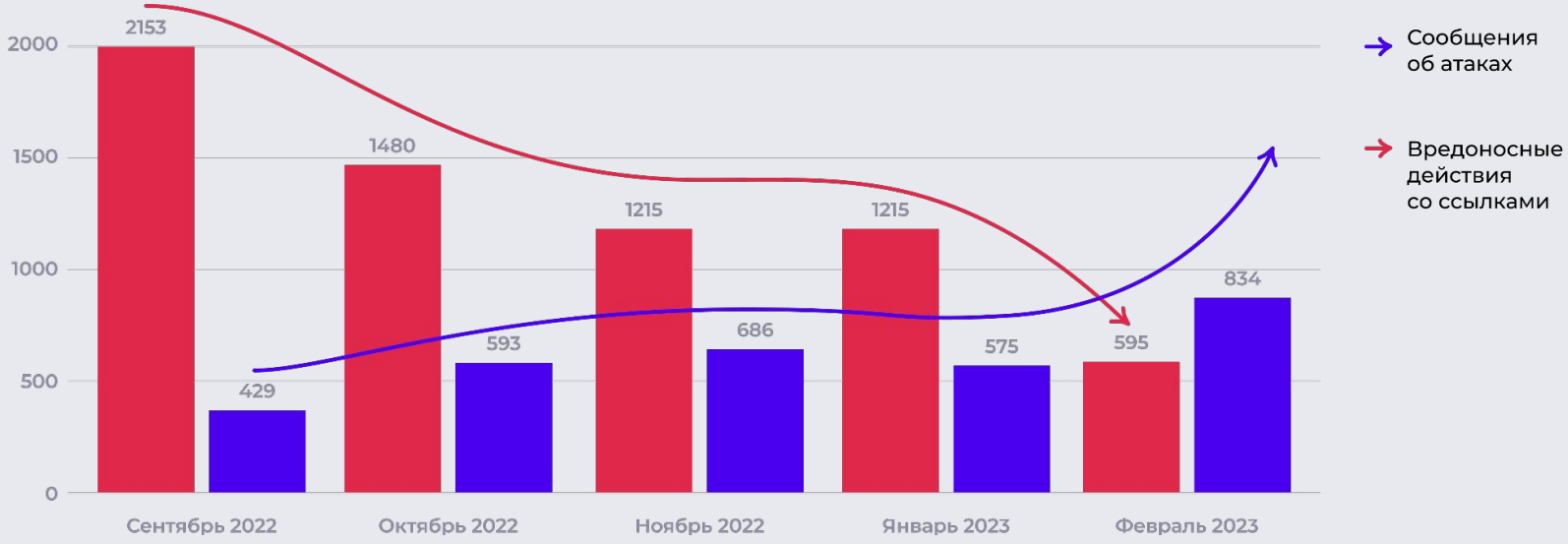
~в 6 раз
сократился переход на фишинговый сайт

Start AWR

Как Start AWR повышает защищенность компании

При применении Start AWR сотрудники начинают вести себя безопасно в рабочих процессах

Динамика поведения сотрудников в компании с 33 000 сотрудников за 5 месяцев использования Start AWR



Start AWR

Как Start AWR повышает защищенность компании

Повышается вовлеченность сотрудников в процессы информационной безопасности компании: они чаще сообщают о фишинге. Обратная связь от сотрудников встроена и работает в интеграции с процессами Security Operations Center (SOC).

Доля сообщений о фишинговых письмах

Start AWR

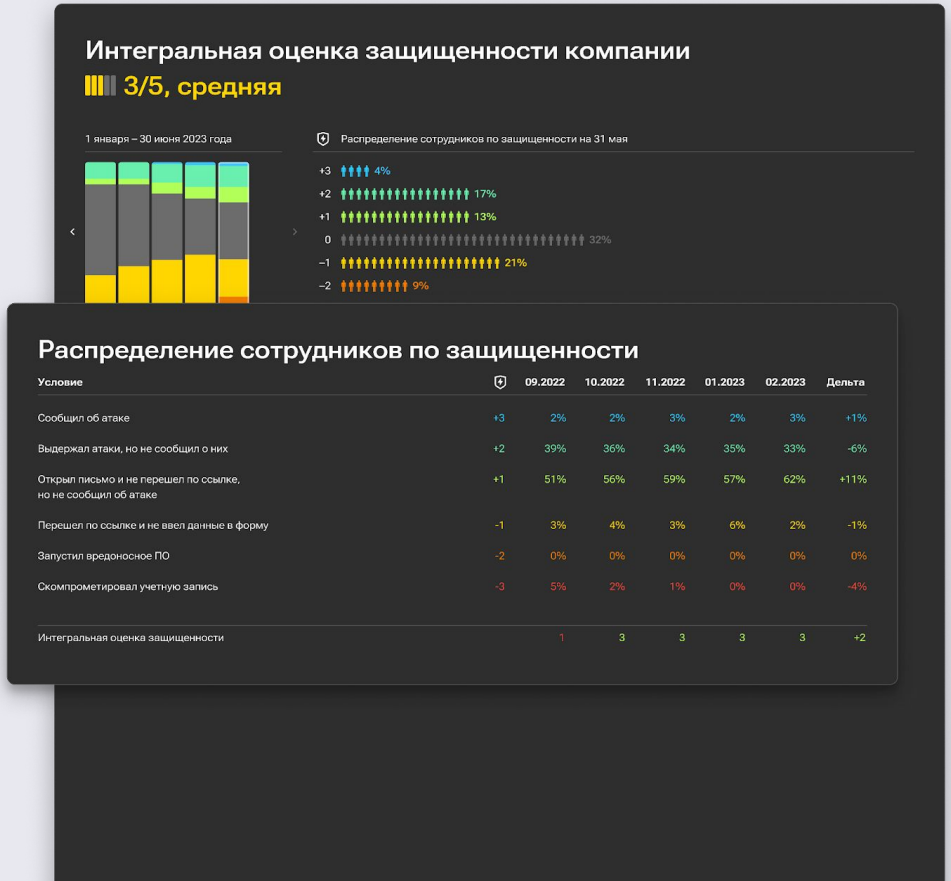
Как Start AWR повышает защищенность компании

Start AWR помогает развивать культуру информационной безопасности в компании

Люди понимают правила безопасности, знают, что от них требуется, умеют работать безопасно. Обсуждают и комментируют вопросы информационной безопасности на внутренних порталах.

Человеческий фактор превращается в управляемый цифровой актив компании

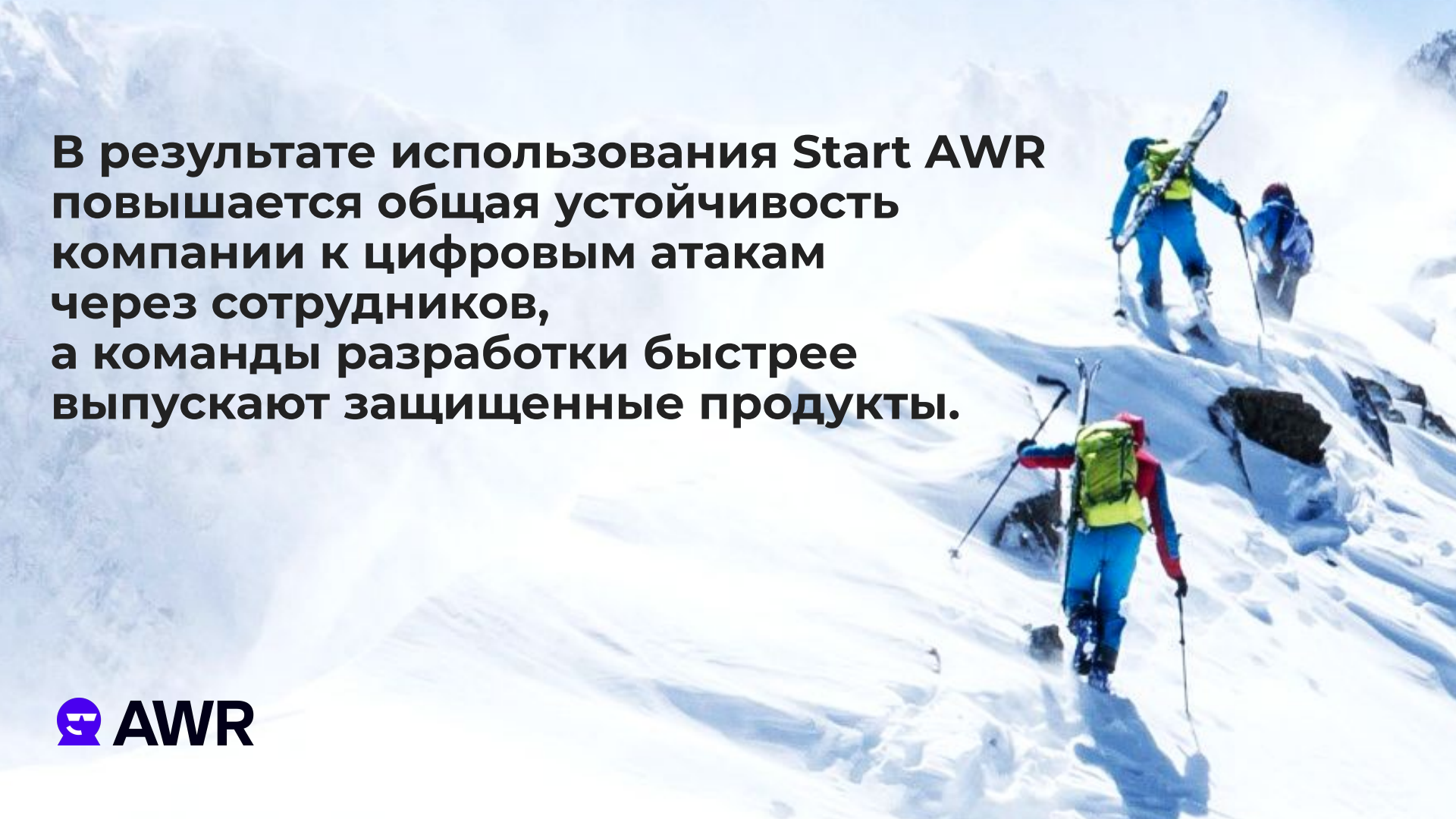
Start AWR непрерывно оценивает защищенность и уровень риска для каждого сотрудника по результатам его действий. На основе этого выводится интегральная оценка защищенности компании от цифровых атак на сотрудников. Все это позволяет отслеживать текущий уровень безопасности в компании и управлять им.



Как Start AWR повышает защищенность компании

Интеграции Start AWR со средствами защиты и ИТ-системами повышают защищенность компании. У наших клиентов работают интеграции с IDM/IAM, SIEM, IRP/SOAR, DLP, и другими СЗИ:

В результате использования Start AWR повышается общая устойчивость компании к цифровым атакам через сотрудников, а команды разработки быстрее выпускают защищенные продукты.



AWR

Контакты

Start X

+7 (499) 677 19 07

marketing@startx.team

STARTX.TEAM

2023

startx.team