СКАРЫНА

система повышения осведомленности

Описание

Система повышения осведомленности СКАРЫНА предназначена для повышения осведомленности сотрудников в области информационной безопасности и укрепления их устойчивости к кибератакам, основанным на социальной инженерии

Решает задачи:

- Выявляет сотрудников, наиболее подверженных фишинговым атакам
- Обучает сотрудников на конкретных примерах, выявленных в ходе рассылки
- Повышает общую защищенность организации от киберугроз

Возможности

Организация фишинговых рассылок

Запуск реалистичных фишинговых кампаний для оценки устойчивости сотрудников и выявления пробелов в знаниях по вопросам информационной безопасности

Анализ результатов рассылок

Предоставление инструментов для анализа результатов рассылок, включая данные о числе пользователей, поддавшихся фишингу,и их действиях

Группировка пользователей и целевое обучение

Ведение учета пользователей с возможностью группировки для целевого обучения и создания обучающих кампаний, адаптированных под конкретные потребности

Шаблоны фишинговых писем

Библиотека готовых и настраиваемых шаблонов писем, ускоряющая подготовку и запуск рассылок

Особенности

Продвинутые социотехнические атаки

Поддержка таких атак как:

- ClickFix / FakeCaptcha
- FileFix
- и другие

Нестандартные файловые вложения

Вложения с генерацией полезной нагрузки: архивы, офисные документы, замаскированные файлы, необычные расширения файлов (.msi,.scr)

Мониторинг отчетов сотрудников

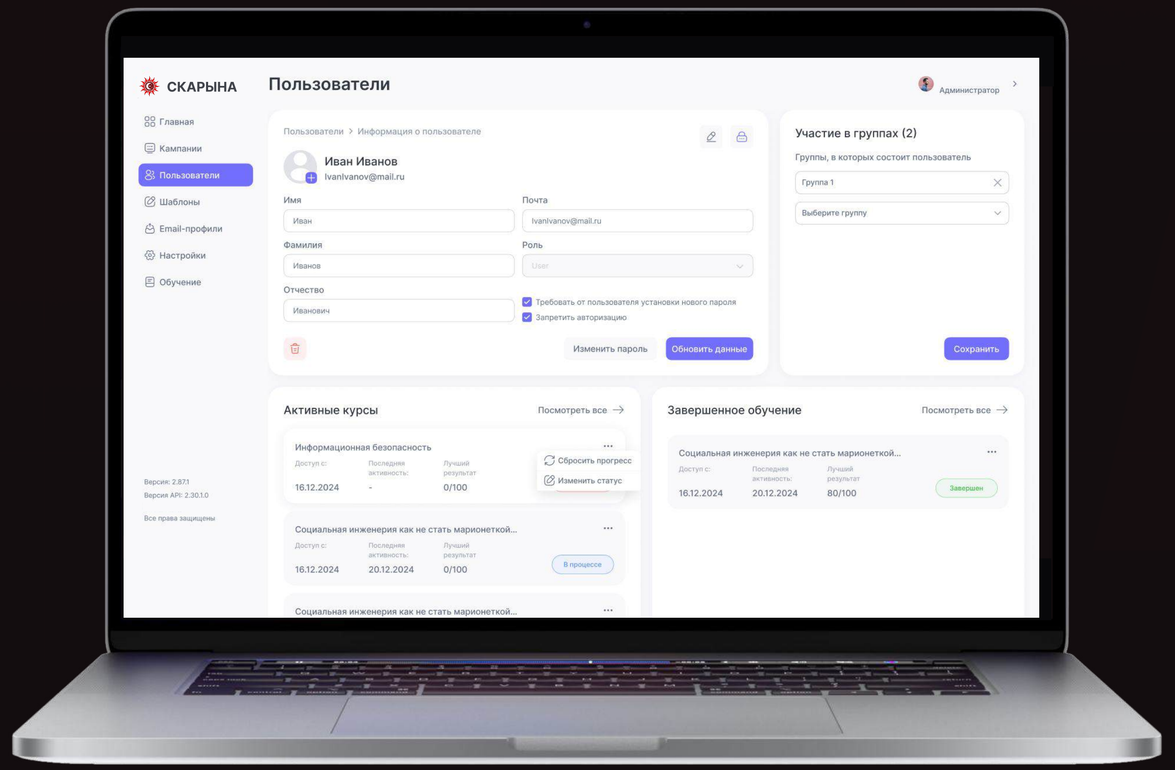
Отмечайте внимательных сотрудников, отчитавшихся о получении фишинговых атак в Security Operations Center

SURTE IT

Процесс работы

1. Подготовка

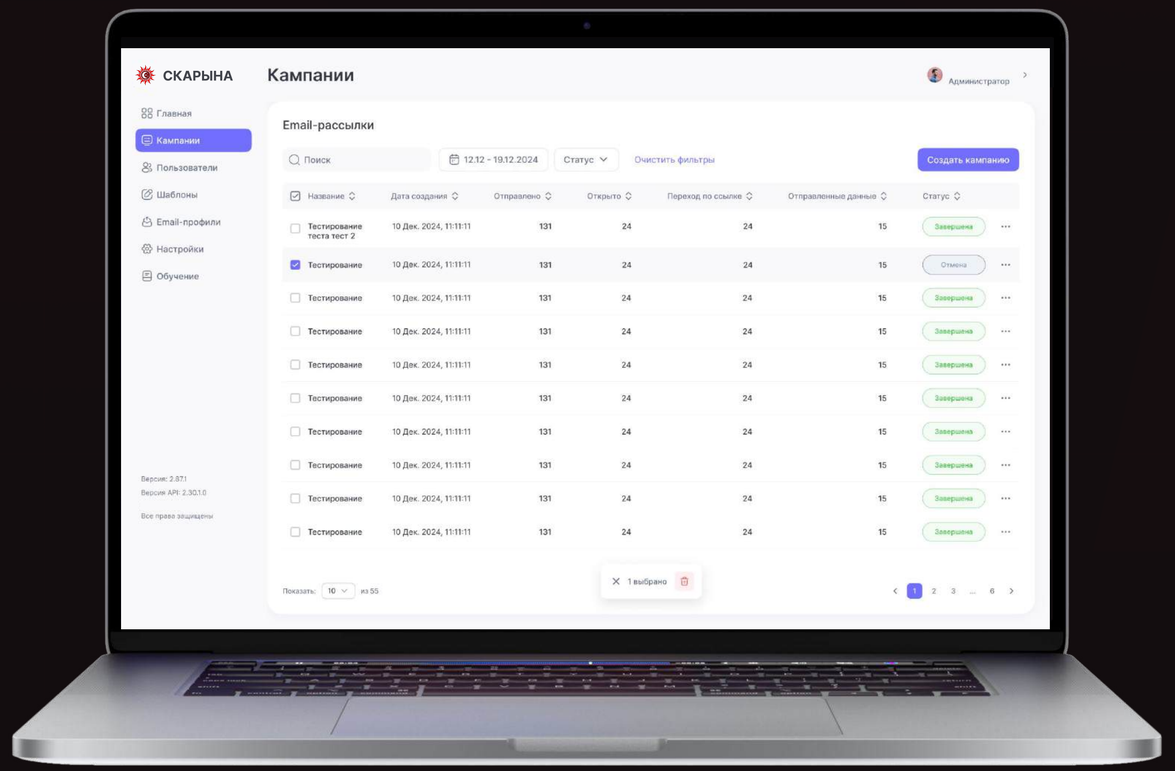
- Подготовьте шаблоны писем и сайтов — или выберите из более 100 готовых;
- Заведите или импортируйте сотрудников;
- Создайте целевую группу для рассылки.



Процесс работы

2. Моделирование фишинга

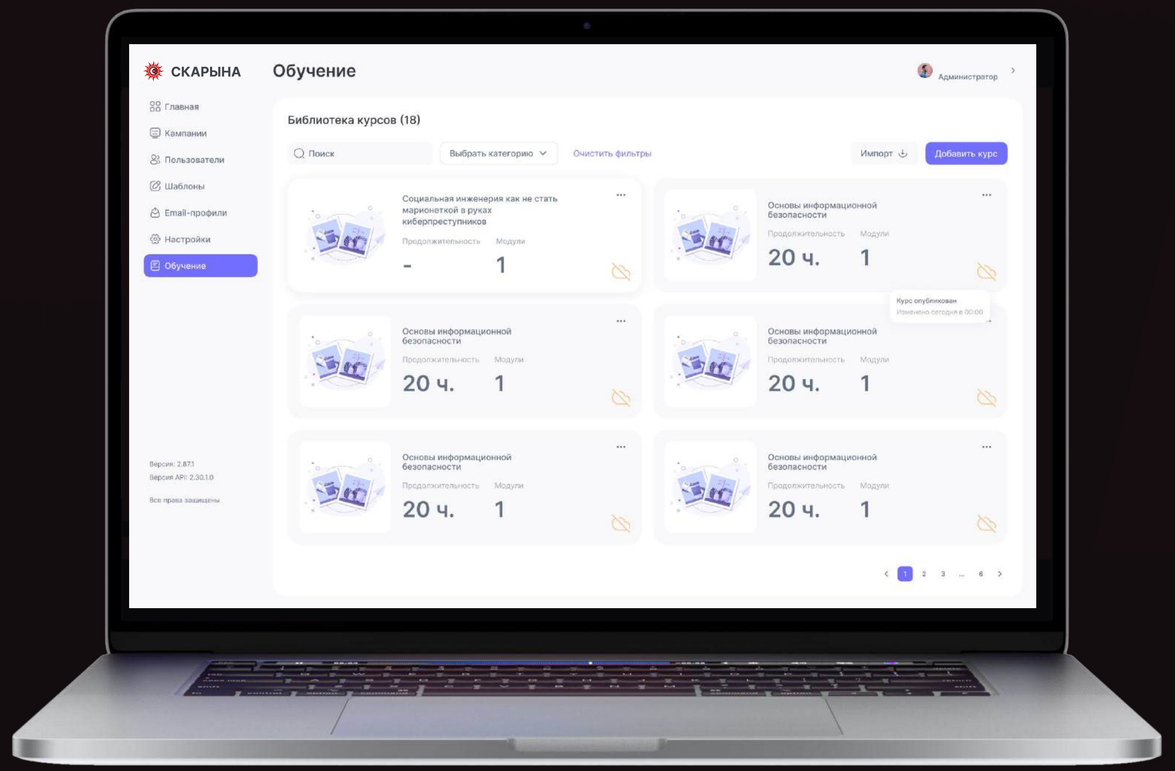
- Создайте кампанию для рассылки;
- Выберите шаблоны для письма и фишинговой страницы;
- Запустите рассылку и наблюдайте за результатами в реальном времени.



Процесс работы

3. Направление
на обучение

- Администратор назначает обучение
для сотрудников;
- Сотрудник проходит обучение на назначенных курсах;
- Обучение включает в себя обучающий материал и контрольные тестирования.



Темы образовательных курсов

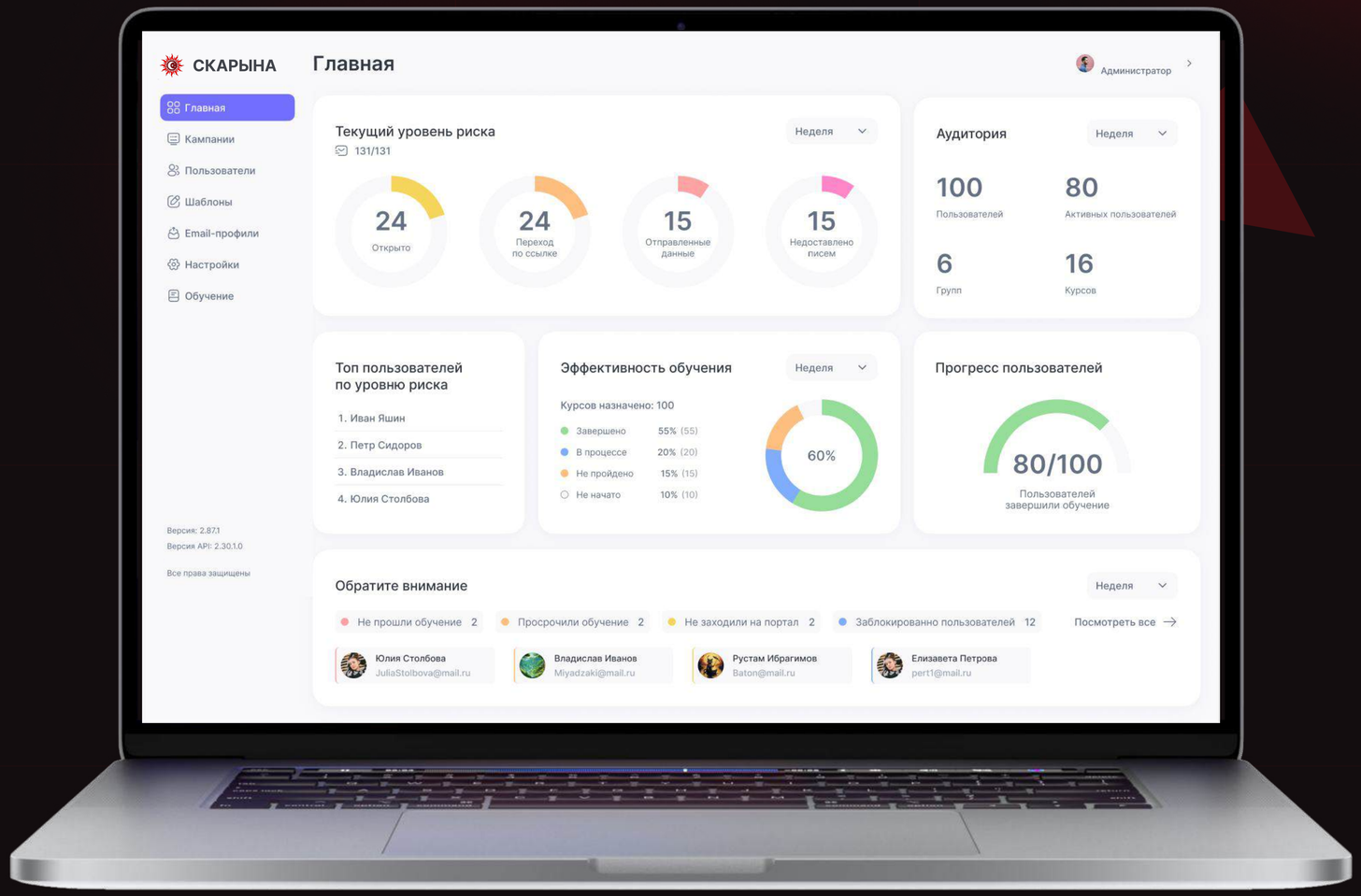
Пример

- Угрозы и последствия нарушений безопасности
- Реагирование на инциденты
- Безопасность в офисе
- Работа с конфиденциальной информацией
- Личная ответственность сотрудника в области информационной безопасности
- Спам и целевой Фишинг
- Угрозы для мобильных пользователей – как мошенники могут взломать ваш ноутбук или смартфон
- Психологические приемы и актуальные примеры атак
- Способы проверки отправителя, ссылки, вложенного файла
- Работа с VPN и двухфакторной аутентификацией
- Работа в недоверенных беспроводных сетях
- Правила получения доступов
- Физическая защита, блокировка и поиск потерянных устройств
- Проверка обновлений на ноутбуках и смартфонах
- Правила безопасности в публичных местах и поездках
- Работа с паролями

SURTE IT

Дашборд

Пример



Преимущества

в 3X

Повышается уровень осведомленности сотрудников

100+

Шаблонов фишинговых писем

на 80%

Снижается число инцидентов уже в первый месяц использования системы

20

Образовательных курсов по информационной безопасности

Спасибо!

surte.by vz@surte.by +375 (29) 114 81 69