Ваша безопасность – наша ответственность. Использование внешних компетенций при построение ИБ в компании

Михаил Юденков
Бизнес-консультант по безопасности
Группа развития продаж решений ИБ в ЦФО и ЮФО
Отдел территориальной экспертизы Департамента ИБ
Т +7(473) 250-20-23 доб. 6247 | М +7 (920) 210 31 95 |
Mikhail.Yudenkov@softline.com

Внешние факторы

We know we can

softline

Вызовы Нового Времени

— А что вообще в мире делается?
— Стабильности нет. Террористы опять захватили самолет.

Художественный фильм «Москва слезам не верит»

Вызовы Нового Времени

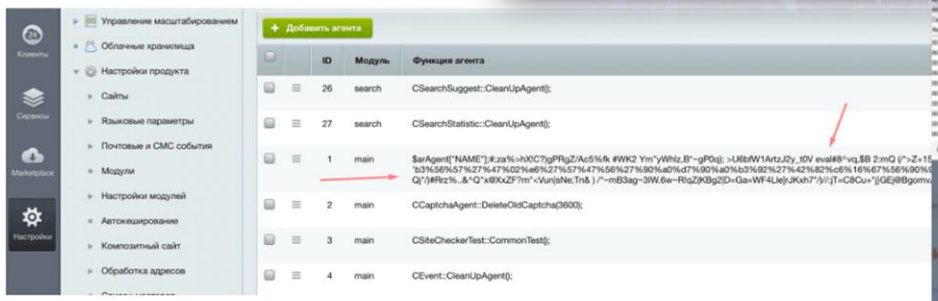
Массовый взлом сайтов на Битрикс 2023

Массовый дефейс веб-сайтов .РФ

Средний · 7 мин · 50K

Блог компании RUVDS.com, CMS*, Информационная безопасность

Кейс

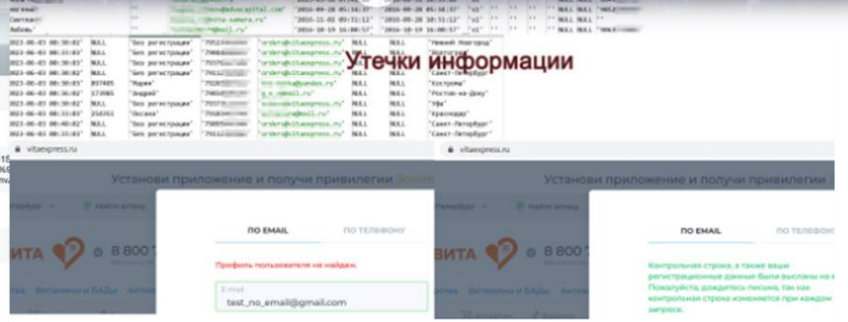


26 мая 2023 года произошёл массовый дефейс веб-серверов национального сегмента сети интернет .РФ. В качестве цели атаки выступила CMS «Битрикс».

Продолжается "слив" данных из крупных компаний. Хакер уже "слил" данные book24.ru, askona.ru, gloria-jeans.ru, «Ашан», «Твой Дом», «Буквоед», «Едим Дома», «Леруа Мерлен» и «ТВОЕ».

Сейчас были выложены в свободный доступ частичные дампы с информацией клиентов/пользователей предположительно: книжных интернет-магазинов *«Читай-город» и «Эксмо»*, сайтов издательства *«АСТ»* и горного курорта *«Роза Хутор»*.

Утечки информации



Вчера в открытый доступ были выложены фрагменты *SQL*-дампа из CMS *«Bitrix»* предположительно интернет-аптеки *«Вита»* (*vitaexpress.ru*).

В двух файлах находится **частичная информация** из таблиц заказов и зарегистрированных пользователей.

В свободно доступных фрагментах: 666,944 записи пользователей (645 тыс. уникальных адресов эл. почты и 654 тыс. уникальных номеров телефонов) за период с 29.08.2015 по 23.03.2023 и 351,708 заказов (933 и 943 уникальных адреса и номера

Битрикс24

We know we can

softline

Вызовы Нового Времени

Милош Вагнер также рассказал журналистам, что киберпреступники в настоящее время преимущественно атакуют небольшие организации малого и среднего бизнеса, которые на сегодняшний день не могут обеспечить высокий уровень информационной безопасности и защиты данных, в отличие от крупного бизнеса, который в последние 1,5 года смог подстроиться под атаки хакеров, выстроив надёжную защиту своей IT-инфраструктуры.

StormWall: во время майских праздников в России произошёл всплеск DDoS-атак

Дата: 12.05.2023. Автор: Артем П. Категории: Новости по информационной безопасности

Специалисты по информационной безопасности профильной компании StormWall обнаружили, что во время прошедших майских праздников был зарегистрирован всплеск DDoS-атак, которые проводились на многие отечественные культурные учреждения, интернет-сервисы для бронирования билетов и гостиниц, а также на транспортные сервисы.

2023: ИБ-центр ФСБ фиксирует более 170 кибератак на Россию каждый день

Ежедневно на информационные российские ресурсы фиксируется более 170 комплексных компьютерных атак, сообщил заместитель директора Национального координационного центра по компьютерным инцидентам (НКЦКИ) Николай Мурашов 25 мая 2023 года.

ии Интернет-приемная RU

Банки в январе — марте 2023 года отразили 2,7 млн атак кибермошенников на счета клиентов и таким образом предотвратили хищения на 712 млрд рублей, говорится в «Обзоре отчетности об инцидентах информационной безопасности при переводе денежных средств». Банк России впервые раскрывает в своих материалах информацию о попытках злоумышленников похитить деньги у граждан.

Тем не менее мошенникам удалось провести 252,1 тыс. операций без согласия клиентов, их объем составил 4,5 млрд рублей. Больше всего денег злоумышленники похитили через переводы с помощью онлайн-банкинга, в том числе это были заемные средства.

Проблемы Информационной безопасности 2023

К 2025 году почти 50% руководителей отделов кибербезопасности сменят работу

12:01 / 25 февраля, 2023 Gartner ИБ информационная безопасность взлом

Отчёт Gartner показал, какие факторы повлияют на спад числа квалифицированных сотрудников.

Согласно новому отчёту компании Gartner, к 2025 году почти 50% руководителей в области кибербезопасности сменит работу, 25% — перейдут на другие должности исключительно из-за многочисленных факторов стресса, связанных с работой.

Персональная ответственность

Повышенные риски в связи с текущей обстановкой

Давление со стороны регуляторов и бизнеса

… а ещё дефицит кадров…

Проблемы Информационной безопасности 2023

Сейчас просматривает 1 человек

Инженер по информационной безопасности

200 000 – 300 000 руб.

Москва

Опыт от 3 до 6 лет

Работодатель сейчас онлайн

Откликнуться

Сейчас просматривает 1 человек

Специалист по информационной безопасности

170 000 – 200 000 руб.

Москва

Опыт от 3 до 6 лет

Откликнуться

Больше 30% открытых вакансий в ИБ приходится на Москву

Регион

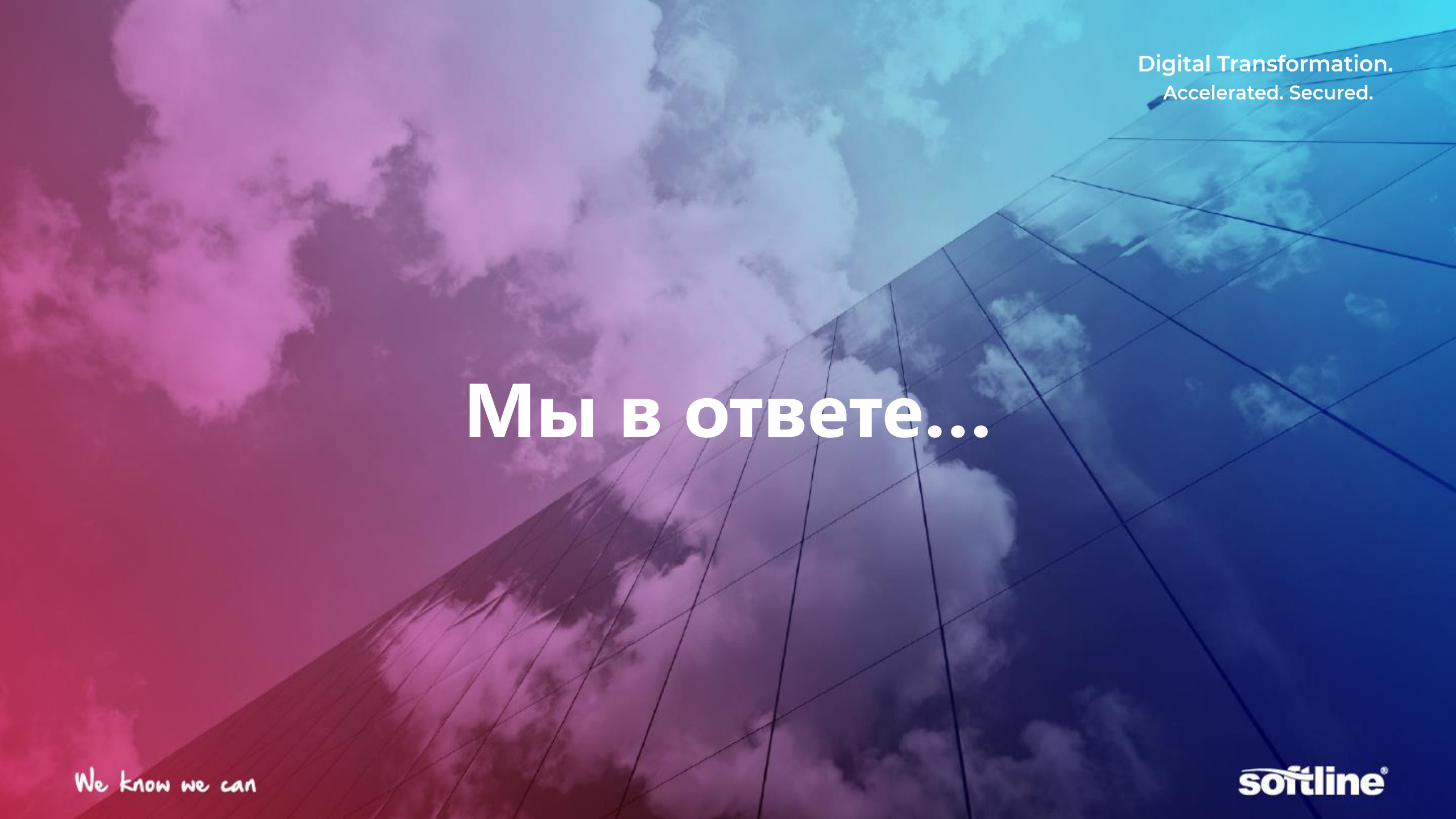
- Россия *2 902*
- Москва *1 169*
- Санкт-Петербург *321*
- Краснодарский край *114*
- Свердловская область *93*

Штат из 2х специалистов по ИБ

2 * 12 * 200 000 = 4 800 000

+ страховые взносы(30%)

4 800 000 * 1,3 = 6 240 000 в год


Digital Transformation.
Accelerated. Secured.
Мы в ответе...
We know we can
softline

Цитата

«— 007, я ваш новый ассистент.
— Это какая-то шутка?
— Потому что я не в белом халате?
— Потому что вы слишком юны.
— Моя внешность вряд ли имеет значение.
— Ваш опыт — имеет.»

007: Координат ы «Скайфолл» (Skyfall)

Рейтинги


Крупнейшие поставщики решений в сфере информационной безопасности в России
по выручке за 2020 год (в млн рублей)
kaspersky 50 784
softline 20 320
BI.ZONE 8 971
infotecs 7 290
Информзащита Системный интегратор 7 282
Jet 6 970
Ростелеком Солар 6 553
КОД безопасности 5 854
positive technologies 5 803
INNOSTAGE 4 646
TADVISER


Крупнейшие поставщики решений в сфере информационной безопасности в России
по выручке за 2021 год (в млн рублей)
kaspersky 1 55 388 +9,1%
softline 2 22 311 +9,8%
Ростелеком Солар 12 270 +46,9%
GIS ГАЗИНФОРМ СЕРВИС 3 10 511 +17,6%
BI.ZONE 10 448 +16,5%
Jet 8 838 +26,8%
infotecs 8 469 +16,2%
positive technologies 7 076 +28%
INNOSTAGE 6 114 +31,6%
ANGARA SECURITY 6 113 +91,7%
TADVISER
2021 год
2020 год
Динамика выручки 2021/2020
1 - Глобальная выручка компании
2 - По оценке TAdviser
3 - Выручка из открытой бухгалтерской отчетности. Без НДС

Почему SL?

Инфраструктура

- Безопасное рабочее место
- Сетевая безопасность (NGFW, IPS, ATP)
- Облачная безопасность (CASB)
- Защищенные каналы связи (VPN)
- Аудит изменений
- Безопасная совместная работа с контентом
- Защита баз данных (DAM)
- Безопасная мобильность (MDM, EMM)
- Контроль целостности
- Безопасность почтового и веб траффика

Защита данных

- Тренинги/проверки сотрудников (awareness)
- Защита данных (DLP)
- Управление доступом (IDM, PAM, PIM, 2FA)
- Шифрование данных

Безопасность приложений

- Анализ кода
- Безопасность приложений (WAF)
- Управление конфигурациями
- Тесты на проникновение (pentest)

Управление ИБ

- Управление инцидентами (SIEM, IRP)
- Security Operation Center (SOC)
- Индустриальные стандарты
- Управление рисками
- Соответствие законам (152ФЗ, GDPR, СТОБР, 382П. 683-684П. 187ФЗ)
- Авторские продукты (ETHIC)
- КИИ

НАШИ СЕРВИСЫ:

Проектирование

Пилотирование

Внедрение

Техподдержка

Управляемые сервисы

Почему SL?

Я всегда могу выбрать, но я должен знать, что даже в том случае, если я ничего не выбираю, я тем самым всё-таки делаю выбор.

Жан-Поль Сартр

50 000 р

VS

500 000 р

Разрушители мифов

Популярные суеверия:

- Мы не хотели бы чтобы третьи лица получили доступ к нашей информации, это не безопасно…
- Сегодня мы вам расскажем что у нас с ИБ, а завтра нас взломают…
- У нас принято решать задачи внутренними ресурсами…
- Это дорого
- Антивирус и Микротик отлично справляются…

We know we can t

На самом деле:

- Нам не нужна ваша информация. Большинство сервисов построены на сборе и анализе логов. Передача ведётся по шифрованным каналам.
- Репутация в сфере ИБ – это всё. Любой реальный прецедент и можно ставить крест на этом бизнесе. И наши пентестеры бесплатно не работают ☺
- Это отлично. Но не всегда хватает самих ресурсов на задачи связанные с внедрением и мониторингом ИБ.
- А с чем вы сравниваете стоимость? Инфобез это та сфера, где от компетенций и опыта зависит всё! А реальные инциденты могут стоить миллионы…
- К сожалению нет. В наше время подобных средств катастрофически не достаточно для защиты от сложных и направленных атак. И мы готовы вам это доказать…

softline®


Digital Transformation.
Accelerated. Secured.
Мы знаем.
Мы можем.
We know we can
softline

Что такое пентест?

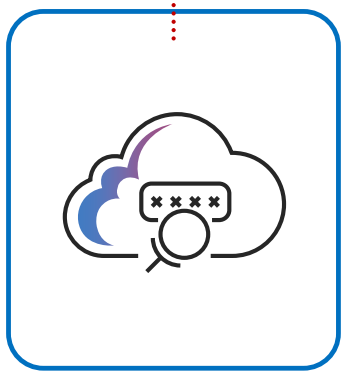
Тестирование на проникновение (пентест, penetration test) это эмуляция действий реальных злоумышленников, использование тех же векторов атак, инструментов и последовательностей действий, которые используют злоумышленники в реальных атаках.

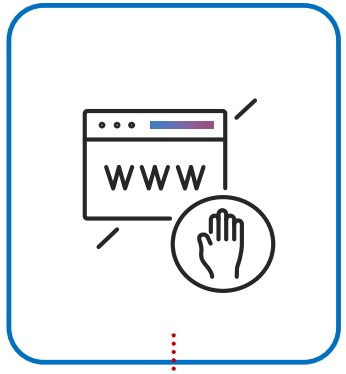
Задачи пентеста:

- определение наличия угроз безопасности систем и информации;
- оценка возможности последствий хакерской атаки
- определение уязвимостей в защите системы; оценка эффективности средств защиты;
- получение аргументов для обоснованности вложений в систему ИБ;
- формирование мер, которые помогут снизить возможность реализации хакерских атак;
- Соответствие требованиям регуляторов (PCI DSS, ГОСТ, Положения Банка России).

Виды пентеста

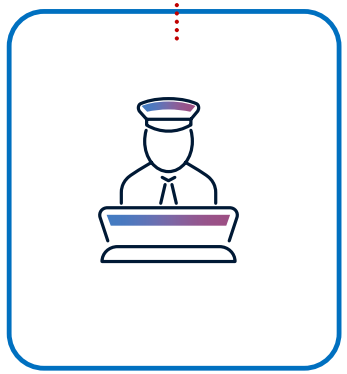
Пентест **web-приложений**

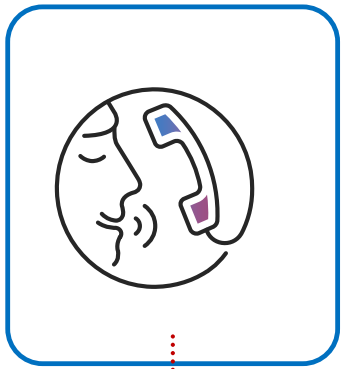




Пентест **внешнего периметра**

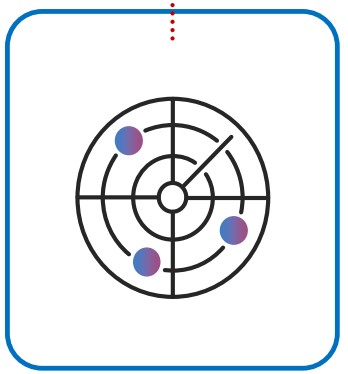
Пентест **внутреннего периметра**





Социотехнический пентест

Пентест **Wi-Fi сетей**



Анализ кода

82% уязвимостей содержатся в коде приложений

>50% уязвимостей веб-приложений относятся к критически серьёзным

60% утечек связаны с незакрытыми уязвимостями приложений

158 дней в среднем занимает устранение каждой из уязвимостей

В связи с низкой безопасностью разрабатываемого ПО растет ущерб от инцидентов ИБ

Кривая Боэма: экспоненциальный рост стоимости исправления дефектов

Итоговые документы

INFOSECURITY

ТЕХНИЧЕСКИЙ ОТЧЕТ

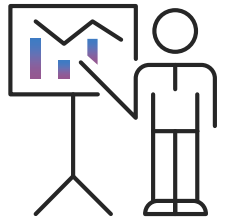
- структурированное описание полученных данных о целевой инфраструктуре (видение целевой инфраструктуры с позиции потенциального злоумышленника)
- описание выявленных уязвимостей
- описание предпринятых попыток проникновения и результатов их выполнения
- аналитические выводы о текущем уровне защищенности целевой информационной инфраструктуры
- перечень разработанных рекомендаций по повышению уровня защищенности

ОТЧЕТ ДЛЯ РУКОВОДСТВА (EXECUTIVE SUMMARY)

- краткий отчет для руководства, написанный не техническим языком
- основные выводы/рекомендации

Отчёт для руководства разрабатывается вместе с Техническим отчётом и содержит описание наиболее критичных уязвимостей и оценку уровня защищённости тестируемых объектов

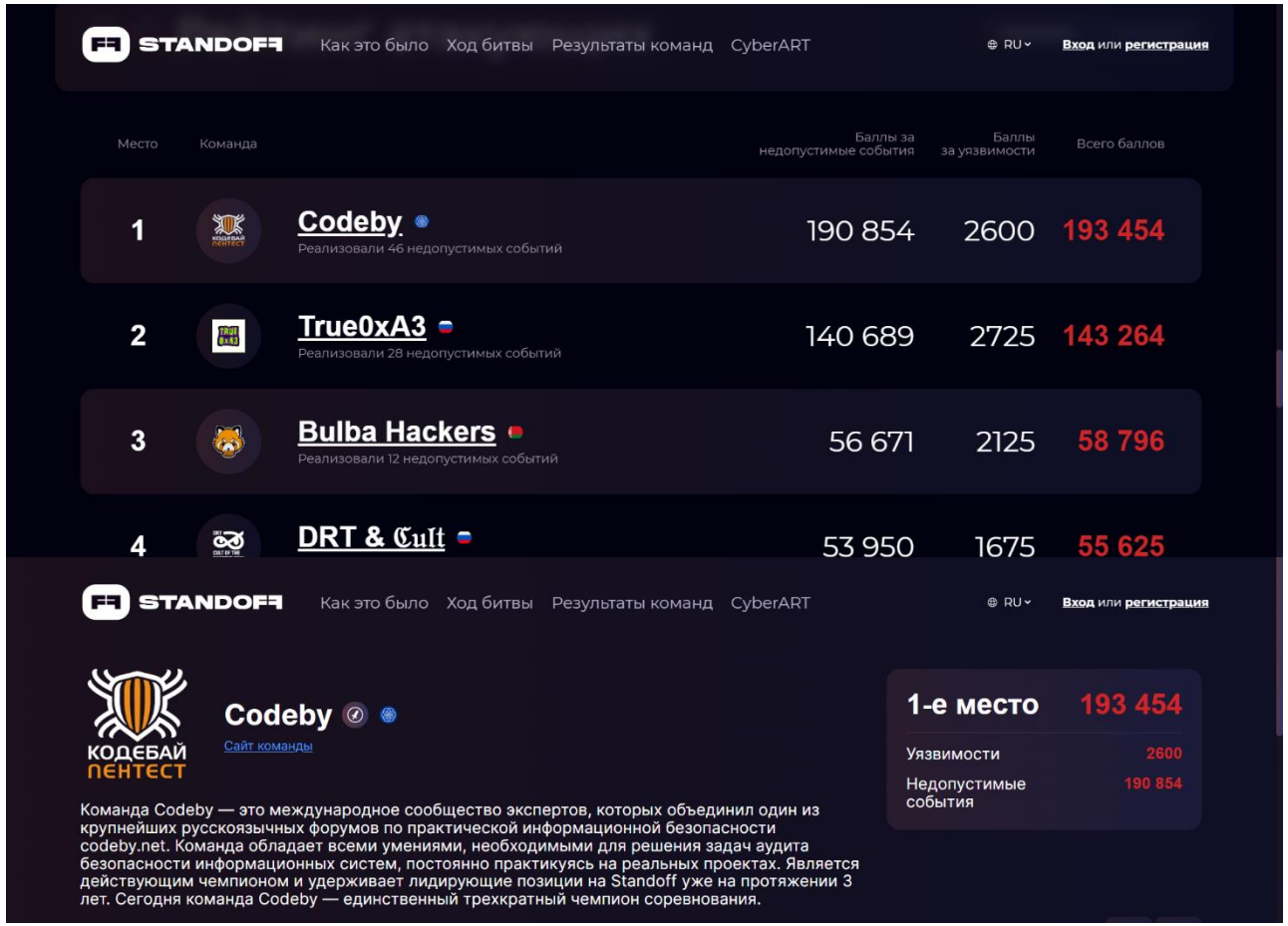
ОПЦИОНАЛЬНО:



ИТОГОВАЯ ПРЕЗЕНТАЦИЯ

ОБУЧАЮЩИЙ СЕМИНАР ПО ИТОГАМ ПЕНТЕСТА

Компетенции



ОПЫТ В СФЕРЕ ИБ

- Эксперт по анализу защищенности (пентестер) – 8 лет
- Входит в команду Codeby

КОМПЕТЕНЦИИ

- Аудит информационной безопасности
- Анализ защищённости беспроводной и сетевой инфраструктуры
- Продвинутые навыки работы с операционными системами семейства Linux и Windows
- Опыт работы с инструментами и средствами для проведения анализа защищённости и аудита информационной безопасности (Nessus, OpenVAS, Metasploit, Cobalt Strike, Intercepter-NG, Scapy, Burp Suite, etc.)
- Разработка инструментов для тестирования на Python,Golang

КУРСЫ И СЕРТИФИКАТЫ

- Red Team operation
- eCPTX_v2
- Cybernetics HackTheBox lab
- APT HackTheBox lab

ЗАЧЕМ НУЖЕН SOC

ЦЕЛИ:

1. Снижение рисков хищения данных и денежных средств
2. Обеспечение непрерывности бизнеса
3. Снижение тяжести последствий инцидентов

ПОДХОД:

1.Выявление инцидентов на основе корреляции данных из разных источников сети клиента и реакция на кибератаку на ранних стадиях;

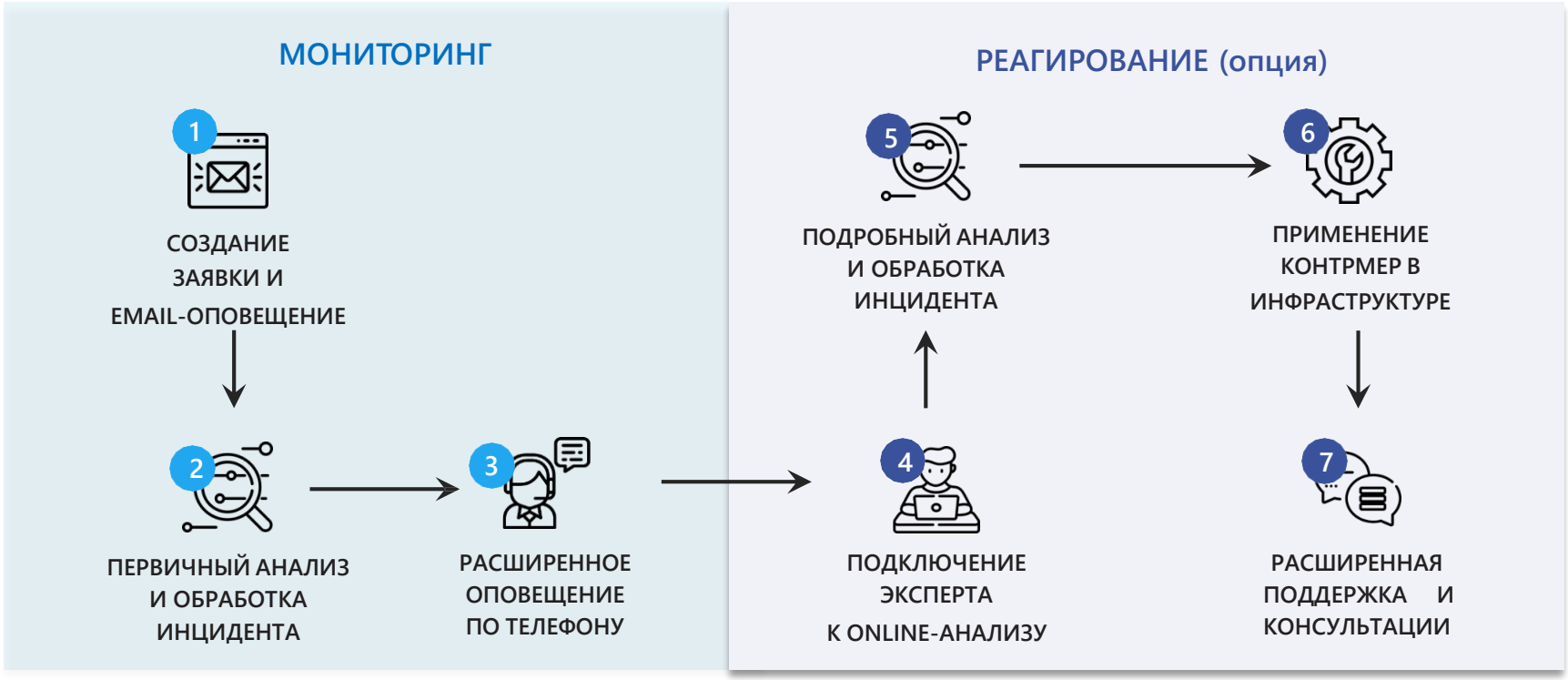
2. Быстрый экспертный разбор инцидентов, выдача рекомендаций службам компании;

3.Реагирование на инциденты, их локализация в инфраструктуре клиента, нейтрализация последствий и предотвращения инцидентов.

4. Подключение к ГосСОПКА

КАК РАБОТАЕТ ISOC

Ваша инфраструктура



КОМАНДА ISOC (INFOSECURITY SOC)

В команде более **40 экспертов**, занимающихся **непосредственно** мониторингом и расследованиями инцидентов.

Всего с SOC взаимодействуют более 60 профильных инженеров по различным направлениям информационной безопасности.


Q&A

GO GLOBAL

GO CLOUD

GO INNOVATIVE

Digital Transformation and Cybersecurity Solution Service Provider