Контур
staffcop

Система расследования инцидентов
внутренней информационной безопасности

О компаниии

13 лет

Экспертизы в информационной безопасности

3000

Клиентов в 40 странах мира

>250 тыс

ПК под защитой Staffcop

25

Клиентов из ТОП-100 РБК

Forbes ADVISOR

Лучшее ПО по версии
Forbes Advisor 2023 и 2024

СКБ Контур

Входим в ГК СКБ Контур

Импортонезависимый продукт.
Российский разработчик

ФСТЭК России
Федеральная служба по
техническому и экспортному контролю

4 уровень доверия

АРПП
Отечественный софт

Минцифры России

Sk Участник

РУС СОФТ

Статистика по ИБ

>1,12 млрд.

Скомпрометированных учетных записей за 2023 г.
(на 60% больше, чем в 2022 г.)*

*Исследование ГК InfoWatch от Утечки информации ограниченного доступа в России за 2022-2023 от 11.03.24

87%

На одну утечку в среднем пришлось больше записей, чем в 2022 г.*

*По данным РКН от 28.01.23

x3

Втрое выросла доля утечек информации категории «государственная тайна» (относительно 2022 г.)*

*Исследование ГК InfoWatch

>80%

Более 80% утечек информации произошли в результате кибератак*

*Исследование ГК InfoWatch

Актуально

>66%

Социальная инженерия

Подкуп

Шантаж и угрозы

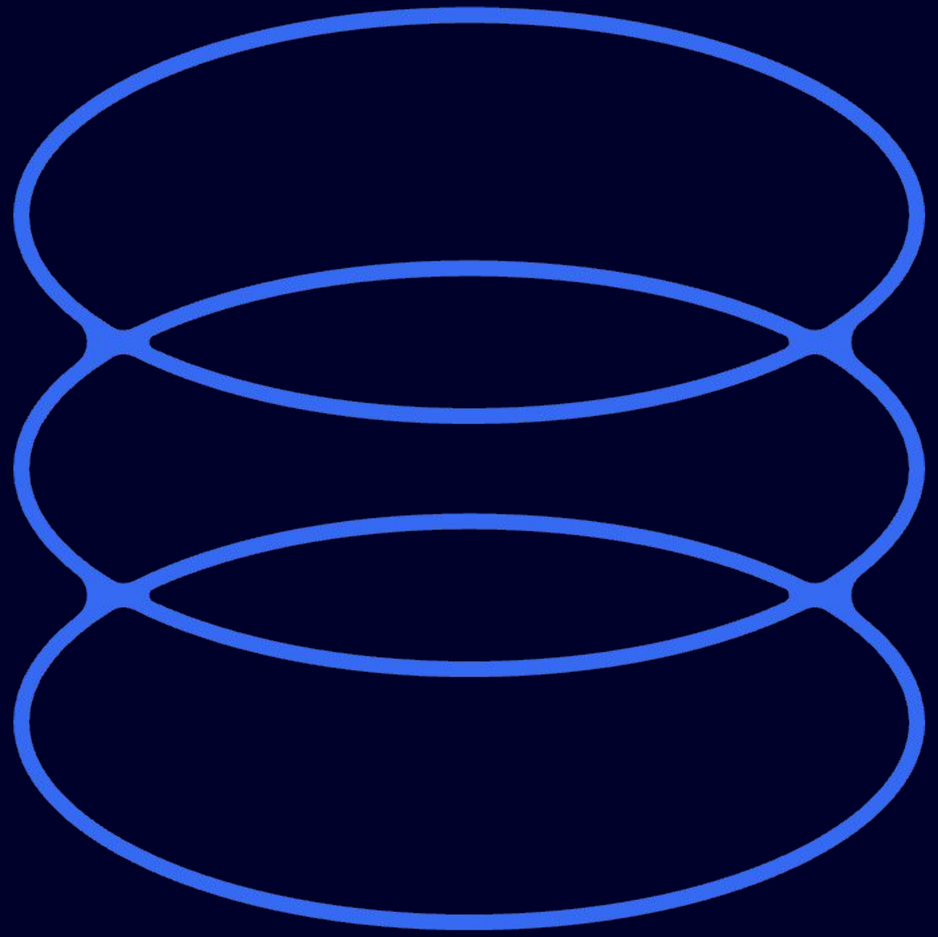
Введение в заблуждение
(Кибербезграмотность)

Примеры внутренних инцидентов

- Фиктивные списания оборудования;
- Проекты на стороне;
- Утечка персональных данных клиентов;
- Утечка коммерческой информации;
- Слив клиентской базы;
- Слив активных заявок от клиентов;
- Вторая работа у сотрудника;
- Нарушение трудовой дисциплины.

Репутационные риски, штрафы, недополученная прибыль компании.

Кейсы



Продажа маршрутизаторов

Инцидент:

IT-специалист списывал рабочее оборудование под видом сломанного и продавал на Авито

Что сделали:

1. Изучили историю браузинга и данные скриншотов, а также кейлогера
2. Сверили объявления и данные бухгалтерии

Итог:

Махинация обнаружена, сотрудник был уволен, в одном из похожих кейсов один из клиентов передал данные в полицию

Проекты на стороне

Инцидент:

Инженер конструкторского бюро работал над «сторонними» проектами во время основной работы

Что сделали:

1. Совместили «работа в приложении» и «файл не в типовом месте» или «работа в нерабочие часы»
2. Обнаружили факт работы с файлом на рабочем столе вместо хранилища
3. По скриншотам увидели работу со «сторонним» проектом

Итог:

С сотрудником и клиентом провели разъяснительную работу, доработали локальные нормативные акты и регламенты

Утечка скана паспорта и номера карты

Инцидент:

Сотрудница банка отправляла
с личной почты и через мессенджеры
сканы паспорта и номера карт
клиентов

Что сделали:

1. Нейросеть в Staffcop определила, что среди передаваемых изображений есть скан паспорта
2. Сработал алгоритм Луна
3. Детально изучили информацию и скриншоты

Итог:

Справедливость восторжествовала, но результат нам неизвестен из-за NDA

Подготовка к увольнению

Инцидент:

Сотрудник перед увольнением прошёл собеседование у конкурента

Что сделали:

1. Использовали словарь на основных конкурентов в посещённых сайтах, email-адресах, сообщениях
2. Изучили отправленные тексты

Итог:

Сотруднику ограничили доступ к информации внутреннего контура компании и пригласили на беседу с HR

Слив заказов конкурентам

Инцидент:

Фирма по производству пластиковых окон заметила, что конкуренты перезванивают клиентам по их заявкам

Что сделали:

1. Изучили бизнес-процесс в компании
2. Пометили файл специальной меткой, чтобы увидеть перемещения
3. Настроили словарь на фразу-метку
4. Выявили сотрудника, который «сливал» данные конкурентам

Итог:

Сотрудника уволили, компания изменила бизнес-процессы, важные файлы перестали хранить в открытом доступе

Скачал файлы на флешку с ПК коллеги

Инцидент:

Сотрудник планировал уволиться
и решил захватить файлы
с компьютера коллеги. Знал,
что в организации есть Staffcop

Что сделали:

1. Сработал алерт на слив информации
2. Изучили, куда был записан файл
3. Посмотрели, как и кем флешка использовалась до этого

Итог:

Непричастный сотрудник был оправдан,
а причастный — уволен

Вот и лето прошло

Инцидент:

В августе понизилась активность у всего отдела. Не выполнили план месяца из-за того, что занимались подготовкой детей к школе

Что сделали:

1. Проанализировали активность в рабочее время
2. Обнаружили активность на маркетплейсах, сидели на Ozon, WB по несколько часов в день

Итог:

Работодатель вынес предупреждение всему отделу

Телефонные мошенники

Инцидент:

Офис-менеджеру пришло сообщение в Telegram от генерального директора с просьбой отправить документы. Попросил сделать это с личной почты, торопил и говорил, что вопрос очень важный.

Что сделали:

1. Нейросеть в Staffcop определила, что среди передаваемых изображений есть скан паспорта
2. Сработал словарь на номер автомобиля
3. Отследили, кто скинул файлы на флешку

Итог:

Предотвратили кражу денег в компании

Любитель откатов

Инцидент:

Сотрудник фирмы ездил на личные встречи с заказчиками, брал с собой ноутбук, тет-а-тет договаривался об «откатах»

Что сделали:

1. Изучили календарь встреч сотрудника
2. Настроили конфигурацию для записи звука
3. Расшифровали записи с помощью Speech-to-text
4. Изучили текст, прослушали спорные записи

Итог:

Сотрудника уволили и оптимизировали цепочки поставок

Жадный сотрудник у туроператора

Инцидент:

Сотрудник, получив 100 тыс. рублей от клиента за тур, распечатывает два договора: один на 100 тыс., другой на 80 тыс. рублей. Он уничтожает договор на 100 000 рублей и отдаёт в бухгалтерию договор на 80 тыс., присваивая себе разницу.

Что сделали:

1. Изучили файлы, которые уходили на печать
2. Сравнили с документами, которые предоставлялись в бухгалтерию
3. Изучили скриншоты, которые окончательно подтвердили мошеннические действия сотрудника

Итог:

Сотрудника уволили, ввели процессы сверки платежей и документов

Импортонезависимость

Риски использования зарубежного ПО:

- Неожиданно перестает работать
- Отсутствуют репутационные риски производителя
- Не понятно какие данные собираются и куда отправляются
- Не понятное влияние на «зоопарк» решений
- Встроенные угрозы
- Отсутствие технической поддержки

Использование отечественного и независимого ПО

Технологии сервера: компоненты, не требующие лицензирования и покупки

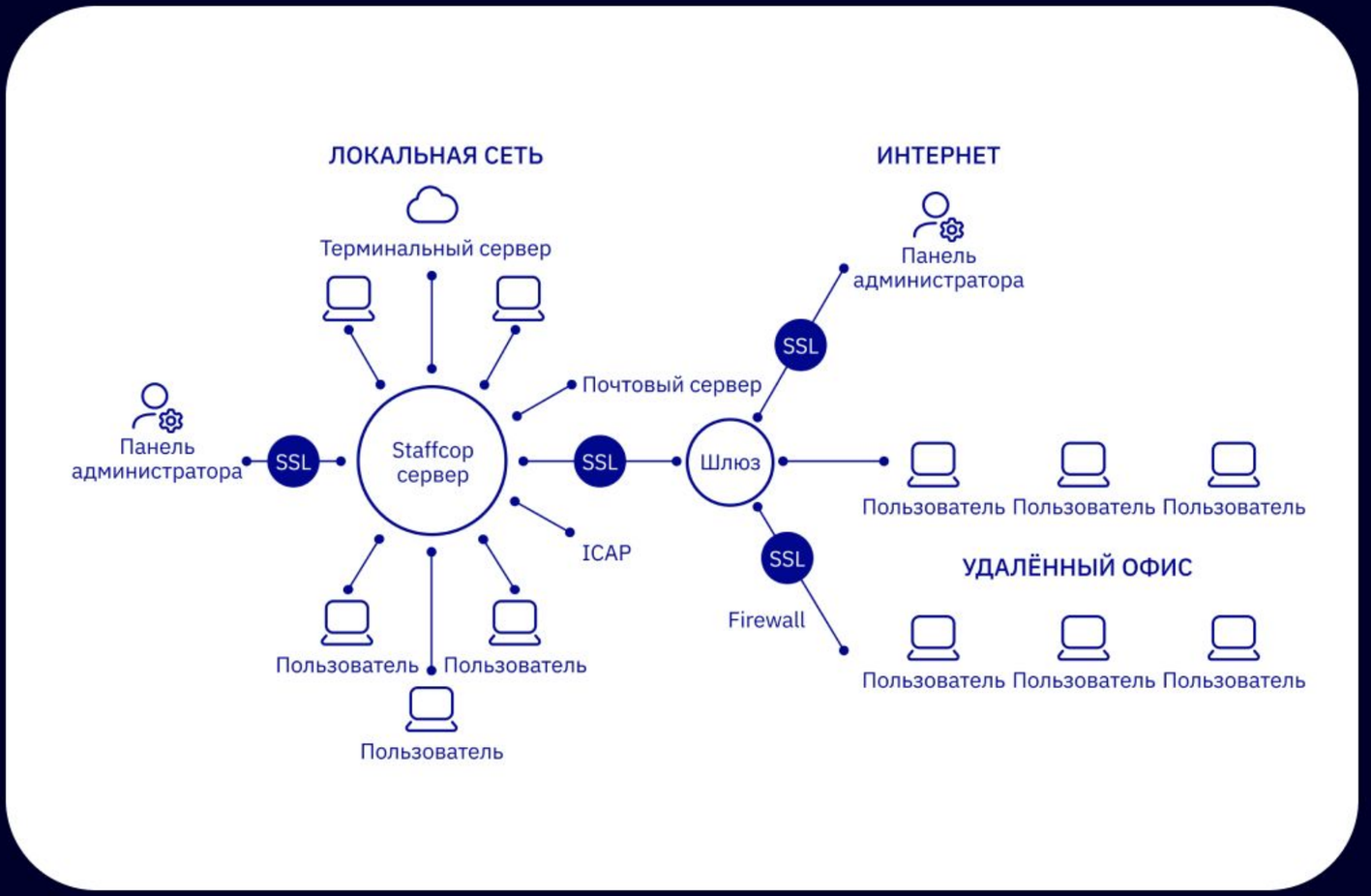
ASTRA LINUX®
open source initiative
ClickHouse
Jatoba
PostgreSQL
NGINX

Доказано совместимы с:

ASTRA LINUX®
РЕДОС
SIEM
ROSA
base alt
Ankey ASAP
AlterOS

Эффективные архитектурные решения

- Единая консоль управления
- 100 ПК = 6 CPU, 32 RAM
  1000 ПК = 12 CPU, 96 RAM
- Для работы достаточно одного виртуального сервера
- Агент для Windows, Linux, macOS
- Минимальные требования к железу
- Импортонезависимое ПО
- Масштабируемая архитектура
- OLAP-технология



Решаемые задачи:

Информационная безопасность

Расследование инцидентов внутренней информационной безопасности

Выявление инсайдерской деятельности

Выявление случаев мошенничества и коррупционных схем

Поиск нелояльных сотрудников, выявление групп риска

Предотвращение утечек и сливов чувствительной информации

Своевременное оповещение о нарушении политик безопасности

Удаленное администрирование

Расследование причин сбоев на рабочих станциях пользователей

Выявление использования «нелегального» ПО

Удаленное консультирование пользователей

Защита локальной сети блокировкой USB-носителей

Блокировка не относящихся к работе программ и сайтов

Повышение эффективности труда

Контроль удаленных сотрудников и офисов

Блокировка не относящихся к работе программ и сайтов

Выявление сотрудников, желающих сменить место работы

Выявление «узких» мест в бизнес-процессах

Сравнение сотрудников / отделов по ключевым показателям

Контроль присутствия на рабочем месте

Возможности

Расследования

Инцидентов внутренней информационной безопасности

Причин неэффективной работы

Уведомления

Оповещение на почту или в Telegram по инцидентам, которые вас интересуют

Выявление

Коррупционных схем и мошенничества внутри компании

Нелояльных сотрудников, работающих на конкурентов

Блокировка

Копирования на съемные носители

Пересылки конфиденциальной информации

Доступа к нерегламентированным ресурсам

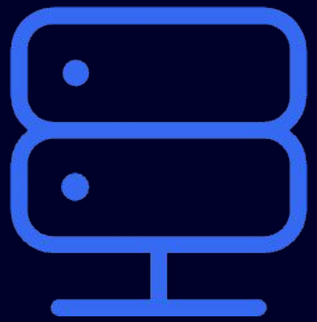
Собственникам бизнеса

ИБ специалистам

Сотрудникам HR

IT специалистам

Аспекты внедрения



Этика внедрения

Технологические вопросы

Юридические вопросы

Преимущества Staffcop Enterprise

Плюсы сотрудничества

Лёгкое внедрение в существующую инфраструктуру

Индивидуальный подход, закреплённый менеджер

Качественная и доступная техподдержка

Расширенный тестовый период с полным функционалом

Эффективная стоимость конечного владения

Доступ к регулярным обновлениям

Преимущества продукта

Сертифицирован ФСТЭК и ФСБ, входит в реестр отечественного ПО

Быстрый и лёгкий

Поддерживает различные ОС и ИБ-системы, открытое API

Импортонезависимый и опенсорсный

Работает в любых сетях

Единый веб-интерфейс для управления

Строит многомерные отчёты и выгружает аналитику

Качественная и подробная документация

Тестируйте уже сейчас

Быстро

Развертывание пилотного проекта
обычно занимает не более одного дня

Легко

Требуется минимум усилий
и ресурсов для запуска

Комплексно

Вы сможете оценить сразу весь
комплекс решаемых задач
и принять правильное решение

Бесплатный аудит

Позволит вскрыть точки роста
в Вашей системе ИБ

Staffcop Enterprise — единственное решение для мониторинга и защиты данных, сочетающее выгодную стоимость владения и лучший уровень клиентского сервиса без компромиссов в функциональности.