софтлайн РЕШЕНИЯ

Информационная безопасность

Услуги и продукты

Хлебников Андрей

Руководитель департамента технологического развития

О компании

INFOSECURITY

специализированный сервис-провайдер,
уже более 15 лет оказывающий услуги в сфере

- информационной безопасности
- лицензиат ФСБ России и ФСТЭК России

Компания успешно внедряет и сопровождает системы защиты информации в различных отраслях:

- финансы
- промышленность
- медицина
- государственный сектор

и др.

Специализация

- Техническая поддержка
- Внедрение
- Compliance
- Аналитическая поддержка
- Безопасность как сервис (MSSP)
- Проектирование
- Консалтинг
- Обучение
- Аудит
- Awareness

>25 000	>300	>20	>350
угроз выявляем ежемесячно	профессионалов в команде	сервисов и услуг для защиты бизнеса	компаний под нашей защитой

Ключевые сервисы

Консалтинг

Проводим оценку рисков и состояния СЗИ, выстраиваем системы менеджмента, помогаем соответствовать требованиям регуляторов

Услуги на основе вендорских продуктов

- Kaspersky
- Positive Technologies
- F6 (FACCT)
- Security Vision
- АйТи Бастион
- ...
- Infowatch
- Код безопасности
- UserGate
- Check Point
- R-Vision
- ...

Комплексный подход

Проводим полный цикл работ под ключ

- Обследование, аудит
- Планирование
- Пилотирование решений
- Проектирование
- Реализация
- Управление и оптимизация +

Собственные продукты и услуги

- ISOC+
- ETHIC.DRP
- ETHIC.CPT
- Awareness
- Pentest
- Управление уязвимостями
- Киберполигон
- Техподдержка 24x7, 9x5
- Аутсорсинг

Информационная безопасность

- Безопасность АСУ ТП
- Мониторинг и реагирование на инциденты ИБ
- Анализ исходного кода (DevSecOps)
- Управление уязвимостями (VM)
- Анализ сетевого трафика (NTA)
- Обнаружение и реагирование на угрозы на конечных точках (XDR)
- Антивирусная защита (AV)
- Защита мобильных устройств (MDM/UEM)
- Защита от целевых угроз (AntiAPT, Sandbox)
- Управление привилегированным доступом (PAM)
- Многофакторная аутентификация (MFA)
- Защита от утечек и расследование инцидентов (DLP)
- Управление правами и учетными записями (IDM)
- Инфраструктура ложных целей (DDP)

udv|group, ASP, INFOWATCH, positive technologies, kaspersky

SECURITM, ПАНГЕО РАДАР, RUSIEM, R-Vision, Security Vision, positive technologies, kaspersky

SWORDFISH SECURITY, APPSEC SOLUTIONS, solidlab, Hexway, SOLAR, positive technologies, kaspersky

ФРОДЕКС, Security Vision, positive technologies, RED Check, R-Vision

kaspersky, ГАРДА, F6, positive technologies

F6, positive technologies, kaspersky

Dr.WEB, kaspersky

RUPOST, НИИ СОКБ

F6, positive technologies, kaspersky

КОМПАНИЯ ИНДИД, INFRASCOPE

Identity Blitz, КОМПАНИЯ ИНДИД, MULTIFACTOR, AVANPOST

ГАРДА, ZECURION, SEARCHINFORM, INFOWATCH, SOLAR

AVANPOST, OCTOPUS, 1С, ГАРДА, SOLAR

xello

Инфраструктура. Надёжная. Защищённая.

софтлайн РЕШЕНИЯ

Защита инфраструктуры

- Создание физической инфраструктуры
- Создание виртуальной инфраструктуры
- Системы резервного копирования
- Почтовые системы
- Корпоративный защищенный обмен данными
- Защита приложений (AppSec)
- Системы DAG/DCAP
- Обучение и тестирование сотрудников
- Защита электронной почты
- Защита от DDoS
- Контроль и управление конфигурацией сетевого оборудования
- Сетевая безопасность (NGFW)
- Криптографическая защита каналов связи
- Система контроля сетевого доступа (NAC)
- Единая биометрическая система

Инфраструктура. Надёжная. Защищённая.

софтлайн РЕШЕНИЯ

Консалтинг

Оценка зрелости ИБ

Экспресс-аудит ИБ

- Для компаний с низким уровнем зрелости ИБ
- Верхнеуровневая оценка зрелости процессов
- Разработка перечня мероприятий без приоритизации внедрения
- Оценка рисков не проводится

Срок выполнения: 1 месяц

- Быстро
- Базовый анализ процессов

Middle-аудит ИБ

- Для компаний с низким и средним уровнем зрелости ИБ
- Оценка зрелости по best practices
- Качественная оценка рисков ИБ
- Разработка дорожной карты развития ИБ

Срок выполнения: 1,5 месяца

- Сбалансированный подход к анализу
- Формирование дорожной карты

Оценка зрелости и дорожная карта

- Для компаний со средним уровнем зрелости ИБ
- Оценка зрелости по best practices
- Оценка рисков в денежном выражении
- Дорожная карта развития с учетом влияния на бизнес

Срок выполнения от 2 месяцев

- Глубокая аналитика
- Оценка рисков с влиянием на бизнес
- Дорожная карта развития

Стратегия ИБ

- Для компаний с высоким уровнем зрелости ИБ
- Анализ зрелости процессов, рисков и отраслевых трендов
- Оценка рисков в денежном выражении
- Разработка стратегии ИБ с учетом бизнес- и IT-стратегии

Срок выполнения от 3 месяцев

- Глубокая аналитика
- Комплексный анализ
- Синергия бизнеса и ИТ/ИБ
- Долгосрочное развитие

Оценка рисков ИБ

1 Определение области охвата

- Поможем определить область охвата – выделим критичные направления бизнеса

2 Формализация процесса

- Разработаем методику оценки рисков ИБ, включая критерии оценки и порядок ее проведения

3 Обследование

- Определим недопустимые события и связанные с ними бизнес-метрики
- Составим перечень защищаемых активов
- Проведем оценку процессов и мер ИБ

4 Оценка рисков

- Оценим последствия сценарий реализации рисков
- Разработаем реестр рисков ИБ с указанием их величины и владельцев

5 Обработка рисков

- Составим перечень мероприятий по совершенствованию процессов и мер обеспечения ИБ

6 Информирование

- Отчет для руководства по результатам оценки рисков ИБ

Системы менеджмента ИБ

Выстраивание процесса риск-менеджмента

- Выстраиваем процессы риск-менеджмента (ISO 31000, ISO/IEC 27005, Open Fair, MITRE ATT&CK, ENISA)
- Проводим качественную и количественную оценку рисков от недопустимых событий или от несоответствий в операционной деятельности
- Поддерживаем процессы риск-менеджмента операционно – берем рутину на себя и предоставляем фактуру для принятия решений

Кибербезопасность поставщиков

- Классифицируем поставщиков по уровням риска, формируем требования по безопасности для каждой категории
- Оцениваем уровень кибербезопасности поставщиков и риски
- Контроль безопасности поставщиков на всех стадиях жизненного цикла взаимодействия

Экспертиза vCISO

- Оказываем экспертную поддержку по вопросам ИБ на стратегическом и операционном уровнях, помогаем выстраивать процессы управления ИБ, адаптировать практики защиты к бизнес-задачам и повышать зрелость ИБ

Система управления ИБ в ДЗО

- Создаем единую систему требований к процессам и мерам ИБ в рамках управления дочерними и зависимыми обществами (ДЗО);
- Разрабатываем референсную модель и систему оценки;
- Приводим процессы и меры обеспечения ИБ в ДЗО

Внедрение систем менеджмента

- Выстраиваем системы менеджмента в соответствии с требованиями международных стандартов (ISO/IEC 27xxx, ISO 22301, ISO/IEC 20000 и др.).
- Формализуем процессы ИТ и ИБ, обеспечиваем их соответствие требованиям ISO, NIST, COBIT, Сбера

Управление непрерывностью бизнеса

1 Обследование активов и процессов компании

- Определим бизнес-процессы Компании
- Проведем инвентаризацию активов

3 Разработка стратегии непрерывности

- Определим способы обеспечения непрерывности деятельности Компании
- Определим параметры восстановления сервисов

5 Обучение персонала и тестирование планов

- Разработаем обучающие материалы для персонала
- Проведем тестирование и корректировку планов

2 Выявление критических процессов и оценка рисков

- Проведем анализ воздействия на бизнес
- Проведем оценку рисков прерывания деятельности

4 Разработка планов действий в ЧС

- Разработаем инструкции для персонала Компании, задействованного в восстановлении

6 Обновление и улучшение

- Разработаем дорожную карту развития

Система управления кибербезопасностью поставщиков

Обследование активов и процессов компании

- Определим перечень поставщиков по типам
- Проведем оценку контрольной среды в области ИБ

1

Внедрение новых правил

- Окажем консультационную поддержку в ходе внедрения разработанных регламентов

3

Оценка кибербезопасности поставщиков

- Отчеты с указанием выявленных недостатков, рисков и рекомендациями по их минимизации

5

2

Формализация процесса

- Разработаем регламент обеспечения ИБ при взаимодействии с поставщиками
- Определим критерии оценки и отбора поставщиков

4

Аудит поставщиков

- Разработаем регламент управления аудитами второй стороны, программу аудитов
- Разработаем отчеты по результатам аудитов с рекомендациями

6

Обучение

- Программа обучения персонала, взаимодействующего с поставщиками
- Обучающие курсы под профили работников

Собственные продукты и услуги

Virtual CISO

Оценка эффективности и улучшение

- Разработка показателей эффективности процессов ИБ
- Подготовка отчетности для руководства
- Выработка рекомендаций по улучшению

Планирование и стратегия

- Разработка программы развития ИБ
- Приоритизация и прогнозирование потребностей
- Разработка политик и процедур

Управление программами и проектами по ИБ

- Внедрение технических решений
- Управление программой проектов
- Выбору и настройке СЗИ
- Организация IT- и бизнес-процессов
- с учетом практик безопасности

Управление рисками ИБ

- Разработка методологии
- Внедрение процесса управления рисками
- Построение модели угроз и оценка рисков
- Разработка плана обработки рисков

Аудит и контроль

- Проведение аудитов ИБ
- Контроль выполнения стандартов и процедур
- Управление инцидентами

Формирование команды и обучение

- Создание отдела ИБ, поиск и найм экспертов
- Повышение осведомленности персонала
- Программа обучения и повышения
- квалификации

ISOC

Базовый сервис ISOC

Автоматический Мониторинг
(базовые правила для базовых источников)

1

Создание заявки и email/tg оповещения

Реагирование
(базовый анализ и верификация)

2

Первичный анализ и обработка инцидента

3

Верификация, оповещение, базовые рекомендации

4

Подключение эксперта к онлайн-анализу

5

Подробный анализ и обработка инцидента

Реагирование
(плейбуки для типовых инцидентов)

6

Консультационное реагирование – рекомендации по контрмерам

Реагирование
(расширенное, не по плейбукам)

7

Расширенная поддержка, консультации, сопровождение специалистов заказчика по применению выдаваемых рекомендаций.

+

дополнительные опции сервиса

ISOC+

Визуализация и отчетность

Расследования и расширенная аналитика

Реагирование на инциденты

Автоматический мониторинг и выявление инцидентов ИБ

- Подключение типовых источников
- Подключение нетиповых источников
- Настройка источников
- Канал ГОСТ СКЗИ
- Расширенный мониторинг (KEDR MSSP)
- Разработка кастомных правил корреляции
- Расширенный срок хранения событий

- Кастомизация плейбуков
- Применение контрмер
- Сценарии автоматического реагирования
- Разработка кастомных сценариев реагирования
- Интеграции с системами клиента (ITSM, почта, CMDB)

- Расследование инцидентов
- Аналитика и экспертные консультации
- Проактивный поиск угроз

- Доработка базовых отчетов/дашбордов
- Разработка кастомных отчетов/дашбордов
- Подготовка нестандартных отчетов (в т.ч. аналитических)
- Регулярные встречи с командой SOC
- Передача информации в НКЦКИ/ФинЦЕРТ

Безопасность приложений «под ключ»

Стратегия и управление

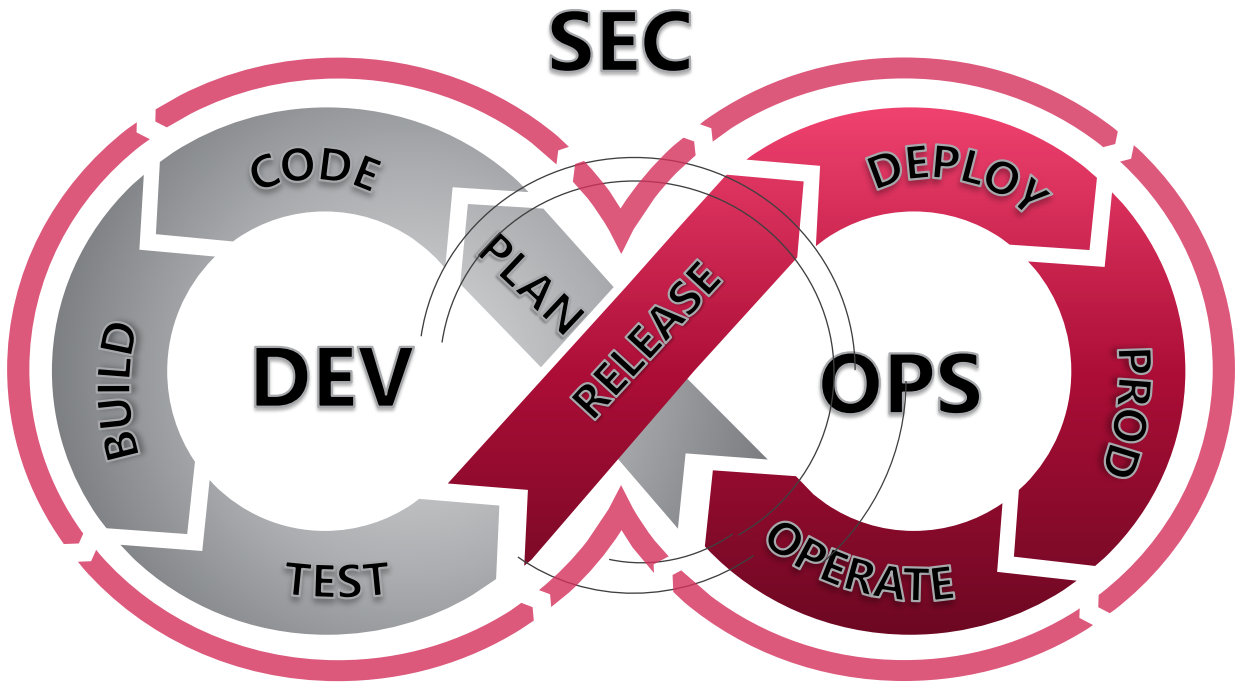
- Разработка стратегии, проектирование процессов (ГОСТ | BSIMM | SAMM)
- Тренинги и электронные курсы для разработчиков
- Программа SecChamp

Онбординг приложений

- Разработка требований по ИБ к приложениям
- Типизация и стандартизация архитектурных решений
- Моделирование угроз и оценка рисков
- Контроль безопасности при приемке

Автоматизация и харденинг

- Встраивание сканеров кода и сборок в CI/CD
- Выстраивание сквозного процесса управления уязвимостями ПО
- Харденинг инфраструктуры разработки и эксплуатации
- Контроль сред контейнеризации и оркестрации (container sec)



Тестирование на проникновение

- Внешний периметр
- Внутренний периметр
- Веб-приложения
- Wi-Fi сети
- Социотехническое тестирование
- Мобильные приложения
- Анализ исходного кода
- Continuous Penetration Testing

Проводим пентест методами «черного ящика» (black box) и «серого ящика» (grey box) без уведомления системных администраторов/ИТ-специалистов заказчика

- Наши специалисты входят в топ-10 пентестеров России
- Сертифицированные сотрудники со стажем более 13 лет
- Опыт работы в различных отраслях SMB и Enterprise-компаний
- С 2019 года специалисты занимают первые и вторые места в CTF-соревнованиях «Игры Кодебай»

Ethic.DRP защита от внешних цифровых угроз

Сокращает риски в безопасности и репутационные потери

Защищает от социальной инженерии и фишинга

Выявляет утечки корпоративных данных и учетных записей

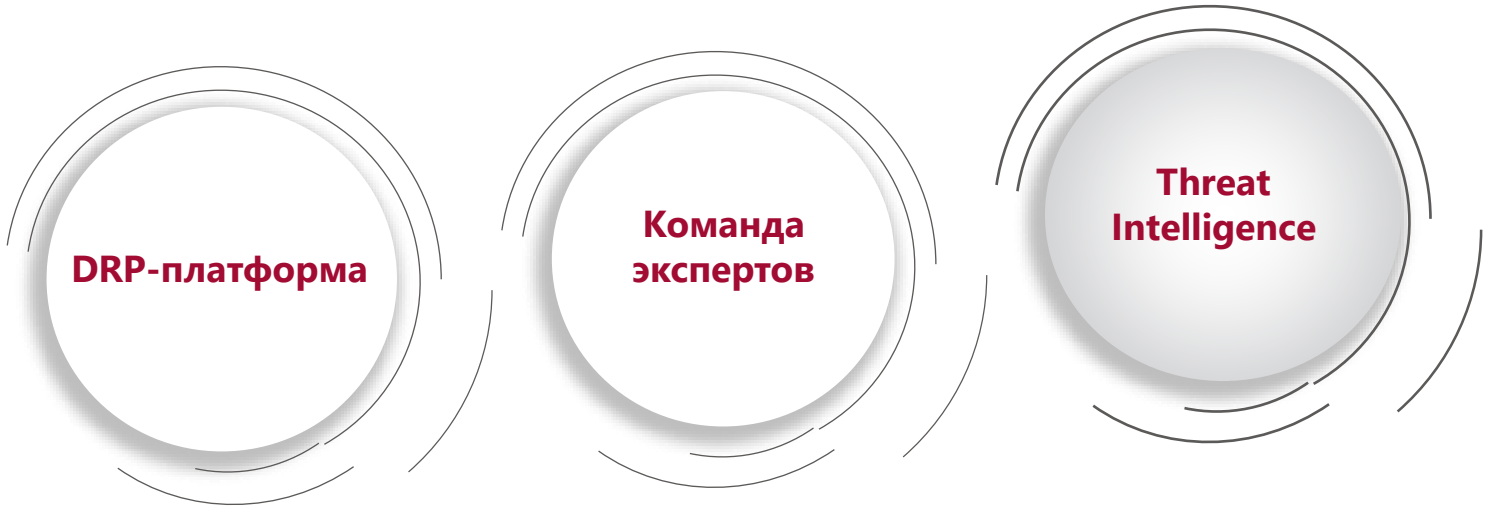
Обнаруживает информационные атаки

Защищает бренд в интернете

Выявляет нелояльных сотрудников

Проверяет контрагентов на неблагонадежность

Анализирует тренды черного рынка



Ethic.CPT непрерывный мониторинг периметра

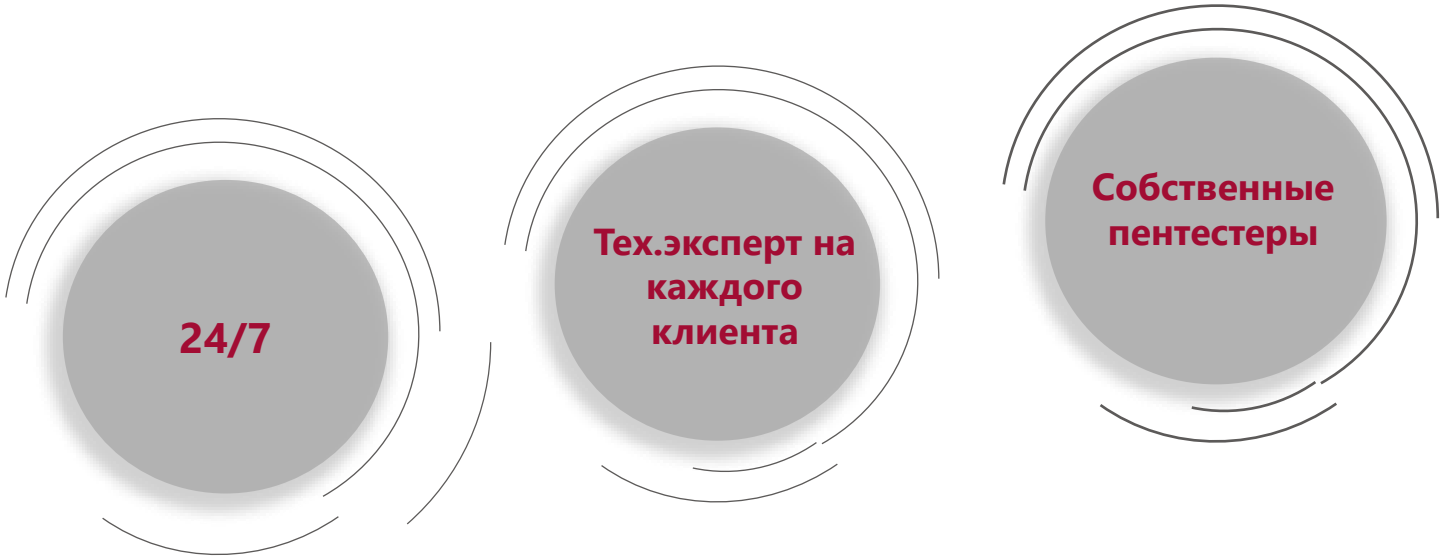
Защита ресурсов на внешнем периметре

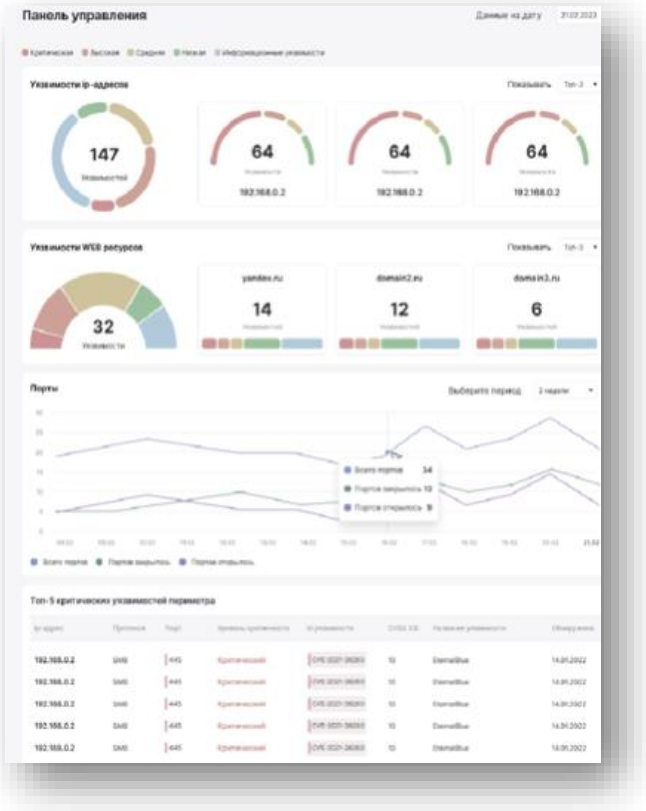
Проверка безопасности новых сервисов, включенных во внешний периметр

Информированность состояний безопасности ИТ-инфраструктуры, быстрое устранение слабых мест

Отслеживание изменений состояния действующего периметра

Снижение рисков инцидентов ИБ





Управление уязвимостями

- Обследование инфраструктуры
- Проектирование и документирование процесса выявления и устранения уязвимостей в ИТ инфраструктуре
- Внедрение и настройка инструмента управления уязвимостями
- Интеграция с внешними системами
- Внедрение процесса управления уязвимостями
- Техническая поддержка и консультирование

Мониторинг уязвимостей → Анализ уязвимостей → Триаж и приоритизация уязвимостей → **Устранение уязвимостей** → **Контроль устранения**

Сервис обучения сотрудников

Быстрый старт
От 3 рабочих дней

15+ готовых
интерактивных курсов

50+ шаблонов
для учебного фишинга

Конструктор шаблонов
для собственных писем

Доступ к платформе 24/7

Проводите обучение, когда удобно независимо от региона и часового пояса

Гибкий процесс обучения

Всегда можно вернуться к тому месту, на котором остановился процесс и продолжить

Оценка прохождения курсов

Контрольный тест - 10 вопросов по окончании каждого электронного курса

Планирование учебных атак

Отправляйте учебные фишинговые письма по заранее спланированному расписанию и сразу выявляйте слабые места

Команда Infosecurity поможет

- Защититься от кибератак и снизить риски
- Сократить затраты на устранение последствий кибератак
- Повысить цифровую грамотность
- Снизить вероятность инцидентов
- Разработать индивидуальные программы для разных уровней подготовки
- Разработать кастомизированные обучающие материалы

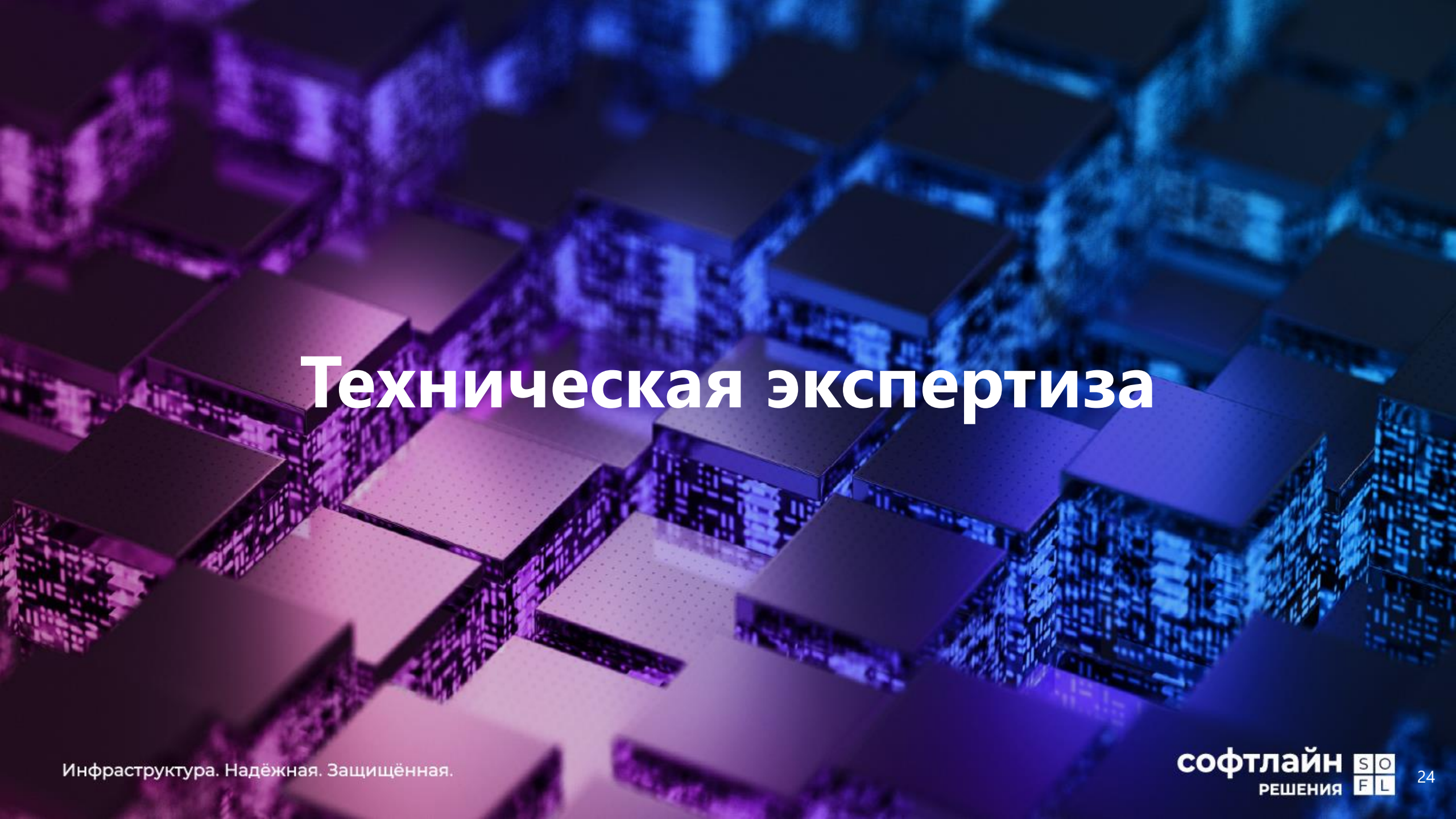
Техподдержка 24x7

Основные направления поддержки

- Мониторинг ИТ- и ИБ-систем 24/7
- Регистрация и обработка обращений – круглосуточный прием заявок и решение инцидентов
- Техническое обслуживание оборудования – поддержание в работоспособном состоянии, выявление и устранение сбоев
- Интеграция с IT-инфраструктурой – подготовка оборудования к промышленной эксплуатации, внесение изменений в настройки
- Выездные работы (Field Service) – оперативный выезд специалистов при необходимости
- Представление интересов заказчика перед вендором – взаимодействие с производителями
- Аутсорсинг – предоставление услуг по эксплуатации ИБ решений

Наши преимущества

- **15**+ лет опыта – экспертиза в ИБ и ИТ, работа с критически важными системами
- 250+ специалистов – инженеры разных профилей, мультивендорная поддержка
- Контроль и единая точка входа – централизованное управление задачами по ИБ
- Разные пакеты сопровождения – от базового до расширенного, под любые потребности
- Круглосуточное реагирование – решаем сразу, не ждем начала следующего дня
- Широкий отраслевой опыт – работаем с финансовыми, промышленными, торговыми, энергетическими компаниями



Техническая экспертиза

Сетевая безопасность

Криптографическая защита каналов связи и VPN

Ключевые вендоры: КБ, Инфотекс, С-Терра

Система защиты почты и пользовательского веб-трафика

Ключевые вендоры: Kaspersky, Solar

Межсетевые экраны L4 и NGFW

Ключевые вендоры: UserGate, КБ, Инфотекс, PT, Ideco, Check Point

Управление конфигурацией активного сетевого оборудования

Ключевые вендоры: Газинформсервис (Efros), NetHub

ИБ-аудит сетевого оборудования

Собственные услуги

Система контроля сетевого доступа (NAC)

Ключевые вендоры: NETAMS (WNAM), Сакура

Защита конечных точек

Защита конечных точек (EPP)

Внедряем и сопровождаем EPP-системы для обеспечения базовой защиты от известных угроз.

Ключевые вендоры: Kaspersky, Dr.Web

Защита конечных точек от комплексных угроз (EDR)

Внедряем и сопровождаем системы EDR, обеспечивающие защиту конечных точек, выявление и нейтрализацию сложных угроз.

Ключевые вендоры: Kaspersky, PT, F6

Управление мобильными устройствами (MDM/UEM)

Внедряем и сопровождаем MDM/UEM-решения, обеспечивающие управление безопасностью мобильных устройств.

Ключевые вендоры: SafeMobile, WorksPad, Kaspersky

Харденинг

Усиливаем безопасность конечных точек за счет встроенных механизмов защиты, путем формирования детальных требований по их настройке – Linux, Windows, Cisco, iOS, Android и других

Корпоративные СЗИ

Системы управления инцидентами ИБ

Внедряем и сопровождаем SIEM-решения, обеспечивающие контроль инцидентов

Ключевые вендоры: Kaspersky, PT, RuSIEM, R-Vision

Защита от целевых угроз

Внедряем и сопровождаем решения Anti-APT, Sandbox, NDR, NTA, выявляющие и блокирующие целевые атаки

Ключевые вендоры: Kaspersky, PT, F6, AVSoft

Системы анализа уязвимостей

Внедряем и сопровождаем анализаторы уязвимостей

Ключевые вендоры: PT, RedCheck, R-Vision, Vulns.io, ScanFactory

Системы управления безопасностью и рисками

Разрабатываем и внедряем процессы управления инцидентами и решения SOAR / IRP / SGRC

Ключевые вендоры: Security Vision, R-Vision, Securitm

Системы предотвращения утечек информации

Внедряем и сопровождаем DLP-решения, снижающие риск утечек информации

Ключевые вендоры: InfoWatch, Solar, Zecurion

Инфраструктура ложных целей (DDP)

Внедряем и сопровождаем DDP-решения, нацеленные на выявление атак на ранних стадиях

Ключевые вендоры: Xello, AVSoft, R-Vision, Гарда

Контроль и автоматизация доступа

Многофакторная аутентификация (MFA, IDP, SSO)

Внедряем и сопровождаем системы MFA, IDP, SSO. Проекты включают в себя организацию многофакторной аутентификации и построение единого сервиса аутентификации для информационных систем

Автоматизация управления доступом (IDM)

Проводим полный цикл работ по внедрению и сопровождению IDM-систем, от аудита бизнес-процессов и выбора подходящего решения до настроек системы отчетности, корректировки ролевой модели и технической поддержки

Выстраивание процесса управления доступом

Анализируем процессы управления учетными записями и доступом, определяем требования к их авторизации и аутентификации, документируем роли и обязанности, обеспечиваем контроль, прозрачность и соответствие требованиям

Контроль привилегированных пользователей (PAM)

Внедряем и сопровождаем PAM-системы для устранения рисков, связанных с утечкой, злоупотреблением или компрометацией привилегированных учетных записей

Системы защиты для технологических сетей

Проектирование и внедрение СОИБ

Внедряем ИБ-решения для обеспечения непрерывности бизнеса и защиты корпоративных данных от киберугроз

Комплексная защита критической инфраструктуры

Осуществляем полный комплекс работ по обеспечению информационной безопасности критичных систем на всех этапах

Безопасность АСУ ТП

Обеспечиваем комплексную защиту автоматизированных систем управления технологическими процессами

NGFW для ТСПД

Осуществляем подбор и внедряем МСЭ для защиты промышленных систем с учетом специфики

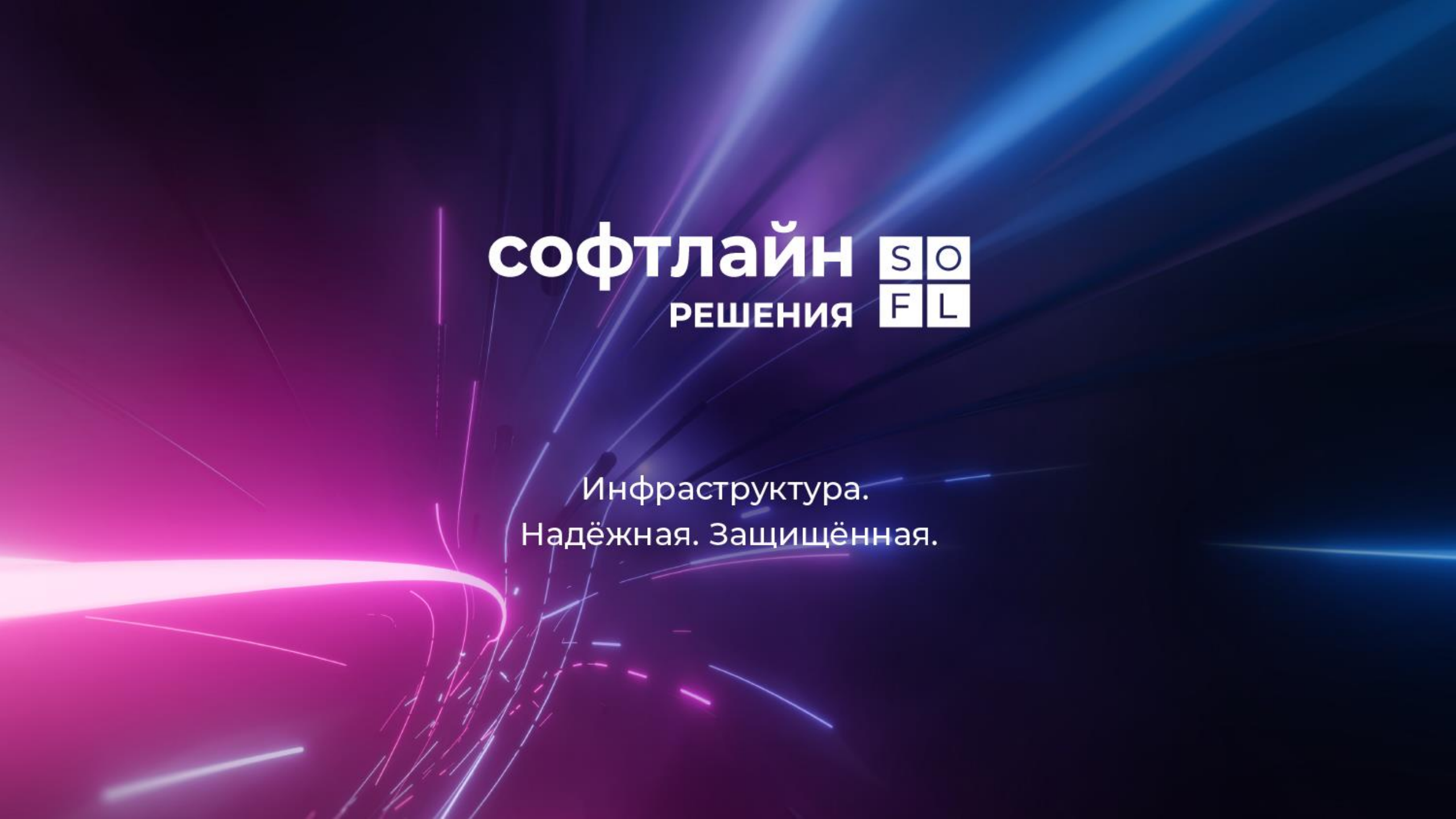
Мониторинг промышленного трафика (NTA)

Внедряем решения для мониторинга и обнаружения вторжений, контроля изменений и уязвимостей
в промышленной сети

Защита конечных точек в ТСПД

Осуществляем подбор и внедряем антивирусные решения для защиты рабочих станций, серверов и виртуальных сред

Q&A


софтлайн
РЕШЕНИЯ
SOFL
Инфраструктура.
Надёжная. Защищённая.