Комплексная кибербезопасность на базе российских решений и сервисов Softline

Шкатов Александр

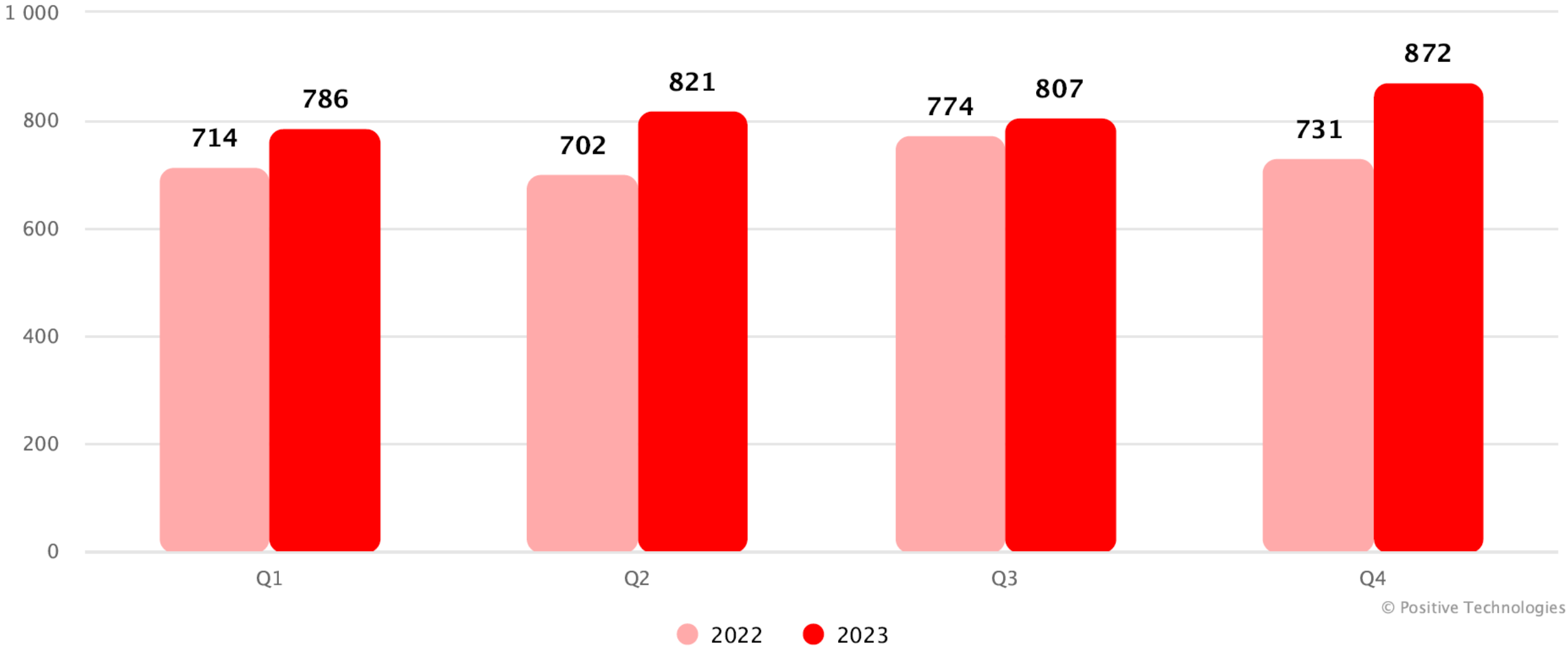
Ведущим менеджер группы развития продаж решений информационной безопасности в ЦФО

T +79601171278

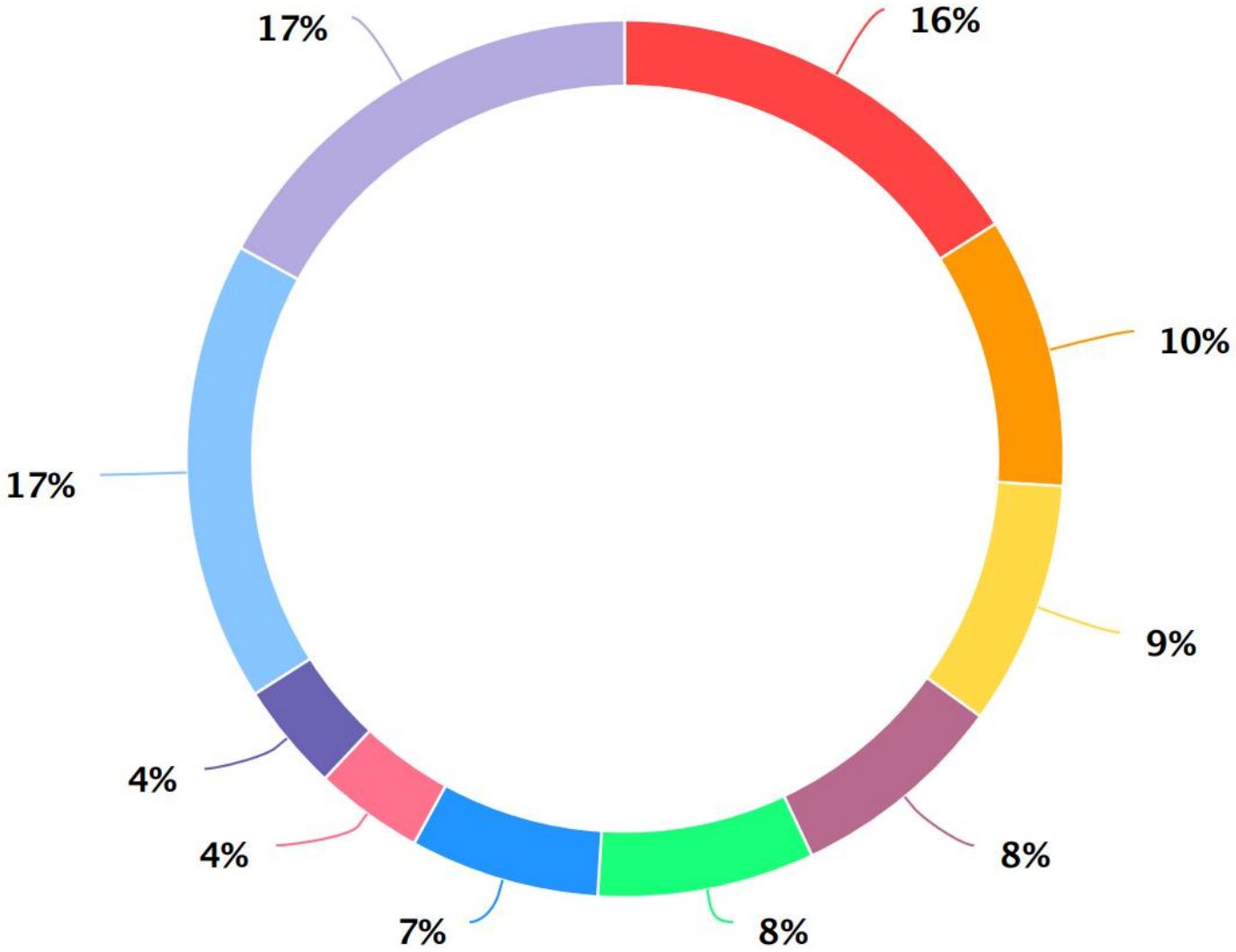
Alexander.Shkatov@softline.com

Фактическая ситуация

Сводная статистика



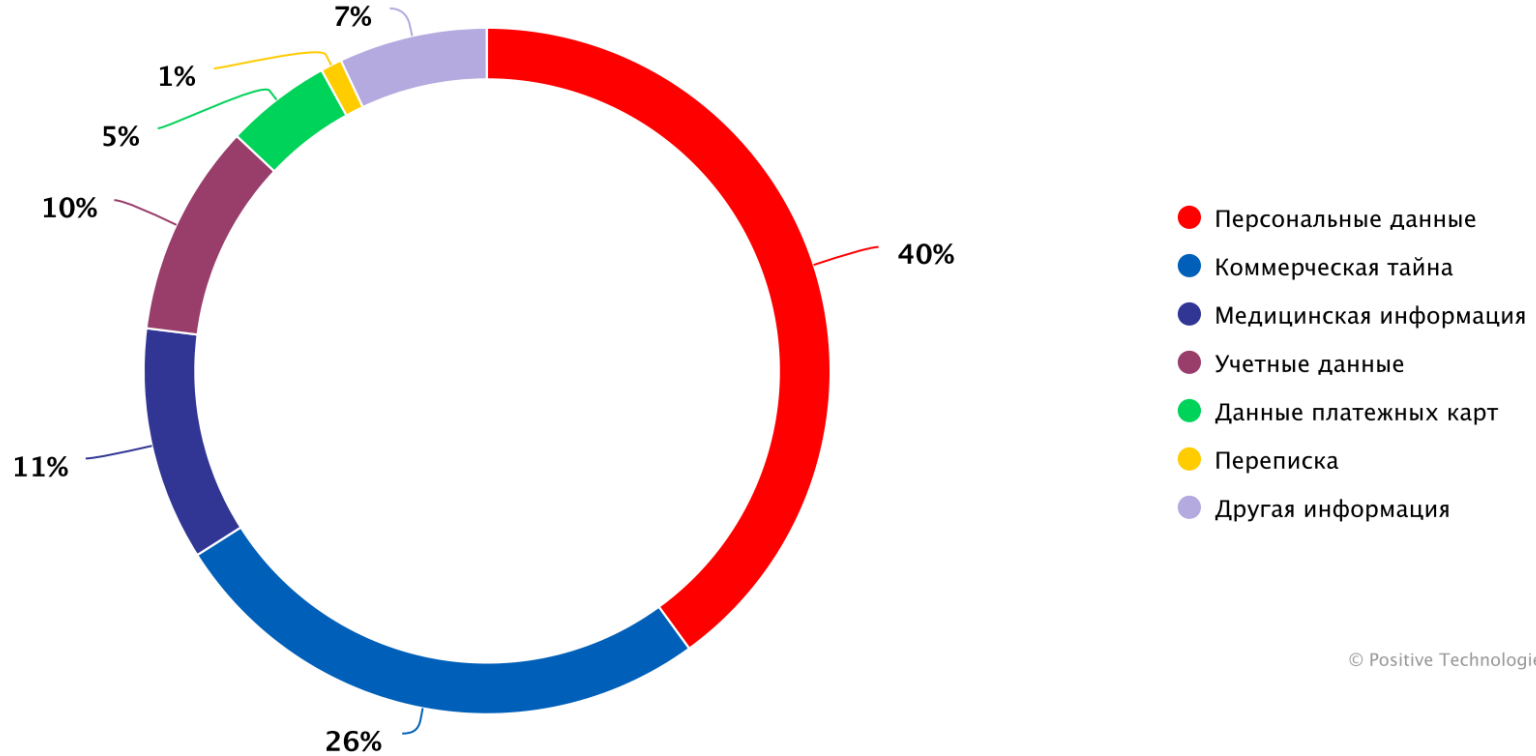
Категории жертв среди организаций

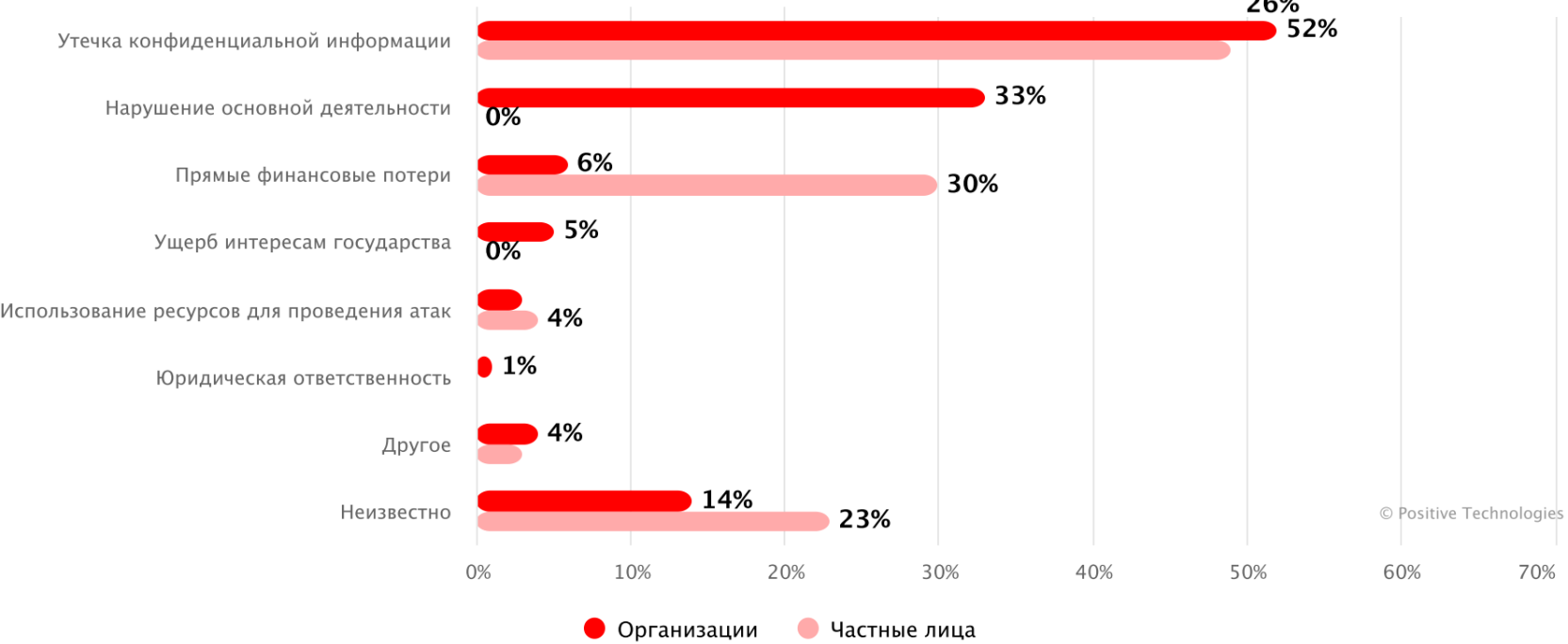


- Госучреждения
- Медицинские учреждения
- Финансовые организации
- Промышленность
- Наука и образование
- IT-компании
- Блокчейн-проекты
- Транспорт
- Другие
- Без привязки к отрасли

Последствия атак

Типы украденных данных





Информационная безопасность в Softline

Кибербезопасность

Инфраструктура

- Безопасное рабочее место
- Сетевая безопасность (NGFW, IPS, ATP)
- 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
- Управление инцидентами (SIEM, IRP)

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 и соответствие

- Security Operation Center (SOC)
- Индустриальные стандарты
- Управление рисками
- Соответствие законам (152ФЗ, GDPR, СТОБР, 382П. Гост 57580. 187ФЗ)
- Авторские продукты (ETHIC)

НАШИ СЕРВИСЫ:

Проектирование

Пилотирование

Внедрение

Техподдержка

Управляемые сервисы

Портфель импортонезависимых вендоров

Безопасность инфраструктуры

NGFW • VPN • **Web filtering** • Mail security • **NTA (ex ATP)** • NAC • **Firewal management**
AV&EDR • MDM • **DB Security** • DAM/DBF • **SIEM** • IRP • **SOAR** • vSecurity

R-Vision, T-Soft, RUSIEM, AVSOFT, Wise-Mon, TCC, Security Vision, Гарда, Код безопасности, Group IB, NGRSOFTLAB, positive technologies, kaspersky, s-terra, infotecs, xello Deception, Smart-Soft, Dr.WEB, Solar Security, Фактор-ТС, UserGate, Фактор-ТС, SkyDNS, Пангео Радар, DALLAS LOCK, GIS, ideco, SAFEPHONE, SEARCHINFORM, IT EXPERTISE

Безопасность приложений

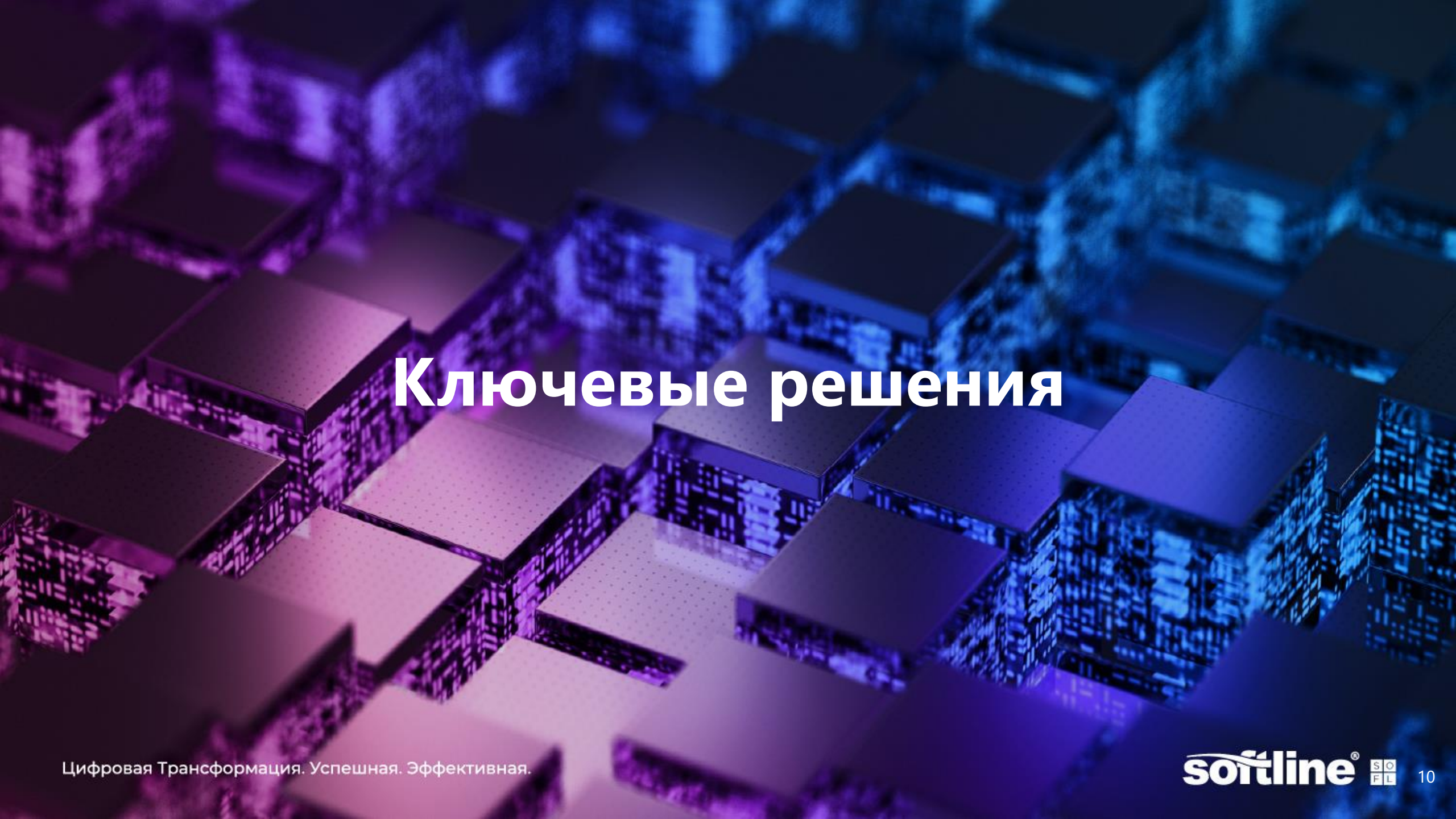
WAF • Anti-DDoS • **Vulnerability Management** • Pentest • **Security code source** • Secure IoT
Data Masking • Container Security • **Configuration Management** • DevSecOps

Cloudflare, positive technologies, RedCheck, Starforce, RCNTEC, Эшелон, TRLHACK, Solar Security, Qrator Labs, kaspersky, PENTESTIT, R-Vision VM, solidlab, Вебмониторэкс, Гарда, Код безопасности, SCAN FACTORY, Vulns.io VM

Безопасность данных

DAG • DLP • **VDR** • IDM • **PAM** • Audit File Access • **MFA** • Encryption

StaffCop, perimetrix, Group IB, Avanpost, MULTIFACTOR, Аладдин, КриптоПро, MFLASH, WorksPad, INFOWATCH, АйтиБастион, ZECURION, Стахановец, INDEED ID, Solar Security, NGRSOFTLAB, SEARCHINFORM, falcongaze, CyberPeak, Гарда, АПКШ, Орлан, MAKVES, RCNTEC, EVERYTAG, Identity Blitz



Ключевые решения

Защита конечных точек

АНТИВИРУСЫ

kaspersky

КОД безопасности

Dr.WEB

EDR

kaspersky

F.A.C.C.T.

PT POSITIVE TECHNOLOGIES

Защита сети и почтового трафика

МЕЖСЕТЕВЫЕ ЭКРАНЫ

UserGate

ideco

КОД безопасности

SMART-SOFT

infotecs®

ЗАЩИТА ПОЧТЫ

kaspersky

Dr.WEB

F.A.C.C.T.

Защита от целенаправленных атак

СИСТЕМЫ АНАЛИЗА ТРАФИКА

- kaspersky
- POSITIVE TECHNOLOGIES
- ГАРДА ТЕХНОЛОГИИ
- F.A.C.C.T.

ПЕСОЧНИЦЫ

- F.A.C.C.T.
- kaspersky
- POSITIVE TECHNOLOGIES
- Dr.WEB

Защита приложений

WAF

- POSITIVE TECHNOLOGIES
- QRATOR LABS
- solidwall
- КОД безопасности
- Вебмониторэкс — защита веб-приложений

ЗАЩИТА ОТ DDOS

- kaspersky
- QRATOR LABS
- StormWall

Защита от утечек\контроль пользователей

СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ

INFOWATCH

Стахановец
система контроля сотрудников

SEARCHINFORM
INFORMATION SECURITY

SOLAR SECURITY
software&services

staffcop

ZECURION

Сканеры уязвимостей

СКАНЕРЫ УЯЗВИМОСТЕЙ

PT POSITIVE TECHNOLOGIES

SCAN FACTORY

R-Vision VM

RED Check

Vulns.io VM

Двухфакторная аутентификация

СИСТЕМЫ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Avanpost

Identity Blitz

Аладдин

СКБ Контур

MULTIFACTOR

INDEED ID

Реагирование на события ИБ

СИСТЕМЫ СБОРА И КОРРЕЛЯЦИИ СОБЫТИЙ

- POSITIVE TECHNOLOGIES
- NGRSOFTLAB
- RUSIEM — Всё под контролем
- SEARCHINFORM — INFORMATION SECURITY
- kaspersky

СИСТЕМЫ АВТОМАТИЗАЦИИ РЕАГИРОВАНИЯ

- Security Vision
- R-Vision

Осведомленность пользователей в сфере ИБ

Awareness

kaspersky

StopPhish

phishman

secure-t

Киберполигон

Киберполигон Ampire – программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак.

Данный комплекс предназначен для обучения, подготовки и тренировки специалистов по информационной безопасности для государственных организаций, кредитно-финансовой сферы, объектов критической информационной инфраструктуры, телекома и других отраслей.

AMPIRE

Ampire зарегистрирован в **Едином реестре** российских программ для электронных вычислительных машин и баз данных **20.09.2019 г. (рег. номер ПО 5861)**

Типы проводимых занятий на Ampire

Киберучения

Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации

Противодействие группе реальных нарушителей (концепция Red Team и Blue Team)

Лабораторные работы по настройке средств безопасности и прикладных сервисов

Ключевые сервисы SOFTLINE

Полный цикл реализации проекта

От подбора решения и поставки до внедрения и технической поддержки

- Собственный Производственный блок
- Развитая экспертная команда:
  ИТ, ИБ и Консалтинг
- Собственный Учебный центр
- Собственная система Service Desk, Служба технической поддержки и Сервисный центр
- Гибкая модель предоставления услуг – от внедрения и сопровождения до аутсорсинга
- Выделенные и разовые услуги по запросу

Техническая поддержка

Сопровождение функционирования и эксплуатации систем информационной безопасности на протяжении их жизненного цикла

Состав услуги:

- Базовая, 1-я линия: регистрация и ведение заявок, передача информации/логов в поддержку Производителя и отслеживание статуса
- Стандартная (консультационная), 2-я линия: базовая + консультационные услуги по функционалу, настройке, восстановлению работоспособности
- Расширенная (инцидентная), 3-я линия: стандартная + подключение эксперта к решению инцидентов

Аутсорсинг

Регулярное администрирование систем информационной безопасности

Состав услуги:

- Запрос на физическое обслуживание на месте размещения объекта
- Регламентные выезды в рамках профилактического визита
- Услуги конфигурирования: создание и внесение изменений
- Обновление: установка и применение
- Мониторинг 24x7:
- Подключение обслуживаемых систем к средствам мониторинга
- Реагирование на инциденты и эскалация выявленных событий

Сервисные модели

Security as a Service

- Лицензия, программное обеспечение
- Вычислительные ресурсы Softline Cloud – Infrastructure as a Service

Тип Сервиса		Позиции	Детализация
Managed Security Service, MSS	**Security as a Service, SECaaS**	Лицензия, ПО	Лицензия на право использование средства защиты информации
		Infrastructure as a Service, IaaS SL Cloud (вычислительные ресурсы)	IaaS, vCloud, vCPU
			IaaS, vCloud, vRAM
			IaaS, vCloud, SAS
			Интернет-канал
			Veeam B&R, vCloud, VM
			Cloud Veeam, хранение на СХД
	Постановка на Сервис		
	Управление Сервисом		

Managed Security Service

- Лицензия, программное обеспечение
- Вычислительные ресурсы Softline Cloud – Infrastructure as a Service
- Интеграция и постановка на Сервис
- Техническая поддержка, сопровождение эксплуатации и управление Сервисом

MSSP

Сервисы вокруг систем контроля и предотвращения утечек информации

Разовые услуги:

- Анализ потребностей и подбор оптимального решения;
- Внедрение системы и подключение источников данных;
- Сбор перечня критичных для организации документов;
- Настройка индивидуальных правил, удобных Заказчику;
- Подготовка сопроводительной документации или её доработка.

Аналитика:

- Оперативное информирование о потенциальных инцидентах;
- Сбор информации из архива по запросу Заказчика;
- Актуализация настройки при изменениях в компании;
- Помощь в построении процессов реагирования;
- Обеспечение детального контроля критичных элементов.

Техподдержка:

- Выявление проблемы, проведение диагностики и её устранение;
- Решение проблем совместно с вендором, сбор диагностической информации для её передачи;
- Оптимизация процесса обработки и хранения данных;
- Проведение обновления системы.

Сервис SOC

Что это

- Мониторинг состояния ИБ в режиме 24x7
- Выявление кибератак на ранних стадиях
- Минимизация потерь за счет оперативного разбора инцидентов

Зачем нужно клиенту

- Возможность оперативно и сравнительно недорого запустить SOC
- Уникальные компетенции, которые сложно найти и еще сложнее удержать

Варианты реализации

- Basic – базово необходимые возможности SOC, позволяющие запустить процессы мониторинга в круглосуточном режиме. Рекомендовано для средних компаний (1000 – 1500 ПК)
- Extended – расширенные возможности, включающие автоматизированную реакцию и углубленный разбор инцидентов ИБ

Преимущества сервиса iSOC

Предустановленные настройки

Относительно быстрый старт сервиса за счёт постоянно пополняемых набора сценариев реагирования и коннекторов к различным источникам событий для большинства техник матрицы MITRE ATT&CK

Экспертиза в удовлетворении требований регуляторов

Мы имеем обширный опыт в реализации требований ФЗ 187, ГОСТ 57580 и т.д. Имеем соглашение с НКЦКИ, являемся центром ГОССОПКА, можем осуществлять обмен данными с ФИНЦЕРТ и НКЦКИ

Сертифицированные российские решения в ядре SOC

KUMA и IRP/SOAR Security Vision составляющие ядро ISOC, сертифицированы ФСТЭК России и находятся в реестре отечественного ПО

Автоматизация реагирования

Экспертный набор playbooks для реагирования на инциденты, включающий управление ИБ в компании (от обучения до разработки документации). Оперативное обнаружение и реагирование на уровне конечных устройств – интеграция ISOC с KEDR

Кастомизация сервиса

Оперативно самостоятельно разрабатываем новые правила корреляций и плейбуки как по требованиям заказчика, так и при появлении новых угроз

Экосистема сервисов Infosecurity

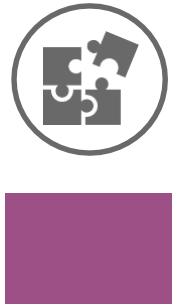
Интеграция ISOC с другими сервисами Infosecurity по защите от киберугроз и сопровождению ИТ-инфраструктуры заказчика – зона ответственности по реагированию в единой точке

Повышение осведомлённости пользователей

Оценка текущего состояния осведомлённости сотрудников, профессиональных компетенций

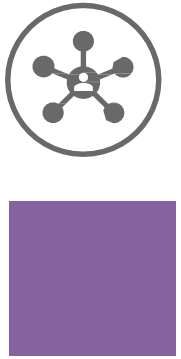
тестирование сотрудников заказчика

Платформы класса Awareness



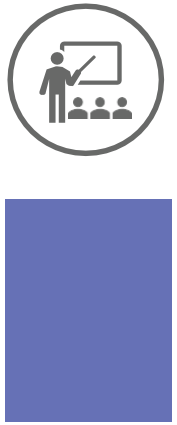
PHISHMAN, ASAP, Антифишинг, СтопФиш, Secure-T

Сервис повышения осведомленности



- Платформа в облаке
- Платформа в облаке+сервис
- Эл.курсы по подписке
- Фишинг по подписке

Коробочные электронные учебные курсы для СДО заказчика

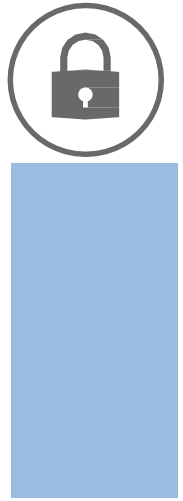


Более 30+ курсов по разным темам ИБ

Разработка материалов для заказчика

- Электронные курсы и тесты
- Видеоролики
- Плакаты, скринсейверы
- Дайджесты
- Комиксы
- Игры
- День по ИБ
- Вебинары

Разработка стандарта повышения осведомленности работников в области ИБ



- По направления
- По ролям

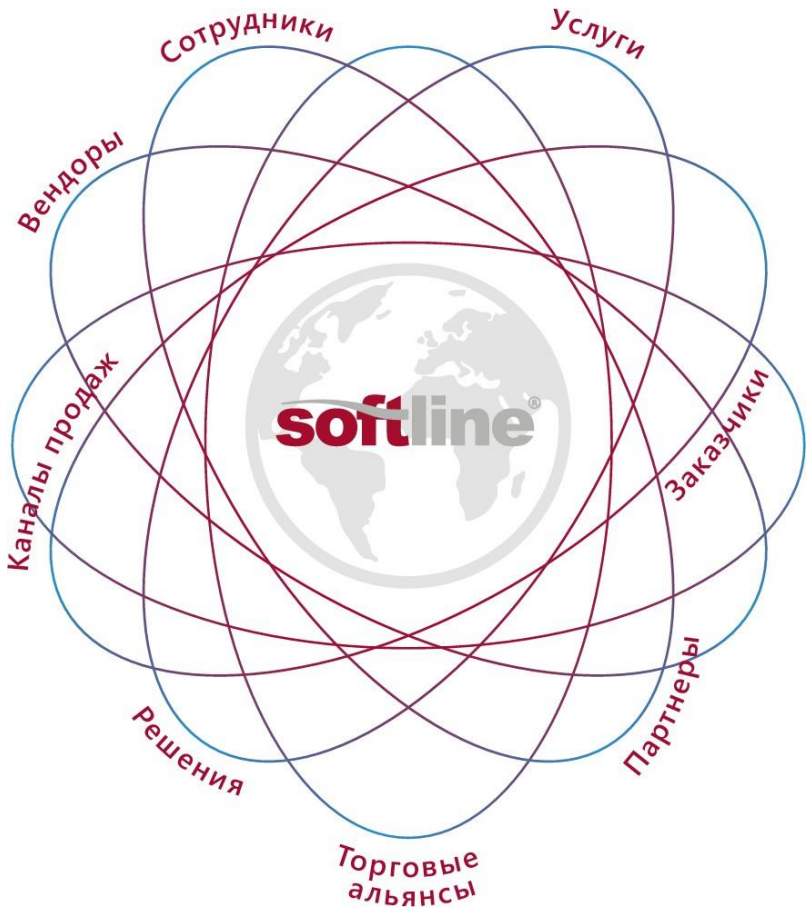
Соответствие требованиям

Соответствие требованиям

- Приведение в соответствие 187-ФЗ; (235 и 239 приказ ФСТЭК)
- Приведение в соответствие 152-ФЗ (21 приказ ФСТЭК);
- Приведение в соответствие требованиям ГИС/МИС (17 приказ ФСТЭК);
- Специальные проверки и специальные исследования;
- Аттестация объектов автоматизации.

Почему Softline

Глобальный лидер в цифровой трансформации и информационной безопасности



Краеугольный камень цифровой трансформации

30 лет	3000+	3600+	1000+	800+
На IT рынке	Реализованных проектов	Сотрудников	Менеджеров	Инженеров

Лидер информационной безопасности

380	ТОП-3	ФСБ, ФСТЭК	Инфосекьюрити, ТЦ Инженер
Инженеров по направлению ИБ	Крупнейших в РФ компаний в сфере ИБ по рейтингу Cnews	Лицензии	Входят в ГК Софтлайн

Цифровая Трансформация. Успешная. Эффективная.

Рейтинг


Топ-10 игроков рынка информационной безопасности
Выручка в 2022 г. в ₽тыс. с НДС
27 400 000
24 966 485
23 427 994
19 440 445
14 400 000
13 991 023
11 300 000
9 500 800
8 598 000
7 531 344


Крупнейшие поставщики решений в сфере информационной безопасности в России
по выручке за 2022 год (в млн рублей)
51 549 -6,9%
23 428 +5%
17 156 +64,2%
15 552 +48%
14 400 +17,1%
13 800 +74,7%
11 300 +27,9%
9 501 +55,4%
8 598 +1,5%
6 751 +13,9%
TADVISER

Пилотное тестирование

Практическая проверка функциональных возможностей и требований к решению

- **Устав** пилотного проекта
- **Программа** и методика испытаний
- **Детализированный отчёт** по результатам тестирования
- **Выдача рекомендаций** по покрытию векторов угроз
- **Демонстрация** функциональных возможностей
- **Качественный переход и реализация** проекта по внедрению

softline®

Цифровая Трансформация.
Успешная. Эффективная.

Шкатов Александр

Ведущий менеджер группы развития продаж решений информационной безопасности в ЦФО

T +79601171278

Alexander.Shkatov@softline.com