softline SOFL

Решения и услуги по информационной безопасности

Группа Компаний Softline

ГК Softline – инвестиционно-технологический холдинг с более чем 30-летним опытом и широким региональным присутствием в России, Казахстане, Узбекистане, Вьетнаме, Индонезии и ОАЭ. Мы специализируемся на проектах в области информационных технологий, информационной безопасности, а также цифровой трансформации бизнеса

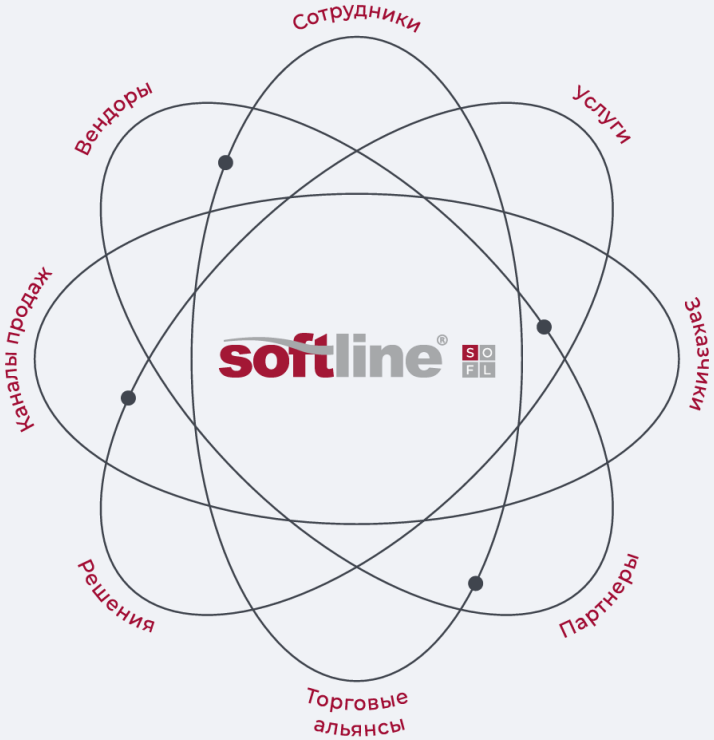
Краеугольный камень цифровой трансформации (DX)

25+
Компаний в группе

>5000
Производителей

>100 000
Клиентов

Полный набор
Услуг и решений для цифровой трансформации



Ведущая ИТ компания в России

30+
Представительств в 6 странах

30+
Лет на ИТ-рынке

>120,6 млрд руб.
Оборот 2024

>11 100
Сотрудников

Тренды рынка информационной безопасности 2025-2028

Регуляторное давление

Нормативы, как GDPR, CCPA, HIPAA, включая Закон Республики Казахстан „О персональных данных и их защите“, сделали соответствие требованиям основным драйвером инвестиций в защиту данных.

Рост бюджетов

85% компаний планируют увеличить бюджеты на кибербезопасность, каждая пятая — на 15% и более.

Защита данных

Безопасность, ориентированная на идентичность: 86% компаний внедряют модели Zero Trust.

Мониторинг и анализ угроз

Фокус на угрозы идентификации: 98% атак используют методы социальной инженерии; растет число дипфейков на базе ИИ.

Угрозы нового поколения

85% специалистов по кибербезопасности отмечают, что злоумышленники активно используют генеративный ИИ для атак.

Рост финансовых потерь

Финансовые последствия очевидны: средняя стоимость утечки данных в мире достигает $4,88 млн.

Нехватка кадров

Компании активнее привлекают внешние SOC-центры, сервисы мониторинга и управление инцидентами «под ключ»

Необходимость интеграции

К 2026 году 53% организаций будут отдавать приоритет инструментам ИИ и МО для усиления защиты, что повысит спрос на услуги интеграции.

Источники: pwc.com, Fortinet.com, JPMorganChase.com, vikingcloud.com, finance.yahoo.com.

Крупные инциденты в Казахстане

Компания/организация

Национальная база данных населения.

Сектор

Госсектор

Суть инцидента

Утечка данных

Выявленные уязвимости и проблемы безопасности

- Отсутствие мониторинга и аудита доступа в реальном времени, устаревшие системы.

Репутационный ущерб

- Подрыв доверия к электронным программам правительства.
- Репутационный ущерб национальной цифровой инфраструктуре.

Материальный ущерб

- Возможные затраты на кредитный мониторинг, исправление системы и возможные штрафы регулирующих органов.
- Нарушения конфиденциальности данных ~16 миллионов граждан.

Выводы

- Необходим проактивный подход.
- Нужно обеспечить целостую киберустойчивость.

Крупные инциденты в Казахстане

Компания/организация

Государственные структуры

Сектор

Госсектор

Суть инцидента

Целевой фишинг с заражением вредоносным ПО (DownEx/STILLARCH)

Выявленные уязвимости и проблемы безопасности

- Уязвимость к социальной инженерии, слабая защита конечных точек

Репутационный ущерб

- Взлом конфиденциальных правительственных данных и систем.
- Сбор важных сведений, которые могут быть использованы в интересах субъекта, представляющего опасность.

Материальный ущерб

- Затраты на расследование и реагирование на инциденты
- Потенциальные затраты на утечку данных (интеллектуальная собственность, гос. тайна).

Выводы

- Нужно непрерывное обучение сотрудников и многоуровневая защита (Defense-in-Depth), особенно для госсектора.

Портфель решений Softline по информационной безопасности

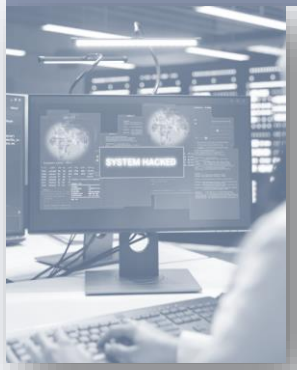
Защита данных

- DLP
- IAM
- PAM
- MFA/Биометрия

Услуги по обеспечению информационной безопасности

- Консалтинг и аудит
- Интеграция с системой кибербезопасности
- Повышение осведомленности
- DevSecOps
- Pentest

Мониторинг и аналитика



- SIEM
- SOAR
- TI
- VM
- DRP

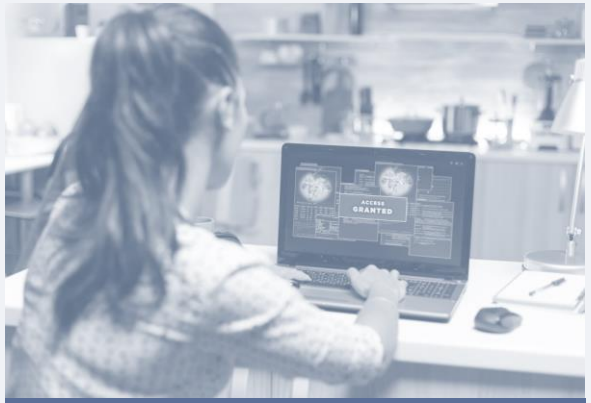
Защита инфраструктуры

- WAF
- EDR/XDR
- Защита от DDoS
- Сетевая безопасность
- Безопасность ICS/OT

❶ Защита данных

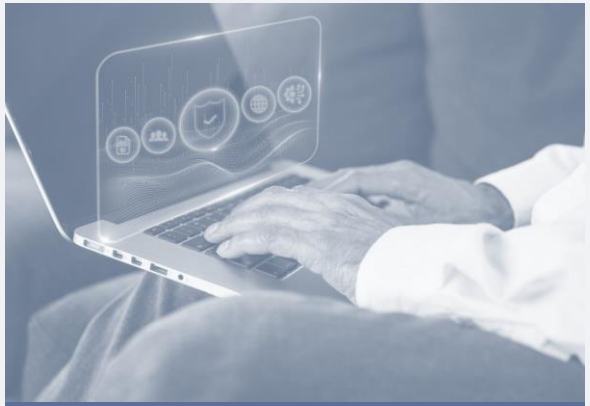
DLP

- Обнаружение и классификация данных.
- Применение политик.
- Мониторинг и оповещения в режиме реального времени.
- Шифрование данных.
- Реагирование на инциденты.



IAM

- Комплексное управление жизненным циклом учетных записей.
- Определение и применение политик доступа для пользователей на основе ролей при соблюдении принципа привилегий.



PAM

- Контроль и запись сеансов привилегированных пользователей.
- Управление административными учётными данными за счет защищенных хранилищ.
- Оперативный доступ минимизирует предоставление постоянных привилегий.

MFA/Биометрия

- Динамически настраивает требования к проверке на основе контекстуальных факторов (географическое положение, репутация в сети и т.д.).
- Множество факторов аутентификации (распознавание лиц и поведенческая биометрия).

На 80%

меньше инцидентов, связанных с ненадлежащим доступом

в организациях с развитыми процессами IAM

На 80%

меньше инцидентов безопасности, связанных с неправильным использованием учетных записей

в организациях с привилегированным контролем доступа.

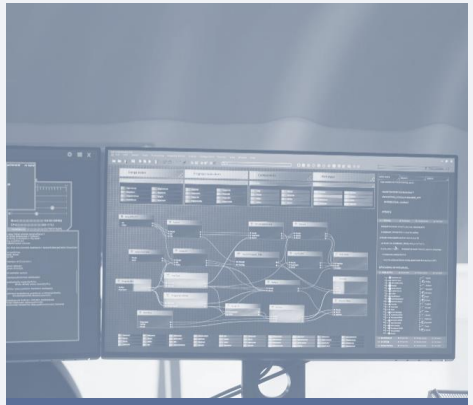
99,9%

атак на компрометацию аккаунта

может предотвратить внедрение MFA

softline®

❷ Мониторинг и аналитика

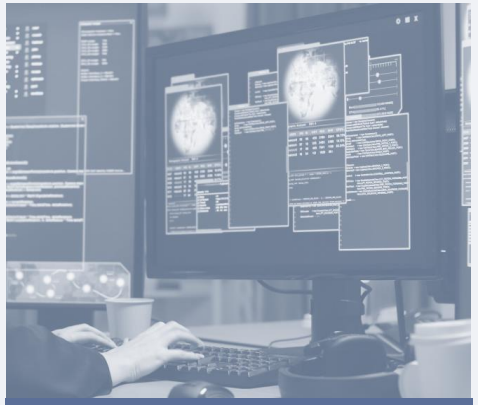


SIEM

- Сбор и корреляция событий со всей IT-среды.
- Поиск аномалий и приоритизация инцидентов с помощью ИИ.

SOAR

- Объединение оповещений путём интеграции с уже имеющимися инструментами.
- Сценарии для унификации и автоматизации рабочих процессов реагирования.
- Централизованный контроль инцидентов.

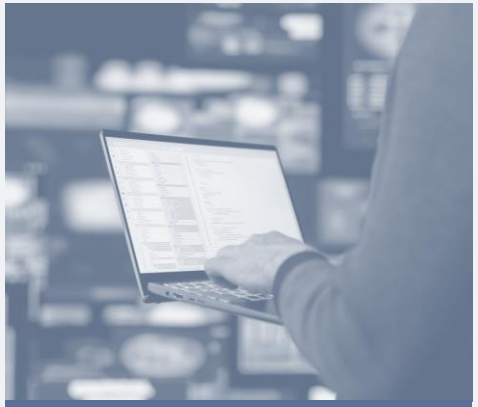


TI

- Предоставление информации об участниках угроз, их тактике, методах и процедурах (TTP), а также индикаторах компрометации (IOCs), помогающих понимать и предвидеть атаки.

VM

- Выявление, классификация, расстановка приоритетов и устранение уязвимостей.
- Использование искусственного интеллекта для расстановки приоритетов рисков на основе реальной возможности их использования и контекста угроз.



DRP

- Мониторинг открытого Интернета, даркнета и социальных сетей.
- Выявление угроз (подмена бренда, мошеннические домены и раскрытие критически важных активов).

До 60%
Меньше
ложных срабатываний (благодаря SIEM)

В 10 раз
Быстрее
реагирование на инциденты, значительная экономия средств и снижение эмоционального выгорания

На 40-60%
повышение точности обнаружения угроз за счет использования инструментов анализа угроз

На 24%
сокращается время обнаружение уязвимостей нулевого уровня, используя инструмент управления уязвимостями

Сервис кибербразведки CYBERDEF

Защита бренда в интернете и обнаружение внешних угроз, включает в себя:

DRP-платформу

Круглосуточно мониторит миллионы ресурсов, выявляет опасную информацию для бизнеса и фиксирует в веб-интерфейсе

Команду экспертов

Эксперты Infosecurity анализируют угрозы, устраняют нарушения и расследуют мошеннические схемы

Threat Intelligence

Кибербразведка выявляет и реагирует на угрозы до их реализации, предотвращая ущерб

CYBERDEF не просто сервис – это команда экспертов, которая мониторит и устраняет инциденты в режиме 24/7

>20	>270	>20	> 320	MSSP
проектов реализовываем ежемесячно	профессионалов в команде	сервисов и услуг для защиты бизнеса	проектов реализовано	Модель оплаты

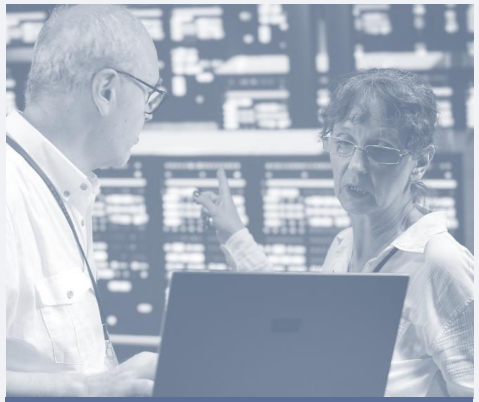
❸ Защита инфраструктуры

WAF

- Проверка и контроль сетевого трафика в режиме реального времени.
- Обнаружение и предотвращение угроз на основе сигнатур и поведения пользователей.

EDR/XDR

- Круглосуточный мониторинг и поиск угроз.
- Объединение данных с конечных точек, сети, идентификационных данных и облака.
- Использование аналитики и искусственного интеллекта для обнаружения угроз.

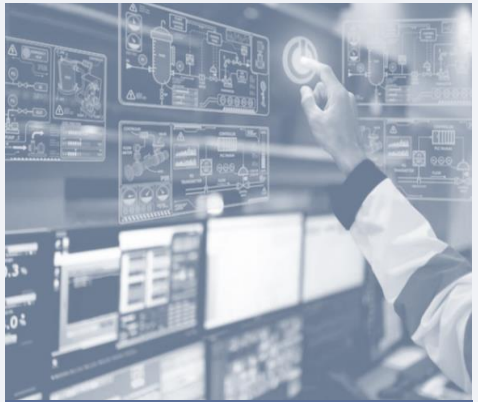


Защита от DDoS

- Защита как от сетевых атак, так и от атак на прикладном уровне.
- Поведенческий анализ для выявления и фильтрации вредоносного трафика.

Сетевая безопасность

- Отслеживание сетевого трафика и производительности для обнаружения аномалий и потенциальных угроз.
- Сегментация сети и контроль доступа.



Безопасность ICS/OT

- Обнаружение угроз для промышленных сетей в режиме реального времени.
- Всесторонний обзор и управление активами для сложной среды OT.

До 99%

Сокращение времени реагирования на инциденты
благодаря WAF, что позволяет быстрее обнаружить угрозы и устранить последствия

До 80%

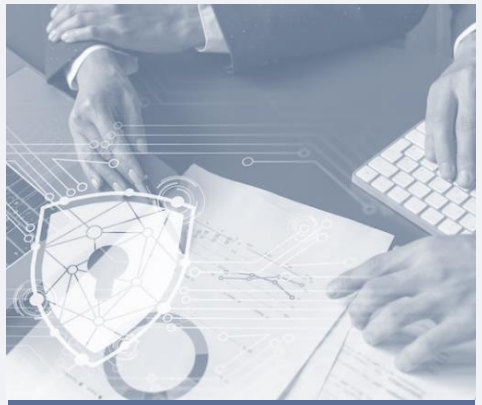
Сокращение времени на смягчение последствий атак, используя инструменты для предотвращения DDOS-атак

До 93%

Снижение числа кибератак в организациях, использующих унифицированные платформы безопасности в ИТ- и ОТ- сферах

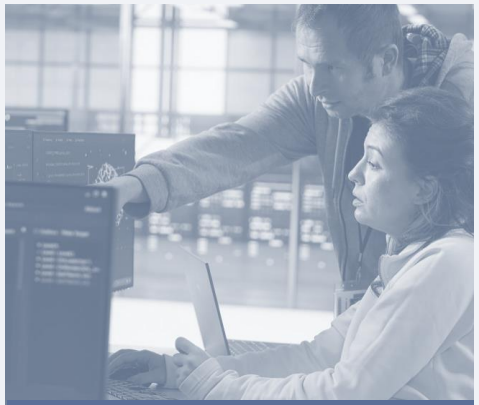
softline®

❹ Услуги по обеспечению информационной безопасности



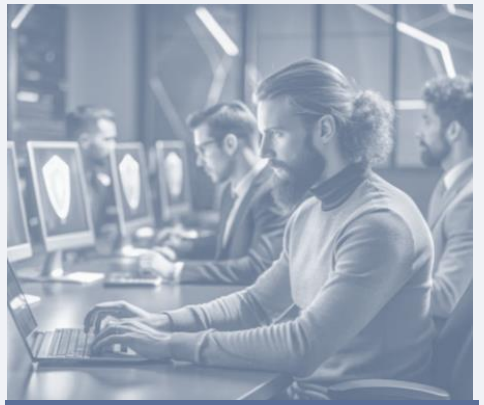
Консалтинг и аудит

- Внедрение фреймворков (NIST CSF, ISO 27001 и др.).
- Оценка/разработка программы безопасности на основе рисков.
- Аудит соответствия.



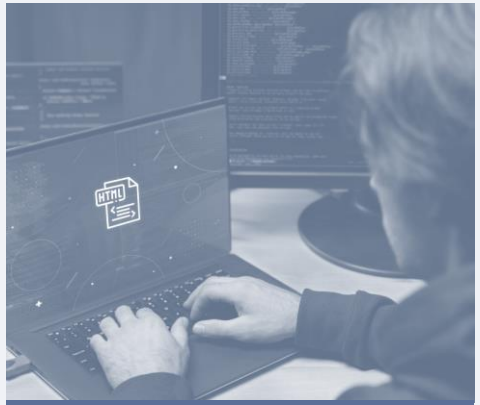
Интеграция с системой кибербезопасности

- Проектирование архитектуры безопасности.
- Развёртывание инструментов (фаерволы, SIEM, IDS/IPS, облачные системы безопасности, IAM и др.).



Повышение осведомленности

- Ролевое обучение сотрудников для распознавания угроз (фишинг, социнженерия).
- Тестирование на основе обучения.



DevSecOps

- Непрерывное тестирование безопасности.
- Автоматическое применение политик и мониторинг.
- Zero Trust Runtime Security.

Pentest

- Автоматизированное обнаружение сложных уязвимостей.
- Тестирование безопасности на базе ИИ.
- Продвинутое сканирование уязвимостей.

В 8.3 раза

реже попадают в публичные списки утечек данных организации с регулярным проведением обучения по кибербезопасности

До 30%

улучшение соответствия нормативным требованиям благодаря сервисам DevSecOps, устраняющим риски безопасности на ранних этапах цикла разработки

71%

Компаний считают использование pentest критичным для соответствия стандартам

softline®

Финансовая организация с ~4 500 сотрудниками и ~100 информационными системами.

Задачи

- Создать дорожную карту развития кибербезопасности.

Решение

- Проведена оценка зрелости кибербезопасности.
- Идентифицированы и оценены ключевые риски.
- Сформированы портфель проектов и дорожная карта по внедрению.
- Результаты согласованы с топ-менеджментом.

Результаты

- Детальная трёхлетняя дорожная карта по развитию кибербезопасности разработана и утверждена руководством.

Энергетическое предприятие с ~800 сотрудниками и ~50 информационными системами.

Задачи

- Внедрить систему управления информационной безопасностью в соответствии с ISO/IEC 27001 и пройти сертификационный аудит.

Решение

- Проведён gap-анализ.
- Ответственность прозрачно распределена между кибербезопасностью, IT и другими подразделениями.
- Все процессы и меры безопасности, требуемые ISO/IEC 27001, были созданы и внедрены.
- Оказана поддержка во время сертификационного аудита.

Результаты

- Процессы ИБ спроектированы и формализованы (создана ролевая модель, учтены требования ISO 27001 и специфика компании).
- Сотрудники обучены основам ИБ, а также специализированным функциям.
- Процессы работают по новым правилам, собрана вся необходимая документация.
- Сертификационный аудит успешно пройден.

Тамаровская
Наталья

Руководитель направления ИБ

Международное управление бизнесом

M +7 777 773-11-36 | Natalya.Tamarovskaya@softline.com

www.softline.com

centralasia@softline.com

Softline. Центральная Азия в Telegram, LinkedIn

Цифровая Трансформация. Успешная. Эффективная.