ГРУППА КОМПАНИЙ
АНТЭН

ДЛЯ ВАШЕЙ ИТ-ИНФРАСТРУКТУРЫ

Быстрые
Компетентные
Решения

Информационная
Безопасность



ГРУППА КОМПАНИЙ
АНТЭН

Быстрые Компетентные Решения

Быстрые

Скорость реакции и обработки

- ✓ Оперативный отклик на запрос
- ✓ Типовые решения — от 2 недель
- ✓ Собственный склад и логистический центр
- ✓ Собственное производство
- ✓ Квалифицированная техподдержка

Компетентные

Экспертиза

- ✓ Профильные инженеры с допусками
- ✓ Сертификаты ФСБ и МЧС
- ✓ Опыт внедрений для госсектора и крупного бизнеса
- ✓ Сокращение издержек при сделке

Решения

Результат

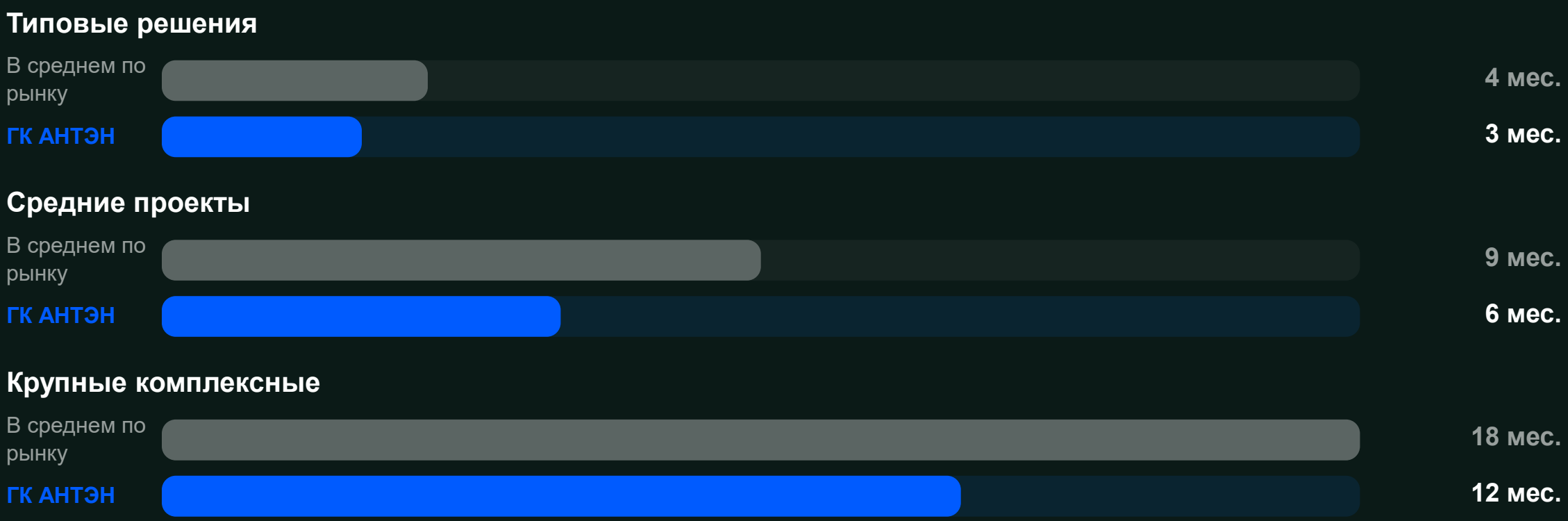
- ✓ Долгосрочное планирование инфраструктуры заказчиков
- ✓ Проект под ключ с интеграцией в ваши системы
- ✓ Сопровождение и поддержка после внедрения

ГРУППА КОМПАНИЙ
АНТЭН

Как мы сокращаем время от заявки до поставки

Нашим подходом мы сокращаем путь от заявки до поставки: меньше согласований, своё производство и склад, отработанные сценарии внедрения

Сроки по типам проектов — в среднем по рынку и у ГК АНТЭН



ГРУППА КОМПАНИЙ АНТЭН

КОМПАНИЯ В ЦИФРАХ

Основные показатели компании

Более 4 млрд ₽

Оборот

30 лет

На ИТ-рынке

с 1995 года — три десятилетия на рынке

Свыше 3000

Реализованных проектов

для госсектора и крупного бизнеса

98

Городов поставок

от Калининграда до Дальнего Востока

16

Сервисных центров

поддержка и обслуживание на местах

4

Страны присутствия

Россия, Армения, Казахстан, Узбекистан

30 лет на ИТ-рынке, поставки в 98 городов, 16 сервисных центров и работа в четырёх странах — надёжный партнёр для государственных задач

ГРУППА КОМПАНИЙ АНТЭН

НАПРАВЛЕНИЕ ИБ

Партнёры по информационной безопасности

Вендоры

ПРОИЗВОДИТЕЛИ РЕШЕНИЙ ИБ

- Аванпост
- Айдеко
- АйТи БАСТИОН
- Гарда Технологии
- Код Безопасности
- Лаборатория Касперского
- С-Терра
- BI.ZONE
- Check Point
- CTRL Hack
- Dr.Web
- F6
- Fortinet
- Indeed
- InfoWatch
- Phishman
- Positive Technologies
- R-Vision
- Solar
- UserGate
- GuardDo

Дистрибьюторы

ПОСТАВКА И ЛОГИСТИКА

- МОНТ
- Axoft
- OCS
- Proway

ГРУППА КОМПАНИЙ
АНТЭН

ХРОНОЛОГИЯ

Этапы реализации проектов

2–4 недели	1–2 месяца	2–4 месяца	1–2 месяца
Обследование	**Проектирование**	**Поставка и внедрение**	**Опытная эксплуатация**
Анализ процессов, сбор требований, формирование ТЗ	Архитектура решения, проектная документация	Поставка ПО, настройка, интеграция, обучение	Пилотный запуск, доработка по итогам, стабилизация

ГРУППА КОМПАНИЙ
АНТЭН

ПОЧЕМУ ВЫБИРАЮТ НАС

Надёжность, подтверждённая лицензиями и опытом

Лицензии ФСБ и МЧС

Работаем с критической инфраструктурой на законных основаниях

Аккредитованная лаборатория

Собственная лаборатория для тестирования и сертификации решений

Опыт с госзаказчиками

Десятки проектов для государственных учреждений и крупных компаний

Поддержка 24/7

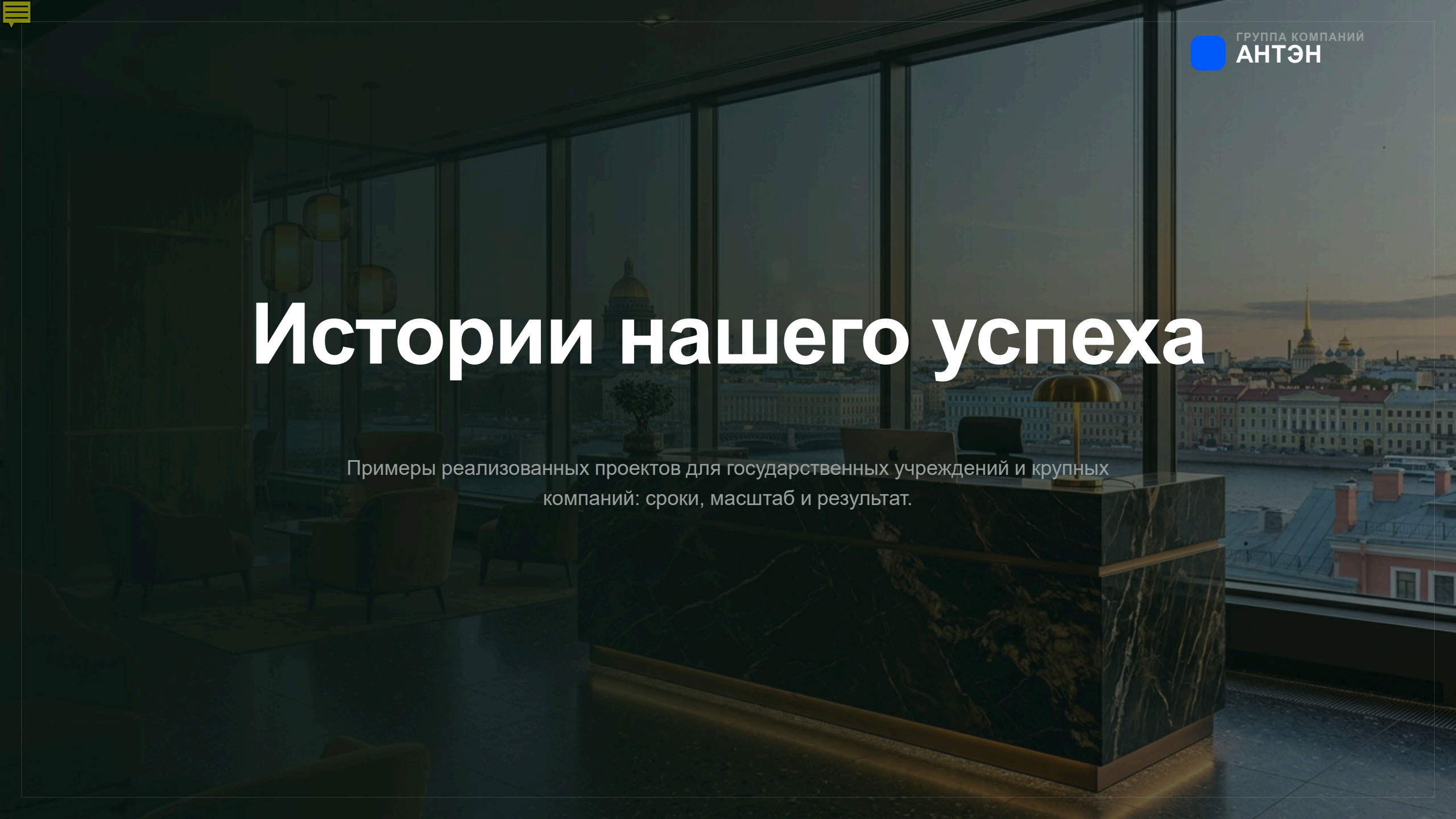
Круглосуточная гарантийная поддержка и SLA с быстрым реагированием

Собственная разработка и производство

Разрабатываем и производим сами — контроль качества и сроков на всех этапах, от идеи до внедрения

Безопасность данных

Защита информации на всех уровнях: от шифрования до физической изоляции



ГРУППА КОМПАНИЙ
АНТЭН

Истории нашего успеха

Примеры реализованных проектов для государственных учреждений и крупных компаний: сроки, масштаб и результат.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 1

Муниципальное управление: управление уязвимостями и инвентаризация ИТ-активов

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Муниципальная администрация крупного города

ЗАДАЧА

В корпоративном контуре не было централизованного выявления и учёта уязвимостей: требовался инструмент для регулярного обследования инфраструктуры и организации работы по устранению найденных проблем. Дополнительно — инвентаризация ИТ-активов: заказчику нужно понимать состав оборудования и ПО, подлежащего контролю.

РЕШЕНИЕ

Выбрана система управления уязвимостями Positive Technologies. До внедрения проведён пилот в инфраструктуре заказчика: критерии успеха определены совместно со специалистами администрации, обследованы сетевые активы, проверено соответствие требованиям и уточнён объём дальнейшей интеграции. После успешного пилота — поставка, внедрение и обучение специалистов.

РЕЗУЛЬТАТЫ

Заказчик получил централизованный инструмент выявления и учёта уязвимостей; инвентаризация ИТ-активов и управление уязвимостями объединены в одной системе; специалисты обучены и готовы к самостоятельной эксплуатации. Особенность проекта — полный цикл работ: от анализа потребности и проверки решения в реальном контуре до внедрения и передачи системы подготовленной команде заказчика.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 2

Оборонная промышленность: защита конфиденциальной информации в изолированных контурах

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Крупное промышленное предприятие оборонного профиля

ЗАДАЧА

Обеспечить контроль конфиденциальной информации и защиту от утечек в двух раздельных контурах: изолированном и открытом, с ограниченным доступом в интернет. Главная сложность — применить единый подход к защите информации без сетевого объединения контуров и нарушения установленных требований к их разграничению.

РЕШЕНИЕ

Спроектирована архитектура DLP-системы под каждый контур; поставка и интеграция выполнены вместе со специалистами предприятия. Масштаб — около 3 000 агентов. Помимо контроля передачи конфиденциальной информации подключены модули поведенческой аналитики для выявления рискованных действий. Специалисты заказчика обучены у производителя.

РЕЗУЛЬТАТЫ

DLP-защита работает в обоих контурах с сохранением их изоляции; контроль передачи конфиденциальной информации на охваченных рабочих местах организован; служба безопасности получила инструменты анализа действий пользователей; команда подготовлена к эксплуатации. Особенность — масштабное внедрение DLP при строгом разделении контуров. Название предприятия и производитель не раскрываются.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 3

Электроэнергетика: защита веб-ресурсов, управление уязвимостями и мониторинг событий

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Крупная электросетевая компания

ЗАДАЧА

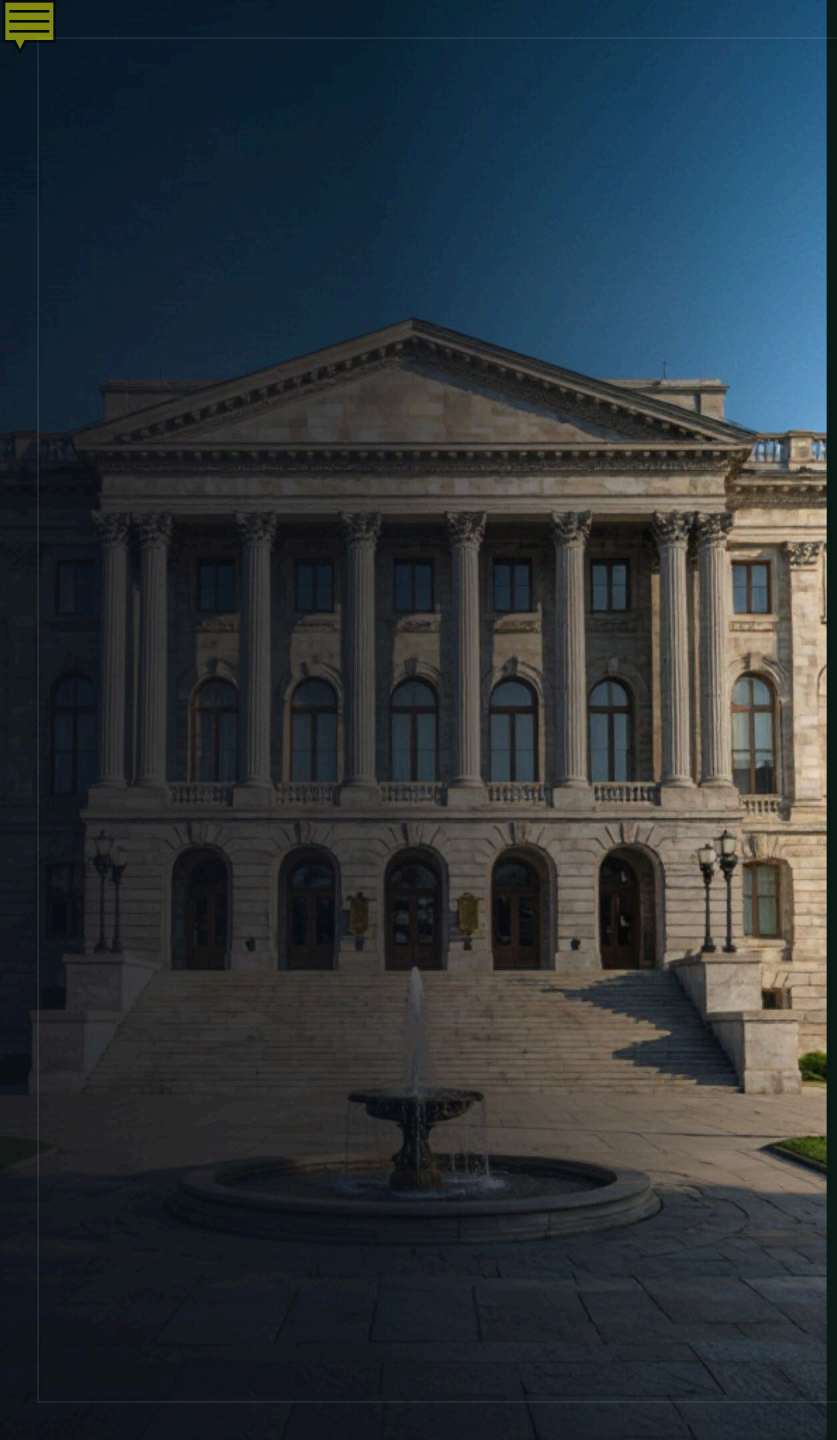
Отдельные средства защиты не давали целостной картины по ИБ. Нужно было закрыть три направления сразу: защиту внешних веб-ресурсов, управление уязвимостями внутренних систем и централизованную обработку событий безопасности.

РЕШЕНИЕ

Обследование инфраструктуры: зоны риска, защищаемые системы, источники событий. После сравнительного тестирования выбран комплекс Positive Technologies: MaxPatrol SIEM, решения классов VM и WAF. Проектирование, поставка, внедрение, обучение и испытания; далее — интеграторская поддержка. Полный цикл занял около девяти месяцев.

РЕЗУЛЬТАТЫ

Комплексная система защиты по трём взаимодополняющим направлениям; мониторинг событий централизован; налажены работа с уязвимостями и защита веб-приложений; специалисты обучены и получили канал взаимодействия с интегратором. Особенность — не поставка ПО, а интеграция нескольких классов решений с испытаниями и сопровождением.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 4

Высшее образование: защита персональных данных и выявление утечки на этапе внедрения

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Государственный университет

ЗАДАЧА

Университет обрабатывал большой объём персональных данных студентов и другой чувствительной информации. Требовалось организовать контроль её передачи внутри корпоративного контура и снизить риски утечек, связанные с действиями внутренних пользователей. До внедрения специализированной системы достаточной видимости таких событий у заказчика не было.

РЕШЕНИЕ

Проведены обследование и инвентаризация чувствительной информации: критичные категории данных определены и промаркированы для контроля. Внедрена DLP-система Solar Dozor — она отслеживает передачу защищаемой информации и фиксирует события для расследования. Уже на этапе интеграции выявлена попытка утечки со стороны внутреннего пользователя. После внедрения — консультации и помощь в обучении специалистов.

РЕЗУЛЬТАТЫ

Университет получил работающую систему контроля передачи конфиденциальных данных; выявлен инцидент, ранее невидимый существующими средствами контроля; служба безопасности получила материалы для анализа; специалистам даны консультации по эксплуатации. Особенность — ценность системы проявилась прямо в процессе внедрения: реальный инцидент обнаружен до завершения проекта.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 5

Ритейл: централизованная защита более 3 000 рабочих мест

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Крупный торговый холдинг в сфере строительных материалов с территориально распределённой инфраструктурой

ЗАДАЧА

Обеспечить единый уровень антивирусной защиты в распределённой сети и централизовать управление парком устройств. Ручная установка ПО и политик на каждом рабочем месте перегружала ИТ-службу. Требовался задел под расширение по мере роста компании.

РЕШЕНИЕ

Поставка и развёртывание отечественного решения защиты конечных точек: более 3 000 автоматизированных рабочих мест и серверная инфраструктура. Управление и единые политики безопасности централизованы. Архитектура готова к масштабированию — новые рабочие места подключаются без повторной интеграции, с учётом лицензирования.

РЕЗУЛЬТАТЫ

В распределённой инфраструктуре внедрён единый подход к защите рабочих станций; управление защитой и политиками безопасности централизовано; создана основа для подключения новых устройств по мере расширения бизнеса; сокращена потребность в индивидуальном администрировании защиты каждого рабочего места. Особенность проекта — масштаб внедрения и готовность системы к росту распределённой торговой сети.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 6

Металлургия: централизованный контроль привилегированного доступа

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Крупный российский металлургический холдинг

ЗАДАЧА

Сделать работу администраторов и пользователей с расширенными правами управляемой и прозрачной для службы информационной безопасности. Критичные промышленные системы требуют контролируемого доступа: цена ошибки в подключениях с повышенными правами особенно высока.

РЕШЕНИЕ

Проведён аудит процессов управления доступом в промышленной инфраструктуре заказчика. Совместно определены критичные системы и требования к контролю подключений пользователей с повышенными правами. Внедрено решение Indeed PAM: привилегированный доступ к охваченным системам переведён под централизованный контроль в согласованном контуре защиты.

РЕЗУЛЬТАТЫ

Служба ИБ видит действия администраторов, а подключения с расширенными правами идут по управляемому процессу в согласованном контуре. Особенность проекта — мы закрываем риски не только обычных пользователей, но и самой чувствительной категории: административного доступа к промышленным системам.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 7

Атомная отрасль: уязвимости находим до ввода ПО в эксплуатацию

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Предприятие крупного российского холдинга в атомной отрасли

ЗАДАЧА

Усилить безопасность разрабатываемого ПО ещё до ввода в эксплуатацию: находить уязвимости в уже работающих системах и поздно, и дорого. Требовался контроль качества кода прямо в процессе разработки, с учётом корпоративных политик безопасности и ограничений доступа на объект.

РЕШЕНИЕ

Обследована среда разработки: определены языки программирования, особенности жизненного цикла и требования корпоративных политик безопасности. Внедрена платформа Solar appScreener для автоматизированного анализа исходного кода — проверки идут прямо в процессе разработки, с учётом ограничений доступа на объект.

РЕЗУЛЬТАТЫ

Уязвимости выявляются до выхода ПО в промышленную эксплуатацию, а разработчики получают конкретные рекомендации по их устранению. Особенность проекта — смена подхода от реагирования к профилактике: эту модель мы предлагаем тиражировать на другие предприятия отрасли.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 8

Нефтегазовый сектор: комплексная трансформация ИБ

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Крупная международная энергетическая компания с распределённой инфраструктурой в России и за рубежом

ПРОБЛЕМА

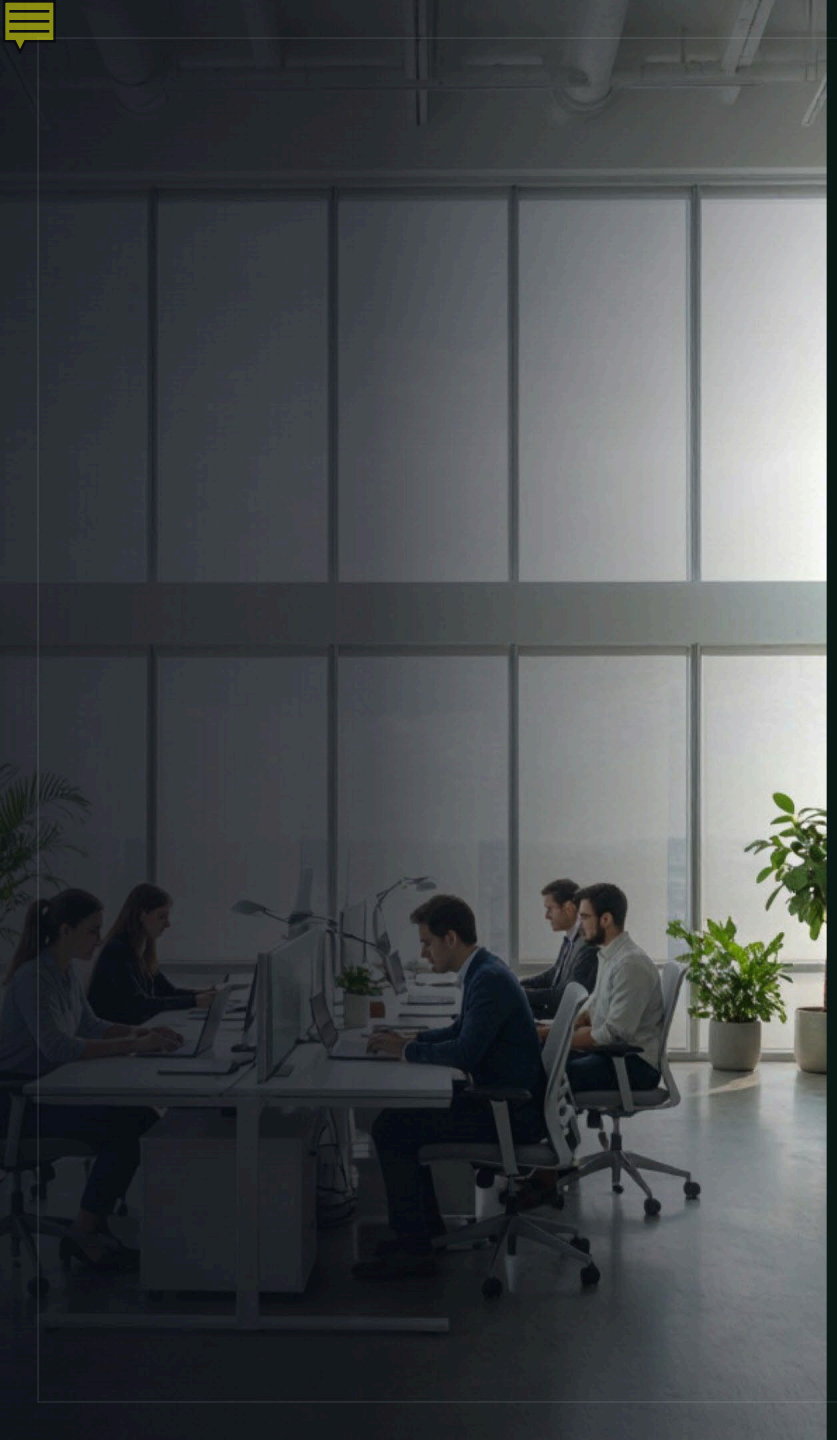
ИТ-ландшафт фрагментирован: часть систем локально, часть за рубежом, что не отвечало требованиям надёжности. Нужна консолидация в РФ, аудит зрелости ИБ, соответствие нормам и защита критичных технологических данных.

РЕШЕНИЕ

Аудит сетевой архитектуры и зрелости ИБ, оцифровка трудозатрат, трёхмесячный план трансформации и пакет ЛНД; миграция ключевых сервисов по модели IaaS с многоуровневым бэкапом (immutable-копии, лента); микросегментация сети, кластер NGFW Active-Active, защита облачного периметра и MFA; DLP и on premise Vulnerability Management с предиктивным анализом.

РЕЗУЛЬТАТЫ

Зависимость от зарубежных мощностей устранена, инфраструктура локализована в защищённом российском контуре; построена «цифровая крепость» без единой точки отказа; непрерывность бизнес-процессов гарантирована многоуровневым планом восстановления данных (Disaster Recovery).



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 9

Юридический консалтинг: защищённая облачная инфраструктура и MDM

НАПРАВЛЕНИЕ

Информационная безопасность

ЗАКАЗЧИК

Международная консалтинговая компания с офисами в России и Европе

ПРОБЛЕМА

Мобильность консультантов и работа с конфиденциальными данными клиентов с личных устройств (BYOD). Нужен отказ от локальных серверов в пользу облака без снижения стандартов безопасности.

РЕШЕНИЕ

Перенос сервисов из on-premise в облако провайдера; виртуальный NGFW и MFA для удалённых подключений; MDM по модели Managed Service / SaaS без капзатрат; Security Awareness от Phishman как Managed Service, 30 лицензий.

РЕЗУЛЬТАТЫ

Защищённый доступ сотрудников к корпоративным ресурсам из любой точки мира; минимизированы риски утечки конфиденциальных данных клиентов с мобильных устройств; снижены затраты на владение ИТ (OpEx).



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 10

Промышленное производство: отказоустойчивая сетевая защита и внутренний контроль

НАПРАВЛЕНИЕ

Информационная безопасность и защита сетей

ЗАКАЗЧИК

Крупный российский производитель металлоконструкций и трубной продукции

ПРОБЛЕМА

Вся инфраструктура в локальном контуре (on-premise), где любой сетевой сбой останавливает производственные линии. Нужна защита от внешних атак (DDoS) и от утечек технологической, финансовой и конструкторской информации.

РЕШЕНИЕ

Отказоустойчивый периметр Active-Active на комплексах NGFW; сегментация сети с изоляцией технологических сегментов; защита от DDoS на базе анализа NetFlow; DLP на 100 станциях и MDM на 50 устройствах; Security Awareness от Phishman как Managed Service, 100 лицензий.

РЕЗУЛЬТАТЫ

Исключены простои оборудования из-за отказов сетевых шлюзов; обеспечена защита от внешних сетевых угроз и целевых DDoS-атак; внутренний периметр передачи коммерческих и технологических данных взят под полный контроль.



ГРУППА КОМПАНИЙ АНТЭН

ИСТОРИЯ УСПЕХА · КЕЙС 11

Банковский сектор: регуляторный аудит и надёжное импортозамещение

НАПРАВЛЕНИЕ

Информационная безопасность и импортозамещение

ЗАКАЗЧИК

Банк из финансового сектора, проходящий регулярные проверки ЦБ РФ и ФСТЭК

ПРОБЛЕМА

Межсетевой экран отечественного вендора постоянно отказывал: аппаратные сбои, замена комплектующих, внеплановые расходы. При этом системы банка должны были безотказно работать и проходить проверки регуляторов.

РЕШЕНИЕ

Регуляторный аудит всей ИТ-инфраструктуры на соответствие требованиям финансового сектора; замена нестабильного оборудования на отказоустойчивый комплекс NGFW; перенос политик безопасности с разграничением доступа к АБС и процессинговым сегментам.

РЕЗУЛЬТАТЫ

Проверки ЦБ РФ и ФСТЭК пройдены без замечаний; отказы устранены, критические системы работают стабильно; снижена совокупная стоимость владения (TCO).

ГРУППА КОМПАНИЙ
АНТЭН

ФИНАЛ

Готовы работать уже сейчас

Готовы обсудить сотрудничество и подготовить коммерческие предложения по вашим задачам.

ПОЧТА

site@anten.ru

mail@anten.ru

ТЕЛЕФОНЫ

+7 (812) 703-04-00

+7 (495) 136-41-30

САНКТ-ПЕТЕРБУРГ

Наличная ул., д. 44, к. 1, стр. 1

199397

МОСКВА

ул. Большая Спасская, д. 8

anten.ru

ЕКАТЕРИНБУРГ

ул. Малышева, д. 51

офис в центре города

ТЮМЕНЬ

ул. 30 лет Победы, д. 27а

офис № 408