Timsoh

Центр мониторинга кибербезопасности

Тренды на рынке ИБ

Нехватка квалифицированных ИБ-специалистов

Из-за кадрового голода компаниям сложно найти высококвалифицированных экспертов и предложить конкурентные условия

Появление новых требований регуляторов

Новые законодательные акты в области обеспечения кибербезопасности

Стремительное рост количества кибератак

Методологии атак становятся все сложнее. Количество инцидентов ежегодно увеличивается на 20-30%

Timsoh

Бизнесу нужны

- команда квалифицированных специалистов
- инновационные технологии
- выстроенные процессы

=

Центр мониторинга кибербезопасности (SOC)

Исследование SOC

67%

начали использовать SOC в течение последних 3 лет

45%

выбрали MSSP модель

Почему выбирают MSSP:

- Нехватка ресурсов и экспертизы
- Быстрый доступ к новым технологиям
- Сокращение расходов на ИБ

Timsoh

ЧТО ПРЕДЛАГАЕМ БИЗНЕСУ

- Мониторинг и информирование об инцидентах 24/7
- Аналитический разбор выявленных инцидентов
- Оперативное предоставление рекомендаций по реагированию
- Хранение и оперативное предоставление информации для расследования
- Соответствие требованиям законодательства
- Разработка сценариев выявления инцидентов под требования заказчика
- Ведение базы знаний
- Прозрачное управление киберинцидентами

Timsoh

Форматы подключения SOC

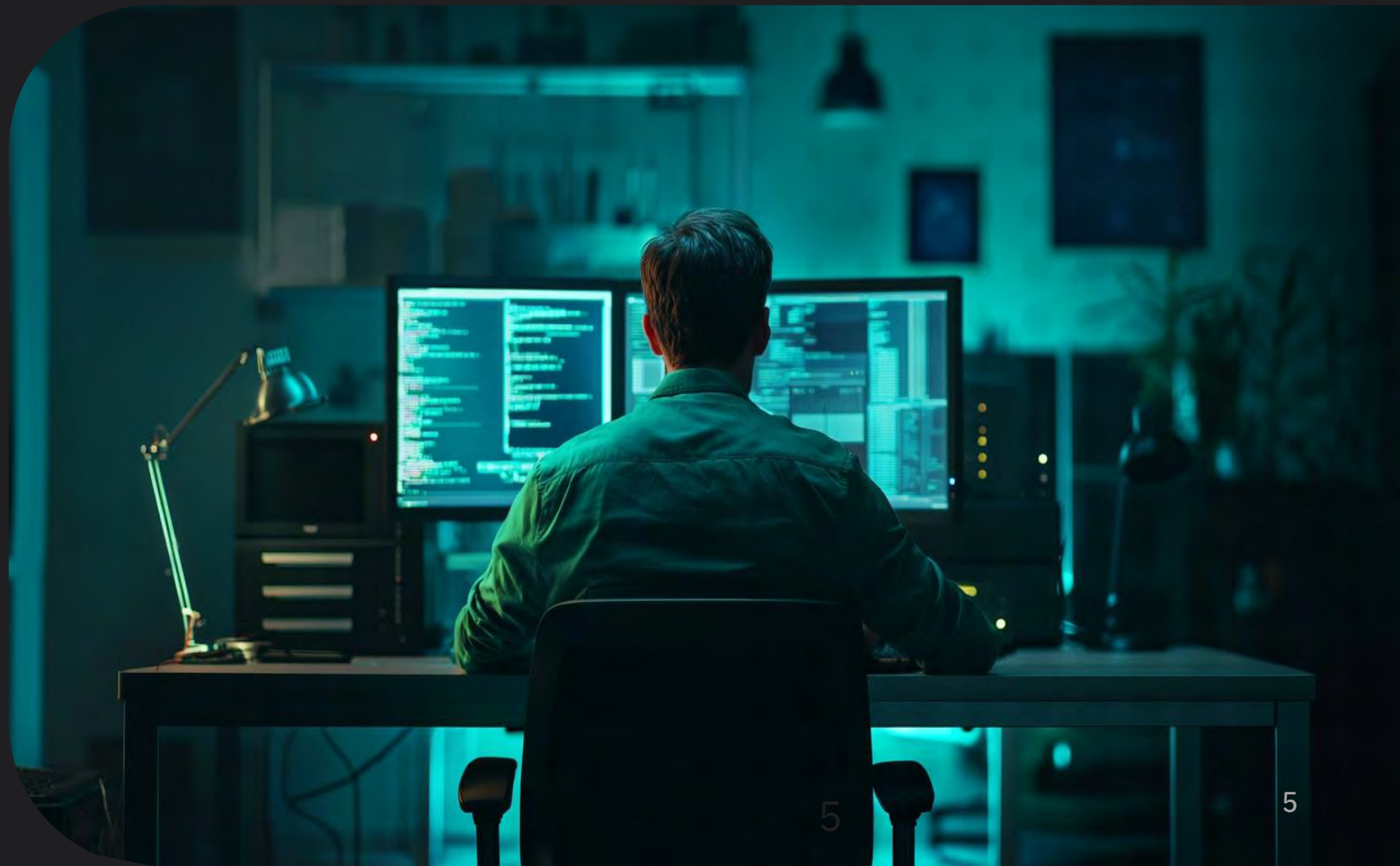
Выбор инсталляции зависит от потребностей и зрелости клиента, действующей инфраструктуры и имеющегося бюджета

MSSP SOC

на базе Kaspersky KUMA и защищенной облачной платформы Timsoh

Гибридный

- Зоны ответственности по владению и мониторингу разделены
- SIEM размещена в вашей инфраструктуре



Timsoh

5

Как происходит подключение к SOC

01
Подготовительные работы
Утверждение регламента взаимодействия, перечня источников, SLA

02
Построения защищенного канала связи
Безопасный канал передачи данных между SOC и инфраструктурой клиента

03
Установка и настройка SOC
Функционирующие устройства сбора событий в инфраструктуре клиента

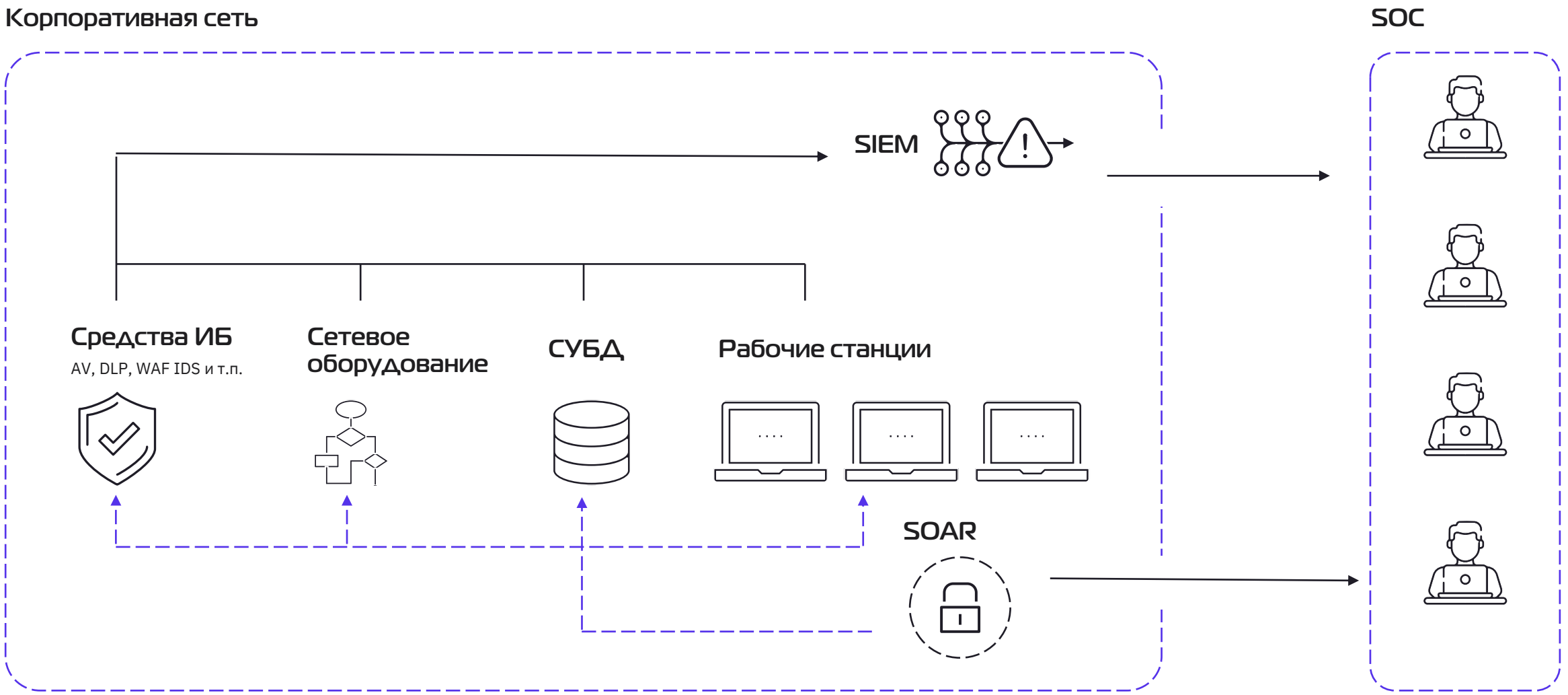
04
Подключение источников событий к SOC
Источники событий — объекты ИТ-инфраструктуры или СЗИ клиента

05
Мониторинг и анализ инцидентов ИБ
Отчеты и рекомендации по реагированию на инциденты ИБ

- Дополнительная разработка правил
- Дополнительное подключение источников

Timsoh

Работа SOC в вашей инфраструктуре



Timsoh

Усильте свою безопасность с дополнительными услугами

Расследование инцидентов

- Анализ кибератак и план по устранению их последствий
- Сводная информация о возможных точках проникновения

Тест на проникновение

- Определение слабых мест в вашей инфраструктуре благодаря имитации действий злоумышленников, эксплуатирующих уязвимости, и разработка рекомендаций по их устранению

Консалтинг

- Экспертный аудит состояния ИБ
- Разработка документации по требованиям законодательства в части ИБ
- Повышение осведомленности пользователей с помощью учебных фишинговых рассылок

Выявление и анализ уязвимостей

- Регулярные или разовые сканирования уязвимостей внешнего, внутреннего периметра и веб-ресурсов, разработка рекомендаций по их устранению в порядке приоритета

Потоки данных с индикаторами компрометации (TI)

- Подключение потоков данных об индикаторах компрометации для быстрого и точного обнаружения угроз, повышения качества анализа событий за счет детального контекста

Моделирование угроз

- Моделирование угроз безопасности по требованиям методических рекомендаций

VPN

- Специализированный защищенный канал связи с использованием криптоалгоритмов, в соответствии с законодательством и отраслевыми стандартами

Техподдержка ИБ

- Поддержка уже установленных СЗИ, а также услуги по реагированию на инциденты ИБ

Дополнительные сервисы ИБ

- Дополнительные сервисы по MSSP-модели: WAF, Anti-DDoS, NGFW, Anti-Bot

Timsoh

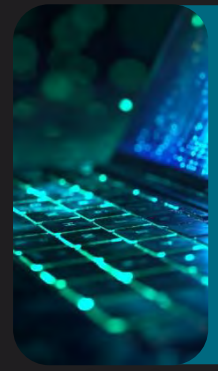
Вместе с нами вы получаете

Персонального менеджера

Обслуживание по типу «одного окна» с выделенным сервис-менеджером

Оптимальный SLA с реакцией на инцидент от 20 минут

Учитываем потребности и возможности каждого заказчика



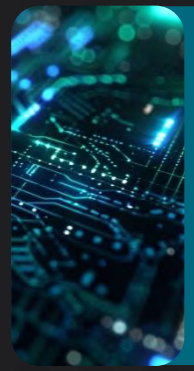
Быстрый старт

Экспертный опыт позволяет осуществить первоначальное внедрение типовых источников за 2 недели

MSSP

Отраслевую экспертизу

Подтвержденный опыт реализации проектов с учетом специфики отрасли



Криминалистическую экспертизу

Выявление границ инцидента, установление возможных причин инцидента и оперативное формирование отчета

SOC из надежного облака

Доверенная обработка большого объема данных без потери скорости

Соответствует требованиям безопасности хранения данных

MSSP

- Реальный опыт администрирования и эксплуатации СЗИ: более 20 различных продуктов
- Компетенции в реализации проектов по построению различных ИТ-инфраструктур: более 450 проектов
- Обширная партнерская сеть: более 400 вендоров

Проектный опыт

SOC в соответствии с требованиями законодательства

Оператор крупной государственной информационной системы

Задача

Система доступна через Интернет и крайне критична к задержкам: к ней обращаются десятки тысяч пользователей и организаций по всей стране.

Заказчик обязан обеспечить процессы мониторинга инцидентов безопасности в соответствии с требованиями законодательства.

Решение

Внедрен сервис SOC, предоставляющий комплексные услуги по покрытию всех основных задач оператора в области ИБ и требований законодательства.

В состав услуг входят периодическая инвентаризация системы, анализ уязвимостей, тестирование на проникновения, реагирование на инциденты и др.

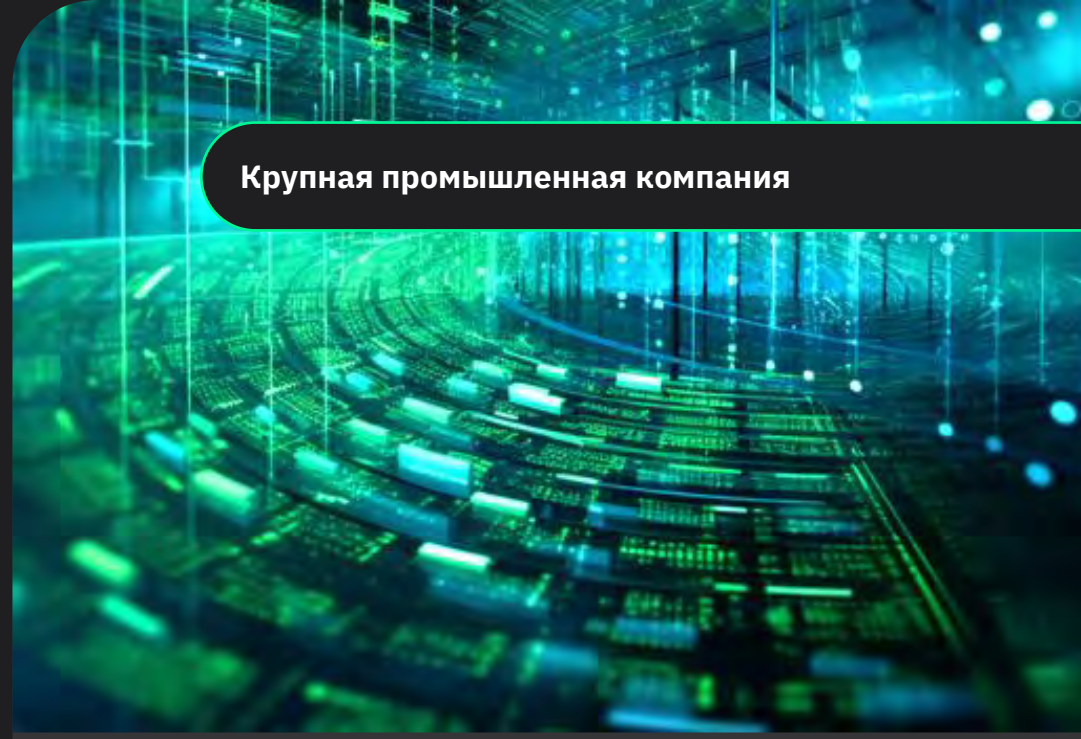
Результат

- Требования регуляторов выполнены
- Мониторинг осуществляется в режиме 24/7

Timsoh

Проектный опыт

SOC для компании с разнородными и удаленными друг от друга ИТ-компонентами



Задача

Крупная компания имеет распределенную информационную инфраструктуру с разнородными и удаленными друг от друга компонентами. Это затрудняет их обслуживание и администрирование специалистами ИБ и упрощает возможность совершения атак злоумышленниками

Решение

Специалисты SOC Timsoh проводят выявление инцидентов, анализ уязвимостей, тестирование на проникновения, внедрение и обслуживание SIEM-систем, сканеров защищенности и т.п.
В режиме онлайн аналитики осуществляют контроль происходящих ИБ-событий, отслеживают критичные изменения, организуют процессы реагирования и нейтрализации инцидентов.

Результат

- Минимизация ущерба по критическим бизнес-процессам
- Снижение репутационных и регуляторных рисков
- Снятие нагрузки со штатных ИТ и ИБ-специалистов

Timsoh

Проектный опыт

Сопровождение средств защиты информации ГИС

Задача

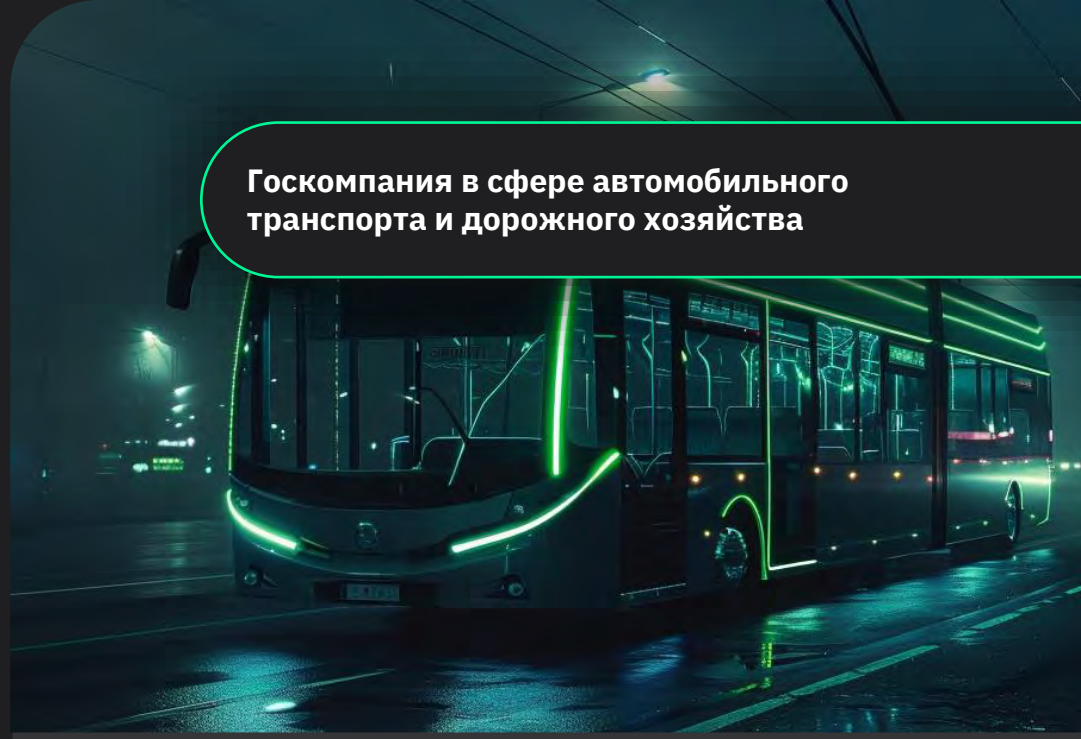
Необходимо сопровождение средств защиты информации государственных информационных систем, в том числе мониторинг и актуализация организационно-распорядительных документов.

Решение

Наш собственный сервис SOC позволил выполнить все основные требования законодательства в области защиты персональных данных.

Мониторинг событий в области информационной безопасности осуществлялся в режиме 24/7, мы ежемесячно предоставляли отчеты об инцидентах и рекомендации по корректировке документов заказчика.

Кроме того, в услуги входила проверка корректной работоспособности средств защиты информации и масштабирование средств защиты информации на АРМы клиента



Госкомпания в сфере автомобильного транспорта и дорожного хозяйства

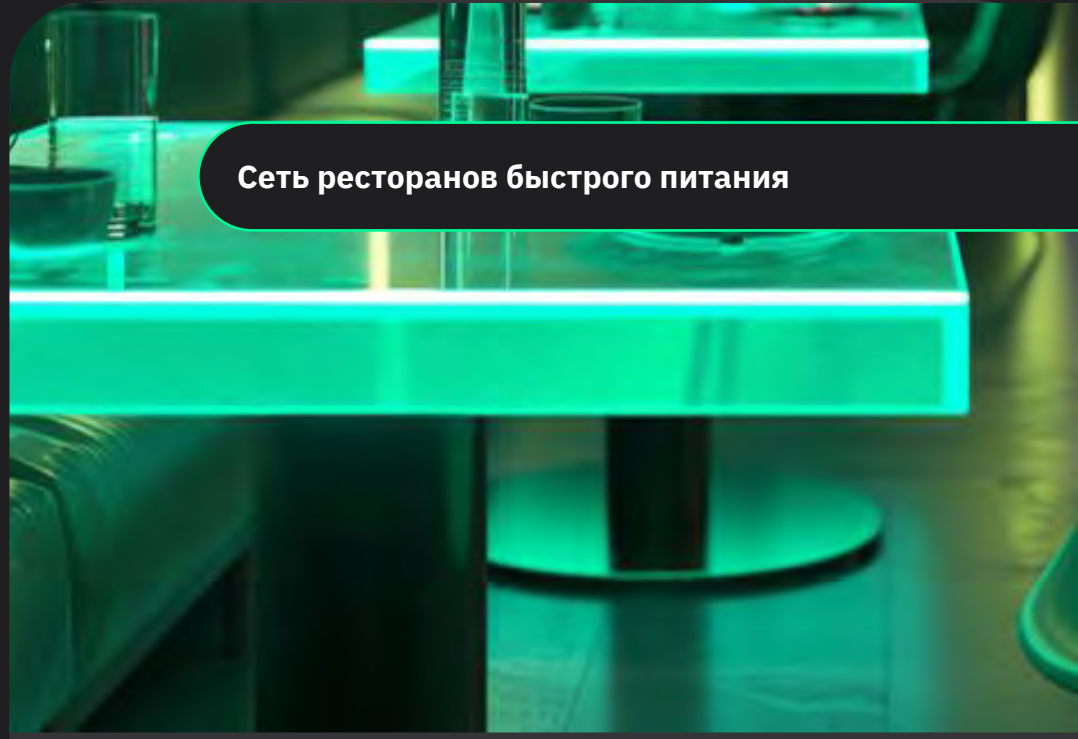
Результат

- Регулярные рекомендации по улучшению уровня безопасности
- Мониторинг осуществляется в режиме 24/7

Timsoh

Проектный опыт

Защита от кибератак сети ресторанов быстрого питания



Задача

Компания столкнулась с проблемами во время локализации своей ИТ-инфраструктуры в России. Незадолго до старта проекта подверглась целенаправленной кибератаке со стороны злоумышленников. Было принято решение в сжатые сроки осуществить переход на российские ИБ-решения.

Решение

Timsoh предоставила услуги своего центра мониторинга инцидентов ИБ — SOC. За две недели к системе мониторинга были подключены все основные Windows-устройства, далее в течение месяца — оставшаяся инфраструктура.
Это позволило в короткие сроки и с минимальными потерями выявить точки, через которые шла атака, и отразить ее.
Кроме того, в рамках проекта зарубежные средства защиты были замещены на российские решения.

Результат

- Экспресс-подключение SOC
- Требования регуляторов выполнены

Timsoh

Наша экспертиза

>100

Специалистов в группе компаний с профессиональными сертификатами в области информационной безопасности

>2000

Реализованных проектов в области ИБ

>80

Партнеров-вендоров ИБ

Кастомизированный подход к каждой задаче

Выделенная команда техподдержки

Наличие необходимого комплекта лицензий регулирующих органов

Timsoh

Прозрачность в управлении киберинцидентами

Timsoh

Свяжитесь с нами

Андрей Заикин

Руководитель направления «Кибербезопасность»

AZaikin@timsoh.uz

Иван Бессолов

Старший менеджер по продвижению решений

IBessolov@timsoh.uz