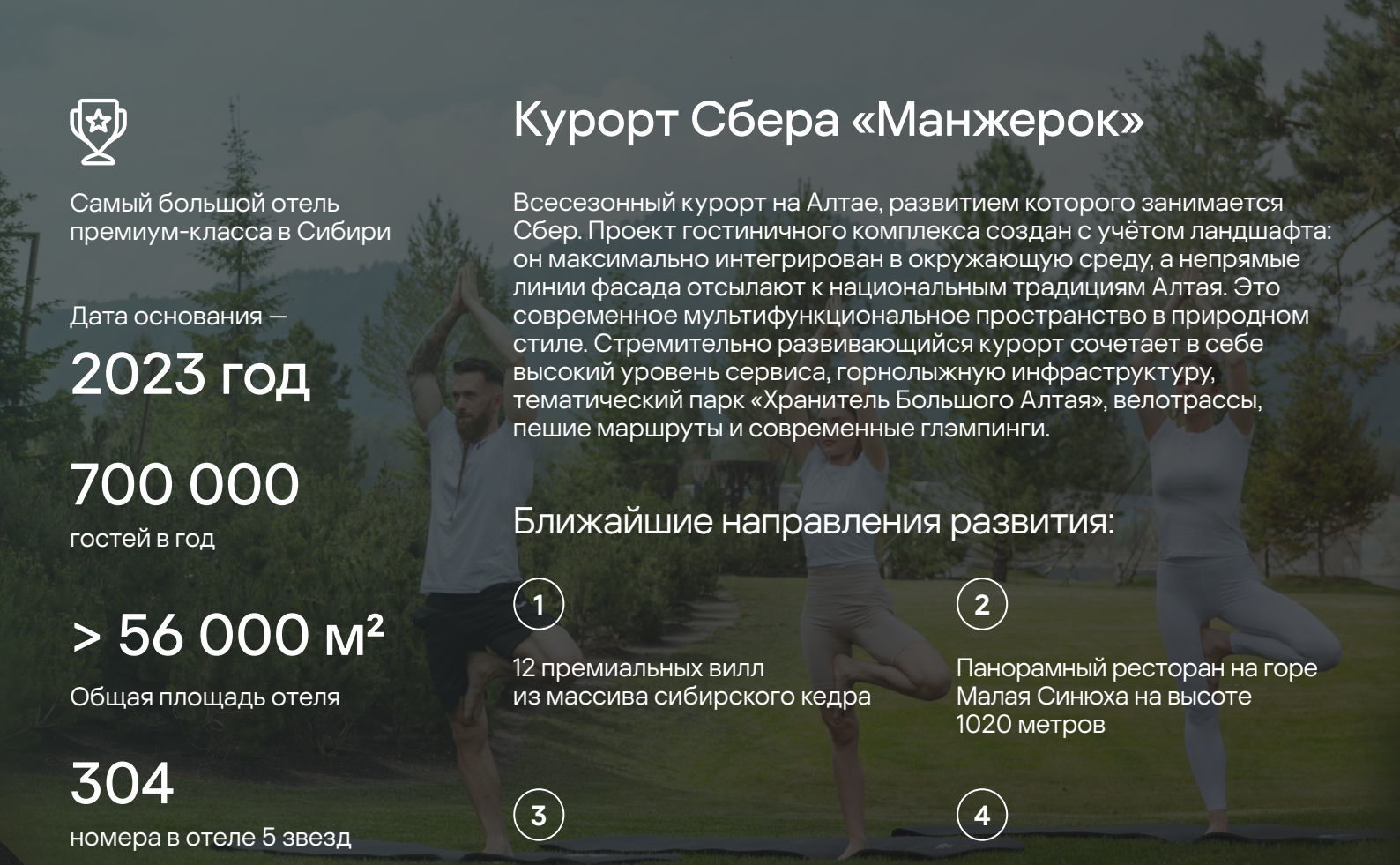
Повышение уровня защищенности сети

горнолыжного курорта «Манжерок»

kaspersky активируй будущее

МАНЖЕРОК



Самый большой отель премиум-класса в Сибири

Дата основания —

2023 год

700 000

гостей в год

> 56 000 м²

Общая площадь отеля

304

номера в отеле 5 звезд

Курорт Сбера «Манжерок»

Всесезонный курорт на Алтае, развитием которого занимается Сбер. Проект гостиничного комплекса создан с учётом ландшафта: он максимально интегрирован в окружающую среду, а непрямые линии фасада отсылают к национальным традициям Алтая. Это современное мультифункциональное пространство в природном стиле. Стремительно развивающийся курорт сочетает в себе высокий уровень сервиса, горнолыжную инфраструктуру, тематический парк «Хранитель Большого Алтая», велотрассы, пешие маршруты и современные глэмпинги.

Ближайшие направления развития:

1. 12 премиальных вилл из массива сибирского кедра
2. Панорамный ресторан на горе Малая Синюха на высоте 1020 метров
3. 67 км горнолыжных трасс
4. Более 30 км байк-трасс и 15 км пеших маршрутов

Система управления

Решение поддерживает протокол KNX, который широко применяется в гостиничном бизнесе для автоматизации инженерных систем, управления эксплуатационными расходами и обслуживания клиентов.

Современные технологии для защиты курортного объекта

В 2023 году перед заказчиком встала задача по повышению уровня защищенности систем управления автоматизации здания и инженерных систем гостиничного комплекса. Для этого необходимо было снизить риски и последствия неавторизованных подключений к инженерным сетям, несанкционированного изменения настроек и режимов работы оборудования, в том числе со стороны подрядчиков с неавторизованными устройствами.

Для реализации этих защитных мер специалисты интегратора STEP LOGIC предложили заказчику решение KICS for Networks, предназначенное для анализа трафика в промышленной сети с целью обнаружения вторжений, несанкционированных сетевых устройств, новых сетевых взаимодействий, запрещенных системных команд и прочих аномалий.

Интересно, что в данном случае KICS for Networks внедрялся на курортном объекте, где автоматизированные системы управления зданиями и инженерными системами работают как классическая АСУ ТП. То есть имеют соответствующее разделение на уровни и используют распространенные промышленные сетевые протоколы.

Kaspersky Industrial CyberSecurity for Networks

Программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Kaspersky Industrial CyberSecurity for Networks анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети. Программа входит в состав решения Kaspersky Industrial CyberSecurity.

Преимущества Kaspersky KICS for Networks

- Возможность интеграции с решением для защиты серверов и промышленных рабочих станций Kicks for Nodes
- Поддержка более 50 промышленных протоколов и их анализ на прикладном уровне
- Возможность активного опроса промышленной сети
- Топологическая карта сети с возможностью определения проблемных объектов и сетевых взаимодействий
- Риск-ориентированный подход и формирование отчетов
- Наличие сертификатов совместимости с решениями АСУ ТП отечественных и зарубежных производителей

Процесс внедрения

Для реализации мер защиты систем управления автоматизации здания и инженерных систем горнолыжного курорта «Манжерок» было внедрено решение Kaspersky Industrial CyberSecurity for Networks (KICS for Networks). Специализированное решение для мониторинга промышленной сети успешно закрыло потребности заказчика в повышении уровня защищенности сети на предприятии, относящей к отрасли инжиниринга и автоматизации зданий, согласно статистике Kaspersky ICS CERT за второе полугодие 2023 года входящей в тройку отраслей по количеству компьютеров АСУ, на которых были заблокированы вредоносные объекты.

Внедрение выполнялось интегратором STEP LOGIC по рекомендованной «Лабораторией Касперского» схеме.

KICS for Networks развернут на выделенном физическом сервере. Сбор трафика осуществляется по протоколу RSPAN на 26 коммутаторах, используются 10GE интерфейсы.

Система несколько месяцев находилась в режиме обучения, после чего была переведена в режим наблюдения. По итогам работы в режиме обучения в системе было создано более 40 000 правил контроля сети и процессов. На текущий момент KICS for Networks осуществляет мониторинг 13 различных инженерных систем с более чем 500 устройствами. Текущая средняя скорость трафика, поступающего с инженерных систем, около 10 Мбит в секунду.

Параллельно с этим в гостиничном комплексе была проведена модернизация инженерных систем и сетевого оборудования, из-за чего возникло большое число «false-positive» событий. Благодаря функции импорта данных, которая значительно упрощает работу с большим количеством устройств и изменением их параметров, удалось быстро изменить конфигурацию и решить проблему.

Современный уровень автоматизации управления крупными инфраструктурными объектами предъявляет высокие требования к защищенности, поскольку даже небольшие простои, вызванные сбоем инженерных или систем безопасности, ведут к крупным финансовым потерям.

Результаты и отзывы

Благодаря KICS for Networks заказчику удалось снизить риски подключения неавторизованных устройств к промышленной сети и дальнейших вмешательств в работу инженерных систем.

Андрей Баранов

Директор по информационным технологиям всесезонного курорта «Манжерок»

Внедрение KICS for Networks позволило снизить затраты на обнаружение инцидентов информационной безопасности и ликвидацию их последствий. Благодаря повышенной безопасности и надёжности работы систем мы можем гарантировать непрерывность и высокое качество предоставляемых услуг. Это в свою очередь способствует росту лояльности клиентов, укреплению положительного имиджа бренда. Мы рады сотрудничеству с «Лабораторией Касперского» и надеемся на его расширение. Отдельно хотел бы поблагодарить за помощь в реализации проекта наших партнёров в лице компании STEP LOGIC. Мы продолжим уделять приоритетное внимание инновациям и улучшению наших систем, чтобы предоставлять гостям качественный и надёжный сервис.

Николай Забусов

Директор департамента ИБ STEP LOGIC

На этапе внедрения наши специалисты настроили более двух десятков коммутаторов для сбора трафика по протоколу RSPAN. Несколько месяцев система работала в режиме обучения, в результате было создано более 40 000 правил контроля сети и процессов. Кроме основных задач, с помощью функционала KICS for Networks, мы также смогли успешно выявлять ошибки конфигурации устройств нижнего уровня. К другим плюсам решения можно отнести поддержку функции импорта данных из файлов. Это сильно упростило работы по корректировке параметров большого количества устройств в рамках процесса устранения ложных срабатываний, вызванных параллельными работами по модернизации инженерного и сетевого оборудования. На сегодняшний день KICS for Networks является одним из наиболее продвинутых отечественных решений в области обнаружения вторжений потенциально враждебных действий в промышленной сети.

Марина Усова

Директор по корпоративным продажам «Лаборатории Касперского» в России

Сегодня для поддержания устойчивости и конкурентоспособности компании внедряют специализированные решения для киберзащиты. Мы рады, что наше решение KICS for Networks, разработанное для мониторинга трафика в АСУ ТП, теперь используется для защиты промышленного трафика в инженерных системах горнолыжного курорта «Манжерок». «Лаборатория Касперского» предлагает целый комплекс решений для защиты систем инжиниринга и автоматизации зданий – сферы, которая развивается высокими темпами и все чаще становится целью кибератак.

Kaspersky Industrial CyberSecurity for Networks

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее