«Лаборатория Касперского» защитит спортсменов в Катаре

с Олимпийским комитетом Катара

kaspersky активируй будущее

قطر QATAR

اللجنة الأولمبية القطرية
Qatar Olympic Committee

Организация с государственным участием

Доха, Катар

Поддержка при реагировании на инциденты

Более 500 сотрудников

Олимпийский комитет Катара

Олимпийский комитет Катара сосредоточен на развитии спорта в стране и представляет ее на международных спортивных мероприятиях.

Организуя инновационные спортивные программы и первые соревнования такого рода на Ближнем Востоке, Олимпийский комитет Катара стремится внести максимальный вклад в обеспечение мира на земле. Организация ведет популяризацию спорта среди населения, дает спортсменам доступ к самым современным спорткомплексам и другим возможностям для тренировок и поддерживает их на международной арене.

Использует Kaspersky Security для бизнеса, платформу Kaspersky Anti Targeted Attack, Kaspersky Private Security Network, Kaspersky CyberTrace, потоки данных «Лаборатории Касперского» об угрозах, Kaspersky Threat Lookup и Kaspersky Endpoint Detection and Response

Заключение соглашения

Олимпийский комитет Катара заключает соглашение с «Лабораторией Касперского» для защиты международных спортивных мероприятий от кибератак.

Предыстория

Осознавая активное развитие киберугроз в стране, Олимпийский комитет Катара искал партнера, способного защитить его от новейших угроз, обеспечив безопасность данных и предотвратив потенциальный репутационный ущерб.

Это крупная организация с государственным участием, которая серьезно относится к своей репутации и безопасности. Сейчас страна выступает организатором спортивных мероприятий мирового уровня и планирует подать заявку на проведение Олимпийских игр, поэтому вопрос безопасности встает еще острее. Дело в том, что такие крупные события существенно повышают риск кибератаки, и, если преступникам удастся скомпрометировать данные, последствия могут быть катастрофическими.

Инциденты кибербезопасности могут навредить репутации и деловым отношениям, поэтому организация решила внедрить проактивный подход, сосредоточившись на предотвращении инцидентов, а не на устранении их последствий.

Не менее серьезно Олимпийский комитет Катара относится к обеспечению конфиденциальности данных, внутренних и внешних коммуникаций. Поэтому организация искала решение для защиты конфиденциальной информации, которое не снижало бы эффективности повседневных операций.

Число киберугроз и их сложность растут по всему миру, и Катар не исключение. Расположение страны и ее растущая активность на международной арене делают Катар привлекательной мишенью для киберпреступников.

Для защиты сетей от угроз Олимпийский комитет Катара использует систему управления данными и инцидентами безопасности (SIEM), и его целью было расширить возможности аналитики угроз с помощью решения надежного поставщика.

Сотрудники «Лаборатории Касперского» прислушались к нашим требованиям и дали нам продукт, который не просто соответствует нашим ожиданиям, а превосходит их. Мы уверены, что наша сеть надежно защищена решением, созданным экспертами в области кибербезопасности.

Рашид Аль Нахлави

Консультант по IT-безопасности, Олимпийский комитет Катара

Путь к надежности

«Лаборатория Касперского» предложила Олимпийскому комитету Катара комплексное интегрированное решение, в состав которого входят Kaspersky Security для бизнеса, платформа Kaspersky Anti Targeted Attack, Kaspersky Private Security Network и Kaspersky CyberTrace.

Kaspersky
Endpoint Security
for Business

Kaspersky Security для бизнеса

Развернув Kaspersky Security для бизнеса на всех рабочих местах, включая рабочие станции и мобильные устройства, наряду с решением для безопасности почтовых серверов, организация обеспечила несколько уровней адаптивной защиты своих рабочих мест от фишинга, социальной инженерии и атак шифровальщиков. Для работы с защитными решениями используются легкие агенты, управление которыми осуществляется из централизованной панели мониторинга, позволяющей решать и другие задачи, такие как удаленное управление защитой и установка исправлений на рабочих местах. Это позволяет устранять уязвимости сразу же по мере выхода исправлений.

Kaspersky
Anti Targeted
Attack

Платформа Kaspersky Anti Targeted Attack

Платформа Kaspersky Anti Targeted Attack позволяет специалистам центра мониторинга и реагирования (SOC) Олимпийского комитета Катара быстро обрабатывать инциденты и реагировать на них. Отслеживая данные с многочисленных датчиков, расположенных на рабочих местах, в локальной сети и на почтовых серверах, и анализируя их в режиме реального времени, платформа мгновенно оповещает специалистов об инцидентах и подозрительном поведении, позволяя изолировать и анализировать угрозы в улучшенной песочнице и проверять эффективность реагирования до его реального развертывания. Возможность поиска угроз в ручном режиме позволила команде реализовать проактивный подход к защите сети и рабочих мест.

Kaspersky Anti Targeted Attack — уникальная платформа. Ни один другой поставщик не предлагает подобных продуктов. Нам доступно семь передовых технологий для анализа, обнаружения и блокирования угроз для рабочих мест, почтовых угроз и веб-атак. Это существенно повышает гибкость и эффективность обнаружения и реагирования по сравнению с другими методами. Платформа Kaspersky Anti Targeted Attack выходит далеко за рамки традиционных решений обнаружения и реагирования, которые оказывают скорее вспомогательную функцию. Это настоящий «швейцарский нож» со встроенными инструментами обнаружения угроз, их активного поиска и криминалистического анализа. Решение практически мгновенно обнаруживает угрозы и предоставляет четкие и полные данные об их возможном происхождении. Эти данные существенно углубили наши знания об угрозах, и теперь я и моя команда чувствуем себя гораздо увереннее при выборе способов борьбы с ними. Платформа предлагает эффективные инструменты активного поиска угроз, которые способствуют более глубокому анализу отдельных событий. Нам не нужно использовать несколько приложений для подтверждения инцидента и переключаться между окнами — это очень удобно.

Рашид Аль Нахлави

Консультант по IT-безопасности, Олимпийский комитет Катара

Обнаружение

Решения повышают процент обнаружения и скорость реагирования

Производительность

У штатных специалистов появились новые инструменты для нейтрализации атак и укрепления безопасности

Экономическая выгода

Широкий спектр возможностей доступен по выгодной цене

Техподдержка

Эксперты «Лаборатории Касперского» всегда готовы прийти на помощь

Kaspersky Private Security Network

Kaspersky CyberTrace

Аналитика угроз

Для получения актуальных данных об угрозах Олимпийский комитет Катара использует решения Kaspersky Private Security Network и Kaspersky CyberTrace. Kaspersky Private Security Network предоставляет аналитику угроз в режиме реального времени, а Kaspersky CyberTrace сопоставляет полученные данные с другими источниками и передает их в SIEM-систему. Таким образом организация может проактивно обнаруживать угрозы на основе аналитических данных.

Kaspersky Private Security Network предоставляет точную облачную аналитику угроз с минимальным процентом ложных срабатываний, не отправляя данные за пределы сети организации. Вместе эти решения позволяют специалистам SOC быстро обнаруживать киберугрозы и эффективно реагировать на них. Помимо решений кибербезопасности, «Лаборатория Касперского» предоставляет комитету сервис всестороннего анализа инцидентов и реагирования на них.

Результаты

Олимпийский комитет Катара отметил высочайшее качество поддержки, которую «Лаборатория Касперского» оказала организации на этапе внедрения решений и во время реагирования на инциденты, и теперь комитет рассматривает возможность перехода к модели управляемых услуг.

Партнерство с «Лабораторией Касперского» помогло Олимпийскому комитету Катара повысить уровень защищенности и развернуть более эффективные функции реагирования на эволюционирующие киберугрозы, число которых постоянно растет.

С решениями «Лаборатории Касперского» Олимпийский комитет Катара может гораздо быстрее обнаруживать угрозы и эффективно предотвращать атаки. Решения регулярно обновляются. Это значит, что поставщик непрерывно отслеживает новые угрозы и оперативно развертывает меры борьбы с ними. Продукты «Лаборатории Касперского» отразили множество атак, которые наши прежние решения не смогли бы даже идентифицировать, а интеграция с SIEM-системой повысила качество обнаружения угроз. Теперь у специалистов SOC есть полный набор инструментов для нейтрализации любой атаки. Они интуитивно понятны, просты в использовании и освоении. Наши команды стали продуктивнее и могут сосредоточиться на приоритетных задачах, а не на постоянной борьбе с уже начавшимися атаками. Выбранные решения легко масштабируются, и в ближайшие годы мы воспользуемся этой возможностью.

Рашид Аль Нахлави

Консультант по IT-безопасности, Олимпийский комитет Катара

Kaspersky Anti Targeted Attack

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее