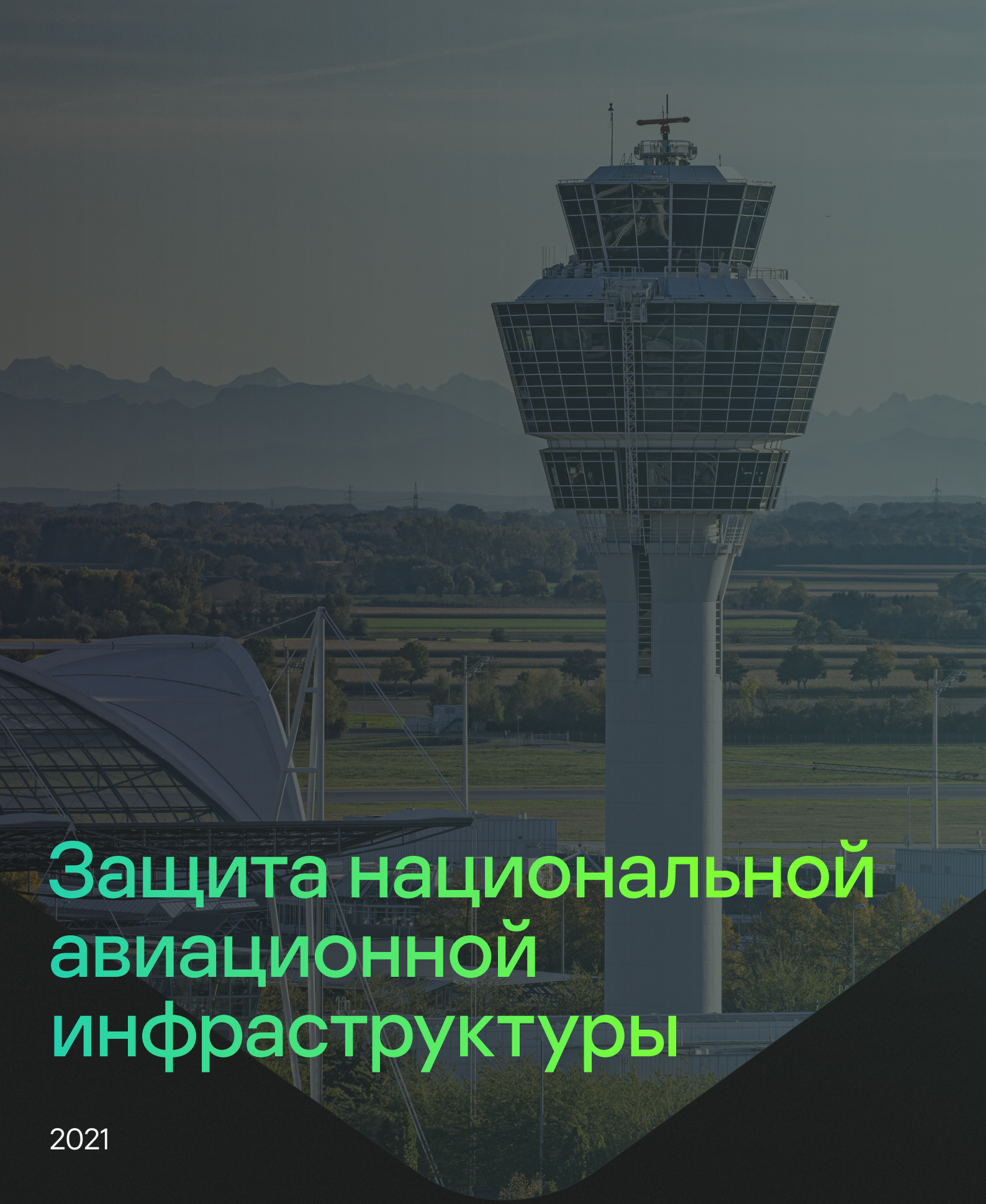

Защита национальной авиационной инфраструктуры

2021

kaspersky активируй будущее

1992
год основания

38 000
сотрудников

300%
прирост менее чем за 30 лет

≈ 50 млн
миллионов пассажиров в год

О клиенте

Аэропортом Мюнхена ежегодно пользуются почти 50 млн пассажиров. Он первым получил престижный пятизвездочный рейтинг компании Skytrax. Ежегодно более 90 авиакомпаний выполняют рейсы из Мюнхена в 210 пунктов назначения, расположенных в 63 странах.

Этот авиатранспортный узел находится всего в 30 минутах езды от столицы Баварии и обеспечивает работой около 38 000 человек, которые трудятся на более чем 500 предприятиях самого разного профиля, на территории хаба есть даже собственная пивоварня!

- Мюнхен, Германия
- Использует сервисы Kaspersky Threat Intelligence

Надежное партнерство

Комплекс сервисов информирования об угрозах Kaspersky Threat Intelligence основанный на данных киберразведки, обеспечивает проактивный подход к безопасности, помогая аэропорту Мюнхена предупреждать кибератаки.

Вызовы

Для такого крупного аэропорта, представляющего собой сложный конгломерат разных организаций и играющего критически важную роль в авиасообщении страны, надежная защита комплексной IT-инфраструктуры является приоритетом. Для обеспечения бесперебойных и безопасных авиаперевозок клиентам и авиакомпаниям, администрации аэропорта, предприятиям розничной торговли, службам экстренной помощи, а также другим вспомогательным организациям требуются актуальные данные и IT-системы, работающие без сбоев.

Аэропорт Мюнхена — крупный транспортный хаб, который занимает площадь более 15 квадратных километров, не уступая размером небольшому городку. Известность и экономическая значимость аэропортов делают их очевидными мишенями для киберпреступников, которые стремятся нарушить работу воздушного транспорта, украсть данные или получить деньги, проводя атаки на IT-системы организаций или отдельных сотрудников. Понимая привлекательность такого крупного объекта для злоумышленников и его критическую важность для региона, руководитель службы IT-безопасности аэропорта Марк Линдике и его команда постоянно ищут новые способы укрепления киберзащиты.

«Для нас особенно важно получать как можно больше данных о глобальных киберугрозах, чтобы мы могли действовать на упреждение, защищая тысячи людей в аэропорту, которые полагаются на наши IT-системы. Для этого нам нужен доступ к наиболее свежей и качественной информации и аналитическим данным из самых надежных источников».

Kaspersky
Threat Intelligence

Преимущества Kaspersky Threat Intelligence

- Актуальные данные о новых угрозах и уязвимостях, позволяя действовать на опережение
- Информация в реальном времени о возникающих угрозах и индикаторах компрометации
- Усилениесуществующие средства защиты, повышение эффективности обнаружения и предотвращения сложных атак
- Целостное представление о цифровых активах и выявляет наиболее уязвимые цели для атак

Решение «Лаборатории Касперского»

В 2018 году между Марком Линдике и немецким подразделением «Лаборатории Касперского» начались переговоры, целью которых было понять, какие сервисы кибербезопасности помогут укрепить защиту систем аэропорта. В результате было запущено тестирование портфолио Kaspersky Threat Intelligence, которое позволило Марку Линдике и его команде в полной мере оценить производительность, удобство и экономическую эффективность этих решений.

Сервис аналитических отчетов об APT-угрозах

Сервис отчетов об APT-угрозах (от англ. advanced persistent threat — комплексная целевая угроза) предоставляет уникальный постоянный доступ к текущим расследованиям и аналитической информации «Лаборатории Касперского», раскрывая тактики, техники и процедуры, используемые киберпреступниками. Поскольку APT-угрозы относятся к наиболее опасным и сложным категориям кибератак, в отчетах «Лаборатории Касперского» подробно описывается, как работает каждая атака, откуда она исходит и на какой тип инфраструктур она, скорее всего, будет нацелена.

Индикаторы компрометации

Ключевые фрагменты криминалистических данных, обнаруженных экспертами «Лаборатории Касперского», — предоставляют таким организациям, как аэропорт Мюнхена, оперативную информацию, позволяющую укреплять сетевые экраны и другие средства обнаружения вторжений.

Марк Линдике и его команда также протестировали и приобрели доступ к поисковому порталу Kaspersky Threat Lookup.
Это решение обеспечивает глобальную прозрачность ландшафта угроз и их взаимосвязей благодаря возможности выполнять поиск в режиме реального времени по огромным объемам данных, которые собирает, классифицирует и анализирует «Лаборатория Касперского». Пользователь сервиса может отправить подозрительные файлы или объекты на анализ и получить всю необходимую информацию о них, которую «Лаборатория Касперского» собирала десятилетиями.

Наконец, аэропорт Мюнхена подписался на ряд потоков данных об угрозах Kaspersky Threat Data Feeds, с помощью которых «Лаборатория Касперского» круглосуточно каждые 10 минут предоставляет клиентам информацию о новейших вредоносных программах и другой подозрительной активности.

Сервисы Kaspersky Threat Intelligence играют очень важную роль, помогая нам защищать от кибератак всех, кто работает в аэропорту Мюнхена.

Эти сервисы помогают нам получить более полное представление о мировом ландшафте угроз и о том, какие из них могут быть актуальными для аэропорта Мюнхена.

Kaspersky Threat Intelligence Portal предоставляет простой и удобный доступ к потокам данных об угрозах, отчетам об APT-угрозах и поисковому порталу Kaspersky Threat Lookup, а также удобные программный интерфейс и инструменты для внедрения автоматизированной обработки данных в наши существующие защитные решения.

Марк Линдике (Marc Lindike),

Руководитель службы IT-безопасности, аэропорт Мюнхена

Мировой ландшафт угроз

За комплексом сервисов стоит глобальный центр исследований и анализа угроз (GReAT) «Лаборатории Касперского», заслуживший мировое признание благодаря вкладу в расследование громких киберпреступных кампаний.

GReAT помогает противодействовать даже очень изощренным атакам, постоянно предоставляя отчеты о тактиках, техниках и процедурах, используемых злоумышленниками в масштабных межотраслевых кампаниях кибершпионажа.

Эксперты «Лаборатории Касперского» — самые опытные охотники за APT-угрозами. Они немедленно оповещают клиентов о любых изменениях в тактике киберпреступных группировок. По итогам пробного периода мюнхенский аэропорт заключил долгосрочный контракт с «Лабораторией Касперского» на предоставление аналитических отчетов об угрозах для защиты всей IT-инфраструктуры руководства аэропорта, авиакомпаний, предприятий розничной торговли и других организаций, расположенных на территории воздушной гавани.

Защита

Поддержание стабильной и надёжной работы ключевой международной инфраструктуры

Эффективность

Центр GReAT признан одним из лучших в мире

Управление

Удобный доступ к данным и аналитике через Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее