positive technologies

Пулково

ИСТОРИЯ УСПЕХА

КАК PT ISIM ОБЕСПЕЧИВАЕТ КИБЕРУСТОЙЧИВОСТЬ ИНЖЕНЕРНЫХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ АЭРОПОРТА ПУЛКОВО

PT ISIM

О КОМПАНИИ

Пулково — один из крупнейших и динамично развивающихся авиатранспортных узлов России, который функционирует с 1932 года.

Сейчас в аэропорту работает около

4000
сотрудников

Аэропорт обеспечивает пассажиропоток

в 20+ млн
человек в год

Инфраструктура аэропорта включает 88 стоек регистрации, 107 кабин транспортного контроля, 16 телетрапов, 110 стоянок воздушного контроля, 6 багажных лент, 65 лифтов, 31 эскалатор и 37 выходов на посадку.

ПРЕДПОСЫЛКИ ПРОЕКТА И ПРОБЛЕМАТИКА

Аэропорт Пулково, являющийся объектом критической информационной инфраструктуры (КИИ), с 2022 года создавал комплексную систему информационной безопасности полностью на российских решениях. Масштабный проект предусматривал внедрение системы класса NTA[1] для мониторинга аномалий в промышленном трафике АСУ ТП[2]. До этого, несмотря на сегментацию, взаимодействие элементов индустриальной инфраструктуры между собой и аномалии в трафике не отслеживались.

Главный вопрос оставался открытым: как получить полную видимость промышленной инфраструктуры и контроль над ней, обеспечив бесперебойную работу критических систем в условиях высокоинтенсивных кибератак?

1. Класс решений по кибербезопасности, предназначенный для мониторинга, глубокого анализа и обнаружения аномалий в сетевом трафике.
2. Автоматизированная система управления технологическим процессом.

КАК ВЫБИРАЛИ РЕШЕНИЕ

Служба ИБ Пулково искала продукт отечественной разработки, который бы выполнял широкий перечень мер защиты АСУ ТП в соответствии с требованиями регуляторов (Федеральный закон № 187-ФЗ, приказы ФСТЭК № 239 и 31) и имел сертификат ФСТЭК.

Кроме того, нужно было решение, которое обеспечит безопасность в соответствии с положениями национальных стандартов и законодательства в области кибербезопасности промышленных сетей (ГОСТ Р МЭК 62443), безопасности потенциально опасных и промышленных объектов (Федеральные законы 384-ФЗ, 116-ФЗ, ГОСТ Р 56875), антитеррористической защищенности (СП 132.13330.2011).

В числе главных критериев выделяли высокую точность результатов и минимальное число ложных срабатываний в специфической индустриальной среде, а также удобство, легкость использования и интуитивно понятный интерфейс.

Изучив подходящие на рынке решения и проведя пилотные проекты с несколькими производителями, команда «Воздушных Ворот Северной Столицы» выбрала для масштабного внедрения систему обеспечения киберустойчивости PT ISIM[3] Positive Technologies.

Специалистов привлекло то, что продукт полностью отвечает требованиям по надежности, обладает высоким уровнем отказоустойчивости и поддерживает результативную работу в сложных производственных инфраструктурах. Система разбирает десятки общесетевых и отраслевых протоколов, определяет широкий спектр индустриального ПО и оборудования, легко интегрируется как со специализированными системами управления и безопасности, так и со сторонними средствами защиты.

Среди других преимуществ PT ISIM специалисты Пулково назвали простоту развертывания и настройки, не требующих специальных знаний и позволивших быстро запустить систему для получения реального результата защищенности.

«Прежде всего PT ISIM заинтересовал нас тем, что может максимально подстроиться под наши потребности, в том числе и будущие. Решение на его базе гибко масштабируется и экономично в плане аппаратного обеспечения»

Сергей Савченко,
начальник службы по обеспечению информационной безопасности
«Воздушных Ворот Северной Столицы»

КАК ЭТО РАБОТАЕТ

Сейчас сенсоры PT ISIM, каждый из которых в среднем обрабатывает около 10 млн событий в сутки, развернуты в 10 технологических сегментах. С их помощью контролируется электроснабжение, водоснабжение и водоотведение, а также другие системы аэропорта.

PT ISIM стал единой точкой мониторинга, которая собирает события ИБ со всех возможных источников в промышленной среде аэропорта — узконаправленного ПО и техники, автоматизированных рабочих мест и конечных точек, коммутаторов, контроллеров и средств защиты — передает их в SIEM-систему и незамедлительно уведомляет операторов об аномалиях.

РЕЗУЛЬТАТЫ ПРОЕКТА

Благодаря PT ISIM подразделение кибербезопасности аэропорта в режиме реального времени выявляет:

Запрещенные подключения из изолированного АСУ ТП сегмента вовне;

Узлы, ранее неизвестные командам ИТ и ИБ;

Неавторизованные соединения между узлами внутри технологической сети;

Нелегитимные сетевые подключения, например к SCADA[4]-серверу;

Попытки эксплуатации уязвимостей или передачу по сети вредоносного ПО;

Аномальное поведение сотрудников и подрядчиков;

Ошибки в конфигурациях отслеживаемых систем и факты нарушения правил безопасности;

Нецелевое использование ресурсов и другие подозрительные операции.

«При помощи PT ISIM сотрудники Пулково видят бóльшую часть индустриальной инфраструктуры как на ладони, понимают ее состав и цифровые коммуникации между элементами, выявляют неучтенные сетевые узлы и внутренних нарушителей, не влияя на технологические процессы»

Евгений Орлов,
руководитель направления ИБ промышленных систем Positive Technologies

Такой комплексный подход на базе продуктов Positive Technologies уже в течение трех лет обеспечивает киберустойчивость Пулково и дает топ-менеджменту уверенность, что их предприятию не будет причинен непоправимый ущерб.

4 Программно-аппаратный комплекс для диспетчерского управления и сбора данных.