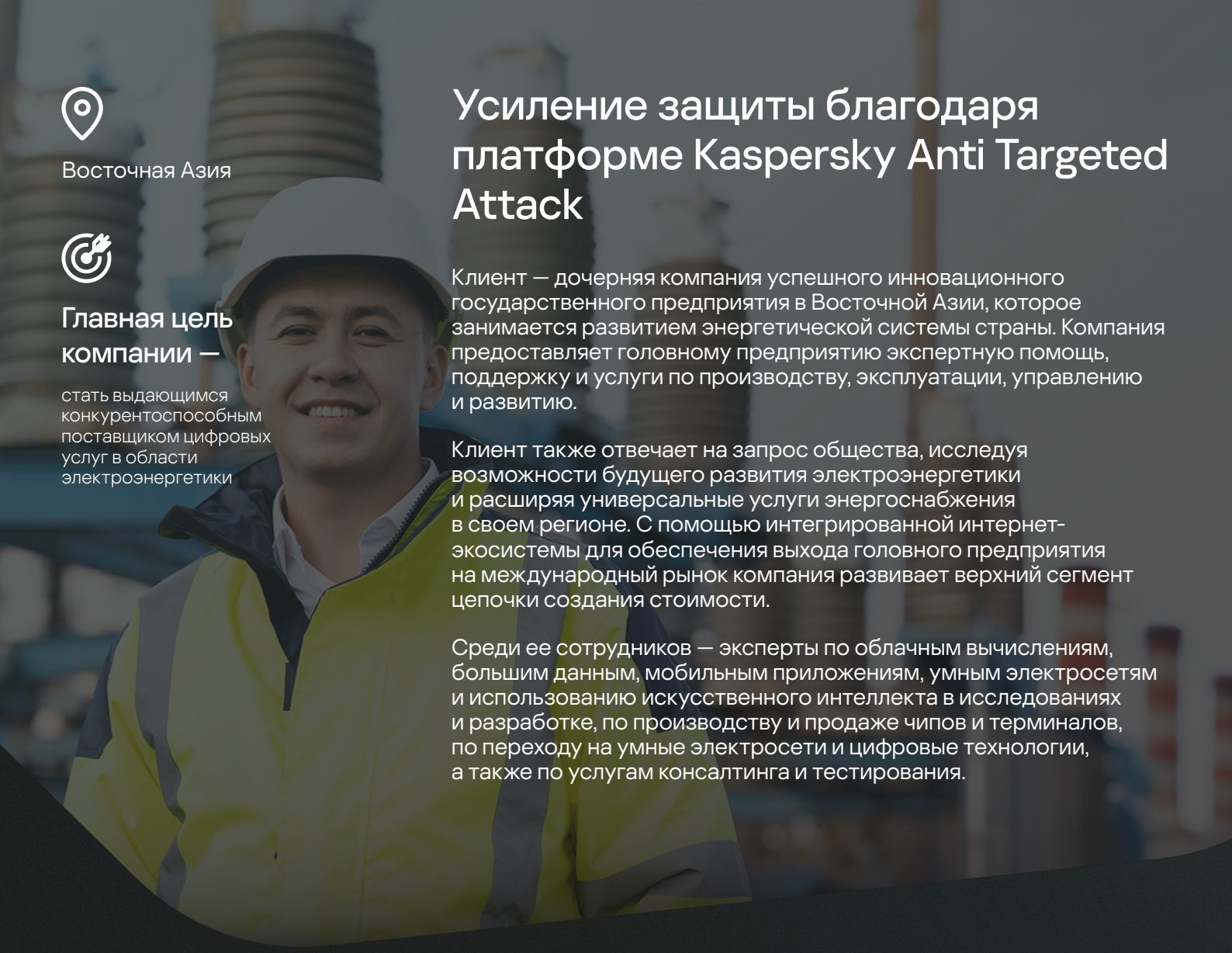
Крупная энергетическая компания в Восточной Азии

2022

kaspersky активируй будущее



Восточная Азия

Главная цель компании —

стать выдающимся конкурентоспособным поставщиком цифровых услуг в области электроэнергетики

Усиление защиты благодаря платформе Kaspersky Anti Targeted Attack

Клиент — дочерняя компания успешного инновационного государственного предприятия в Восточной Азии, которое занимается развитием энергетической системы страны. Компания предоставляет головному предприятию экспертную помощь, поддержку и услуги по производству, эксплуатации, управлению и развитию.

Клиент также отвечает на запрос общества, исследуя возможности будущего развития электроэнергетики и расширяя универсальные услуги энергоснабжения в своем регионе. С помощью интегрированной интернет-экосистемы для обеспечения выхода головного предприятия на международный рынок компания развивает верхний сегмент цепочки создания стоимости.

Среди ее сотрудников — эксперты по облачным вычислениям, большим данным, мобильным приложениям, умным электросетям и использованию искусственного интеллекта в исследованиях и разработке, по производству и продаже чипов и терминалов, по переходу на умные электросети и цифровые технологии, а также по услугам консалтинга и тестирования.

Потребность в усилении защиты

Научно-исследовательский институт одного из новаторов в области энергетики обратился к «Лаборатории Касперского» за помощью в укреплении и стандартизации своей системы сетевой безопасности.

Предыстория

После пандемии количество киберинцидентов, затрагивающих инфраструктуры АСУ ТП, резко возросло: 50% организаций сообщили об увеличении числа инцидентов по сравнению с 2019 годом. При этом общий ущерб от кибератак на промышленную инфраструктуру на 59% выше среднего ущерба, который несут крупные компании в других областях.

В условиях очень специфичного и постоянно меняющегося ландшафта угроз для клиента стала очевидной необходимость усиления и стандартизации существующей системы кибербезопасности.

Компания, которая уже использовала Kaspersky Hybrid Cloud Security, проанализировала ряд международных поставщиков и остановила свой выбор на «Лаборатории Касперского», в частности на платформе Kaspersky Anti Targeted Attack и ее песочнице.

Нас привлекла надежная технология обнаружения угроз и низкое число ложноположительных срабатываний, — пояснил официальный представитель компании. — Мы искали международно признанного поставщика сервисов с большим опытом долгосрочного сотрудничества. Партнера, который вместе с нами выстроит хорошо организованную и эффективную защиту для нашей системы мониторинга энергоснабжения.

Официальный представитель компании

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response Expert

Путь к надежности

Платформа Kaspersky Anti Targeted Attack базируется на Kaspersky Endpoint Detection and Response Expert и работает как расширенное EDR-решение. Она предлагает комплексную защиту от сложных и целевых угроз с опорой на всесторонние аналитические данные и матрицу MITRE ATT&CK.

Автоматизация сбора и анализа данных, а также возможность расследования инцидентов и реагирования на них из единой веб-консоли — преимущества, позволяющие клиенту увеличить скорость обработки инцидентов и продуктивность ИБ-специалистов. Когда все потенциальные точки входа угроз оказываются под их контролем, у них появляется возможность для обзора всей инфраструктуры: сети, электронной почты, настольных компьютеров и ноутбуков, серверов и виртуальных машин.

Исследователи кибербезопасности, работающие в Центре мониторинга и реагирования (SOC) клиента, особенно высоко ценят появившуюся у них возможность автоматически выявлять и анализировать подозрительные файлы в системе регулировки электроэнергии. Помимо прочего, решение легко интегрируется в различные системы безопасности.

Преимущества решения

С самого начала внедрения клиент остается более чем доволен решением «Лаборатории Касперского». Специалисты компании в особенности отмечают расширенные функции и высокую точность решения, а также эффективность песочницы при обнаружении вредоносных ссылок. Платформа обнаруживает вредоносное ПО, скрытое в ссылках, и предотвращает его проникновение во внутреннюю сеть, где оно может причинить серьезный ущерб.

Среди других ее преимуществ — импорт трафика, интеграция через API, автоматический импорт подозрительных файлов и анализ вредоносного ПО. Широкий набор функций помогает увеличить эффективность защиты, при этом сэкономив время и ресурсы клиента.

Традиционная защита не позволяет справиться со сложными и целевыми угрозами, поэтому необходим многоуровневый подход с использованием технологий расширенного обнаружения. Платформа Kaspersky Anti Targeted Attack задействует как базовые методы (например, уникальный набор правил IDS для анализа трафика на основе исследований APT-атак и данные о глобальном ландшафте угроз), так и передовые технологии машинного обучения и искусственного интеллекта для определения поведения, типичного для той или иной организации.

А интегрированная аналитика угроз, поступающая в режиме реального времени, и настраиваемые инструменты обнаружения помогают выявлять даже многовекторные атаки, не использующие вредоносное ПО.

Высокая точность и эффективность обнаружения угроз, продвинутые технологии «Лаборатории Касперского» и гибкость ее решения с поддержкой API-интерфейсов и сторонних интеграций — все это действительно выделяет компанию среди конкурентов, — говорит официальный представитель клиента. — Мы рекомендуем «Лабораторию Касперского» любым организациям, в особенности работающим в области электроэнергетики. С ее решениями не сравнятся никакие другие.

Официальный представитель компании

Kaspersky Anti Targeted Attack

Подробнее

Kaspersky Endpoint Detection and Response Expert

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее