Проактивное принятие решений для эксперта по киберразведке

2025

kaspersky активируй будущее

>10 000

злоумышленников выявлено с помощью защитного решения «Лаборатории Касперского»

0

инцидентов безопасности

> 1 000 млн

записей данных телеметрии, нуждающихся в защите

О клиенте

Мониторинг рисков — необходимая часть работы этой американской компании, специализирующейся на анализе данных о киберугрозах. Ее клиенты должны быть абсолютно уверены в том, что компания в состоянии непрерывно обрабатывать данные более чем из 650 000 источников информации.

- Пенсильвания, США
- Использует Kaspersky APT Intelligence Reporting, Threat Data Feeds и Kaspersky Threat Infrastructure Tracking.
- Глубина обзора, которая дает полное понимание ландшафта угроз, крайне важна для кибербезопасности компании.

Лаборатория Касперского обеспечивает непревзойденный уровень защиты для компании — лидера рынка и эксперта в области анализа угроз. Эта компания и ее клиенты не дают нам права на ошибку. Они ожидают получить — и получают — только самое лучшее.

Вызовы

Эта компания-эксперт в сфере кибербезопасности уже более пяти лет пользуется решением «Лаборатории Касперского» для защиты нескольких тысяч конечных устройств от постоянно растущего числа угроз, вирусов и атак программ-вымогателей.

В своей операционной деятельности компания сталкивается с уникальными проблемами и задачами. Ей необходимо постоянно быть в курсе новейших угроз и тенденций в сфере кибербезопасности и адаптировать свои защитные меры к динамично меняющемуся ландшафту угроз.

Чтобы обеспечивать проактивную защиту своих операций, компании нужна своевременная и точная информация о новейших угрозах и уязвимостях по всему миру. Поскольку в мире постоянно появляются новые киберугрозы, направленные на широкий спектр платформ и операционных систем, компании необходим партнер, способный обеспечить надежный и универсальный подход к кросс-платформенной безопасности.

Требования, предъявляемые компанией к кибербезопасности, предполагают проведение глубокого технического анализа для понимания тактик, техник и процедур злоумышленников и особенностей вредоносного ПО. Поэтому организация искала партнера, облдающего необходимой экспертизой для проведения тщательного технически сложного анализа инцидентов и уязвимостей.

Необходимо было решение, которое обеспечило бы полный обзор всех конечных точек в корпоративной сети и дало возможность ИБ-аналитикам компании обнаруживать, расследовать и реагировать на угрозы в режиме реального времени. Кроме того, это решение должно было учитывать растущее количество конечных точек и сложную IT-структуру компании.

Решение

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence предоставляет доступ к широкому спектру данных, собранных нашими аналитиками и исследователями со всего мира, чтобы помочь вашей организации эффективно противостоять современным киберугрозам. Тактические, операционные и стратегические данные о динамично меняющемся ландшафте угроз позволят вам оставаться защищенным.

Для решения поставленных задач эксперты «Лаборатории Касперского» предложили комплекс сервисов Kaspersky Threat Intelligence, который на основе аналитической информации из разных источников, потоков данных об угрозах и данных собственных расследований компании формирует комплексную картину глобального ландшафта угроз. Предложенное решение включает в себя подписку на аналитические отчеты Kaspersky APT Intelligence Reporting, потоки данных об угрозах Kaspersky Threat Data Feeds и сервис Kaspersky Threat Infrastructure Tracking.

Отчеты Kaspersky APT Intelligence Reporting отслеживают даже самые технически сложные целевые атаки и другую активность киберпреступников и предоставляют компании актуальную информацию о масштабных кампаниях кибершпионажа, сформированную с учетом ее потребностей.

В дополнение к этому постоянно обновляемые потоки данных об угрозах Kaspersky Threat Data Feeds позволяют в автоматическом режиме обнаруживать вредоносную активность в корпоративной сети компании.

Решение развернуто централизованно в штаб-квартире организации в Пенсильвании, но при этом оно охватывает более 650 000 источников информации и миллиарды записей данных телеметрии.

Kaspersky APT Intelligence Reporting

Kaspersky APT Intelligence Reporting

Ключевые особенности

- Актуальные сведения о наиболее опасных угрозах
- Доступ к результатам конфиденциальных расследований
- Актуальные сведения для технических специалистов и директоров ИБ

Благодаря отчетам Kaspersky APT Intelligence Reporting компания имеет доступ к эксклюзивным аналитическим данным об APT-угрозах со стороны более 200 киберпреступных группировок из 85 стран, что позволяет ей эффективно выявлять наиболее сложные и опасные целевые атаки, кампании кибершпионажа, вредоносное ПО, шифровальщики и другую активность киберпреступников.

Эксперты «Лаборатории Касперского» отслеживают деятельность 1100 с лишним киберпреступных групп и операций. Подробное описание более 200 из них размещено на Kaspersky Threat Intelligence Portal.

Только небольшой процент расследований «Лаборатории Касперского» доступен широкой публике, но действующие клиенты, такие как эта компания-эксперт в области аналитики угроз, имеют доступ ко всей информации. Что помогает им заблаговременно развернуть эффективные инструменты для обнаружения угроз и снижения рисков, чтобы противостоять атакам со стороны этих APT-группировок.

Каждый отчет содержит описание вредоносной кампании с указанием затронутых отраслей и регионов, вероятных целей атаки и стоящих за ней злоумышленников, а так же подробный технический анализ и список соответствующих IoC и YARA-правил.

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Ключевые особенности

- Уникальные источники
- Анализ данных
- Качество данных
- Скорость обновления
- Простота интеграции
- Данные об угрозах для промышленных предприятий

Поступающие в компанию аналитические данные об угрозах собираются из множества разнообразных надежных источников, таких как сеть Kaspersky Security Network (KSN), поисковые вэб-краулеры «Лаборатории Касперского», сервис мониторинга ботнет-угроз (круглосуточное слежение за активностью ботнетов и их мишенями) и спам-ловушки.

«Лаборатория Касперского» получает данные от исследовательских групп, из даркнета, от своих партнеров и из собранных за 28 лет архивов информации о вредоносных объектах.

Эксперты тщательно проверяют собранную информацию и в режиме реального времени уточняют с помощью различных методов предварительной обработки, таких как анализ на основе статистических критериев, анализ с помощью Kaspersky Threat Analysis «Лаборатории Касперского» («песочницы», эвристических движков, инструментов сходства, профилирования поведения и т.д.), проверка аналитиками и проверка по «разрешающему списку». Это означает, что потоки данных Kaspersky Threat Data Feeds содержат тщательно проверенную информацию об индикаторах угроз, полученную со всего мира в реальном времени.

Kaspersky Threat Infrastructure Tracking

Kaspersky Threat Infrastructu Tracking

Ключевые особенности

- Понимание уровня безопасности в стране в соответствии с распространением таких инфраструктур
- Выявление новых активных инфраструктур, используемых злоумышленниками в конкретной стране
- Определение, кто именно из известных злоумышленников стоит за конкретными атаками

Сервис Kaspersky Threat Infrastructure Tracking выявляет IP-адреса инфраструктуры, являющейся источником продвинутых угроз. Он помогает аналитикам безопасности, работающим в группах экстренного реагирования на инциденты (CERT), центрах мониторинга и реагирования (SOC) и агентствах национальной безопасности, отслеживать развертывание новых вредоносных программ, а затем принимать меры, необходимые для минимизации ущерба от текущих и предстоящих атак.

Сервис обновляется ежедневно с учетом новых результатов, полученных Глобальным центром исследований и анализа угроз «Лаборатории Касперского» (GReAT), который обладает значительным опытом успешного обнаружения APT-кампаний по всему миру.

Для каждого IP-адреса указывается имя APT-группировки, кампании или вредоносного ПО, с которым он связан, поставщик услуг доступа в интернет и автономная система, информация о хостинге связанных IP-адресов, а также даты первого и последнего обнаружения.

Список IP-адресов можно скачать в машиночитаемом формате, а затем загрузить его в имеющиеся защитные решения для автоматизации обнаружения угроз.

Главные достоинства «Лаборатории Касперского» — это глобальное видение угроз и наличие команды высококвалифицированных технических аналитиков. Ее обширная сеть сенсоров и других источников данных позволяет отслеживать и анализировать угрозы в мировом масштабе. Такая широта обзора позволяет выявлять новейшие угрозы, тенденции и уязвимости по всему миру, помогая таким клиентам, как мы, оставаться всегда на ход впереди постоянно развивающихся киберугроз.

Мы уверены в том, что получаем качественно разработанные продукты и актуальные аналитические данные об угрозах. Дополнительное преимущество для нашей компании — возможность прямых контактов с опытнейшими исследователями при необходимости более глубокого погружения в тему.

Директор отдела технических исследований компании

Результаты

Предложенное «Лабораторией Касперского» решение показывает настолько высокий уровень видимости угроз, который превосходит все ожидания компании. Оно предоставляет исчерпывающую информацию о самом широком спектре киберугроз — от обычных атак вредоносного ПО до технически сложных целевых атак.

Такая глубина обзора дает компании полное понимание ландшафта угроз, что крайне важно для обеспечения ее кибербезопасности. Подробный технический анализ, содержащийся в отчетах «Лаборатории Касперского», — это ключевой проверенный временем инструмент для выполнения приоритетных требований наших клиентов в области аналитики данных об угрозах.

Тщательно изучая данные сетевого трафика и дополняя их информацией, полученной из сети Kaspersky Security Network, аналитики могут выявлять закономерности и аномалии, указывающие на потенциальные угрозы или вредоносную активность. Полученные данные преобразуются в сигнатуры, которые затем устанавливаются на сетевые сенсоры для автоматизации процессов обнаружения и оповещения об угрозах. Такой подход не только повышает скорость обнаружения угроз, но позволяет обеспечить активный подход к защите критически важных систем и данных нашего заказчика. Кроме того, интеграция в систему общих сигнатур YARA является важнейшим фактором при поиске соответствующих им артефактов на серверах компании. В результате появляется возможность идентификации бинарных файлов, имеющих общий код с представляющими интерес артефактами. Сочетание анализа сетевых протоколов и развертывания сигнатур YARA на серверах формирует комплексный подход к обнаружению и устранению угроз.

Полученные в результате этих процессов данные телеметрии представляют собой бесценные сведения, позволяющие выявлять новые тактики, техники и процедуры киберпреступников, что было бы невозможно без использования решений «Лаборатории Касперского». Это, в свою очередь, позволяет постоянно уточнять и дополнять уже имеющиеся данные кибермразведки, что повышает общий уровень кибербезопасности компании и ее способность противостоять любым новым угрозам, нацеленным на ее собственных клиентов.

Заказчик утверждает, что, по его опыту, важнейшее достоинство решений «Лаборатории Касперского» — способность предоставлять своевременную и имеющую практическое применение аналитическую информацию. Это значит, что компания в режиме реального времени получает сведения о потенциальных угрозах и уязвимостях, а также четкие практические рекомендации по их устранению. И хотя разработка безупречного продукта, полностью готового для распространения, может занимать некоторое время, представители компании отмечают, что «Лаборатория Касперского» публикует отчеты аналитиков, которые достаточно информативны, актуальны и позволяют быстро получать необходимую информацию.

Решение, предложенное «Лабораторией Касперского», демонстрирует степень видимости угроз, которая превосходит все наши ожидания. Оно позволяет получить исчерпывающую информацию о широком спектре киберугроз.

Директор по исследованиям компании

«Лаборатория Касперского» завоевала репутацию надежного партнера в сфере кибербезопасности благодаря своей прозрачности, техническому превосходству и бескомпромиссному подходу к исследованию угроз.

Клиент утверждает, что отчеты «Лаборатории Касперского» не просто содержат гипотезы аналитиков — они подкреплены надежными техническими и аналитическими данными, что является их неоспоримым преимуществом. «Самоотверженные усилия экспертов «Лаборатории Касперского» по исследованию угроз в любом регионе мира — свидетельство глобального подхода компании к вопросам кибербезопасности», — говорит директор по исследованиям компании.

В заключение компания отмечает, что комплексный анализ угроз, который обеспечивают решения «Лаборатории Касперского», играет ключевую роль в поддержании надежной системы

Безопасность

Предоставление аналитических данных без права на ошибку

Обнаружение

Решения «Лаборатории Касперского» позволяют повышать процент обнаруженных угроз и сокращают время реагирования на них

Уверенность

Качественно разработанные продукты и актуальные аналитические данные об угрозах

Соблюдение требований

Соответствие региональным, национальным и международным нормам

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее

Новости о киберугрозах:
www.securelist.ru

Новости IT-безопасности:
business.kaspersky.ru

Кибербезопасность для крупных предприятий:
kaspersky.ru/enterprise