Kaspersky®
Anti Targeted
Attack

Специализированная платформа для противодействия комплексным угрозам на уровне сети

В эпоху цифровой трансформации корпоративная служба информационной безопасности должна стать ключевым звеном цифровой бизнес-стратегии организаций. Построение надежной системы защиты корпоративной инфраструктуры от передовых угроз и целевых атак, а также оперативное выявление инцидентов, уменьшение объема ручных операций, оптимизация трудозатрат и повышение эффективности работы ИБ-служб и команд SOC позволяют обеспечить устойчивое развитие крупного бизнеса.

Преимущества платформы Kaspersky Anti Targeted Attack

- Сокращение рисков информационной безопасности;
- Повышение продуктивности и качества работы сотрудников ИТ и ИБ департаментов;
- Оптимизация трудозатрат высококвалифицированных кадров;
- Сокращение количества рутинных ручных операций;
- Увеличение количества обрабатываемых инцидентов без дополнительных трудозатрат;
- Сбор, хранение и предоставление информации об инцидентах ИБ в рамках требований внутреннего и внешнего регулирования и отраслевого законодательства.

Сертифицированное решение

Платформа Kaspersky Anti Targeted Attack внесена в единый реестр российского ПО, соответствует требованиям ФСБ к средствам обнаружения компьютерных атак класса В и имеет сертификат ФСТЭК России на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) — по 4 уровню контроля и технических условий.

Минимизация последствий от целевых атак путем оперативного выявления направленных действий злоумышленников

Kaspersky Anti Targeted Attack позволяет своевременно обнаруживать многоступенчатые действия злоумышленников в сети и противодействовать им на всех этапах за счет:

- наглядной визуализации и прозрачности корпоративной инфраструктуры;
- автоматизации процесса сбора и хранения информации и цифровых улик;
- сформированного процесса анализа инцидентов с помощью передовых технологий на базе машинного обучения;
- сокращения количества задач по ручному обнаружению угроз;
- сопоставления данных, получаемых в режиме реального времени, с ретроспективными данными и вердиктами от механизмов детектирования;
- сведения всех полученных данных в единый ИБ инцидент для оперативного расследования и реагирования;
- автоматизации задач по расследованию инцидентов и, как следствие, оптимизации расходования ресурсов служб ИТ, ИБ и команды SOC.

Независимая международная оценка

Качество защитных технологий, предлагаемых «Лабораторией Касперского», подтверждено результатами многочисленных испытаний. В ходе независимых тестов Advanced Threat Defense за 2017 и 2018 гг., проводимых международной компанией ICSA Labs, платформа Kaspersky Anti Targeted Attack показала 100% результат обнаружения угроз, не допустив ни одного ложного срабатывания.

По результатам сравнительного анализа рынка решений для защиты от APT-угроз, проводимого исследовательской компанией Radicati Group в 2018 г., решение Kaspersky Anti Targeted Attack продолжает занимать ведущую позицию в категории новаторов, постепенно улучшая свое положение по сравнению с предыдущими годами, что дает основание предполагать дальнейший переход решения в категорию лидеров рынка.

Следование региональному и международному законодательству

Платформа Kaspersky Anti Targeted Attack помогает организациям соответствовать стандартам банковской отрасли, PCI DSS, а также нормативным требованиям GDPR и ориентирована на содействие ФСБ в установлении причин и условий возникновения компьютерных инцидентов с учетом требований российского законодательства:

- Указа Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
- Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Ключевые компоненты платформы Kaspersky Anti Targeted Attack

Динамический анализ и эмуляция угроз

Высокопроизводительная песочница позволяет запускать подозрительные объекты в изолированной среде и осуществлять их многоуровневый анализ с использованием виртуальных машин с разными операционными системами. Данный компонент эффективно противодействует современным методам обхода обнаружения и осуществляет мониторинг взаимодействий вредоносных объектов с интернет-ресурсами без допуска этих объектов в реальную инфраструктуру. Данный подход дает возможность детально исследовать поведение анализируемых объектов и использовать полученную информацию в расследовании сложных инцидентов.

Передовые технологии обнаружения

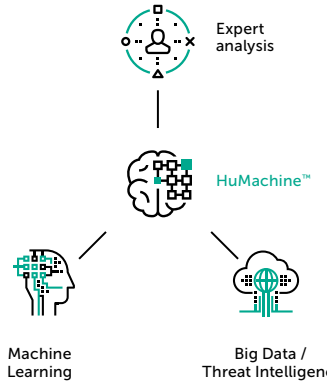
Набор передовых технологий обнаружения, в том числе антивирусный движок, анализ сетевых пакетов, проверка репутации URL и доменных имен, использование YARA-правил, анализ мобильных приложений на наличие вредоносной активности, проверка достоверности подписанных сертификатов и др., а также наглядное централизованное представление полученных от этих механизмов вердиктов позволяют своевременно выявлять действия злоумышленников.

Анализатор целевых атак

Динамическое машинное обучение, поведенческий анализ и автоматизированное сопоставление вердиктов, полученных от песочницы и механизмов обнаружения, с ретроспективными данными и данными, получаемыми в режиме реального времени, позволяют проводить детальную оценку сложности и состава киберугроз. Анализатор целевых атак способствует формированию максимально полного представления обо всех этапах спланированной злоумышленниками атаки. Собранная из набора разрозненных событий общая картина инцидента дает возможность оперативно реагировать на угрозы и значительно экономит трудозатраты служб ИБ.

Репутационная база угроз

Автоматизированный доступ к глобальной системе сбора сведений об угрозах Kaspersky Security Network позволяет оперативно получать данные о новых угрозах, что повышает вероятность раннего обнаружения атак, упрощает расследование инцидентов и реагирование на них. В организациях со строгими политиками конфиденциальности Kaspersky Anti Targeted Attack может работать в изолированном режиме, используя для получения сведений об угрозах запатентованную технологию Kaspersky Private Security Network. Это дает возможность использовать все преимущества глобальной репутационной базы «Лаборатории Касперского», не передавая какую-либо информацию за пределы организации и не нарушая требования ИТ-безопасности для корпоративных сетей с действующими политиками по изоляции от внешних ресурсов.



www.kaspersky.ru

#ИстиннаяБезопасность