Сервисы «Лаборатории Касперского»

kaspersky

Содержание

Сервисы «Лаборатории Касперского»

Ландшафт угроз постоянно меняется, и чтобы защититься от новейших и сложных угроз, необходимо обладать всей полнотой информации, развивать экспертизу специалистов, своевременно реагировать на инциденты и регулярно проводить анализ защищенности систем.

«Лаборатория Касперского» предлагает широкий набор сервисов, которые повышают уровень безопасности компаний и помогают встретить во всеоружии угрозы любого типа и масштаба.

Сервисы

Сервисы информирования помогают укреплять систему безопасности с помощью потоков данных об угрозах и специализированных отчетов.

Сервисы реагирования на инциденты помогают снизить ущерб и устранить уязвимые места в инфраструктуре.

Сервисы поиска угроз позволяют проводить проактивный поиск существующих атак и активно противодействовать новым угрозам.

Тренинги по кибербезопасности повышают экспертизу специалистов ИБ в актуальных областях.

Экспертные сервисы позволяют узнать об уровне защищенности систем и устранить уязвимости, которые могут использовать киберпреступники.

Лидирующие позиции в области кибербезопасности

Признание экспертов. «Лаборатория Касперского» шесть лет подряд входит в число «Лидеров» магического квадранта Gartner в области защиты конечных устройств.

Рекордное количество мест в независимых тестах. В 2017 году «Лаборатория Касперского» уверенно опередила других производителей, заняв первое место в 72-х из 86 тестов.

Более 130 OEM-производителей, включая Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent и др., используют наши технологии в своих продуктах и сервисах.

Опыт работы с организациями всех отраслей и уровней. Сервисами «Лаборатории Касперского» пользуются тысячи организаций, в том числе государственные структуры и крупные корпорации.

Сервисы информирования об угрозах

Наблюдать за постоянно эволюционирующими киберугрозами, анализировать их, вовремя реагировать на атаки и сводить к минимуму их последствия — процесс чрезвычайно трудоемкий. Сервисы информирования «Лаборатории Касперского» открывают доступ к информации об угрозах, полученной нашими аналитиками и исследователями. Эти данные помогут любой организации выстроить защиту от киберугроз.

«Лаборатория Касперского» обладает глубокими знаниями, богатым опытом и уникальными сведениями обо всех аспектах IT-безопасности. Вы можете использовать весь этот потенциал для повышения уровня IT-безопасности вашей компании.

Сервисы Kaspersky Threat Intelligence включают:

- Потоки данных об угрозах
- Аналитические отчеты об APT-атаках
- Кастомизированные отчеты
- Kaspersky Threat Lookup
- Мониторинг ботнет-угроз
- Мониторинг фишинговых угроз
- Отчеты об угрозах для финансовых организаций
- Kaspersky Cloud Sandbox

Сервисы «Лаборатории Касперского»

Сервисы информирования об угрозах

Потоки данных об угрозах
Аналитические отчеты об APT-атаках
Кастомизированные отчеты
Kaspersky Threat Lookup
Мониторинг ботнет-угроз
Мониторинг фишинговых угроз
Kaspersky Cloud Sandbox

Активный поиск угроз

Тренинги по кибербезопасности

Сервисы реагирования на инциденты

Сервисы анализа защищенности

Потоки данных об угрозах

В современной динамичной среде для эффективного отражения киберугроз специалистам по IT-безопасности нужно быть всегда на шаг впереди киберпреступников. Для этого им необходимо использовать самые актуальные аналитические данные.

«Лаборатория Касперского» предлагает клиентам постоянно обновляемые потоки данных об угрозах: используя их, специалисты по IT-безопасности могут своевременно узнавать о существующих угрозах и эффективнее противодействовать атакам.

Сценарии использования и преимущества для клиентов

Данные об угрозах, предоставляемые «Лабораторией Касперского»:

- дополняют решение SIEM данными о вредоносных URL-адресах – фишинговых URL-ссылках, а также URL-адресах командных серверов ботнетов;
- повышают эффективность таких решений для защиты сети, как сетевые экраны, системы обнаружения и предотвращения вторжений, системы SIEM, технологии противодействия APT-угрозам, «песочницы», UTM-устройств, с помощью постоянно обновляемых сведений об угрозах;
- расширяют возможности экспертного анализа, предоставляя службе безопасности ценную информацию об угрозах и возможность раскрыть структуру целевых атак;
- помогают в исследовательской работе – сведения о вредоносных URL-адресах и MD5-хэши вредоносных файлов вносят весомый вклад в проекты по исследованию угроз.
- помогают выявить индикаторы компрометации в логах или трафике пользователя, такие как командные центры, IP-адреса, вредоносные URL-адреса или файловые хеши, с детальной контекстной информацией. Это позволяет приоритизировать атаки, оптимально распределять затраты на IT и ресурсы и устранять в первую очередь те угрозы, которые наиболее опасны для вашей организации.

Описание потоков данных

- **Данные о репутации IP-адресов** – список IP-адресов с контекстной информацией, сообщающий о подозрительных и вредоносных узлах.
- **URL-адреса вредоносных и фишинговых ссылок** — список URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.
- **URL-адреса командных серверов ботнетов** – список URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.
- **URL-адреса командных серверов ботнетов для мобильных устройств** – список URL-адресов командных серверов ботнетов для мобильных устройств. Идентификация зараженных устройств, обменивающихся данными с командными серверами.
- **URL-адреса программ-вымогателей** – ссылки на страницы, где размещены программы-вымогатели (ransomware) или к которым обращаются такие программы.
- **Индикаторы заражения APT** – вредоносные домены, хосты, IP-адреса и файлы, используемые злоумышленниками для осуществления APT-атак.
- Хеши вредоносных объектов – список файловых хешей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы.
- **Хеши вредоносных объектов для мобильных устройств** – список файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства на базе Android и iOS.
- **Данные о троянцах P-SMS** – список хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS-сообщения, отвечать на них и удалять их.
- **Данные белых списков** – систематизированный список хэшей надежных файлов, доступный для использования решениями и сервисами третьих сторон.
- **Трансформы для Maltego** – набор трансформов для пользователей Maltego, которые позволяют сверять URL-адреса, хеши и IP-адреса с данными потоков «Лаборатории Касперского», включая определение категории объекта и полезную контекстную информацию.

Аналитические отчеты

Детальные аналитические отчеты «Лаборатории Касперского» — для повышения осведомленности о масштабных кампаниях кибершпионажа, а также об угрозах, направленных против конкретных организаций.

Информация из этих отчетов и предоставляемые «Лабораторией Касперского» инструменты помогут быстро реагировать на новые угрозы и уязвимости: заблокировать атаки с известных направлений, уменьшить ущерб от сложности атак и усовершенствовать стратегию безопасности.

Отчеты об угрозах класса APT

Новости об обнаружении угроз класса APT не всегда сообщаются сразу, а во многих случаях такая информация вообще не объявляется публично. Наши подробные отчеты позволят вам в числе первых получать эксклюзивную информацию об APT-угрозах.

Подписчики на такие отчеты* получают уникальный доступ к результатам расследования и техническим данным в различных форматах по каждой APT-угрозе сразу после появления этих данных. В 2016 году было подготовлено более 100 отчетов об APT-атаках

Отчеты «Лаборатории Касперского» — это:

- **Эксклюзивный доступ** к техническим описаниям новейших угроз уже в ходе расследования, до публичного объявления.
- **Непубличные данные об APT-угрозах.** Не обо всех масштабных угрозах сообщается публично. Некоторые угрозы так и остаются тайной из-за специфики своих жертв, особой конфиденциальности данных, самой природы устранения уязвимости или привлечения правоохранительных органов. Однако наши клиенты получают доступ к таким отчетам.
- **Подробные технические данные**, образцы и инструменты, в том числе расширенный список индикаторов компрометации (IoC), доступный в стандартных форматах (включая openIOC и STIX), а также доступ к нашим Yara-правилам.
- **Непрерывный мониторинг APT-кампаний.** Доступ к ценным аналитическим данным в ходе расследования (информация о распространении APT-угрозы, индикаторы заражения, инфраструктура командных центров).
- **Ретроспективный анализ.** В течение периода подписки предоставляется доступ ко всем ранее выпущенным закрытым отчетам.
- **Портал с аналитическими отчетами об APT-угрозах.** Все отчеты, включая информацию о последних индикаторах компрометации, наши клиенты могут найти на удобном портале.

*** Примечание об ограничении подписки**

Отчеты, предоставляемые данным сервисом, содержат конфиденциальную информацию, поэтому мы вынуждены ограничить подписку, предоставляя ее только доверенным правительственным, общественным и частным организациям.

Кастомизированные отчеты об угрозах

Отчеты об угроз, созданные специально для вашей организации.

Какие векторы атаки и какие сведения доступны злоумышленнику, который решит атаковать вашу компанию? Возможно, атака уже организована или начнется в ближайшем будущем?

Кастомизированные отчеты «Лаборатории Касперского» отвечают на эти и другие вопросы. Наши эксперты выстраивают полную картину текущей ситуации с угрозами, выявляют уязвимые места в вашей защите и обнаруживают признаки прошедших, текущих и планируемых атак.

В отчетах рассматриваются следующие вопросы:

- **Определение векторов угроз.** Выявление и анализ состояния критических компонентов вашей сети, доступных извне, включая банкоматы, системы видеонаблюдения, телекоммуникационное оборудование и другие виды систем, а также профили сотрудников в социальных сетях и личные учетные записи электронной почты. Любой из этих компонентов может стать целью для атаки.
- **Анализ вредоносных программ и выявление кибератак.** Выявление, мониторинг и анализ любых активных и неактивных образцов вредоносных программ, нацеленных на вашу организацию, текущей и зафиксированной ранее активности ботнетов, а также любой другой подозрительной сетевой активности.
- **Атаки на третьи стороны.** Выявление признаков угроз и активности ботнетов, направленных на ваших клиентов, партнеров и абонентов. Их зараженные системы могут стать источником последующей атаки на вашу компанию.
- **Утечка информации.** Ведя наблюдение за подпольными интернет-форумами и сообществами, мы можем обнаружить данные о планируемой на вашу компанию атаки, если злоумышленники обсуждают их, а также выявить нечистоплотных сотрудников, торгующих ценной информацией.

Kaspersky Cloud Sandbox

Современные целевые атаки невозможно устранить, используя только традиционные инструменты защиты. В статистических данных часто не хватает информации о недавно измененных вредоносных программах, чего не скажешь о технологии песочницы – это мощный инструмент, который позволяет исследовать исходные образцы файлов и выявлять подозрительные активности и связанные объекты для последующего анализа.

Песочница «Лаборатории Касперского» для облачных сред предлагает гибридный подход, сочетающий в себе несколько технологий. Благодаря Kaspersky Security Network и другим репутационным системам происходит сбор информации об угрозах, которая состоит из петабайтов статистических данных. В изолированной среде проводится поведенческий анализ и используются надежные методы блокировки обхода безопасности. Также песочница применяет технологии моделирования поведения человека, такие как автокликер, прокрутка документов и фиктивные процессы. В таких условиях выявить неизвестные угрозы становится гораздо проще.

Ключевые преимущества:

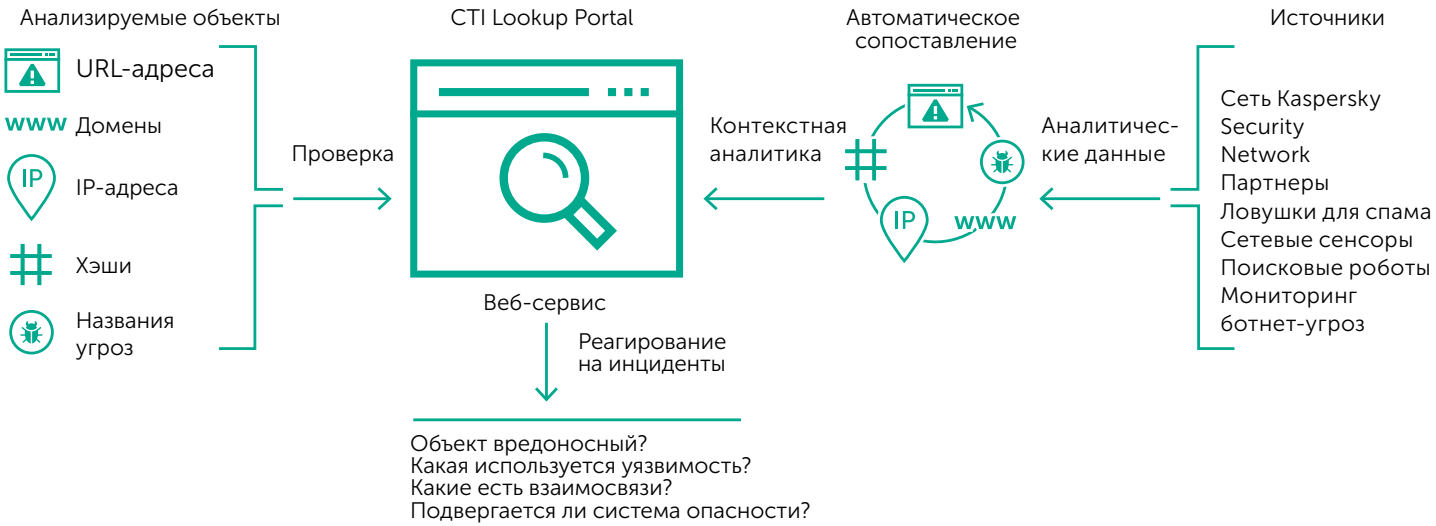
- Эффективное обнаружение целевых и сложных угроз, включая APT
- Рабочий процесс, позволяющий проводить действенное и всестороннее расследование инцидентов
- Масштабирование без необходимости покупать дорогостоящие устройства или беспокоиться о системных ресурсах
- Полная интеграция и автоматизация систем безопасности

Основные возможности

- Загрузка и запуск всех типов файлов, которые запускаются двойным нажатием кнопки мыши (включая DLL)
- Создание взаимных исключений (мьютексы)
- Изменение и создание ключей реестра
- Внешнее соединение с доменными именами и IP-адресами
- Запросы и ответы HTTP и DNS
- Создание процессов выполняемым файлов
- Создание, изменение и удаление файлов
- Дампы памяти процессов и сетевого трафика (PCAP)
- Создание снимков экрана
- Подробная информация об угрозах с контекстными рекомендациями для каждого выявленного индикатора компрометации
- Поддержка API на основе REST
- И многое другое

Kaspersky Threat Lookup

Kaspersky Threat Lookup – это платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях.Сервис предоставляет вашим специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред.Платформа собирает подробные актуальные сведения об угрозах: URL-адреса, домены, IP-адреса, контрольные суммы файлов, названия угроз, статистику и поведенческие данные, данные WHOIS/DNS и другие данные.Это обеспечивает глобальную видимость новых и возникающих угроз, помогает ускорить реагирование и повысить его эффективность.



Архитектура Kaspersky Threat Lookup

Мониторинг ботнет-угроз

Экспертный сервис мониторинга и уведомления об обнаружении ботнетов, угрожающих вашим клиентам и репутации.

Сценарии использования и преимущества

- Проактивные уведомления о ботнет-угрозах, нацеленных на ваших онлайн-пользователей, позволят вам всегда быть на шаг впереди злоумышленников.
- Наличие списка URL-адресов командных центров ботнетов, атакующих ваших клиентов, дает возможность их заблокировать, направив соответствующий запрос в подразделение CERT или правоохранительные органы.
- Повышение уровня безопасности личных кабинетов в системах электронных платежей и интернет-банкинга благодаря пониманию природы атак.
- Возможность обучения ваших онлайн-пользователей распознаванию методов социальной инженерии, применяемых для атак.

Данные, поступающие в режиме реального времени

Сервис включает подписку на персонализированные уведомления с информацией об обнаруженных ботнетах, атакующих онлайн-ресурсы компании клиента. Уведомления отправляются по электронной почте или через RSS в формате HTML или JSON и содержат следующие данные:

- **URL-адреса целей ботнета** – вредоносная программа активизируется и запускает алгоритм атаки в тот момент, когда пользователь посещает сайт атакуемой ботнетом организации;
- **тип ботнета** – подробная информация о вредоносной программе, используемой киберпреступниками для перехвата транзакций (типами такого ПО могут быть, например, ZeuS, SpyEye, Citadel);
- **тип атаки** – информация о том, для чего преступники используют вредоносную программу (веб-инъекция, снятие скриншотов, захват видеоизображения, переадресация на фишинговый URL-адрес и другое);
- **алгоритмы атаки** – сведения об использованном алгоритме внедрения веб-кода: HTML-запросы (GET/POST), данные на веб-странице до и после внедрения и другое;
- **адрес командного сервера** – уведомив интернет-провайдеров о сервере управления ботнетом, можно оперативно ликвидировать угрозу;
- **MD5-хэши вредоносных программ** – «Лаборатория Касперского» предоставляет хэши для идентификации вредоносных программ;
- **расшифрованный конфигурационный файл соответствующего бота** – полный список адресов целей;
- **географическое распределение (ТОП-10 стран)** – статистические данные по глобальному распределению образцов соответствующего вредоносного ПО.

Мониторинг фишинговых угроз

Фишинг – одна из самых распространенных способов мошенничества, похищения учетных данных, проникновения программ-вымогателей в корпоративную сеть и других вредоносных действий.

Сервис мониторинга фишинговых угроз

Сервис активно отслеживает в режиме реального времени появление фишинговых сайтов, угрожающих вашей компании, и своевременно уведомляет о них. Кроме того, сервис снабжает вас точной, детальной информацией о фишинговой активности, нацеленной на ваш бизнес, включая внедряемое ПО и фишинговые URL-адреса, с помощью которых происходит кража учетных данных или конфиденциальной информации.

Уведомления о фишинге

Каждое уведомление о фишинговой угрозе передается с помощью HTTPS и содержит следующие данные:

- Скриншот фишинговой страницы;
- HTML-код фишинговой страницы;
- Файл JSON, содержащий следующие поля:
  - URL фишинговой страницы;
  - название компании, на которую нацелен фишинговый URL;
  - время, когда этот URL был замечен впервые;
  - время, когда этот URL был замечен в последний раз;
  - популярность фишингового URL;
  - местонахождение пользователей, на которых нацелен фишинговый URL;
  - тип похищаемых данных (данные кредитных карт; учетные записи от банковских сервисов, электронной почты, социальных сетей; персональные данные и т. п.);
  - метод атаки (угроза блокирования аккаунта, предложение скачать файл, запрос на обновление персональной информации);
  - преобразованные IP-адреса фишингового URL;
  - данные WHOIS;
  - название использованного Phishing Kit;
  - и многое другое.

Источники данных

Для получения данных сервис использует целый ряд источников, в том числе данные глобальной облачной сети Kaspersky Security Network, насчитывающей более 60 млн пользователей по всему миру, эвристический анализ, данные исследовательских групп, ловушки спама и многое другое. Вся эта информация обрабатывается в режиме реального времени с помощью аналитической системы «Лаборатории Касперского», механизмов белых списков и других технологий.

Активный поиск угроз

Отделы IT-безопасности самых разных компаний из самых разных отраслей объединены общей целью – они стремятся построить систему безопасности, которая бы обеспечивала комплексную и всестороннюю защиту против стремительно меняющихся угроз. Однако большинство специалистов до сих пор полагается на уведомления об угрозах и не замечает многие инциденты. Подобные угрозы могут существовать и действовать внутри корпоративного периметра долгие месяцы, подрывая эффективность работы предприятия и конфиденциальность деловой информации. Именно поэтому возрастает значимость сервисов, которые ищут следы существующей атаки. Сервисы активного поиска угроз «Лаборатории Касперского» (Kaspersky Threat Hunting) помогают обнаружить сложные угрозы при помощи передовых проактивных технологий, передовых технологий и опытных профессионалов.

Сервисы «Лаборатории Касперского»

- **Сервисы информирования об угрозах**
- **Активный поиск угроз**

  Обнаружение целевых атак Kaspersky Managed Protection
- **Тренинги по кибербезопасности**
- **Сервисы реагирования на инциденты**
- **Сервисы анализа защищенности**

Сервис обнаружения целевых атак

Сервис «Лаборатории Касперского» по обнаружению целевых атак будет полезен, если вы обеспокоены атаками, направленными на вашу отрасль, заметили подозрительную активность в собственных системах или ваша организация хочет провести плановую профилактическую проверку.

Сервис поможет выявить:

- активные атаки;
- атаки, произошедшие в прошлом;
- скомпрометированные системы.

Кроме того, вы получите рекомендации по устранению последствий атаки и предотвращению подобных атак в будущем.

Порядок выполнения работ

Наши эксперты выявят, идентифицируют и проанализируют как активные атаки, так и произошедшие в прошлом, установят список систем, которые были скомпрометированы в ходе этих атак. Мы поможем вам обнаружить вредоносные действия, найти возможные источники инцидентов и спланировать наиболее эффективные действия по устранению последствий.

Для этого мы выполняем следующие работы:

- анализируем ландшафт угроз, специфичных для вашей организации;
- проводим глубокую проверку вашей IT-инфраструктуры и данных (например, файлов журналов) на наличие признаков компрометации;
- анализируем ваши исходящие сетевые соединения на предмет любых подозрительных действий;
- выявляем возможные источники атаки и определяем, какие еще системы могли подвергнуться компрометации.

Результаты

Результаты работ будут представлены в подробном отчете, содержащем:

- общие сведения, подтверждающие наличие или признаков компрометации в вашей сети;
- анализ собранных аналитических данных об угрозах и выявленных индикаторах компрометации (IoC);
- описание возможных источников атаки и скомпрометированных компонентов сети;
- рекомендации по устранению последствий, позволяющие минимизировать последствия выявленного инцидента и защитить ваши ресурсы от подобных атак в будущем.

Подробное описание сервиса

Сервис «Лаборатории Касперского» по обнаружению целевых атак включает следующие действия:

Сбор и анализ данных об атаках. Цель этого шага – получить данные о ландшафте атак, которые были направлены или выполняются против информационных активов компании злоумышленниками. Мы исследуем внутренние и внешние источники данных, включая подпольные сообщества киберпреступников, а также используем внутренние системы мониторинга «Лаборатории Касперского». Анализ этой информации позволяет нам выявить, например, слабые места в вашей инфраструктуре, представляющие интерес для киберпреступников, и скомпрометированные учетные записи.

Сбор данных на инфраструктуре заказчика. В рамках данного этапа будут собраны данные с рабочих станций, серверов, SIEM-систем и другого оборудования из инфраструктуры заказчика. Часть указанных данных собирается с помощью ПО, которое будет предоставлено заказчику в рамках сервиса.

Анализ данных. На основе данных, собранных на предыдущем этапе, эксперты «Лаборатории Касперского» выявляют инциденты в корпоративной сети. Основная задача данного этапа – определить тип инцидента и оценить его воздействие на инфраструктуру, что позволит выбрать адекватные меры реагирования. На этом этапе задействуются данные журналов с рабочих станций, данные сетевой активности, а также другие контекстуальные и исторические сведения; сбор дополнительных данных напрямую с компрометированных систем не производится.

Первичное реагирование на инцидент. На этом этапе предоставляются базовые рекомендации в отношении первоначальных шагов по реагированию на выявленные инциденты. В ряде случаев, чтобы подтвердить и классифицировать инцидент, экспертам «Лаборатории Касперского» могут понадобиться дополнительные данные, такие как различные файлы операционных систем, приложений и сетевого оборудования, дампы сетевого трафика, образы жесткого диска, дампы памяти и другие типы данных. Дополнительные данные заказчик может предоставить по требованию (по электронной почте или через различные сетевые ресурсы – в зависимости от типа и объемов запрашиваемых данных).

Подготовка отчета. Результатом проведенных в рамках сервиса работ является финальный отчет. Он содержит результаты анализа данных из внешних источников, а также описания обнаруженных атак на базе анализа собранных данных в инфраструктуре заказчика. Кроме того, отчет содержит рекомендации по устранению последствий обнаруженных атак.

Дополнительные сервисы

В случае необходимости наши эксперты исследуют симптомы инцидента, проводят глубокий цифровой анализ систем, идентифицируют исполняемый файл вредоносной программы (если он существует) и выполняют ее анализ. По результатам работы дополнительных сервисов составляются отдельные отчеты с дальнейшими рекомендациями по устранению последствий. Кроме того, по запросу мы можем развернуть решение **Kaspersky Anti Targeted Attack (KATA)** в вашей сети. Эта платформа объединяет новейшие технологии и аналитические данные глобального уровня, благодаря чему она быстро выявляет целевые атаки и реагирует на них на любом этапе их жизненного цикла в системе.

Kaspersky Managed Protection

Круглосуточная служба анализа событий информационной безопасности, созданная «Лабораторией Касперского» — признанным лидером в области исследований целевых атак.

На протяжении многих лет «Лаборатория Касперского» проводит исследования, направленные на выявление самых сложных кибератак. Высокое качество этих исследований подтверждается многочисленными успешными результатами тестов наших продуктов. Однако с появлением целевых атак подобные исследования необходимо перенести в инфраструктуру конкретного предприятия. Kaspersky Managed Protection – операционный сервис активного поиска киберугроз, направленных на вашу организацию.

Ключевые преимущества

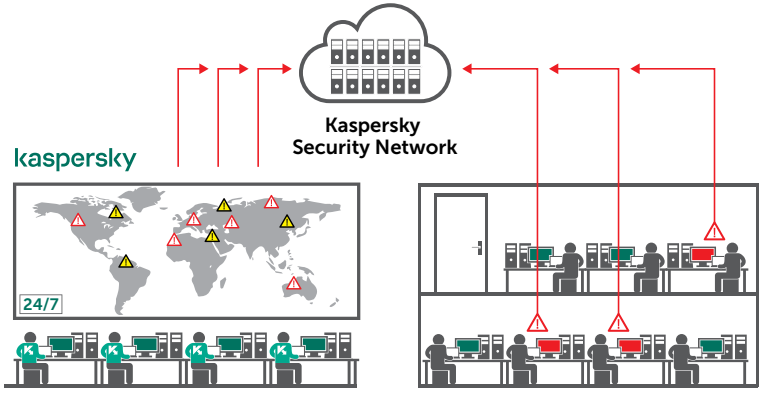
- Комплексный подход к противодействию угрозам: предотвращение атак с использованием признанной системы защиты рабочих мест Kaspersky Security для бизнеса, обнаружение и расследование – там, где автоматическое предотвращение технически невозможно, и активный поиск угроз высококвалифицированным аналитиком в случае скрытых целевых атак, требующих глубокого исследования.
- Обнаружение бесфайлового вредоносного ПО (file-less), атак, выполняемых без применения вредоносного ПО (malware-less attacks) или с применением неизвестных ранее инструментов проведения атак.
- Моментальное противодействие атаке через используемую систему защиты рабочих мест.

Дополнительные преимущества

- Не нужно разворачивать и конфигурировать дополнительные агенты и сервера управления — в качестве сенсоров используются уже развернутые продукты.
- Снижение совокупных затрат на обеспечение безопасности — не нужно нанимать и обучать штатных специалистов.
- Минимальное количество ложных срабатываний.
- Уверенность от осознания того, что вы защищены даже от самых сложных и инновационных атак.
- Сведения об атакующих вас злоумышленниках, их мотивации, методах и средствах.

Как работает Kaspersky Managed Protection

В рамках оказания сервиса эксперты Центра мониторинга кибербезопасности «Лаборатории Касперского» осуществляют анализ расширенной телеметрии с установленных в сетях заказчика продуктов Kaspersky Security для бизнеса и Kaspersky Anti Targeted Attack, выступающих в качестве сенсоров. Это достигается, в частности, за счет проактивного сбора метаданных сетевой и системной активности. Полученная информация агрегируется с использованием Kaspersky Security Network и исследуется аналитиками на основе данных об угрозах (Threat intelligence), собранных «Лабораторией Касперского» за все время деятельности, что позволяет обнаружить актуальные тактики, техники и процедуры злоумышленников.



Центр мониторинга

* Защищаемая корпоративная инфраструктура

Круглосуточная служба анализа событий безопасности:

- оперативно выявляет инциденты информационной безопасности посредством многоэтапного анализа расширенной телеметрии сенсоров, размещенных в инфраструктуре заказчика;
- собирает информацию, достаточную для классификации выявленных инцидентов (ложное или корректное срабатывание);
- инициирует процесс реагирования на выявленные инциденты;
- при наличии технической возможности, инициирует обновление баз средств защиты, чтобы заблокировать угрозу;
- проводит ретроспективный анализ системной и сетевой активности процессов и приложений с целью расследования инцидентов.

Тренинги по кибербезопасности

Инновационные тренинги, в рамках которых «Лаборатория Касперского» делится своими экспертными знаниями и опытом в сфере информационной безопасности, а также уникальными данными о киберугрозах.

Количество и сложность угроз постоянно растет, и для успешной защиты от них требуются не только передовые решения, но и квалифицированные сотрудники.

Тренинги «Лаборатории Касперского» помогут IT-профессионалам получить актуальные знания, расширить свою экспертизу и развить практические навыки в выбранных областях кибербезопасности.

Тренинги охватывают широкий спектр тем в области кибербезопасности, а также различных методик и практик, которые могут быть полезны как начинающим специалистам, так и опытным экспертам.

Все тренинги сочетают теоретическую и практическую часть. По завершении курса проводится оценка усвоенного участниками материала.

Тренинги проводятся как дистанционно, так и на территории заказчика.

Сервисы «Лаборатории Касперского»

- **Сервисы информирования об угрозах**
- **Активный поиск угроз**
- **Тренинги по кибербезопасности**
  - Цифровая криминилистика
  - Анализ и обратная разработка вредоносного ПО
  - Экспертная цифровая криминалистика
  - Экспертные анализ и обратная разработка вредоносного ПО
  - Реагирование на индциденты YARA
  - Администрирование KATA
  - Анализ инцидентов KATA
- **Сервисы реагирования на инциденты**
- **Сервисы анализа защищенности**

Преимущества тренингов

Цифровая криминалистика и продвинутая цифровая криминалистика

Повысьте экспертизу ваших экспертов в области цифровой криминалистики и реагирования на инциденты. Задача тренинга – укрепить знания специалистов во всем, что касается поиска следов киберпреступления и анализа различных типов данных с целью установить источник и временные параметры атаки. После завершения тренинга участники смогут успешно проводить расследование компьютерных инцидентов, что повысит уровень безопасности компании в целом.

Анализ вредоносного ПО и обратная разработка (начальный и экспертный уровни)

Тренинг по обратной разработке поможет специалистам в области реагирования на инциденты успешнее проводить расследование вредоносных атак. Курс предназначен для сотрудников IT-департамента и системных администраторов. В ходе тренинга участники учатся анализировать вредоносное ПО, собирать индикаторы компрометации (IoCs), писать сигнатуры для обнаружения вредоносного ПО или зараженных машин, а также восстанавливать зараженные/зашифрованные файлы и документы.

Реагирование на инциденты

Тренинг поможет сотрудникам службы IT-безопасности больше узнать обо всех стадиях расследования инцидентов и даст все необходимые сведения для успешного самостоятельного устранения последствий инцидента.

YARA

Тренинг поможет узнать, как правильно писать, эффективно тестировать и улучшать правила YARA таким образом, чтобы с помощью них можно было успешно обнаруживать атаки.

Администрирование Kaspersky Anti Targeted Attack Platform

Тренинг по администрированию Kaspersky Anti Targeted Attack Platform (KATA) позволит узнать, как установить и настроить решение, а также как управлять им с максимальной эффективностью.

Анализ инцидентов KATA

Тренинг включает в себя множество упражнений, основанных на часто встречающихся на практике сценариях обнаружения угроз. Важную роль в них играет обработка уведомлений KATA – отслеживание, интерпретация,реагирование.

Описание программы

Темы	Продолжительность	Навыки
Основы информационной безопасности		
· Обзор черного рынка киберугроз и хакерских услуг · Спам, фишинг, безопасность электронной почты · Технологии защиты от мошенничества · Эксплойты, угрозы для мобильных устройств и целенаправленные атаки · Основы расследования инцидентов с помощью общедоступных веб-инструментов · Безопасность рабочего места	Онлайн-тренинг	· Обнаружение инцидентов безопасности и принятие решений по их устранению · Снижение нагрузки на отделы информационной безопасности · Повышение безопасности рабочего места каждого сотрудника с помощью дополнительных средств · Проведение простых расследований · Анализ фишинговых писем · Распознавание зараженных и поддельных веб-сайтов
Общие вопросы цифровой криминалистики		
· Введение в цифровую криминалистику · Оперативное реагирование и сбор цифровых улик · Внутренняя структура реестра Windows · Анализ артефактов в Windows · Криминалистический анализ браузера · Анализ электронной почты	5 дней	· Организация лаборатории цифровой криминалистики · Сбор цифровых улик и порядок обращения с ними · Воссоздание хронологической картины инцидента с помощью меток времени · Выявление следов вторжения посредством анализа артефактов в ОС Windows · Анализ истории браузера и электронной почты · Умение применять инструменты цифровой криминалистики
Основы анализа и обратной разработки вредоносного ПО		
· Цели и методы анализа и обратной разработки вредоносного ПО · Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86 · Базовые методы статического анализа (извлечение строк, анализ импортов, анализ точек входа исполняемого файла, автоматическая распаковка и т. д.) · Базовые методы динамического анализа (отладка, инструменты мониторинга, перехват трафика и т. д.) · Анализ файлов .NET, Visual Basic, Win64 · Методы анализа сценариев и программ, отличных от исполняемых файлов (пакетные файлы, Autoit, Python, Jscript, JavaScript, VBS)	5 дней	· Глубокий анализ файловой системы · Восстановление удаленных файлов · Анализ сетевого трафика · Обнаружение вредоносной активности по дампам памяти · Восстановление хронологии инцидента

Темы	Продолжительность	Навыки
Цифровая криминалистика (экспертный уровень)		
· Экспертная криминалистика в ОС Windows · Восстановление данных · Сетевая и облачная криминалистика · Криминалистический анализ дампов памяти · Хронологический анализ · Практическая криминалистика реальных целевых атак	5 дней	· Глубокий анализ файловой системы · Восстановление удаленных файлов · Анализ сетевого трафика · Обнаружение вредоносной активности по дампам памяти · Восстановление хронологии инцидента
Анализ и обратная разработка вредоносного ПО (экспертный уровень)		
· Цели и методы анализа и обратной разработки вредоносного ПО · Методы расширенного статического и динамического анализа (статический анализ шелл-кода, синтаксический анализ заголовка исполняемого файла, блоки переменных окружения потока (TEB) и окружения процесса (PEB), загрузка функций на основе различных алгоритмов хэширования) · Методы расширенного динамического анализа (структура исполняемого файла, ручная и экспертная распаковка, распаковка вредоносных архивов, содержащих полный исполняемый файл в зашифрованной форме) · Обратная разработка APT-угроз (полная проработка сценария APT-атаки, начиная с фишингового сообщения электронной почты и заканчивая как можно более глубоким анализом) · Анализ протоколов (анализ зашифрованных коммуникаций по протоколу C2, методы расшифровки трафика) · Анализ руткитов и буткитов (отладка загрузочного сектора при помощи IDA и VMWare, отладка ядра при помощи двух виртуальных машин, анализ образцов руткитов)	5 дней	· Использование передовых методов обратной разработки и распознавание методов защиты от обратной разработки (обфускация, защита от отладки) · Расширенный анализ руткитов и буткитов · Анализ шелл-кода эксплойтов, внедренного в различные виды файлов, а также вредоносных программ для сред, отличных от Windows
Реагирование на инциденты		
· Общие сведения о реагировании на инциденты · Обнаружение и первичный анализ · Цифровой анализ · Создание правил обнаружения (YARA, Snort, Bro)	5 дней	· Отделение APT от других типов угроз · Понимание различных методов атаки и анатомии целевых атак · Применение специальных методов мониторинга и обнаружения · Выполнение процедуры реагирования на инциденты · Восстановление хронологической картины и логики инцидента · Создание правил обнаружения и подготовка отчетов

Темы	Продолжи-тельность	Навыки
YARA		
· Введение в синтаксис правил YARA · Способы быстрого и эффективного создания правил · YARA-генераторы · Тестирование правил YARA на ложные срабатывания · Поиск новых необнаруженных образцов с помощью VirusTotal · Использование внешних модулей в YARA для эффективного поиска угроз · Поиск аномалий · Множество примеров из реальной практики · Набор упражнений для совершенствования навыков работы с YARA	2 дня	· Создание эффективных правил YARA · Тестирование правил YARA · Дальнейшее совершенствование правил для эффективного обнаружения угроз
Администрирование KATA		
· Стандартная схема развертывания решения и размещения серверов · Системные требования · Модель лицензирования · Сервер «песочницы» · Консоль Central Node · Сенсоры · Интеграция с инфраструктурой · Установка сенсора на рабочих станциях · Добавление лицензии и обновление баз · Алгоритм работы решения	1 день	· Создание плана развертывания, оптимального для среды заказчика · Установка и настройка компонентов KATA · Поддержка и управление решением
Анализ инцидентов KATA		
· Интерпретация уведомлений (алертов) KATA · Объяснение технологий обнаружения и анализа · Объяснение механизмов скоринга и оценки риска	1 день	· Понимание того, как работает скоринг и как он используется механизмами оценки риска · Способность уверенно работать с уведомлениями KATA: отслеживать, интерпретировать, реагировать

Сервисы реагирования на инциденты

Остановить атаку до ее проникновения внутрь вашего периметра защиты не всегда возможно, однако снизить возможный ущерб и предотвратить распространение атаки вполне в ваших силах.

Основная цель реагирования на инциденты – снизить воздействие инцидента на вашу IT-среду.

Сервис реагирования на инциденты включает весь цикл расследования инцидента, от сбора улик на месте до выявления дополнительных индикаторов компрометации, подготовки плана борьбы с последствиями и полного устранения угрозы для вашей организации.

Для этого мы выполняем следующие работы:

- выявляем скомпрометированные ресурсы;
- изолируем угрозу;
- останавливаем распространение атаки;
- находим и собираем улики;
- анализируем улики, а также восстанавливаем хронологию и логику развития инцидента;
- анализируем вредоносные программы, использованные для атаки (если применимо);
- по возможности выявляем источники атаки и определяем, какие еще системы могли подвергнуться компрометации (если возможно).

Сервисы «Лаборатории Касперского»

- **Сервисы информирования об угрозах**
- **Активный поиск угроз**
- **Тренинги по кибербезопасности**
- **Сервисы реагирования на инциденты**
  - Реагирование на инциденты
  - Анализ вредоносного ПО
  - Цифровая криминалистика
- **Сервисы анализа защищенности**

- проверяем вашу IT-инфраструктуру на возможные признаки компрометации;
- анализируем исходящие соединения вашей сети с внешними ресурсами для выявления подозрительных объектов (например, командных серверов);
- устраняем угрозу;
- рекомендуем вам дальнейшие действия по устранению последствий.

В зависимости от наличия у вас собственной группы реагирования на инциденты наши эксперты могут провести расследование полного цикла, либо только выявить и изолировать скомпрометированные машины и предотвратить распространение угрозы, либо выполнить анализ вредоносных программ или цифровую криминалистическую экспертизу.

Работы по реагированию на инциденты ведут опытные аналитики и специалисты по обнаружению проникновения в информационные системы.

Анализ вредоносного ПО

Анализ вредоносного ПО позволяет получить полное представление о поведении конкретных вредоносных программ, использованных для атаки на вашу организацию, а также о целях, преследуемых злоумышленниками.

Эксперты «Лаборатории Касперского» осуществляют всесторонний анализ образца вредоносного ПО, предоставленного вашей организацией, и составляют подробный отчет, содержащий следующую информацию:

- **свойства образца** – краткое описание и вердикт согласно классификации «Лаборатории Касперского»;
- **подробное описание вредоносной программы –** углубленный анализ функций, поведения и целей вредоносной программы, включая индикаторы компрометации, дающий вам информацию, необходимую для нейтрализации угрозы;
- **сценарий устранения последствий** – в отчете будут предложены шаги по обеспечению эффективной защиты вашей организации от угроз данного типа.

Цифровая криминалистика

Цифровой криминалистический анализ может включать в себя анализ вредоносного ПО, если оно будет обнаружено в ходе расследования. Эксперты «Лаборатории Касперского» используют различные источники, например образы жестких дисков, дампы памяти, трассировки сети, чтобы воссоздать полную картину инцидента. Расследование начинается с того, что клиент собирает улики и предоставляет описание инцидента. Эксперты «Лаборатории Касперского» исследуют симптомы инцидента, идентифицируют исполняемый файл вредоносной программы (если он есть) и проводят ее анализ. Клиенту предоставляется подробный отчет с указанием мер, необходимых для устранения последствий инцидента.

Сервисы анализа защищенности

Сервисы анализа защищенности – это услуги специалистов компании, многие из которых являются признанными во всем мире профессионалами. Их знания и опыт служат опорой нашей репутации мирового лидера в области анализа угроз.

Каждая IT-инфраструктура уникальна, а самые опасные атаки специально планируются с учетом уязвимостей конкретной организации. Поэтому при оказании экспертных услуг специалисты компании индивидуально подходят к каждому клиенту. Сервисы могут предоставляться как полностью, так и частично (в любом сочетании).

В состав сервисов анализа защищенности, предоставляемых «Лабораторией Касперского», входят:

- Тестирование на проникновение
- Анализ защищенности приложений
- Анализ защищенности банкоматов и POS-терминалов
- Анализ защищенности телекоммуникационных сетей
- Анализ защищенности промышленных сетей

Сервисы «Лаборатории Касперского»

- **Сервисы информирования об угрозах**
- **Активный поиск угроз**
- **Тренинги по кибербезопасности**
- **Сервисы реагирования на инциденты**
- **Сервисы анализа защищенности**
  - Тестирование на проникновение
  - Анализ защищенности приложений
  - Анализ защищенности банкоматов и POS-терминалов
  - Анализ защищенности телекоммуникационных сетей

Тестирование на проникновение

Надежная защита IT-инфраструктуры от потенциальных кибератак – актуальная проблема любой организации. Особенно сложной эта задача становится для крупных предприятий, где в подразделениях, расположенных в разных городах и странах, работают тысячи сотрудников и эксплуатируются сотни информационных систем. Тестирование на проникновение продемонстрирует возможные сценарии атаки и покажет уровень защиты ваших систем.

Тестирование на проникновения позволит получить более полное представление о проблемных с точки зрения безопасности местах в инфраструктуре, выявить уязвимости, проанализировать возможные последствия атак различного вида и оценить эффективность уже принятых мер защиты, а также получить рекомендации по устранению уязвимостей и повышению безопасности.

Тестирование на проникновение поможет:

- Выявить наиболее уязвимые места в сети, чтобы сосредоточить на них внимание и снизить риски.
- Избежать финансовых, операционных и репутационных потерь, вызванных кибератаками. Заблаговременное обнаружение и устранение уязвимостей позволит предотвратить атаки.
- Выполнить требования государственных, отраслевых или внутренних корпоративных стандартов, предусматривающих подобную форму оценки системы безопасности (например, PCI DSS).

Состав работ и варианты предоставления сервиса

В зависимости от задач и особенностей IT-инфраструктуры вы можете выбрать любые из следующих вариантов тестирования на проникновение:

- Внешнее тестирование на проникновение. Оценка системы безопасности, которая проводится через интернет от лица злоумышленника, не обладающего никакими данными о вашей системе.
- Внутреннее тестирование на проникновение. Сценарии с участием злоумышленника, действующего внутри компании. Это может быть посетитель, у которого есть лишь физический доступ в помещения компании, или подрядчик, имеющий ограниченный доступ к системам.
- Проверка уязвимости к социальной инженерии. Оценка осведомленности персонала об угрозах безопасности. Моделируется применение методов социальной инженерии: фишинг, псевдовредоносные ссылки в сообщениях электронной почты, подозрительные вложения и т. д.
- Оценка безопасности беспроводных сетей. Наши эксперты выезжают к вам и проверяют защищенность сетей Wi-Fi.

Подход «Лаборатории Касперского» к тестированию на проникновение

В рамках тестирования на проникновение происходит контролируемая имитация настоящей кибератаки. Испытания проводят эксперты по безопасности «Лаборатории Касперского», которые соблюдают полную конфиденциальность ваших систем и не нарушают их целостность и доступность. Мы строго следуем международным стандартам и принятым в отрасли методикам, в том числе:

- Penetration Testing Execution Standard (PTES);
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
- Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Web Application Security Consortium (WASC) Threat Classification;
- Open Web Application Security Project (OWASP) Testing Guide;
- Common Vulnerability Scoring System (CVSS).

Специалисты, проводящие работы, — опытные профессионалы, обладающие глубокими и актуальными практическими знаниями. Наши эксперты известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших сервисах и программных продуктах таких компаний, как Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens и SAP.

По окончании работ вы получите итоговый отчет с подробной технической информацией о ходе тестирования, его результатах и обнаруженных уязвимостях. В отчете будут также приведены рекомендации по устранению уязвимостей и краткий итог с результатами тестирования и наглядным описанием векторов атак. В случае необходимости также могут быть подготовлены видеоматериалы и презентации для технического отдела или высшего руководства.

Варианты предоставления сервиса

В зависимости от выбранного метода анализа защищенности, особенностей систем и бизнеса клиента тестирование на проникновение может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно (даже испытание на проникновение изнутри можно организовать через VPN-доступ), однако для оценки безопасности беспроводных сетей и ряда других задач необходимо присутствие специалистов на месте.

Тестирование на проникновение можно проводить в каком-то одном сегменте IT-инфраструктуры, однако мы настоятельно рекомендуем проверять таким образом всю сеть или хотя бы ее крупнейшие сегменты. Ведь результаты тестирования будут более достоверными, если наши специалисты смогут работать в тех же условиях, что и потенциальные злоумышленники.

Анализ защищенности приложений

Вы можете разрабатывать корпоративные приложения самостоятельно или приобретать их у сторонних поставщиков, но в любом случае всего одной ошибки в программном коде достаточно, чтобы создать уязвимость для атак, ведущих к значительным финансовым или репутационным потерям.

В течение жизненного цикла приложения могут возникать новые уязвимости – при обновлении ПО или из-за неправильной настройки компонентов. Могут возникать и новые способы атак, для которых система окажется уязвимой.

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», выявляет уязвимости в приложениях любого типа – от крупных облачных решений, ERP-систем, систем дистанционного банковского обслуживания и других специализированных бизнес-приложений до встроенных программ и мобильных решений на различных платформах (iOS, Android и др.).

Сочетание знаний, практического опыта и передовых международных методов позволяет нашим экспертам обнаруживать бреши в системе безопасности, которые делают вашу организацию уязвимой для следующих угроз:

- кража конфиденциальных данных;
- получение несанкционированного доступа к системам и изменение данных;
- организация атак типа DoS (отказ в обслуживании);
- совершение мошеннических операций.

Наши рекомендации позволяют устранить обнаруженные уязвимости в приложениях и предотвратить подобные атаки

Преимущества для клиентов

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», помогает разработчикам и владельцам приложений:

- **избежать финансовых, операционных и репутационных потерь**, заблаговременно обнаруживая и устраняя уязвимости, посредством которых проводятся атаки на приложения;
- **уменьшить издержки на ликвидацию последствий** возможных атак путем обнаружения уязвимостей на этапах разработки или тестирования и до внедрения в системы в эксплуатацию, после которого исправление недостатков может быть связано с дополнительными расходами и необходимостью остановки бизнес-процессов;
- **организовать жизненный цикл безопасной разработки ПО (S-SDLC),** нацеленный на создание и сопровождение защищенных приложений;
- **выполнить требования государственных, отраслевых или внутренних корпоративных стандартов**, предусматривающих защиту приложений, например PCI DSS или HIPAA.

Состав работ и варианты предоставления сервиса

В рамках сервиса могут оцениваться официальные веб-сайты и бизнес-приложения (стандартные или облачные), в том числе встроенные и мобильные приложения.

Состав работ формируется индивидуально в соответствии с вашими потребностями и особенностями приложений. Он может включать следующие компоненты:

- **Анализ защищенности методом «черного ящика».** Имитируются действия злоумышленника, находящегося вне тестируемой системы.
- **Анализ защищенности методом «серого ящика».** Имитируются действия внутренних пользователей, с различным уровнем доступа.
- **Анализ защищенности методом «белого ящика».** Анализ с полным доступом к приложению, включая исходный код. Этот подход наиболее эффективен с точки зрения количества обнаруживаемых уязвимостей.
- **Оценку эффективности системы превентивной защиты приложений (application firewall).** Приложения проверяются в два этапа: с включенными и с выключенными механизмами защиты, чтобы эффективно выявить уязвимости и убедиться, что атаки выявляются и блокируются.

Подход «Лаборатории Касперского» к анализу защищенности приложений

Анализ защищенности приложений проводится экспертами «Лаборатории Касперского» как с использованием автоматизированных средств, так и вручную. При этом предпринимаются все разумные меры предосторожности для сохранения конфиденциальности, целостности и доступности приложений. Мы строго следуем международным стандартам и принятым в отрасли методикам, в том числе:

- Web Application Security Consortium (WASC) Threat Classification;
- Open Web Application Security Project (OWASP) Testing Guide;
- OWASP Mobile Security Testing Guide;
- а также другим стандартам в зависимости от рода деятельности и расположения вашей организации.

Специалисты, проводящие работы, – опытные профессионалы, обладающие глубоким и актуальным практическим знанием различных платформ, языков программирования и методов атак. Они выступают на важнейших международных конференциях и известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших облачных сервисах и приложениях, включая Oracle, Google, Apple, Facebook и PayPal.

Варианты предоставления сервиса

В зависимости от методов анализа, особенностей тестируемых систем и требований клиента к условиям работы анализ защищенности приложений может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно.

Анализ защищенности банкоматов и POS-терминалов

Комплексная проверка банкоматов и POS-терминалов на наличие уязвимостей, которые могут использоваться атакующими для несанкционированного снятия наличности, выполнения мошеннических транзакций, сбора данных с карт клиентов или организации DoS-атак.

Атаки на банкоматы и POS-терминалы больше не ограничены физическим вмешательством, таким как вскрытие банкоматов или копирование данных карт. По мере того как банки и компании, производящие банкоматы и POS-терминалы, совершенствуют меры защиты, стремительно возрастает и сложность атак против этих устройств. Злоумышленники используют уязвимости в их архитектуре и приложениях, создавая направленные на них вредоносные программы. Анализ защищенности банкоматов и POS-терминалов,

Проводимый «Лабораторией Касперского», помогает распознать недостатки защиты ваших финансовых устройств и снизить риск их компрометации.

Анализ защищенности банкоматов и POS-терминалов помогает производителям и финансовым организациям:

- получить сведения об уязвимостях в своих банкоматах и POS-терминалах и улучшить соответствующие механизмы безопасности;
- избежать финансовых, операционных и репутационных потерь в результате возможной атаки, заблаговременно выявляя и устраняя уязвимости, которые могут использовать злоумышленники;
- обеспечить выполнение требований государственных, отраслевых и внутренних корпоративных стандартов, требующих проведения оценки защищенности (например, PCI DSS).

Состав работ

Сервис предусматривает комплексный анализ банкоматов и POS-терминалов, включая фаззинг и демонстрацию атак в тестовой среде. Работы могут выполняться на одном устройстве или в сети устройств. Мы рекомендуем выбирать для анализа устройства, наиболее широко используемые в вашей организации или те, анализ которых критически важен (например, уже пострадавшие от инцидентов), в типично используемой конфигурации.

Подход «Лаборатории Касперского» к анализу защищенности банкоматов и POS-терминалов

При проведении анализа эксперты не только обнаружат и идентифицируют недостатки конфигурации и уязвимости в устаревших версиях программ, но и глубоко изучат логику процессов, выполняемых банкоматами и POS-терминалами, с целью выявления новых уязвимостей (нулевого дня) на уровне компонентов. В случае выявления уязвимостей, эксплуатация которых может быть выгодна злоумышленникам (например, позволяющих осуществлять несанкционированный вывод наличности), эксперты могут продемонстрировать возможные сценарии атак, используя специально подготовленные автоматизированные утилиты или устройства.

Хотя при анализе защищенности банкоматов и POS-терминалов имитируется настоящая атака, чтобы на практике оценить эффективность защиты, эта процедура полностью безопасна и не вредит вашей инфраструктуре. Работы проводят опытные эксперты «Лаборатории Касперского», которые сделают все необходимое для обеспечения конфиденциальности, целостности и доступности систем в строгом соответствии с международным правом и передовыми методиками. При обнаружении новой уязвимости в банкоматах или POS-терминалах клиента эксперты следуют политике ответственного разглашения, в частности сообщают об уязвимости производителю и проводят консультации по решению проблемы.

Выполняя анализ защищенности банкоматов и POS-терминалов, «Лаборатория Касперского» руководствуется международными стандартами и принятыми в отрасли методиками.

Результаты анализа

По завершении анализа вы получите отчет с подробной технической информацией о процессе тестирования, его результатах, обнаруженных уязвимостях и рекомендациях по их устранению. В отчете также приводятся краткие выводы, основанные на результатах тестирования, и описание возможных векторов атак. Кроме того, в случае необходимости могут быть подготовлены видеоматериалы, демонстрирующие атаки на исследуемые устройства, и презентации для технических подразделений или руководства.

Анализ защищенности телекоммуникационных сетей

IT-инфраструктура любой телекоммуникационной компании состоит из нескольких сетей, выполняющих различные функции и основанных на различных технологиях. Каждый компонент этой инфраструктуры критически важен для бизнеса и должен быть надежно защищен от атак для избежания финансовых, операционных и репутационных потерь.

Сервисы «Лаборатории Касперского» позволяют усилить защиту телекоммуникационных сетей: уязвимости, обнаруженные в ваших системах, можно или устранить, или обезвредить

«Лаборатория Касперского» предлагает следующие сервисы анализа защищенности телекоммуникационных сетей:

- тестирование IT-инфраструктуры на проникновение;
- анализ безопасности конфигурации IT-инфраструктуры;
- анализ защищенности сетей, использующих стандарты GSM, UMTS и LTE;
- анализ защищенности приложений (для приложений, обеспечивающих пользование сервисами, такими как IP-телевидение, порталы самообслуживания и т. д.);
- анализ защищенности средств VoIP-связи;
- анализ защищенности телекоммуникационного оборудования.

Результат работ

По итогам анализа вы получаете технический отчет и общий обзор по недостаткам защиты в ваших телекоммуникационных сетях, а также заключение об эффективности ваших мер безопасности. Эти данные можно применить для повышения уровня безопасности сети и снижения финансовых, репутационных и операционных рисков.

Отчет содержит следующую информацию:

- общее заключение об уровне безопасности;
- описание методологии и процесса проведения работ и анализа;
- подробное описание выявленных уязвимостей, включая уровень критичности, сложность атаки, возможное влияние на систему, а также доказательства наличия уязвимости (по возможности);
- рекомендации по устранению уязвимости, включая изменения конфигурации, обновления, изменение исходного кода или внедрение компенсирующих мер там, где устранить уязвимость невозможно.

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз. Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Более подробная информация доступна на www.kaspersky.ru.

kaspersky

www.kaspersky.ru