KASPERSKY lab

СЕРВИСЫ KASPERSKY SECURITY INTELLIGENCE

2016

Сегодня киберпреступления распространены повсеместно. Технические возможности злоумышленников неуклонно растут, а их атаки становятся все более изощренными. Наша миссия – защищать мир от всех видов киберугроз. Выполнить ее и сделать работу в интернете безопасной можно, лишь имея возможность передавать и получать сведения об угрозах в режиме реального времени. Своевременный доступ к информации абсолютно необходим для эффективной защиты данных и сетей.

Евгений Касперский,
председатель совета директоров и генеральный директор «Лаборатории Касперского»

ВВЕДЕНИЕ

Каждый день появляется все больше разных и сложных для вычисления киберугроз.

При этом единого решения, которое бы обеспечило полную защиту от этих угроз, не существует, и, чтобы эффективно бороться с ними, необходимо знать, откуда ожидать нападения.

Руководители несут ответственность за защиту организации от уже существующих угроз и за предупреждение угроз, которые могут возникнуть в будущем. Чтобы добиться этого, нужно не только обеспечивать ежедневную защиту от уже известных угроз, но и понимать перспективы их развития. Анализ такого уровня своими силами могут провести очень немногие организации.

Помимо надежной защиты от киберугроз для стабильного экономического развития компании необходимо также и долгосрочное бизнес-партнерство.

Мы в «Лаборатории Касперского» это понимаем и всегда готовы поделиться со специалистами вашей организации новейшей информацией об актуальных угрозах. Возможность передачи информации по различным каналам позволит вашей службе IT-безопасности быть во всеоружии и эффективно бороться с любыми интернет-угрозами.

Мы предоставим вам все преимущества сервисов Security Intelligence, даже если ваша организация не пользуется продуктами «Лаборатории Касперского».

ПРИНЦИПИАЛЬНО НОВЫЙ ПОДХОД К БЕЗОПАСНОСТИ

Отличительная особенность нашей компании – лучшая в мире аналитика в области угроз. Она проявляется во всем, что мы делаем, и позволяет предлагать средства защиты от вредоносных программ – самые мощные из доступных на рынке.

Развитие технологий – главный приоритет компании на всех уровнях, в том числе и для нашего генерального директора Евгения Касперского.

Наш глобальный центр исследования и анализа угроз (GReAT) – элитное подразделение экспертов по IT-безопасности – первым обнаружил многие из наиболее опасных вредоносных программ и целевых атак.

К нам за помощью регулярно обращаются многие уважаемые организации, отвечающие за безопасность, и представители правоохранительных органов по всему миру, в том числе Интерпол, Европол, группы экстренного реагирования (CERT), а также полицейские департаменты различных стран.

«Лаборатория Касперского» создает и разрабатывает все базовые технологии внутри компании, что делает наши продукты и сервисы более надежными и эффективными.

Ведущие отраслевые аналитики, в том числе Gartner, Inc., Forrester Research и International Data Corporation (IDC), признают «Лабораторию Касперского» лидером во многих ключевых категориях IT-безопасности.

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

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ

- Программа повышения осведомленности о киберугрозах
- Программа экспертного обучения в области ИБ

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ

- Потоки данных об угрозах
- Мониторинг ботнет-угроз
- Аналитические отчеты

ЭКСПЕРТНЫЕ СЕРВИСЫ

- Расследование инцидентов
- Тестирование на проникновение
- Анализ защищенности приложений

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ

В рамках этих инновационных образовательных программ «Лаборатория Касперского» делится своими экспертными знаниями и опытом в сфере информационной безопасности, а также уникальными данными о киберугрозах.

Для современных предприятий, которые сталкиваются с непрерывно растущим объемом постоянно меняющихся киберугроз, чрезвычайно важно быть в курсе главных проблем IT-безопасности. Эффективная корпоративная стратегия по защите от угроз и минимизации последствий кибератак немыслима без развития у специалистов навыков работы с передовыми технологиями IT-безопасности. При этом все сотрудники без исключения должны владеть базовыми знаниями о киберугрозах и навыками безопасной работы.

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ
- Программа повышения осведомленности о киберугрозах
- Программа экспертного обучения в области ИБ

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ
- Потоки данных об угрозах
- Мониторинг ботнет-угроз
- Аналитические отчеты

ЭКСПЕРТНЫЕ СЕРВИСЫ
- Расследование инцидентов
- Тестирование на проникновение
- Анализ защищенности приложений

Курсы «Лаборатории Касперского» по кибербезопасности ориентированы на компании, которые стремятся защитить свою инфраструктуру и интеллектуальную собственность.

КУРСЫ

ОБУЧЕНИЕ СОТРУДНИКОВ	ОБУЧЕНИЕ ЭКСПЕРТОВ	
Сотрудники	**Уровень 1, базовый**	
ОНЛАЙН-ПЛАТФОРМА	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Базовые знания в области IT	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРАКТИЧЕСКИЙ КУРС Базовые знания в области IT
Линейные руководители	**Уровень 2, средний**	
ИГРОВОЙ ФОРМАТ CYBERSAFETY	ЦИФРОВАЯ КРИМИНАЛИСТИКА Требуются навыки системного администрирования	АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА ВРЕДОНОСНОГО ПО Требуются навыки программирования
Руководители организаций	**Уровень 3, экспертный**	
ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ	ЦИФРОВАЯ КРИМИНАЛИСТИКА (ПРОФЕССИОНАЛЬНЫЙ УРОВЕНЬ) Требуются экспертные навыки системного администрирования	АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА ВРЕДОНОСНОГО ПО (ПРОФЕССИОНАЛЬНЫЙ УРОВЕНЬ) Требуются навыки программирования на языке ассемблер

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ О КИБЕРУГРОЗАХ

Интерактивные учебные онлайн-модули и обучающие игры по кибербезопасности внутри компании предназначены для всех сотрудников, которые пользуются компьютерами или мобильными устройствами.

80% всех инцидентов кибербезопасности происходят по причине человеческого фактора. Компании тратят миллионы, чтобы рассказать сотрудникам о проблемах информационной безопасности (ИБ) и научить их правильному поведению, но мало кто из руководителей соответствующих департаментов доволен результатами. Почему так получается?

Большинство тренингов по кибербезопасности продолжаются слишком долго, переполнены техническими подробностями и рисуют слишком мрачную картину мира. Такие тренинги в результате могут оказаться неэффективными.

Поэтому сегодня организации ищут комплексный подход, стимулирующий правильное поведение сотрудников (например, при помощи разработки соответствующей корпоративной культуры). Только с его помощью инвестиции в программы повышения осведомленности наконец-то начнут приносить весомую и измеримую пользу.

Курсы «Лаборатории Касперского» эффективны благодаря следующим факторам.

- Изменение поведения. Мы поощряем стремление каждого сотрудника к безопасной работе, создавая корпоративную среду, в которой каждый соблюдает правила кибербезопасности, потому что так поступают все остальные.
- Сочетание мотивирующих приемов, обучения в игровой форме, имитации атак и подробных интерактивных тренингов, формирующих навыки кибербезопасности.

ПРИНЦИПЫ РАБОТЫ

Глубина охвата и ясность изложения	Тренинг затрагивает широкий круг вопросов безопасности, освещая как причины утечки данных и особенности вирусных атак через интернет, так и принципы безопасной работы в социальных сетях. А простые упражнения помогают усваивать материал. Благодаря использованию разных методик (работа в группах, интерактивные модули, забавные комиксы и обучение в игровой форме) обучение проходит легко и увлекательно.
Постоянная мотивация	Мы создаем условия для обучения в игровой форме, поддерживая соревновательный дух, а затем в течение года закрепляем материал, моделируя атаки через интернет и проводя оценочные и образовательные активности.
Новый взгляд на ситуацию	Мы рассказываем, что мишенями киберпреступников чаще всего оказываются не машины, а живые люди, и показываем, как соблюдение правил безопасности помогает защитить себя и свое рабочее место от кибератак.
Формирование корпоративной культуры кибербезопасности	Мы готовим руководителей к роли лидеров в борьбе за безопасность на рабочем месте. Только личным примером руководства можно сформировать корпоративную среду, в которой кибербезопасность воспринимается естественно, а не как набор правил, выдуманных IT-специалистами.
Позитивный подход и совместная работа	Мы показываем, как соблюдение правил безопасности повышает эффективность работы всей организации и помогает улучшить сотрудничество с другими подразделениями, в том числе с IT-департаментом.
Измеримый эффект	Мы предоставляем инструменты для измерения навыков сотрудников и проводим оценку на корпоративном уровне, анализируя отношение персонала к кибербезопасности в повседневной работе.

ПРОГРАММА ЭКСПЕРТНОГО ОБУЧЕНИЯ В ОБЛАСТИ ИБ

Эти курсы охватывают самые разные темы и подходы, связанные с обеспечением IT-безопасности, и подразделяются на несколько категорий – от базового до экспертного уровня. Все учебные курсы проводятся в региональных офисах «Лаборатории Касперского» либо на территории заказчика.

Курсы включают как теоретические, так и практические лабораторные занятия. По завершении каждого курса все участники могут пройти тестирование и подтвердить свой уровень знаний.

УРОВНИ: БАЗОВЫЙ, СРЕДНИЙ И ЭКСПЕРТНЫЙ

Программа охватывает широкий круг вопросов: от основ информационной безопасности до цифровой криминалистики и анализа вредоносных программ. Она призвана помочь сотрудникам расширить свои знания в трех важных областях:

- основы IT-безопасности;
- цифровая криминалистика и реагирование на инциденты;
- анализ и обратная разработка вредоносного ПО.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

УРОВЕНЬ 1
Основы информационной безопасности

Администраторы и руководители, отвечающие за информационные технологии и защиту от угроз, получают базовые представления о новейших мерах по обеспечению информационной безопасности.

УРОВЕНЬ 1
Основы информационной безопасности с практическими занятиями

Углубленное изучение вопросов безопасности на практических занятиях с применением современных инструментов.

УРОВНИ 2 и 3
Цифровая криминалистика

Повышение профессионального уровня штатных специалистов, отвечающих за криминалистический анализ и реагирование на инциденты компьютерной безопасности.

УРОВНИ 2 и 3
Анализ и обратная разработка вредоносного ПО

Повышение профессионального уровня штатных специалистов, отвечающих за анализ и обратную разработку вредоносных программ.

ПРАКТИЧЕСКИЙ ОПЫТ

Работа вместе с экспертами мирового класса вдохновит участников и позволит приобрести реальный опыт обнаружения и предотвращения киберпреступлений с помощью новейших технологий.

ОПИСАНИЕ ПРОГРАММЫ

Темы	Продолжительность	Навыки
УРОВЕНЬ 1. 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 комплексные таргетированные угрозы • Основы расследования инцидентов с помощью общедоступных веб-инструментов • Безопасность рабочего места	2 дня	• Обнаружение инцидентов безопасности и выбор способа их разрешения • 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
УРОВЕНЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРАКТИЧЕСКИМИ ЗАНЯТИЯМИ		
• Основы ИБ • Использование общедоступных источников для сбора и анализа информации • Безопасность корпоративной сети • Безопасность приложений и защита от эксплойтов • DDoS-атаки • Безопасность беспроводных сетей и мобильных сетей • Угрозы для банкинга и мобильных устройств • Реагирование на инциденты безопасности в облачной и виртуальной среде	5 дней	• Простые расследования с использованием общедоступных ресурсов, специализированных поисковых систем и социальных сетей • Создание периметра безопасности сети • Базовые навыки тестирования на проникновение • Изучение трафика для обнаружения атак различного типа • Соблюдение безопасности при разработке ПО • Обнаружение инъекций вредоносного кода • Проведение базовых процедур цифровой криминалистики и анализа вредоносного ПО
УРОВЕНЬ 2. 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
УРОВЕНЬ 2. 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 PE-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 PE-файлов (Batchfiles, Autoit, Python, Jscript®, JavaScript, VBS)	5 дней	• Построение безопасной среды для анализа вредоносных программ: развертывание «песочницы» и всех необходимых инструментов • Понимание принципов исполнения программ в ОС Windows • Распаковка, отладка и анализ вредоносного объекта, определение его функций • Обнаружение вредоносных сайтов путем анализа вредоносных скриптов • Проведение экспресс-анализа вредоносного ПО
УРОВЕНЬ 3. ЭКСПЕРТНАЯ ЦИФРОВАЯ КРИМИНАЛИСТИКА		
• 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 • Выявление вредоносных программ по дампам памяти • Восстановление хронологии инцидента
УРОВЕНЬ 3. АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА КОМПЛЕКСНОГО ВРЕДОНОСНОГО ПО		
• Цели и методы анализа и обратной разработки вредоносного ПО • Методы расширенного статического и динамического анализа (ручная распаковка) • Методы деобфускации • Анализ руткитов и буткитов • Анализ эксплойтов (файлы pdf, doc, swf и др.) • Анализ вредоносного ПО для Android™, Linux®, Mac OS®	5 дней	• Использование передовых методов обратной разработки • Распознавание методов защиты от обратной разработки (обфускация, защита от отладки) • Расширенный анализ руткитов и буткитов • Анализ шелл-кода эксплойтов, внедренного в различные виды файлов • Анализ вредоносного ПО для сред, отличных от Windows

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ

Наблюдать за постоянно развивающимися киберугрозами, анализировать их, вовремя реагировать на атаки и сводить к минимуму их последствия – процесс чрезвычайно трудоемкий. Современные организации сталкиваются с нехваткой актуальных и оперативно обновляемых сведений об угрозах IT-безопасности во всех отраслях – а недостаток таких данных усложняет управление соответствующими рисками.

Информационные сервисы «Лаборатории Касперского» дают доступ к информации об угрозах, полученной нашими аналитиками и исследователями мирового класса. Такие данные помогут любой организации выстроить защиту от киберугроз.

«Лаборатория Касперского» обладает глубокими знаниями, богатым опытом и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому компания стала доверенным партнером наиболее влиятельных правоохранительных и правительственных организаций по всему миру, в их число входит Интерпол и подразделения CERT. Вы можете использовать весь этот потенциал для повышения уровня IT-безопасности вашей компании.

Сервисы «Лаборатории Касперского» для анализа угроз предоставляют:

- Потоки данных об угрозах
- Мониторинг ботнет-угроз
- Аналитические отчеты

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ

- Программа повышения осведомленности о киберугрозах
- Программа экспертного обучения в области ИБ

СЕРВИСЫ ИНФОРМИРОВАНИЯ ОБ УГРОЗАХ

- Потоки данных об угрозах
- Мониторинг ботнет-угроз
- Аналитические отчеты

ЭКСПЕРТНЫЕ СЕРВИСЫ

- Расследование инцидентов
- Тестирование на проникновение
- Анализ защищенности приложений

ПОТОКИ ДАННЫХ ОБ УГРОЗАХ

Дополните свои решения для защиты сети постоянно обновляемыми аналитическими данными о киберугрозах и целевых атаках. Такими решениями являются системы SIEM, сетевые экраны, системы обнаружения и предотвращения вторжений, технологии противодействия комплексным таргетированным угрозам (Advanced Persistent Threat – APT-угрозы) и среда моделирования («песочница»).

В последние годы число новых семейств и разновидностей вредоносного ПО стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Чтобы защитить рабочие места от этих угроз, большинство организаций используют классические средства – антивирусные решения и системы предотвращения вторжений и обнаружения угроз. В динамично меняющихся условиях, когда сотрудники отделов IT-безопасности пытаются делать все, чтобы хоть на шаг опережать киберпреступников, для эффективной работы этих классических решений необходим доступ к самым актуальным сведениям об угрозах.

Данные об угрозах, предоставляемые «Лабораторией Касперского», интегрируются в существующие системы управления данными и инцидентами безопасности (SIEM), образуя дополнительный уровень защиты. Интеграция данных об угрозах позволяет сопоставлять журналы, поступающие в SIEM-систему от разных устройств сети, со сведениями об опасных URL-ссылках, предоставляемыми «Лабораторией Касперского». Поддерживается интеграция с системой SIEM HP ArcSight. Также доступны соединительные модули для Splunk® и QRadar®.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ И ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Данные об угрозах, предоставляемые «Лабораторией Касперского»:

- дополняют решение SIEM информацией о вредоносных URL-адресах. В SIEM-систему поступают уведомления о вредоносных и фишинговых URL-ссылках, а также URL-адресах командных серверов ботнетов, содержащихся в журналах, которые передаются в SIEM с различных устройств сети (компьютеров пользователей, прокси-серверов, сетевых экранов и других серверов);
- с помощью постоянно обновляемых аналитических данных об угрозах повышают эффективность основных решений для защиты сети, таких как сетевые экраны, системы обнаружения и предотвращения вторжений, системы SIEM, технологии противодействия APT-угрозам, среды моделирования («песочницы»), UTM-устройства и т. д.;
- расширяют возможности экспертного анализа, предоставляя службе безопасности ценную информацию об угрозах и возможность раскрыть структуру целевых атак;
- поддерживают исследовательскую работу. Сведения о вредоносных URL-адресах и MD5-хэши вредоносных файлов служат весомым вкладом в проекты исследования угроз.

«Лаборатория Касперского» предлагает три типа данных об угрозах:

1) вредоносные URL-адреса и маски;
2) база MD5-хэшей вредоносных объектов;
3) данные об угрозах для мобильных устройств.

ОПИСАНИЕ ТИПОВ ДАННЫХ

URL-адреса вредоносных ссылок – набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.

URL-адреса фишинговых ссылок – набор URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок.

URL-адреса командных серверов ботнетов – набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.

Хэши вредоносных объектов (ITW) – набор файловых хэшей и соответствующих вердиктов, охватывающий наиболее опасные и распространенные вредоносные программы, с которыми сталкивались пользователи сети KSN.

Хэши вредоносных объектов (UDS) – набор файловых хэшей, обнаруженных облачными технологиями «Лаборатории Касперского» (аббревиатура UDS обозначает систему мгновенного обнаружения) по метаданным файла и статистическим данным (без доступа к самому объекту). Такой подход позволяет выявлять новые, только что появившиеся, вредоносные объекты («нулевого дня»), которые нельзя обнаружить другими методами.

Хэши вредоносных объектов для мобильных устройств – набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства.

Данные о троянцах P-SMS – набор хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать сообщения, отвечать на них и удалять их.

URL-адреса командных серверов ботнетов – набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, в том числе мобильных.

МОНИТОРИНГ БОТНЕТ-УГРОЗ

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

Многие сетевые атаки проводятся с использованием ботнетов. Такие атаки могут угрожать обычным пользователям, но чаще нацелены на конкретные организации и их онлайн-пользователей.

Экспертное решение «Лаборатории Касперского» отслеживает активность ботнетов и оперативно (в течение 15 минут) предоставляет уведомления об угрозах, направленных против пользователей платежных и банковских систем. Располагая этими сведениями, вы сможете информировать своих онлайн-пользователей, поставщиков услуг по обеспечению безопасности и правоохранительные органы об актуальных угрозах. Сервис «Лаборатории Касперского» по мониторингу ботнет-угроз поможет вам сохранить репутацию и защитить онлайн-пользователей вашей организации.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ И ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

- 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 онлайн-пользователей, 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.

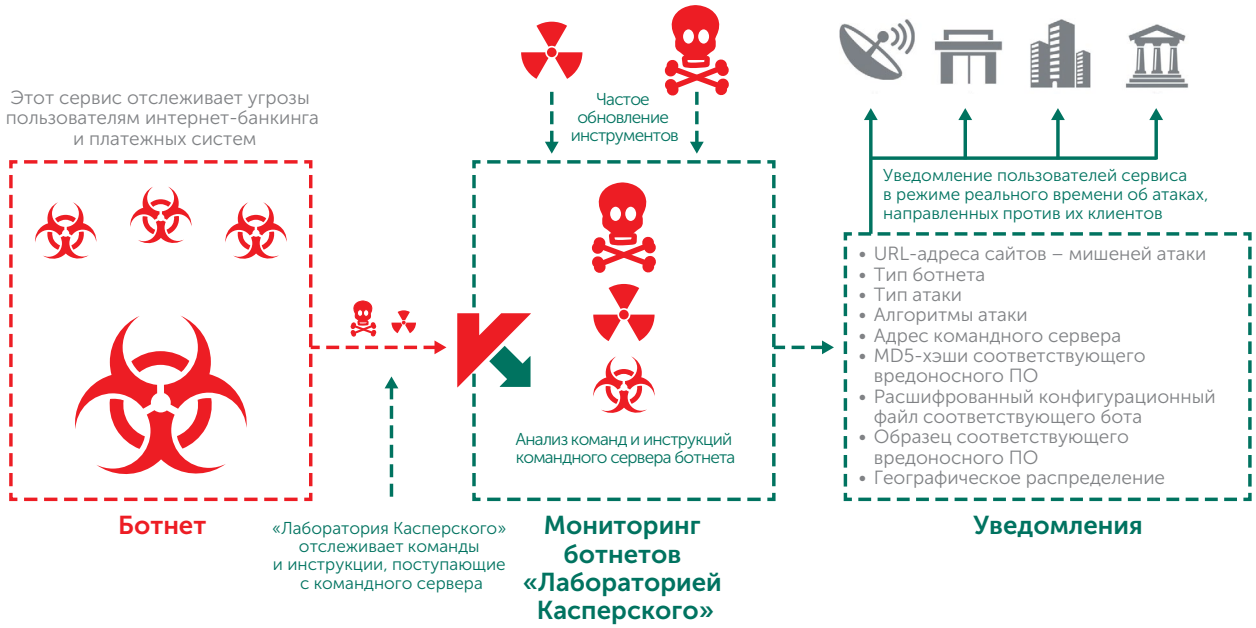
ЗАЩИТИТЕ СВОИХ ОНЛАЙН-ПОЛЬЗОВАТЕЛЕЙ, ОПИРАЯСЬ НА ДАННЫЕ, ПОСТУПАЮЩИЕ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

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

- **URL-адрес цели ботнета**. Вредоносное ПО активизируется и запускает алгоритм атаки в тот момент, когда пользователь посещает сайт атакуемой ботнетом организации.
- **Тип ботнета**. Наименование вредоносного ПО, используемого киберпреступниками для перехвата транзакций клиентов. Типами такого ПО могут быть, например, ZeuS, SpyEye, Citadel.
- **Тип атаки**. Информация о том, каким образом преступники используют вредоносное ПО. Варианты могут включать веб-инъекцию, снятие скриншотов, захват видеоизображения или переадресацию на фишинговый URL-адрес.
- **Алгоритмы атаки**. Сведения об использованном алгоритме инъекции веб-кода: HTML-запросы (GET/POST), данные на веб-странице до и после инъекции и др.
- **Адрес командного сервера**. Уведомив интернет-провайдеров о сервере управления ботнетом, можно оперативнее изолировать угрозу.
- **MD5-хэши вредоносного ПО**. «Лаборатория Касперского» предоставляет хэши для идентификации вредоносного ПО.
- **Расшифрованный конфигурационный файл соответствующего бота**. Полный список адресов целей (по запросу).
- **Географическое распределение (ТОП-10 стран)**. Статистические данные по глобальному распределению образцов соответствующего вредоносного ПО.

МОНИТОРИНГ БОТНЕТ-УГРОЗ: АРХИТЕКТУРА

ОТ КОМАНДНОГО СЕРВЕРА



Предлагаются варианты подписки на сервисы «Лаборатории Касперского» Standard и Premium с различными условиями предоставления услуг и набором отслеживаемых URL-адресов. Обратитесь в «Лабораторию Касперского» или к партнеру, чтобы определить, какой вариант подходит вашей организации.

УРОВНИ ПОДПИСКИ И ПРЕДОСТАВЛЯЕМАЯ ИНФОРМАЦИЯ

PREMIUM

Уведомления по электронной почте или в формате JSON

10 отслеживаемых URL-адресов

- Расшифрованный конфигурационный файл соответствующего бота
- Образец соответствующего вредоносного ПО (по запросу)
- Географическое распределение обнаруженных образцов вредоносного ПО

STANDARD

Уведомления по электронной почте

5 отслеживаемых URL-адресов

- URL сайта-мишени (при посещении которого пользователем программа-бот начинает атаку)
- Тип ботнета (Zeus, SpyEye, Citadel, Kins и т. д.)
- Тип атаки
- Алгоритмы атаки: веб-инъекция, URL-ссылки, снимки экрана, запись видео и т. д.
- Адрес командного центра
- MD5-хэши соответствующего вредоносного ПО

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

Детальные аналитические отчеты «Лаборатории Касперского» повысят осведомленность о масштабных кампаниях кибершпионажа, а также об угрозах, направленных против конкретных организаций.

Информация из этих отчетов и предоставляемые «Лабораторией Касперского» инструменты помогут быстро отреагировать на новые угрозы и уязвимости: заблокировать атаки с известных направлений, уменьшить ущерб от комплексных атак и усовершенствовать стратегию безопасности как вашей организации, так и ваших клиентов.

ОТЧЕТЫ О КОМПЛЕКСНЫХ ТАРГЕТИРОВАННЫХ УГРОЗАХ

Иногда информация об обнаружении комплексных таргетированных угроз (Advanced Persistent Threat – APT) не становится публичной. Наши подробные отчеты позволят вам в числе первых получать эксклюзивные данные о новых APT-угрозах.

Подписчики на такие отчеты при первой возможности получают уникальный доступ к результатам расследования и техническим данным в различных форматах по каждой APT-угрозе – в том числе по тем угрозам, информация о которых никогда не будет опубликована.

Наши эксперты, профессиональные и успешные «охотники» на APT-угрозы, немедленно оповестят вас о любых обнаруженных изменениях в тактике киберпреступников и кибертеррористов. Вы также получите доступ к полной базе отчетов «Лаборатории Касперского» о комплексных таргетированных угрозах, которая дополнит ваш арсенал для борьбы с киберугрозами.

ОТЧЕТЫ «ЛАБОРАТОРИИ КАСПЕРСКОГО» ОБ APT-УГРОЗАХ ПРЕДОСТАВЛЯЮТ:

- **Эксклюзивный доступ** к техническим описаниям новейших угроз уже в ходе их расследования, еще до публичного объявления.
- **Непубличные APT-отчеты**. Не обо всех масштабных угрозах сообщается публично. Некоторые угрозы так и остаются тайной из-за специфики своих жертв, 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 (Indicators of Compromise – IOC), доступные в стандартных форматах, включая openIOC и STIX, и Yara Rules.
- **Непрерывный мониторинг APT-кампаний**. Доступ к ценным аналитическим данным в ходе расследования (информация о распространении APT-угрозы, индикаторы компрометации, инфраструктура командных центров).
- **Ретроспективный анализ**. В течение всего периода подписки предоставляется доступ ко всем ранее выпущенным закрытым отчетам.

ПРИМЕЧАНИЕ ОБ ОГРАНИЧЕНИИ ПОДПИСКИ

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

Как лучше всего атаковать любую организацию? Какие векторы атаки и какие сведения доступны злоумышленнику, который решил атаковать ту или иную компанию? Возможно, атака уже организована, но об этом никто не знает?

КАСТОМИЗИРОВАННЫЕ АНАЛИТИЧЕСКИЕ ОТЧЕТЫ ОБ УГРОЗАХ

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

Эти уникальные данные позволят вам сконцентрироваться на уязвимостях, которые больше всего интересуют киберпреступников, и действовать быстро и точно, чтобы отразить вторжение и свести к минимуму риск успешной атаки.

Кастомизированные отчеты составляются с использованием общедоступных источников для сбора и анализа информации (OSINT), мощных экспертных систем и баз «Лаборатории Касперского» и наших данных о подпольных преступных сетях. В отчетах рассматриваются следующие вопросы.

- **Определение векторов угроз**. Выявление и анализ состояния критических компонентов сети, доступных извне, включая банкоматы, системы видеонаблюдения, телекоммуникационное оборудование и другие виды систем, а также профили сотрудников в социальных сетях и учетные записи электронной почты. Все эти компоненты являются уязвимыми для потенциальной атаки.
- **Анализ отслеживания вредоносных программ и кибератак**. Выявление, мониторинг и анализ активных и неактивных образцов вредоносного ПО, нацеленного именно на исследуемую организацию, а также исторических данных и текущей активности ботнетов и любой другой подозрительной сетевой активности.
- **Атаки на третьи стороны**. Признаки угроз и активности ботнетов, направленной на ваших клиентов, партнеров и абонентов. Их зараженные системы могут стать источником атаки уже на вашу компанию.
- **Утечка информации**. Ведя скрытое наблюдение за обсуждениями на подпольных интернет-форумах и в сообществах, мы можем распознать планы атаки на вашу компанию, а также выявить нечистоплотных сотрудников, которые могут продавать злоумышленникам ценную информацию.
- **Текущее состояние атаки**. APT-угрозы могут оставаться незамеченными в течение многих лет. Если мы обнаруживаем, что вашу инфраструктуру уже атакуют, то даем рекомендации по эффективному реагированию на атаку.

БЫСТРО. УДОБНО. БЕЗ ДОПОЛНИТЕЛЬНЫХ РЕСУРСОВ

Определив параметры специализированных отчетов и предпочтительных форматов данных, вы сможете пользоваться этим сервисом «Лаборатории Касперского», не прибегая к созданию дополнительной инфраструктуры.

Для подготовки аналитических отчетов «Лаборатории Касперского» не используются активные методы анализа, таким образом, сервис не влияет на целостность и доступность ресурсов исследуемой компании.

ЭКСПЕРТНЫЕ СЕРВИСЫ

Экспертные сервисы «Лаборатории Касперского» – это услуги специалистов компании, многие из них являются признанными во всем мире профессионалами, знания и опыт которых служат опорой нашей репутации мирового лидера в области анализа угроз.

Каждая IT-инфраструктура уникальна, а самые опасные атаки специально разрабатываются с учетом уязвимостей конкретной организации. Поэтому и мы при оказании экспертных сервисов индивидуально подходим к каждому клиенту. На следующих страницах описаны сервисы, входящие в наш профессиональный пакет. Работая с вами, мы можем полностью или частично предоставлять их в любом сочетании.

«Лаборатория Касперского» стремится в первую очередь стать личным консультантом, который поможет вам оценить степень риска, усилить безопасность и уменьшить возможные последствия атак в будущем.

Предоставляемые экспертные сервисы:

- расследование инцидентов
- тестирование на проникновение
- анализ защищенности приложений

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Цифровая криминалистика | Анализ вредоносного ПО

Индивидуальная помощь в расследовании инцидентов поможет вашей организации выявить и разрешить инциденты в сфере IT-безопасности.

Кибератаки становятся все более серьезной угрозой для сетей крупных предприятий. Злоумышленники подбирают эксплойты, использующие конкретные уязвимости в системе жертвы. Целью чаще всего становится кража или уничтожение конфиденциальной информации или объектов интеллектуальной собственности, остановка бизнес-процессов, повреждение промышленных систем или хищение денежных средств.

Защитить крупную компанию от таких изощренных, тщательно спланированных атак с каждым днем становится все сложнее. В некоторых случаях даже опытным IT-специалистам трудно определить, является ли их организация объектом атаки.

Сервис «Лаборатории Касперского» по расследованию инцидентов помогает компании-клиенту сформировать собственную стратегию защиты. Для этого мы тщательно проводим постинцидентный анализ и даем практические рекомендации по устранению каждого инцидента.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

Сервис «Лаборатории Касперского» по расследованию инцидентов помогает разрешить актуальные проблемы безопасности, узнать об особенностях поведения вредоносного ПО и последствиях заражения, а также получить практические рекомендации по восстановлению нормальной работы систем. Такой подход позволяет организациям:

- снижать затраты на решение проблем, связанных с заражением вредоносным ПО;
- предотвращать или останавливать возможную утечку конфиденциальной информации с зараженных устройств;
- снижать репутационные риски, связанные с нарушением нормальной работы организации в результате заражения;
- восстановить нормальную работу устройств, нарушенную в результате заражения.

Расследования в «Лаборатории Касперского» ведут опытные аналитики, имеющие большой практический опыт и знания в области цифровой криминалистики и анализа вредоносного ПО. По завершении расследования клиенту предоставляется подробный отчет с полной информацией о результатах расследования и предлагаемой программой действий для восстановления нормальной работы всех систем.

ЦИФРОВАЯ КРИМИНАЛИСТИКА

Цифровая криминалистика – это сервис, позволяющий клиентам с помощью экспертов «Лаборатории Касперского» получить более полное представление об инциденте. Если в ходе расследования инцидента было обнаружено вредоносное ПО, эксперты проведут его анализ. Чтобы воссоздать полную картину инцидента, специалисты «Лаборатории Касперского» анализируют различные исходные данные: образы жестких дисков, дампы памяти, трассировки сети и др.

Клиент начинает процесс расследования, собирая улики и предоставляя описание инцидента. Эксперты «Лаборатории Касперского» изучают особенности инцидента, в том числе идентифицируют исполняемые файлы вредоносных программ (если они есть) и проводят анализ вредоносного ПО. Клиенту предоставляется подробный отчет, содержащий в том числе меры, необходимые для устранения последствий инцидента.

АНАЛИЗ ВРЕДОНОСНОГО ПО

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

Эксперты «Лаборатории Касперского» осуществляют всесторонний анализ вредоносного образца, предоставленного вашей организацией, и составляют подробный отчет, в частности содержащий представленную ниже информацию.

- **Свойства образца**. Краткое описание и вердикт согласно классификации «Лаборатории Касперского».
- **Подробное описание вредоносного ПО**. Углубленный анализ функций, поведения и целей вредоносной программы, включая индикаторы заражения, а также вся информация, необходимая для нейтрализации угрозы.
- **Сценарий восстановления системы**. В отчете будут предложены шаги по устранению последствий заражения.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

Сервис «Лаборатории Касперского» по расследованию инцидентов может предоставляться:

- по подписке, предусматривающей расследование определенного числа инцидентов;
- как расследование единичного инцидента.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Надежная защита IT-инфраструктуры от потенциальных кибератак – актуальная проблема в любой организации. Особенно сложной эта задача становится для крупных предприятий, где в подразделениях, разбросанных по всему земному шару, работают тысячи сотрудников и используются сотни информационных систем.

IT-специалисты и сотрудники отдела безопасности вашей организации упорно работают над тем, чтобы обеспечить защиту каждого компонента сети от злоумышленников, но при этом не затруднять доступ к ресурсам для своих пользователей. Однако киберпреступнику может оказаться достаточно одной-единственной неустраненной уязвимости, чтобы перехватить управление вашими информационными системами.

Тестирование на проникновение – это практическая демонстрация возможных сценариев атаки, позволяющих злоумышленнику обойти средства безопасности корпоративной сети, чтобы получить высокий уровень доступа к важным системам.

«Лаборатория Касперского» предоставляет сервис тестирования на проникновение, который 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, проводимое «Лабораторией Касперского», поможет вашей организации:

- выявить наиболее уязвимые места в сети,
- снизить риски, перераспределив ресурсы;
- избежать финансовых, операционных и репутационных потерь, вызванных кибератаками. Заблаговременное обнаружение и устранение уязвимостей сделает многие атаки просто невозможными;
- выполнить требования государственных, отраслевых или внутренних корпоративных стандартов, предусматривающих подобную форму оценки системы безопасности, например стандарта безопасности данных индустрии платежных карт (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 со стороны сети 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 состояние безопасности сетей Wi-Fi.

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.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Сервис тестирования на проникновение позволяет выявить бреши в системе безопасности, которыми злоумышленники могут воспользоваться для получения несанкционированного доступа к важным компонентам сети. Такими брешами могут выступать:

- уязвимая архитектура сети, ошибки конфигурации сетевого оборудования;
- уязвимости, делающие возможным перехват и перенаправление сетевого трафика;
- ошибки аутентификации и авторизации в различных службах;
- ненадежные пароли пользователей;
- недостатки конфигурации, в том числе предоставление пользователям слишком высоких полномочий;
- уязвимости, вызванные ошибками в коде приложений (внедрение операторов SQL, удаленное выполнение кода, загрузка произвольных файлов, межсайтовое выполнение сценариев и т. д.);
- уязвимости, вызванные использованием устаревших версий оборудования и программного обеспечения, для которых не были установлены последние обновления безопасности;
- разглашение информации.

По окончании работ у вас на руках окажется итоговый отчет с подробной технической информацией о ходе тестирования, его результатах и обнаруженных уязвимостях. В отчете также присутствуют рекомендации по устранению уязвимостей, наглядные иллюстрации направлений атак и выводы, резюмирующие результаты тестирования. В случае необходимости дополнительно могут быть подготовлены видеоматериалы и презентации для технических подразделений или для руководства.

ПОДХОД «ЛАБОРАТОРИИ КАСПЕРСКОГО» К ТЕСТИРОВАНИЯМ НА ПРОНИКНОВЕНИЕ

В рамках тестирования на проникновение имитируются настоящие кибератаки. При этом ситуация остается под полным контролем экспертов по безопасности «Лаборатории Касперского», которые уважают конфиденциальность ваших систем и не нарушают их целостность и доступность. Мы строго следуем международным стандартам и лучшим мировым практикам, 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 обширными и актуальными практическими знаниями. Наши эксперты известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших сервисах и программных продуктах, включая Oracle®, Google™, Apple®, Microsoft, Facebook, Pay Pal, Siemens и SAP®.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В зависимости от выбранного метода анализа защищенности, особенностей систем и бизнеса клиента сервис тестирования на проникновения может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно (так, внутреннее тестирование можно организовать через VPN-доступ), однако для оценки безопасности беспроводных сетей и ряда других задач необходимо присутствие специалистов на вашей территории.

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ

Вы можете разрабатывать корпоративные приложения самостоятельно или приобретать их у сторонних поставщиков, но в любом случае даже одной ошибки в программном коде может быть достаточно, чтобы создать уязвимость для атак, которые приводят к значительным финансовым или репутационным потерям. Новые уязвимости могут также появиться в течение жизненного цикла приложения: в ходе обновления или из-за неправильной настройки компонентов. Кроме того, с течением времени появляются и новые способы атак, перед которыми система может оказаться уязвимой.

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», позволяет выявить уязвимости в приложениях любого типа – от крупных облачных решений, ERP-систем, систем дистанционного банковского обслуживания и других бизнес-приложений до встроенных приложений и мобильных решений для различных платформ (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:

- похищение 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;
- **сэкономить на устранении последствий,** обнаруживая уязвимости в приложениях на этапах разработки и тестирования, до внедрения системы в продуктивную среду, где 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.

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 сервиса подбирается индивидуально в соответствии с вашими потребностями и особенностями приложений. Он может включать:

- **анализ защищенности методом «черного ящика»**. Имитируются действия злоумышленника, действующего извне;
- **анализ защищенности «серого ящика»**. Имитируются действия внутренних пользователей с различным уровнем доступа;
- **анализ защищенности «белого ящика»**. Анализ с полным доступом к приложению, включая исходный код. Этот подход наиболее эффективен с точки зрения количества обнаруживаемых уязвимостей;

- **оценка 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.

РЕЗУЛЬТАТЫ

Сервис анализа защищенности приложений, предлагаемый «Лабораторией Касперского», может обнаружить следующие уязвимости:

- недостатки аутентификации и авторизации, в том числе ошибки реализации двухфакторной аутентификации;
- инъекции кода (внедрение операторов SQL-инъекции, выполнение команд ОС и т. д.);
- уязвимости логики приложения, которые могут использоваться в мошеннических целях;
- уязвимости, приводящие к атакам на пользователей приложения (межсайтовое выполнение сценариев, подделка межсайтовых запросов и т. д.);
- использование слабых криптографических алгоритмов;
- уязвимости при обмене данными между клиентом и сервером;
- незащищенное хранение или передача данных, например отсутствие маскировки номеров PAN в платежных системах;
- ошибки конфигурации, в том числе делающие возможными атаки на сессии пользователей;
- раскрытие конфиденциальной информации;
- другие уязвимости в веб-приложениях, которые позволяют реализовать угрозы, перечисленные в классификации угроз WASC 2.0 и OWASP Top Ten.

Результаты работ представляются в виде итогового отчета с подробной технической информацией об обнаруженных уязвимостях и рекомендациями по их устранению, а также краткими выводами об уровне защищенности приложения. Кроме того, в случае необходимости могут быть подготовлены видеоматериалы и презентации для технических подразделений или руководства.

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.

«Лаборатория Касперского» строго следует международным стандартам и лучшим мировым практикам, среди которых:

- Web Application Security Consortium (WASC) Threat
- Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide

Специалисты, проводящие работы, – опытные профессионалы, обладающие обширными и актуальными практическими знаниями для различных платформ, языков программирования и методов атак. Они выступают на ведущих 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, PayPal.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

В зависимости от метода анализа защищенности, особенностей тестируемой системы и требований клиента к условиям работы сервис анализа защищенности приложений может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно.

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для бизнеса:
www.kaspersky.ru/enterprise

+7 (495) 737-34-12
sales@kaspersky.com

Чтобы получить подробную информацию о продуктах и сервисах, описанных в данном документе, или узнать, как эти сервисы помогут усилить безопасность вашей организации, обращайтесь по адресу intelligence@kaspersky.com.

Условия предоставления сервисов, в том числе объем работ, сроки, доступность местных служб, язык предоставления сервисов и стоимость, зависят от региона.

KASPERSKY lab