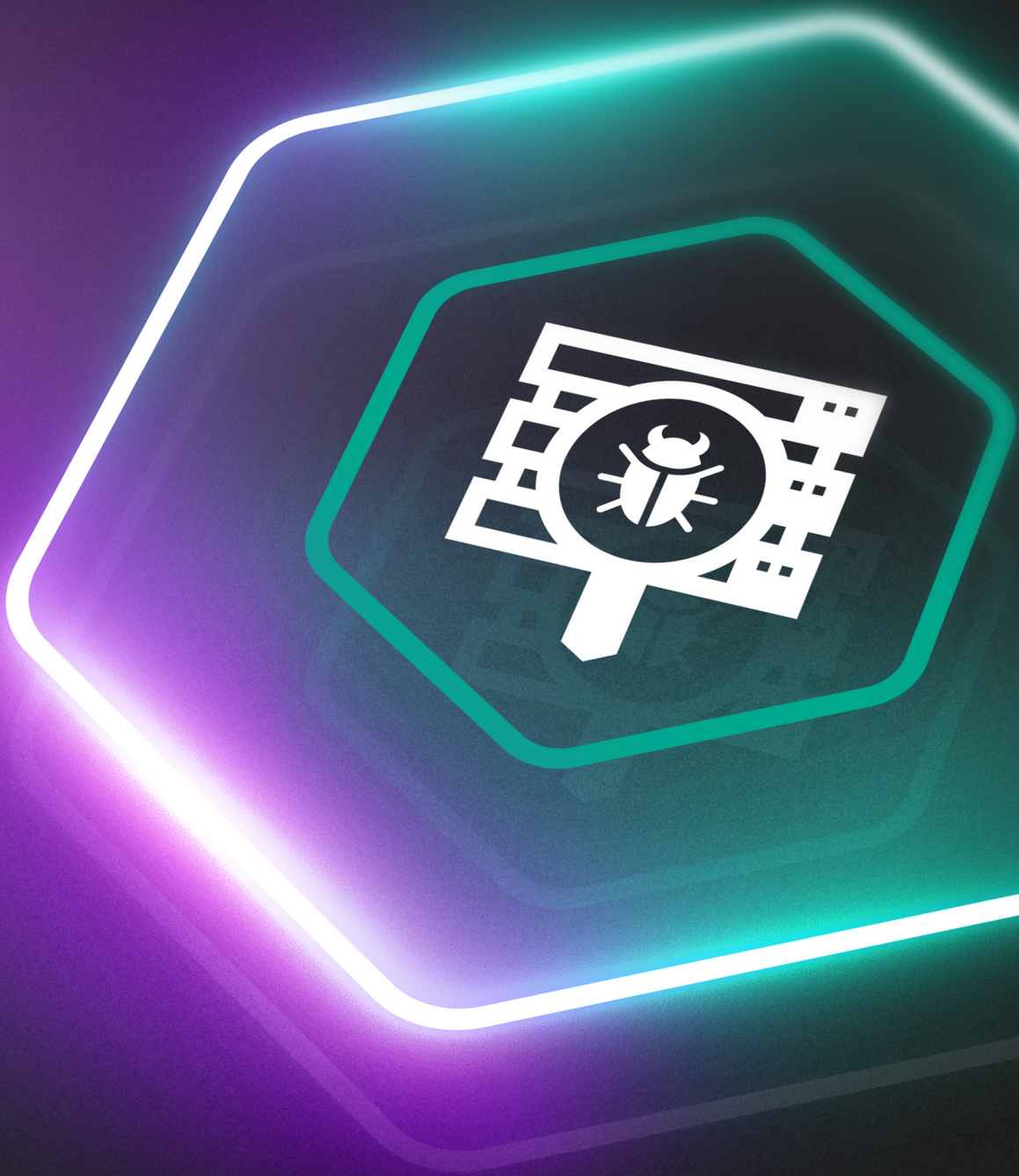

Kaspersky Compromise Assessment

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Что такое Kaspersky Compromise Assessment?

Сервис Kaspersky Compromise Assessment позволит выявить активные кибератаки и ранее неизвестные угрозы, которым удалось обойти используемые средства защиты информации, а также обнаружить следы прошлых взломов.

В рамках сервиса мы проведем комплексный независимый анализ вашей инфраструктуры на предмет следов компрометации, а выявленные инциденты будут валидированы для минимизации риска ложных оповещений. Кроме того, мы поможем организовать эффективное реагирование на выявленные инциденты.

Когда вам потребуется оценка компрометации?

- У вас нет явных подтверждений инцидента, однако есть информация, что вероятность компрометации именно сейчас высока, например:
  - стало известно, что атакована сеть партнера;
  - из достоверных источников известно, что участились атаки на ваш сектор экономики, и многие организации подверглись компрометации;
  - появилась непроверенная информация, что ваша сеть скомпрометирована и это надо проверить.
- Есть требование регулятора проводить такого рода работы на регулярной основе;
- В рамках проекта слияния и поглощения есть необходимость получить независимую экспертную оценку, что интегрируемая инфраструктура не скомпрометирована;
- У вас проводилось полноценное реагирование на инцидент, однако есть необходимость удостовериться, что сеть не взломана другими группировками, использующими иные техники и инструменты.

Киберпреступники каждый день применяют в атаках по 400 000 новых вредоносных файлов

Как работает сервис Kaspersky Compromise Assessment

Проект по оценке компрометации состоит из нескольких этапов:

Сбор данных

Мы сканируем все ваши конечные точки, собираем метаданные для криминалистического анализа и данные журналов безопасности, чтобы обнаружить признаки компрометации. Кроме того, мы собираем журналы систем безопасности сетевого периметра, журналы контроля выхода в Интернет, а при наличии Active Directory – журналы контроллеров домена.

Дополнительно наши эксперты анализируют данные из многочисленных источников, чтобы оценить ландшафт угроз, характерный для вашей организации, включая сведения об APT-группах, действующих в вашей отрасли и\или регионе.

Устранение последствий и отчетность

Мы подготовим итоговый отчет с подробными ответами на следующие вопросы:

- **Нарушена ли безопасность ваших информационных систем?**
  Мы предоставим общие данные, подтверждающие наличие или отсутствие признаков компрометации в вашей сети.
- **Если компрометация имела место, то где и каковы ее следы?**
  Вы получите описание обнаруженных инцидентов в каждом из которых будет предоставлен перечень затронутых систем и выявленных следов компрометации.
- **Что делать дальше?**
  По каждому выявленному инциденту мы дадим рекомендации по реагированию, а также подскажем как защитить свою сеть от аналогичных атак в будущем.

Анализ и Активный поиск угроз

Собранные данные мы обрабатываем и выявляем инциденты в вашей сети. Анализ – многоэтапный процесс, выполняемый на разных стадиях обработки данных (непосредственно на конечных точках, на серверах инфраструктуры сбора и анализа данных), включающий как автоматическое и автоматизированное обнаружение атак(в том числе и с использованием технологий машинного обучения), так и анализ данных вручную непосредственно экспертом.

Некоторые из выявленных инцидентов не требуют дополнительной проверки (например, заражение вредоносным ПО), в этом случае вы сразу же получите рекомендации по реагированию. Другие же необходимо дополнительно валидировать (например, подозрительное поведение пользователя).

Валидация инцидента и раннее реагирование

Для подтверждения серьезных инцидентов и углубленного анализа могут потребоваться дополнительные данные, например, образ скомпрометированной системы, исполняемый бинарный файл или скрипт.

Кроме того, в рамках сервиса может быть организовано срочное реагирование, например, для целей локализации атаки, если такая необходимость будет установлена на этапе анализа.

Результаты Kaspersky Compromise Assessment

По результатам работы сервиса вы получите:

1

Заключение о компрометации вашей сети в данный момент и ранее

2

Аналитические данные об угрозах и индикаторы компрометации (IoC)

3

Рекомендации по устранению последствий и по защите своих ресурсов от аналогичных атак в будущем

Преимущества «Лаборатории Касперского»

Международное признание

«Лаборатория Касперского» активно участвует в независимых тестированиях со многими игроками на рынке и взаимодействует с ведущими аналитическими агентствами. Наши технологии и продукты признаны во всем мире и удостоены многочисленных международных наград.

Актуальные данные об угрозах

Мы анализируем данные об угрозах со всего мира и для быстрого обнаружения составили обширную базу источников угроз.

Адаптивные инструменты и телеметрия

Для обнаружения угроз мы используем индикаторы компрометации (IoC), информацию о тактиках, техниках и процедурах (TTP) злоумышленников, YARA-правила и обширные аналитические данные об угрозах. Мы можем быстро адаптировать правила обнаружения, инструменты и телеметрию к меняющемуся ландшафту угроз, для этих целей мы широко применяем технологии машинного обучения и искусственного интеллекта.

Цифры говорят больше слов

>400 млн

пользователей по всему миру используют наши решения по обеспечению информационной безопасности

>360 тыс

уникальных вредоносных объектов мы обнаруживаем каждый день

>240 тыс

компаний по всему миру мы защищаем от киберугроз

Kaspersky Compromise Assessment

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее