



Kaspersky
Compromise
Assessment

Выявляйте скрытые киберугрозы, прежде чем они нанесут ущерб

~ 22 %

атак остаются незамеченными в течение 135 дней*

Последствия атак, обнаруженных в течение нескольких часов, устраняются за считанные минуты. Если же атака оставалась незамеченной месяцами, ее устранение займет*

> 46 часов



Согласно статистике MDR-инцидентов, после целевой атаки киберпреступники часто возвращаются на место преступления**

Сегодня организации сталкиваются не только с внешними рисками, но и со скрытыми угрозами внутри своей инфраструктуры. Признаки компрометации не всегда очевидны, и надежный способ их обнаружить – провести оценку компрометации (Compromise Assessment).

Kaspersky Compromise Assessment будет полезен вашей организации, если:

- Вы подозреваете компрометацию вашей сети, но не имеете явных доказательств
- Ваш бизнес-партнер подвергся кибератаке
- Вы находитесь в процессе слияния и поглощения
- По данным аналитики угроз (TI), в вашем регионе или отрасли высокие риски атак
- Вы расследуете состоявшуюся целенаправленную атаку и хотите выяснить, не вернулись ли атакующие
- Вам необходимо регулярно проводить оценку компрометации в соответствии с нормативными требованиями

Сервис Kaspersky Compromise Assessment (CA) обнаруживает активные кибератаки и ранее неизвестные угрозы, которым удалось обойти имеющиеся средства и процессы информационной безопасности. Цель сервиса – предоставить независимую экспертную оценку уровня безопасности и дать четкий ответ на вопрос не была ли скомпрометирована ваша сеть.

Как работает сервис Kaspersky Compromise Assessment



Сбор данных

Метаданные для цифровой криминалистики со всех хостов

Журналы SIEM и данные Active Directory

Поиск в Даркнете

Аналитика угроз

Мы всесторонне изучаем вашу инфраструктуру.

- Сканируем хосты и собираем метаданные для форензики
- Анализируем журналы SIEM-систем
- Исследуем конфигурацию Active Directory
- Ищем утечки учетных данных в Даркнете

Актуальные данные



Проактивный поиск угроз

Мы проводим автоматизированный и ручной поиск угроз на основе всех собранных данных и телеметрии. Для этого используем передовые технологии и уникальные данные Threat Intelligence от опытных сертифицированных консультантов.

Выявляем инциденты безопасности в вашей сети и предоставляем рекомендации по реагированию.

Инциденты



Валидация инцидентов

Для подтверждения обнаруженных инцидентов наши специалисты проводят криминалистическое расследование и анализ вредоносного ПО.

Мы используем эффективные инструменты для локализации инцидента и сдерживания угроз.

IoCs / TTPs



Отчет

- Результаты первичного расследования инцидента; описание эксплуатируемых уязвимостей и недостатков системы безопасности, которые могли использовать злоумышленники; источники атаки и потенциально затронутые сетевые ресурсы
- Поддержка экспертов
- Рекомендации по своевременному реагированию
- Анализ текущего состояния защиты

Комплексный подход

kaspersky активируй будущее

* Аналитический отчет «Лаборатории Касперского» по Incident Response, 2023 г.

** Аналитический отчет «Лаборатории Касперского» по MDR, 2023 г.

Что делаем мы

- Сканируем конечные точки с использованием специальных инструментов
- Выявляем скомпрометированные системы и следы прошлых инцидентов
- Валидируем обнаруженные инциденты и определяем тактики, техники и инструменты атаки
- Даем рекомендации по устранению последствий и предотвращению дальнейших атак

Что получаете вы

- Четкое понимание того, была ли скомпрометирована ваша сеть
- Независимую экспертную оценку уровня защиты с детализированным отчетом и резюме для руководства
- Раннее выявление кибератак, уже проникших в вашу сеть
- Минимизация потенциального ущерба, в том числе финансовых потерь
- Усиление защиты компании благодаря ценной информации и практическим рекомендациям

Преимущества Kaspersky Compromise Assessment

1

Комплексный подход

Поиск в Даркнете, анализ тактик, техник и инструментов злоумышленников, валидация обнаруженных инцидентов и мер первичного реагирования, анализ журналов SIEM, автоматизированный и ручной активный поиск угроз на базе телеметрии конечных точек и уникальных индикаторов атаки (IoA).

2

Возможность выезда на ваше предприятие

Если удаленный формат недоступен, все работы могут быть выполнены на вашей территории, так что ваши данные не покинут периметр корпоративной сети.

3

Самые полные данные о киберугрозах

«Лаборатория Касперского» – признанный во всем мире поставщик данных о киберугрозах, используемых в различных сценариях. Наша команда более 27 лет занимается исследованиями угроз и разработкой решений для защиты и нейтрализации одних из самых сложных APT-атак, поддерживаемых государственными структурами. В сервисе Compromise Assessment используются петабайты накопленных данных Threat Intelligence об актуальных киберугрозах.

4

Уникальный опыт и инновации

Наши решения конкурируют с лучшими мировыми продуктами в области кибербезопасности. Эксперты «Лаборатории Касперского» обладают международным опытом работы в разных отраслях и сертифицированы по стандартам GIAC, (ISC)², ISACA, Offensive Security и другим.

5

Минимальная нагрузка на инфраструктуру

Мы разработали методику, которая не создает заметной нагрузки на процессор, оперативную память и сеть. Если в вашей компании уже используется Kaspersky Endpoint Security для бизнеса, процесс анализа выполняется без установки дополнительных агентов.

6

Совместимость со сторонними системами

Мы анализируем журналы, экспортированные из SIEM и других систем безопасности от разных поставщиков.

www.kaspersky.ru

© 2025 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Узнать больше

#kaspersky
#активируйбудущее