Kaspersky Incident Response

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Вы можете стать жертвой кибератаки, и тогда размер ущерба напрямую будет зависеть от умения правильно и быстро отреагировать на инцидент

Почему важно реагировать на инциденты

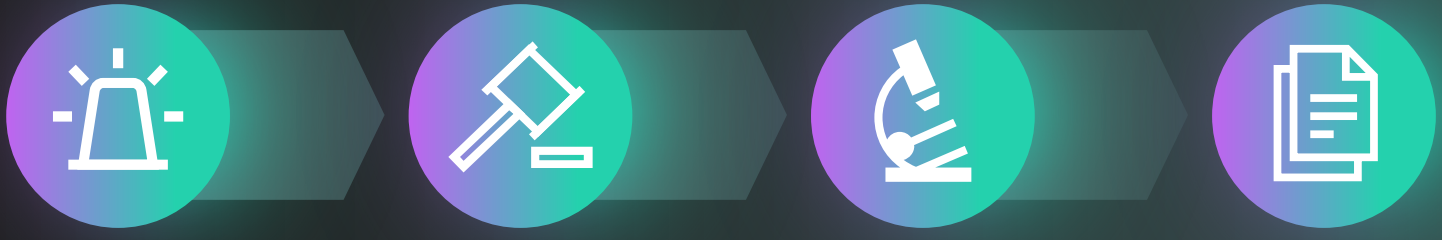
Одна уязвимость может открыть дверь любому киберпреступнику и дать ему возможность получить контроль над вашими информационными системами.

Взломать можно все, что угодно. Если это произошло, очень важно выяснить, как была взломана система, чтобы составить тщательный план по устранению последствий и предотвратить подобные атаки в будущем. Сервис реагирования на инциденты направлен на достижение этих целей.

Kaspersky Incident Response

Как работает сервис

Kaspersky Incident Response — это сервис, направленный на получение подробной картины инцидента. Сервис охватывает полный цикл реагирования на инциденты — от сбора доказательств и раннего реагирования на инцидент до выявления дополнительных следов взлома и подготовки плана устранения последствий атаки.



4 этапа реагирования на инциденты

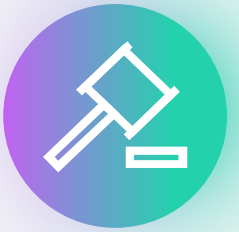
1

Создание запроса

На первом этапе эксперты свяжутся с представителями вашей компании, чтобы узнать детали произошедшего.

Команда «Лаборатории Касперского» проанализирует первоначально предоставленную информацию, чтобы подтвердить наличие инцидента. После этого наши эксперты предоставят краткосрочные рекомендации по дальнейшим этапам реагирования на инцидент.

2



Сбор доказательств

В зависимости от специфики инцидента могут быть использованы следующие подходы к сбору доказательств:

На месте

Сбор доказательств, необходимых для расследования инцидента, осуществляется экспертами «Лаборатории Касперского» с выездом на место работы вашей компании

Удаленно

Сбор доказательств, необходимых для расследования инцидента, осуществляется сотрудниками вашей компании, а наши эксперты предоставляют необходимые инструменты и руководства для самостоятельного сбора данных

Доказательства могут включать: файлы журналов операционных систем, приложений и сетевого оборудования, журналы доступа в интернет (например, с прокси-серверов), дампы сетевого трафика, образы жестких дисков, дампы памяти и любые другие типы информации, которые могут быть полезны для проведения расследования.

3

Анализ доказательств

Эксперты проводят анализ всей доступной информации (включая анализ вредоносных программ, если это необходимо), чтобы воссоздать картину инцидента. В ходе анализа регулярно предоставляются все новые сведения о расследовании. Это позволяет своевременно принимать меры для предотвращения развития атаки.

Если в ходе анализа будут обнаружены новые признаки компрометации, эксперты «Лаборатории Касперского» предоставят инструменты для сканирования информационных ресурсов компании с целью обнаружения других скомпрометированных хостов и сбора дополнительных данных.

4

Подготовка итогового отчета

По окончанию работ вы получите итоговый отчет, содержащий описание результатов расследования и рекомендации о том, как устранить последствия атаки и избежать подобных атак в будущем.

Задачи, которые решает сервис:

- Изолирование угрозы
- Предотвращение распространения атаки
- Поиск и сбор доказательств
- Выявление скомпрометированных ресурсов
- Анализ доказательств и восстановление хронологии и логики инцидента
- Анализ вредоносного ПО, использованного в атаке (если таковое обнаружено)
- Анализ сетевой активности и активностей на конечных узлах
- Устранение угрозы
- Выработки рекомендаций по восстановлению работоспособности ИТ-инфраструктуры организации и по предотвращению повторения подобных атак в будущем

Уникальный опыт и экспертиза мирового уровня

Расследования «Лаборатории Касперского» проводятся высококвалифицированными аналитиками и экспертами GERT.

Эксперты Global Emergency and Response Team (GERT) — сертифицированные специалисты в управлении инцидентами, компьютерной криминалистике, анализе вредоносного ПО, сетевой безопасности и анализе рисков.

Весь наш глобальный опыт в области цифровой криминалистики и анализа вредоносных программ будет использован для разрешения вашего инцидента информационной безопасности.

Помощь наших экспертов

В зависимости от того, есть ли у вас собственная группа реагирования на инциденты, вы можете запросить наших экспертов: выполнить полный цикл расследования; идентифицировать и изолировать скомпрометированные машины и предотвратить распространение угрозы; провести анализ вредоносных программ или цифровую криминалистическую экспертизу.

Что вы получите в результате

В результате угроза будет устранена, и мы предоставим вам подробный отчет о расследованном инциденте, который будет включать:

Подробный отчет

Краткое описание инцидента

Углубленный анализ инцидента с полной хронологией событий

Описание используемых уязвимостей, возможных источников атаки, затронутых сетевых компонентов, а также результаты анализа вредоносных программ

Описание действий атакующих и используемых ими иниструментов

Заключение о наличии или отсутствии признаков компрометации

Рекомендации по устранению последствий атаки и предотвращению повторения подобных атак в будущем

Предоставление сервиса

Подписка доступна на 1, 2 или 3 года

Сервис по реагированию на инциденты доступен по подписке. Существует два тарифа: IR Retainer и IR Retainer Premium.

	IR Retainer	IR Retainer Premium
Минимальное количество часов оказания сервиса	40 часов	80 часов
Сколько инцидентов можно расследовать?	Любое количество инцидентов, которое эксперты могут обработать в рамках оговоренного количества часов	
SLA	Стандартное, 24x7	Расширенное, 24x7
Формат работы	Удаленный формат предпочтительнее и позволяет быстрее взять в работу инцидент. Необходимость выезда экспертов зависит от деталей инцидента и оговаривается в каждом случае отдельно	
Можно ли использовать закупленное, но непотраченное время на другие сервисы?	Нет	Да, можно использовать эти часы для доступа к сервисам Kaspersky Threat Intelligence: • Аналитические отчеты об APT-угрозах и об атаках на основе ПО для автоматизации совершения финансовых преступлений (crimeware) • Kaspersky Threat Lookup • Kaspersky Cloud Sandbox • Потоки данных об угрозах
Погружение в сервис	Мы проведем установочную встречу и подробно обсудим процесс реагирования на инциденты. В случае инцидента вы будете знать, с чего начать и какие совместные действия потребуются	

Экстренное реагирование

Мы готовы вам помочь в случае инцидента, даже если у вас нет подписки. Команда реагирования сделает все возможное, чтобы оперативно расследовать инцидент и подготовить рекомендации по реагированию.

Стоимость сервиса

Цена на сервис зависит от трех параметров:

Количество часов экспертов

Количество часов, необходимых для реагирования (в свою очередь, зависит от уровня сложности инцидентов и их количества)

Формат работы

На месте или удаленно. Удаленная работа не требует командировок, поэтому экономит затраты и время

Тип подписки

IR Retainer со стандартным SLA или IR Retainer Premium с расширенным SLA

Итоговое количество часов оценивается в каждом конкретном случае и может отличаться от оценок в примере.

Уровень сложности инцидента оценивается в самом начале проекта. Пример расчета количества часов в зависимости от уровня сложности не включает время, необходимое для сбора улик.

Уровень сложности	Описание	Сроки исполнения
1	Одна скомпрометированная машина (заражение вредоносным ПО, утечка данных или финансовое мошенничество и т. д.)	40-56 человеко-часов
2	Несколько скомпрометированных машин внутри сети (компрометация определенной бизнес-системы, массивное заражение вредоносным ПО, скомпрометирован домен Active Directory и т. д.)	56-80 человеко-часов
3	Сложная атака, ведущая к компрометации сети (сложная атака в распределенных сетях, APT-атака и т. д.)	80-120 человеко-часов

Почему «Лаборатория Касперского»?

Крупнейшая независимая компания по разработке ПО для обеспечения кибербезопасности компаний по всему миру

Поставщик с несколькими петабайтами данных об угрозах, которые непрерывно собираются со всего мира и анализируются в течение более чем двух десятилетий

Сервис оказывает Global Emergency Response Team (GERT). Это команда экспертов, которая более 10 лет расследует сложные инциденты в компаниях из разных секторов и стран

О «Лаборатории Касперского»

«Лаборатория Касперского» — один из крупнейших в мире поставщиков решений по информационной безопасности, которые помогают нашим клиентам тщательно прогнозировать угрозы, эффективно предотвращать их, обнаруживать раньше и реагировать быстрее.

Компания входит в четверку ведущих мировых поставщиков решений для обеспечения безопасности конечных пользователей. На протяжении своей более чем 20-летней истории «Лаборатория Касперского» остается новатором в области ИТ-безопасности и предоставляет эффективные решения для обеспечения безопасности крупных, малых и средних предприятий и конечных пользователей.

«Лаборатория Касперского» работает почти в 200 странах и территориях по всему миру, обеспечивая защиту более 400 миллионов пользователей.

Всегда рядом

Мы всегда готовы помочь вам точно и своевременно отреагировать на инцидент.

Подробнее

Kaspersky Incident Response

www.kaspersky.ru