Реагирование на инциденты и ликвидация последствий нарушения системы безопасности

Kaspersky Incident Response

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Почему важно реагировать на инциденты

Всего одна уязвимость может открыть дверь любому киберпреступнику и дать ему возможность получить контроль над информационными системами вашей компании. Взломать можно все что угодно, и когда это произойдет, очень важно выяснить, как была взломана система, чтобы составить тщательный план по устранению последствий и предотвратить подобные атаки в будущем.

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

Минимизируйте ущерб от кибератак

При возникновении инцидента размер ущерба будет напрямую зависеть от умения корректно и быстро реагировать на киберугрозы

В числе частых последствий киберинцидентов:

- Потеря прибыли и упущенные деловые возможности
- Ущерб репутации
- Убытки из-за простоев
- Штрафы и пени
- Рост страховых выплат
- Ухудшение кредитного рейтинга

Инцидент

- Шифровальщики
- Утечки данных
- Хищение финансовых средств
- И другие

Сбор доказательств

- Файлы журналов
- Дампы памяти
- Сетевой трафик
- Образы дисков
- И другие

Анализ доказательств

- Скомпрометированные учетные данные пользователей
- Сетевые адреса командных центров
- Список скомпрометированных активов
- Индикаторы компрометации и индикаторы атаки
- И другие

Отчет

- Начальный вектор атаки
- Хронология инцидента
- Техники, тактики, процедуры атакующих
- Рекомендации

Как работает сервис

Процесс реагирования на инциденты выстроен в 4 этапа:

Этап	Содержание
 Создание запроса	После получения обращения эксперты «Лаборатории Касперского» связываются с представителями вашей компании для уточнения деталей инцидента. В случае подтверждения наличия инцидента по результатам анализа первичной информации, наши эксперты предоставляют рекомендации по дальнейшим мерам реагирования.
 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. Наши эксперты оказывают необходимую поддержку, предоставляя рекомендации и инструменты 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.
 Анализ доказательств	Чтобы воссоздать картину инцидента, эксперты проводят анализ всей доступной информации (включая анализ вредоносного ПО, обнаруженного в процессе расследования). Все новые сведения о расследовании регулярно сообщаются. Это позволяет своевременно принимать меры по предотвращению развития атаки. В случае обнаружения новых признаков компрометации, наши эксперты предоставляют инструменты для сканирования информационных ресурсов компании с целью идентификации скомпрометированных хостов и сбора дополнительных данных.
 Подготовка итогового отчета	По окончании работ предоставляется итоговый отчет с описанием результатов расследования, а также рекомендациями по устранению последствий атаки и избежанию 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.

Задачи, которые решает сервис

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

Помощь наших экспертов

Эксперты «Лаборатории Касперского» готовы оказать поддержку вашей внутренней группе реагирования на инциденты по различным направлениям:

1. Выполнение полного цикла расследования
2. Предотвращение распространения угрозы путем идентификации и изолирования скомпрометированных машин
3. Проведение анализа вредоносных программ и цифровой криминалистической экспертизы

Предоставление сервиса

Kaspersky Incident Response доступен по подписке на 1, 2 или 3 года в двух тарифах: IR Retainer и IR Retainer Premium.

Возможности	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 установленного количества часов	
SLA	Стандартное, 4 часа, 24x7	Расширенное, 2 часа, 24x7
Формат работы	Преобладает удаленный формат работы, что позволяет оказывать оперативное реагирование. Необходимость выезда экспертов на объект зависит от деталей инцидента и согласуется 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	Сервис предполагает проведение установочной встречи с целью более подробного обсуждения процесса реагирования. Таким образом, в случае возникновения инцидента, вам будет известно, с чего начать и какие совместные действия потребуются	

Экстренное реагирование

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

Стоимость сервиса

Цена на сервис рассчитывается с учетом следующих параметров:

Количество часов работы 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 минимизирует денежные и временные затраты на передвижение экспертов

Тип подписки

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

Расчет количества часов в зависимости от уровня сложности инцидента

Уровень сложности	Описание	Сроки исполнения
1	Одна скомпрометированная машина (заражение вредоносным ПО, утечка данных, 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

* Пример не включает время, необходимое для сбора улик.

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

Что вы получите в результате

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

Краткое описание инцидента

с определением природы атаки, затронутых ей элементов, оценкой уровня риска и действий по незамедлительному реагированию

Углубленный анализ инцидента

с восстановлением полной хронологии событий

Характеристика действий атакующих

с учетом задействованных ими инструментов

Описание использованных уязвимостей,

включая возможные источники атаки, затронутые сетевые компоненты, а также результаты анализа вредоносных программ

Заключение

о наличии или отсутствии признаков компрометации

Рекомендации

по устранению последствий атаки и предотвращению повторения подобных атак в будущем

Преимущества для бизнеса

- Непрерывное укрепление безопасности
- Минимизация сбоев в бизнес-процессах и ущерба от простоев
- Экспертная поддержка ваших специалистов
- Сохранение отношений с клиентами и укрепление доверия
- Предотвращение крупных штрафов и взысканий
- Обмен экспертными знаниями со штатными специалистами

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

GERT

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

Почему «Лаборатория Касперского»?

«Лаборатория Касперского» — один из крупнейших поставщиков решений в области информационной безопасности, помогающий клиентам по всему миру своевременно обнаруживать даже самые сложные и изощренные киберугрозы и эффективно на них реагировать.

На протяжении своей более чем 25-летней истории мы продолжаем оставаться новаторами в сфере ИТ-безопасности, предоставляя защитные решения и сервисы нового поколения, которые обеспечивают безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей.

Kaspersky Incident Response

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее