Тренинг, направленный
на проверку эффективности
стратегии компании
по реагированию
на инциденты

Kaspersky Tabletop Exercise

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Исследования

Согласно исследованиям IDC, всего у 18% компаний есть собственные методички по реагированию на инциденты безопасности.

Проверьте эффективность и повысьте устойчивость к киберугрозам

Хотите повысить устойчивость к киберугрозам и подготовить вашу команду к борьбе с новейшими видами кибератак?
Тогда вам нужна стратегия реагирования на инциденты безопасности, которая позволит оперативно отражать атаки и сводить к минимуму потенциальный ущерб. Но этим ваша работа не ограничивается – крайне важно обновлять стратегию по мере необходимости и регулярно применять ее в реальных условиях.

Тренинг Kaspersky Tabletop Exercise поможет вам улучшить процессы, связанные с реагированием на инциденты, а также оптимизировать взаимодействие между командами.

Экспертные сервисы по формированию ИБ-процессов и построению SOC

- **Kaspersky Tabletop Exercise**
- Kaspersky SOC Consulting
- Kaspersky Adversary Attack Emulation

Что такое Kaspersky Tabletop Exercise?

Проверка эффективности

Kaspersky Tabletop Exercise – это тренинг с участием экспертов «Лаборатории Касперского», направленный на проверку эффективности стратегии компании по реагированию на инциденты.Он помогает выявить недостатки в стратегии по реагированию на инциденты, четко определить роли и зоны ответственности участников команд, а также наладить совместную работу отделов в ходе урегулирования инцидента.

Сценарии инцидентов от экспертов

Эксперты международной команды «Лаборатории Касперского» Global Emergency and Response Team (GERT) разрабатывают сценарий инцидента, который учитывает актуальный ландшафт угроз, а также специфику компании и ее производственные нужды. Эти сценарии максимально приближены к реальным и основаны на собственном опыте команды GERT по расследованию сложных атак на организации из разных отраслей по всему миру.

Особенности тренинга

Живое взаимодействие и обсуждение реальных инцидентов

Свободная атмосфера, получение практических знаний

Принимать участие в тренинге могут как ИБ-специалисты, так и руководители высшего звена

Ключевые преимущества

Точная оценка

Точная оценка способности вашей команды противодействовать инцидентам

Зоны ответственности

Лучшее понимание руководителями, ИБ- специалистами и менеджерами других отделов своих ролей и зон ответственности в ходе реагирования на инциденты

Сплочение коллектива

Более сплоченная работа отделов

Реалистичные сценарии реагирования на инциденты

Эксперты GERT знакомят игроков со сценарием

Совместная работа по противодействию инциденту

- Совет директоров
- IT-отдел
- Команда по урегулированию кризисов кибербезопасности
- Синяя команда
- Группа реагирования на инцидент
- Специалисты SOC

Как работает сервис

Тренинг может быть организован как очно, так и в удаленном формате.

Инструктаж

Семинар

- Определяют стратегию реагирования на инциденты, принятую в организации
- Определяют рабочую среду
- Выявляют потенциальные болевые точки
- Формируют представление о текущем ландшафте угроз

В рамках первого этапа эксперты «Лаборатории Касперского» проводят инструктаж (в очном или удаленном формате), чтобы определить актуальный для клиента ландшафт угроз, лучше понять его цели и потребности и выявить другие организационные и технические моменты, которые могут иметь значение при проведении тренинга.

Разработка сценария

Работа экспертов

Эксперты «Лаборатории Касперского» разрабатывают сценарий по внедрению киберугроз с учетом стратегии клиента по реагированию на инциденты, учитывающий особенности среды и инфраструктуры компании, а также ее цели и потребности.

Разрабатывается план проекта, включающий регулярные совещания, план проведения тренинга и итоговый отчет, а также опросы участников (по желанию). Все эти шаги направлены на разработку уникального сценария, который позволит заранее оценить эффективность стратегии реагирования еще до появления настоящей угрозы.

Ролевая игра

Этапы

Эксперты распределяют роли среди участников и объясняют им сценарий атаки. Эксперты «Лаборатории Касперского» оценивают работу команды и проверяют, как принятые ею решения соотносятся со стратегией реагирования на инциденты.

К работе с реальным инцидентом обычно привлекаются разные специалисты – и это учитывается в нашем тренинге. В частности, в ходе тестирования возможностей компании по реагированию на инциденты проверяется работа как технических специалистов, так и других заинтересованных сторон, например членов команды по урегулированию кризисов кибербезопасности.

Итоги тренинга

Итоговый отчет

- Пошаговый разбор действий команды в ходе использованного сценария
- Сопоставление ожидаемых и реальных действий участников тренинга
- Рекомендации экспертов

После тренинга формируется отчет, который включает:пошаговый разбор действий команды в ходе разыгранного сценария, информацию о внедренных угрозах, а также пробелы в защите, выявленные по результатам сравнения фактических действий команды и рекомендаций в соответствии с передовыми практиками в области реагирования на инциденты.

В ходе тренингов применяются многие распространенные сценарии атак: фишинг, атаки с использованием шифровальщиков, атаки на цепочку поставок, угрозы

О команде GERT

Тренинг Kaspersky Tabletop Exercise создан экспертами международной команды Global Emergency and Response Team (GERT) с учетом их богатого практического опыта и передовых наработок в сфере реагирования на инциденты безопасности.

GERT – это международная группа экспертов, которая уже более 10 лет расследует сложные инциденты информационной безопасности для организаций из разных отраслей по всему миру. Эксперты GERT являются дипломированными специалистами в таких областях, как управление инцидентами информационной безопасности, цифровая криминалистика, анализ вредоносных программ, защита сетей и оценка рисков.

Kaspersky Tabletop Exercise

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее