Тренинги

Программа тренингов для сотрудников промышленных предприятий

kaspersky активируй будущее

ICS CERT

Больше информации:
ics-cert.kaspersky.ru

Содержание

Kaspersky
ICS CERT

Все тренинги, описанные в этой брошюре, разработаны экспертами Центра исследования безопасности промышленных систем «Лаборатории Касперского» – Kaspersky ICS CERT.

Kaspersky ICS CERT – это глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

В нашей команде работают эксперты по реагированию на инциденты, исследованию и анализу киберугроз и уязвимостей в промышленном ПО и оборудовании.

Kaspersky ICS CERT обучает сотрудников промышленных организаций и технических специалистов основам кибербезопасности, а также проводит тренинги, в ходе которых участники получают практические навыки расследования инцидентов в АСУ ТП и поиска уязвимостей в промышленном ПО и оборудовании.

Наши программы обучения основаны на практическом опыте и реальных кейсах.

Специалисты Kaspersky ICS CERT:

- Исследуют киберугрозы и обнаруживают атаки на промышленные объекты
- Расследуют киберинциденты на промышленных предприятиях и объектах критической инфраструктуры
- Ищут уязвимости в распространённых продуктах и технологиях АСУ ТП и помогают их устранить
- Обучают основам промышленной кибербезопасности, проводят тренинги по расследованию киберинцидентов и поиску уязвимостей
- Помогают разработчикам сделать их продукты безопаснее
- Консультируют промышленные организации по вопросам промышленной кибербезопасности
- Разрабатывают методики, стандарты и регламенты в области промышленной кибербезопасности.

Мы также заинтересованы в сотрудничестве с университетами и другими организациями из академической среды для обмена опытом и проведения совместных исследований.

Основы промышленной кибербезопасности

Тренинги для повышения осведомленности об актуальных тенденциях в области промышленной кибербезопасности и последних инцидентах безопасности. Предназначены для руководителей и менеджеров среднего звена, а также специалистов в области ИТ/АСУ.

Курсы адаптируются в соответствии с составом участников каждой группы.

Базовый курс

Кибербезопасность современных промышленных систем

Программа

- Особенности обеспечения безопасности промышленных систем, архитектура промышленных сетей, классификация основных угроз для АСУ ТП: уязвимости, эксплойты, атаки
- Обзор ландшафта угроз для промышленных предприятий, проблемы безопасности, влияние человеческого фактора, атаки на промышленные сети
- Типы злоумышленников
- Политики и процедуры безопасности
- Основы реагирования на инциденты безопасности
- Методы социальной инженерии

Полученные знания

- Знание основ информационной безопасности на промышленных предприятиях
- Понимание сути инцидентов безопасности и подходов к реагированию
- Владение правилами безопасного поведения в ежедневной работе

Формат

Очный курс с инструктором

Продолжительность

1 день

Численность группы

10-25 человек

Другие варианты

Для больших групп сотрудников мы рекомендуем онлайн-обучение на платформе Kaspersky Automated Security Awareness Platform, программа которого включает также отдельный модуль по основам промышленной кибербезопасности.

Бесплатный пробный доступ: https://www.k-asap.com/ru

Основной курс

Промышленная безопасность

Программа

- Обзор ландшафта угроз для промышленных предприятий, проблемы безопасности, влияние человеческого фактора, примеры атак на промышленные сети
- Типы злоумышленников
- Отличия в защите ИТ- и промышленных сетей
- Концепция защиты в глубину
- Сетевая безопасность в ИТ- и в промышленных сетях
- Промышленные сетевые протоколы
- Методы предотвращения и детектирования угроз, снижения рисков реализации угроз
- Соответствие защищаемых промышленных систем требованиям стандартов и законодательства
- Структура команды информационной безопасности, описание ролей
- Соображения безопасности при работе с поставщиками
- Безопасность изолированных сетей
- Подход к реагированию на инциденты кибербезопасности
- Влияние развития промышленного интернета вещей на кибербезопасность

Полученные знания и навыки

- Основные меры и рекомендации по применению механизмов безопасности в промышленных системах
- Как выявлять инциденты безопасности
- Основы проведения расследований инцидентов
- Рекомендации по организации команды кибербезопасности на предприятии
- Разбор реальных примеров расследований инцидентов в АСУ ТП
- Разработка и внедрение эффективного плана реагирования на инциденты кибербезопасности
- Контрмеры: сегментация сети, использование межсетевого экрана, защита изолированной сети
- Специфика атак на промышленные организации

Формат

Очный курс с инструктором

Продолжительность

2 дня

Численность группы

10-25 человек

Экспресс-курс

Промышленная безопасность

Программа

- Знакомство с основными проблемами кибербезопасности в промышленных средах
- Основные отличия между безопасностью в промышленных сетях и информационных сетях
- Организация и управление эффективной командой информационной безопасностью на предприятиях
- Соответствие защищаемых промышленных систем требованиям стандартов и регулирующих актов в области информационной безопасности

Полученные знания

- Основные понятия кибербезопасности: атаки, злоумышленники, угрозы, уязвимости и прочее
- Понимание ландшафта современных киберугроз и подходов к предотвращению и расследованию инцидентов
- Понимание отличий между безопасностью в ИТ и АСУ ТП
- Основы правового регулирования в сфере информационной безопасности

Формат

Очный курс с инструктором

Продолжительность

3 часа

Численность группы

5-10 человек

Другие варианты

Для менеджеров среднего и высшего звена мы также рекомендуем Kaspersky Interactive Protection Simulation (KIPS) — это стратегическая бизнес-симуляция, командная игра, демонстрирующая связь между эффективностью бизнеса и кибербезопасностью. Участники помещаются в смоделированную бизнес-среду, где они сталкиваются с рядом непредвиденных киберугроз. Варианты KIPS разработаны с учетом специфики нескольких основных отраслей.

Узнать больше: https://www.kaspersky.ru/enterprise-security/security-awareness

Тренинги для технических специалистов

Цифровая криминалистика в АСУ ТП

Цифровая криминалистика в АСУ ТП имеет ряд особенностей и ограничений. Инструменты и методы, применяемые в расследовании инцидентов в ИТ-системах, часто не подходят или оказываются бесполезными для АСУ ТП. Например, сбор улик в этом случае проходит исключительно в ручном режиме. И, конечно, особое внимание уделяется тому, чтобы максимально быстро вернуть контроль над инфраструктурой и обеспечить её нормальное безопасное функционирование. Работая с экспертами «Лаборатории Касперского», участники тренинга смогут изучить все аспекты цифровой криминалистики в АСУ ТП, начиная с установления факта киберинцидента и сбора улик и заканчивая анализом данных и подготовкой отчета о расследовании.

Полученные знания и навыки

- Выявление инцидентов ИБ на системах промышленных предприятий
- Создание плана по расследованию инцидентов в АСУ ТП
- Сбор и обработка улик – как физических, так и цифровых
- Применение специальных инструментов и методов цифровой криминалистики для ПО (например, SCADA) и оборудования (например, контроллеры (PLC)) в промышленных системах
- Поиск следов вторжения на основе обнаруженных улик
- Восстановление картины инцидента и использование временных меток (timestamps) в ПО и оборудовании АСУ ТП
- Составление отчета о проведенном расследовании и подготовка практических рекомендаций по устранению последствий и предотвращению подобных инцидентов в будущем

Кому будет полезен этот курс

- Специалистам по информационной безопасности и безопасности систем АСУ ТП
- Аналитикам из команд быстрого реагирования на инциденты (CSIRT, CERT) и центров обеспечения безопасности (SOC)
- Специалистам по аудиту ИБ и расследованию инцидентов
- Сотрудникам государственных служб и другим специалистам, которые занимаются расследованием инцидентов в промышленных системах

Требования к слушателям

- Общие знания по системному администрированию, сетевым технологиям и практикам информационной безопасности
- Навыки системного администратора Windows, Linux и систем виртуализации
- Опыт анализа вредоносного ПО и знания об архитектуре АСУ ТП и безопасности промышленных систем не являются обязательными, но будут полезны

Программа обучения по дням

1. Основы расследования инцидентов в системах промышленной автоматизации
2. Исследование сети промышленного предприятия, поиск угроз, работа с сетевыми протоколами в АСУ ТП
3. Анализ систем архитектуры Intel X86/X64, включая специализированное ПО для систем промышленной автоматизации
4. Цифровая криминалистика на специализированных устройствах систем промышленной автоматизации
5. Лабораторная работа со всеми этапами реального расследования инцидента на промышленном предприятии

Формат

Очный курс с инструктором

Продолжительность

5 дней

Численность группы

до 10 человек

Поиск уязвимостей в устройствах IoT

Обучение специалистов по безопасности проведению полного и всестороннего исследования устройств интернета вещей (IoT) на наличие уязвимостей и подготовке экспертных рекомендаций по принятию мер для исправления выявленных недочетов. Тренинг основан на выполнении участниками практических задач по исследованию уязвимостей.

Полученные знания и навыки

- Проверка программно-аппаратной части IoT-устройств на наличие уязвимостей
- Анализ выявленных уязвимостей
- Формирование рекомендаций по исправлению выявленных недочетов
- Выбор компенсационных мер для защиты IoT-устройств

Кому будет полезен этот курс

- Исследователям безопасности
- Специалистам по тестированию на проникновение
- Разработчикам
- Техническим менеджерам продукта

Программа обучения

- Введение в IoT: определение термина интернета вещей, отличия IoT-устройств от компьютеров; приложения, архитектура IoT и примеры уязвимостей
- Аппаратные платформы и архитектура IoT, внутренняя память и коммуникационные интерфейсы, отладка устройств с использованием различных интерфейсов
- Угрозы и уязвимости в интернете вещей. Векторы атак для различных уровней: прошивки, аппаратного обеспечения и каналов связи
- Получение и анализ прошивок
- Автоматизация задач реверс-инжиниринга с помощью ПО Ghidra
- Введение в динамический поиск уязвимостей с помочью фаззинга библиотек с открытым исходным кодом
- Статистика по вредоносному ПО для устройств интернета вещей, ботнеты из устройств интернета вещей, анализ уязвимостей IoT и выбор защитных мер

Требования к слушателям

- Знание скриптовых языков (Python или другого)
- Знание основных команд в ОС Linux
- Умение читать фрагменты кода на C/C++
- Базовые знания по реверс-инжинирингу
- Знание основных сетевых протоколов
- Опыт работы с инструментами дизассемблирования также будет полезен

Материалы и оборудование

- Участникам будут предоставлены IoT-устройства для проведения практических работ

Формат

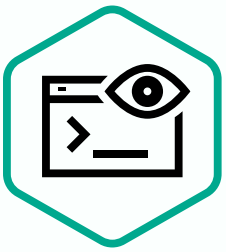
- Очный курс с инструктором

Продолжительность

- 3 дня

Численность группы

- до 10 человек



Обнаружение уязвимостей с помощью фаззинга

Тренинг предназначен для изучения современных методов, техник, подходов и утилит, используемых для выявления уязвимостей в программном обеспечении методом «грубой силы», то есть методом фаззинга. Фаззинг – это техника тестирования ПО, заключающаяся в передаче приложению на вход неправильных, неожиданных или случайных данных, и анализе ошибок, вызванных этими действиями. Данный способ тестирования приложений позволяет на ранних этапах жизненного цикла программного обеспечения выявлять ранее неизвестные уязвимости (уязвимости нулевого дня, 0-day) и проблемы безопасности, с которыми могут столкнуться пользователи.

Тренинг основан на выполнении участниками практических задач по фаззингу библиотек и пользовательского ПО для Linux и Windows x86_64.

Полученные знания и навыки

- Основные понятия и подходы к проведению фаззинга, включая мутацию корпуса, построение функции обратной связи, инструментацию и покрытие кода
- Применение техник фаззинга для поиска уязвимостей как с доступом к исходному коду, так и без него

Кому будет полезен этот курс

- Исследователям безопасности
- Специалистам по тестированию
- Разработчикам

Программа обучения

- Введение в техники фаззинга
- Написание собственного фаззера
- Практическое применение существующих инструментов, таких как Libfuzzer, AFL, DynamoRIO, WinAFL
- Проведение фаззинга как для исходного кода, так и для скомпилированных бинарных образов ПО
- Эмуляция для фаззинга других архитектур (ARM и MIPS)
- Эффективная генерация и мутация корпусов
- Анализ падений и их классификация

Требования к слушателям

- Знание скриптовых языков (Python или другого)
- Знание основ C/C++
- Знакомство с уязвимостями повреждения памяти
- Знакомство со статическим и динамическим анализом кода

Формат

Очный курс с инструктором

Продолжительность

3 дня

Численность группы

до 10 человек

kaspersky

ics-cert@kaspersky.com
ics-cert.kaspersky.ru