Цифровая криминалистика и расследование инцидентов в АСУ ТП

Тренинг

О чем

На тренинге участники осваивают инструменты и методы, необходимые для проведения всех этапов расследования инцидента в АСУ ТП, — от установления факта инцидента и сбора улик до анализа данных и подготовки итогового отчета.

Зачем

Полученные навыки позволят проводить расследование инцидентов на промышленных предприятиях с применением уникальных подходов и стать экспертом в цифровой криминалистике в АСУ ТП.

Для кого

Специалисты по информационной безопасности и безопасности систем АСУ ТП, аналитики из команд быстрого реагирования на инциденты (CSIRT, CERT) и центров обеспечения безопасности (SOC).

Проблематика

Кибератака на промышленное предприятие способна привести к непредсказуемым и тяжелым последствиям. Простой систем АСУ ТП вследствие киберинцидента может повлечь не только прямые финансовые потери, обусловленные остановкой производства и невыполнением обязательств по контракту, но также порчу сырья и выход из строя дорогостоящего оборудования.

Предприятию необходимо как можно скорее вернуть контроль над инфраструктурой и обеспечить ее нормальное функционирование. Для этого команда реагирования на киберинциденты должна уметь оперативно и качественно выполнять множество технических и организационных задач.

- Найти, изучить и обезвредить весь использованный в атаке вредоносный арсенал. Часть его может не обнаруживаться в начале расследования, что потребует обновления средств защиты или использования специальных средств обнаружения.
- Оценить возможное негативное влияние обнаруженного вредоносного инструментария на работу систем технологической

сети и выявить связи атаки со сбоями в работе оборудования, если такие наблюдались.

- Идентифицировать и всесторонне исследовать скомпрометированные системы, оперативно определить и принять меры, исключающие дальнейшее присутствие злоумышленников в сетях предприятия.
- По возможности без остановки технологического процесса предприятия обнаружить и собрать информацию, содержащую следы вредоносной активности, в ИТ- и ОТ-системах.
- Быстро проанализировать собранную информацию и оценить масштаб ущерба.
- Установить цели злоумышленников, спрогнозировать возможное дальнейшее развитие ситуации и выбрать стратегию предотвращения худших из возможных сценариев.
- Восстановить картину происшествия, включая первопричину, основные обстоятельства и временной график развития атаки, а также выяснить, какими проблемами безопасности предприятия воспользовались злоумышленники.
- Оперативно защитить предприятие от развития атаки и сформировать перечень мер для предотвращения подобных ситуаций в будущем.

> Инструменты и методы, применяемые при расследовании инцидентов в ИТ-системах, часто не подходят для АСУ ТП. Поиск и сбор улик здесь требует особой осторожности — стандартные для ИТ-сегмента методы могут приводить к отказу в обслуживании систем АСУ ТП. Поэтому реагирование на инциденты информационной безопасности, затрагивающие или способные затронуть АСУ ТП, требует дополнительных знаний и навыков.

Что мы предлагаем

Готовим экспертов по цифровой криминалистике в АСУ ТП

Наличие собственных специалистов по цифровой криминалистике позволяет предприятию ускорить реагирование на киберинциденты, минимизируя тем самым негативные последствия, а также экономить, привлекая внешних экспертов только в сложных ситуациях.

Содержание тренинга

1. Основы реагирования на инциденты и отличия цифровой криминалистики в ИТ и АСУ ТП.
2. Устройство сетевых протоколов и архитектура решений, применяемых в АСУ ТП.
3. Активный поиск угроз в промышленных сетях.
4. Цифровая криминалистика для рабочих станций и серверов с фокусом на ПО, угрозы и риски, специфичные для АСУ ТП.
5. Цифровая криминалистика, ориентированная на компоненты АСУ ТП (рабочие станции, сервера, специализированное ПО и оборудование).
6. Лабораторная работа, имитирующая расследование инцидента в АСУ ТП.

Программа тренинга может быть доработана в соответствии с пожеланиями заказчика.

Теоретическая часть тренинга включает разбор реальных инцидентов на промышленных предприятиях, информация о которых получена как из открытых источников, так и из опыта расследований, выполненных специалистами «Лаборатории Касперского».

Практическая составляющая тренинга предполагает выполнение упражнений, которые позволяют закрепить теорию путем решения задач по каждому блоку учебной программы. В заключительный день тренинга проходит лабораторная работа по самостоятельному расследованию инцидента на промышленном предприятии.

Предлагаемые сценарии практической части построены на анализе реальных атак на промышленные предприятия, результатах расследований инцидентов, а также исследований уязвимостей компонентов АСУ ТП.

Приобретенные знания и навыки

Теоретические знания по темам

1. Подготовка к реагированию на инциденты, дающая:
   - представление о требованиях к инфраструктуре для обеспечения оперативного реагирования на них;
   - понимание требований к персоналу команды реагирования на инциденты в контуре ОТ;

- понимание возможностей использования информации Cyber Threat Intelligence, результатов аудита защищенности предприятия, анализа уязвимостей и моделирования угроз для планирования и реализации превентивных мер и подготовки к возможным инцидентам.

2. Организация эффективного процесса реагирования на инциденты в ИТ- и ОТ-сетях промышленных предприятий, дающая:
   - понимание ролей, зон ответственности сотрудников предприятия и работающих по контракту экспертов, а также знание правил построения эффективной коммуникации между ними;
   - понимание отличий в организации и проведении расследования инцидентов в ИТ- и ОТ-сетях предприятия, а также требований к инструментарию и процедурам его использования;
   - знание принципов приоритезации задач в ходе расследования и создания плана расследования инцидентов в АСУ ТП;
   - представление о планировании мероприятий по предотвращению подобных инцидентов в будущем.
3. Типичные ошибки, допускаемые при подготовке к реагированию на инцидент и в ходе его расследования, а также способы их предупреждения.

Практические навыки

1. Выявление инцидентов в технологической сети промышленных предприятий с использованием имеющегося инструментария, утилит, находящихся в открытом доступе, коммерческих продуктов и индикаторов компрометации.
2. Реагирование на инциденты в технологической сети промышленных предприятий:
   - сбор и обработка цифровых улик;
   - применение специальных инструментов и методов цифровой криминалистики, ориентированных именно на АСУ ТП;
   - поиск следов вторжения на основе обнаруженных улик;
   - восстановление картины инцидента с использованием временных меток;
   - выбор мер и средств сдерживания и остановки развития инцидента, минимизации его последствий;
   - составление отчета о расследовании.

Продолжительность и формат обучения

- 5 дней — стандартный тренинг.
- 10 дней — тренинг с расширенной практической частью.

Тренинг проводится очно.

Требования к слушателям

Курс адаптируется в соответствии с уровнем подготовки слушателей.

Уровень подготовки, достаточный для освоения базового материала курса

- Общие знания по сетевым технологиям.
- Навыки системного администрирования ОС Windows, Linux и систем виртуализации.
- Знание теоретических основ информационной безопасности.
- Практические навыки в области обеспечения информационной безопасности и защиты ИТ-активов.
- Базовые знания по реагированию на инциденты в ИТ.

Уровень подготовки, необходимый для прохождения курса с усложненной программой

- Опыт анализа вредоносного ПО.
- Опыт обратного инжиниринга исполняемых файлов.
- Глубокие знания по сетевым технологиям и стекам сетевых протоколов.
- Опыт расследования инцидентов в ИТ-сетях.
- Опыт активного поиска угроз в ИТ-сетях.

Программа тренинга

Сертификация

Полученные знания закрепляются итоговой лабораторной работой. Участникам выдается сертификат о прохождении тренинга.

Наши тренеры

Вячеслав Копейцев, ведущий эксперт по исследованиям угроз информационной безопасности Kaspersky ICS CERT

Специализируется на расследовании атак на промышленную инфраструктуру, цифровой криминалистике и реагировании на инциденты в системах различного типа, а также на анализе вредоносных программ. Регулярно выступает на отраслевых конференциях, публикует статьи и отчеты по анализу угроз.

Павел Нестеров, ведущий исследователь угроз информационной безопасности Kaspersky ICS CERT

Специализируется на глубоком анализе уязвимостей в программном обеспечении и оборудовании для АСУ ТП, а также исследовании актуальных угроз. Реализует инфраструктурные проекты. Разрабатывает учебно-методические материалы по безопасности АСУ ТП, практические упражнения и специализированные демонстрационные стенды. Обладает обширной экспертизой в работе с SIEM-системами, от аналитики до внедрения и развертывания.

Запросить консультацию специалиста

Статьи по теме

- Уязвимость в VPN-серверах FortiGate используется в атаках шифровальщика Cring
- Lazarus атакует оборонную промышленность с помощью вредоносного ПО ThreatNeedle
- Атаки на промышленные предприятия с использованием RMS и TeamViewer: новые данные

Рекомендуем дополнительно

- Расследование киберинцидентов на промышленных предприятиях
- Разработка руководства и обучение реагированию на инциденты
- Поток данных об угрозах для систем промышленной автоматизации
- Поток машиночитаемых данных об уязвимостях АСУ ТП
- Информация об уязвимостях и угрозах для АСУ ТП

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com