Программа повышения квалификации в форме профессионального тренинга

**КВАЛИФИКАЦИОННЫЙ ТРЕНИНГ.**

**«ПРАКТИКА РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ**

**В УСЛОВИЯХ ВНУТРЕННИХ И ВНЕШНИХ АТАК РАЗЛИЧНЫХ КЛАССОВ». II-й УРОВЕНЬ**

*Тренинг проводит: руководитель «Санкт-Петербургской школы профессиональных аналитиков» Максим Бочков*

*.*

**Целевая установка:**

Поэтапное тестирование и обучение практическим навыкам управления системой обеспечения информационной безопасности предприятия в условиях внутренних и внешних атак различных классов.

**Категория слушателей**: руководители и специалисты подразделений информационной безопасности и другие категории сотрудников, связанные с решением задач управления защитой ИТ-инфраструктуры и корпоративной информации.

Содержание программы:

|  |  |
| --- | --- |
| Наименование тем и учебных вопросов | Кол-во часов |
| **Модуль 1. Закрепление навыков первого уровня на основе решения задач защиты ИТ-инфраструктуры и корпоративной информации повышенной сложности.** Тестирование защищенности ИТ-инфраструктуры и корпоративной информации с использованием возможностей современных сред генерации эксплоитов. Создание пользовательских проверок (скриптов) обнаружения новых уязвимостей и атак. Автоматизация сбора регистрационной информации на основе языков создания скриптов для ОС семейства Windows и Linux | 8 |
| **Модуль 2. Анализ данных устройств хранения и оперативной памяти.**Создание образов дисков и дампов памяти. Поиск и анализ цифровых отпечатков злоупотреблений пользователей и кибератак. | 4 |
| **Модуль 3. Организация оперативного контроля защищенности ИТ- инфраструктуры и корпоративной информации.** Выявление «теневой» ИТ- инфраструктуры. Выявление фактов утечки корпоративной информации в сетьИнтернет. Создание информационных панелей контроля защищенности. | 4 |
| **Модуль 4. Линия жизни инцидента и механика инцидента.** Расследование инцидентов с помощью DLP и SIEM. Выполнение лабораторных работы,основанных на реальных судебных делах | 12 |
| **Модуль 5. Расследование инцидентов информационной безопасности.** Решение задач выявления цифровых отпечатков реализации внутренних и внешних атак различных классов. Реконструкция сценария нарушений информационной безопасности на основе расширенных возможностей средств анализа трафика. Сбор и визуализация данных из открытых источников с помощью инструментов OSINT | 8 |

|  |  |
| --- | --- |
| Итоговое квалификационное испытание профессиональных навыков и умений. Поддержание защищенности инфраструктуры и информационных ресурсов в условиях внутренних и внешних атак различных классов | 4 |