ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «РОСТОВСКИЙ ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ»

«УТВЕРЖДАЮ»
Директор
ЧОУ ДПО «РЦПК ИТС»

_____ Е.И. Самойлова

«30» октября 2024 г.

Программа дополнительного профессионального образования
«Развертывание системы мониторинга предприятия»

Настоящая программа дополнительного образования «Развертывание системы мониторинга предприятия» (далее - программа) разработана ООО «Солар Секьюрити», компания группы ПАО «Ростелеком»с учётом требований: Федерального закона от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», «Доктрины информационной безопасности Российской Федерации», утвержденной Указом Президента РФ № 646 от 05.12.2016 г., Федерального закона от 28.12.2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», «Методических рекомендаций по разработке программ профессиональной переподготовке и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры. противодействия иностранным техническим разведкам и технической защите информации», утвержденных ФСТЭК России 04.04.2015 г. и примерной программы повышения квалификации, разработанной Минтруда Российской Федерации (письмо Минтруда РФ от 09.09.2013 г.).

Целью обучения по программе является изучение специалистами современных способов управления инцидентами информационной безопасности, получение навыков работы с множеством источников событий аудита ИБ, получение навыков работы в SIEM-системе на продвинутом уровне, получение навыков написания контента для выявления инцидентов ИБ.

Обучающиеся по программе повышения квалификации готовятся к осуществлению следующих профессиональной видов деятельности: аналитик мониторинга Security Operations Center.

Объектами профессиональной деятельности обучающихся являются корпоративные сети.

Поставленная цель достигается решением следующих задач:

Предподготовка по введению в аудит ИБ, категориям и приоритетам событий, архитектурам и механизмам аудита, расширенному аудиту ОС Windows, технологиям Windows Event Forwarding и Windows Event Collector, Sysmon. Также, изучаются типовые корпоративные инфраструктуры в контексте аудита источников в ней.

Изучение и практическая отработка навыков по работе с типовыми источниками событий аудита (ОС Windows, ОС Linux, приложения), практика применения аудита в корпоративных сетях;

Изучение методологии SOC – линии, экспертиза, метрики, процессы.

Изучение последовательности обработки событий в SOC.

Изучение языка написания контента XP в PT MP SIEM. Изучение методологии работы с контентом, структуры контента. Изучение формул нормализации, правил обогащения, правил корреляции.

Навыки контроля за состоянием мониторинга ИБ в корпоративной сети. Ведение статистики срабатываний правил корреляции. Профилирование активности. Работа с исключениями.

Также изучаются другие аспекты работы SOCи аспекты роли аналитика SOC.