Бауманский учебный центр «Специалист»

Программа курса Управление событиями безопасности на базе решений компании Positive Technologies

Код курса: **ДИОПОТЕХ4**

Тема	Ак. часов
Модуль 1. Нормализация событий. Описание таксономии **Практическая работа 1.** Написание правила нормализации событий нестандартного источника. Построение графа нормализации.	**3**
Модуль 2. Корреляция, модельная корреляция. Язык создания правил корреляции **Практическая работа 2.** Модификация системных правил корреляции. **Практическая работа 3.** Создание собственных правил корреляции.	**4**
Модуль 3. Работа с табличными списками **Практическая работа 4.** Создание правил корреляции с использованием табличных списков.	**3**
Модуль 4. Маршрутизация данных внутри системы. Диагностика работоспособности системы **Практическая работа 5.** Поиск неисправностей в системе.	**3**
Модуль 5. Резервное копирование и восстановление компонент MP SIEM	**3**
Аудиторная нагрузка в классе с преподавателем	**16 ак.ч. + 16 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru