Бауманский учебный центр «Специалист»

Программа курса Развертывание и администрирование MaxPatrol SIEM

Код курса: **ДИОПОТЕХ3**

Тема	Ак. часов
Модуль 1. Назначение MaxPatrol SIEM. Упрощенное внедрение системы. Asset management, vulnerability management, SIEM. Компоненты системы, направления развития, потоки данных	**3**
Модуль 2. Asset & vulnerability management. Метрики CVSS 3.0. Контекстные метрики. Банк данных угроз ФСТЭК РФ **Практическая работа.** Задачи, профили, активы • Обнаружение узлов в сети, журналы агента. • Группы активов. • Аудит Windows и Linux. • Назначение контекстных метрик группам.	**3**
Модуль 3. Пользователи и роли **Практическая работа.** Пользователи и роли, инфраструктуры.	**3**
Модуль 4. Сбор и работа с событиями. PDQL и таксономия событий **Практическая работа.** Сбор событий. • Сбор событий по SSH. • Сбор событий с Check Point Gaia по протоколу OPSEC. • Сбор событий Kaspersky Security Center из базы данных Microsoft SQL Server. • Сбор событий по протоколу syslog. • Загрузка событий из файлов. • Поиск событий с помощью языка PDQL. • Группировка событий, создание виджетов и отчетов.	**3**
Модуль 5. Загрузка событий из файла и отладка **Практическая работа.** Загрузка событий. • Загрузка событий модулем filemonitor с отладкой. • Загрузка событий модулем fileimporter. • Аналитика на основе загруженных событий.	**3**
Модуль 6. Доставка уведомлений **Практическая работа.** Доставка почтового уведомления о неполадках источника событий.	**3**
Модуль 7. Установка системы обновлений UCS. Работа с PT KB.	**3**
Модуль 8. Журналы и устранение неполадок	**3**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 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	Для организаций	E-mail
+7 (495) 232-32-16	**+7 (495) 780-48-44**	**info@specialist.ru**