

Курс PCSIEM1 «Администрирование системы мониторинга ИБ McAfee SIEM»



На базе ТОО «Пацифика» во втором квартале 2018 года пройдет СПЕЦИАЛИЗИРОВАННЫЙ КУРС ОБУЧЕНИЯ – «Администрирование системы мониторинга ИБ McAfee SIEM».

SIEM (Security Information and Event Management) – объединение двух терминов, обозначающих область применения ПО: SIM (Security Information Management) – управление информационной безопасностью, и SEM (Security Event Management) – управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий (инцидентов)

безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, устройствами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.

Цель курса

Ознакомление слушателей с вопросами администрирования и внедрения системы мониторинга событий информационной безопасности (SIEM) в компании, а также предоставление системным администраторам, инженерам и специалистам службы информационной безопасности компаний любого масштаба возможности ознакомиться с принципами проектирования, ввода в эксплуатацию и дальнейшего сопровождения системы SIEM на примере продукта McAfee Enterprise Security Manager (ESM). Особенное внимание уделено вопросам, посвященным централизованному управлению и сопровождению инфраструктуры.

Целевая аудитория

Начальники служб ИТ и/или ИБ; технические специалисты, ответственные за защиту информации и информационных технологий.

- **Статус:** Авторский курс учебного центра ТОО «ПАЦИФИКА»
- **Длительность обучения** – 3 дня (30 академических часов)
- **Форма обучения** – аудиторные занятия
- **Стоимость курса:** с одного слушателя 300 000 тг. с учетом НДС
- **На базе центра повышения квалификации:** ТОО «ПАЦИФИКА»
- **Место и даты проведения** – г. Астана, Q2 2018 г.

Требования для прохождения практического курса

Наличие Ноутбука:

1. На ноутбуке должен быть установлен VMware Workstation 11 или более поздняя версия.
2. На VMware Workstation должен быть развернут 64-разрядный Windows Server 2008 (с установленным пакетом исправлений 2 или более поздним) или Windows Server 2012.

Требования к виртуальному серверу:

- a. Процессор:** 64-разрядный процессор Intel Pentium D или выше, с частотой 2,66 ГГц или выше;
- b. Оперативная память:** не менее 2 Гб доступной оперативной памяти (рекомендуется не менее 4 Гб);
- c. Жесткий диск:** не менее 100 Гб доступного дискового пространства.

Пакет слушателя

- Фирменное учебное пособие в электронном виде.

- Организационно-распорядительные и основные нормативно-правовые акты, и методические материалы, на основе которых ведется обучение, дополнительная и справочная информация по тематике курса в электронном виде.

Программа курса

Дата	Наименование	Время
День 1	<ul style="list-style-type: none"> ▪ Вводная презентация к курсу обучения ▪ Вводная презентация по системе McAfee ESM ▪ Установка виртуальной учебной SIEM (3-в-1) ▪ Установка генератора журналов ▪ Первичная настройка через командную строку ▪ Настройка через Веб-консоль ▪ Обзор Веб-консоли ▪ Обзор и добавление источников журналов ▪ Выполнение лабораторных работ 	С 10 час. 00 мин. До 18 час. 00 мин.
День 2	<ul style="list-style-type: none"> ▪ Вводная презентация ко второму дню ▪ Обзор функции автораспознавания источников ▪ Работа с событиями безопасности ▪ Создание Панелей мониторинга (Dashboards) ▪ Обзор Предупреждений (Alarms) ▪ Корреляция событий и движок корреляции ▪ Создание правил корреляции ▪ Выполнение лабораторных работ 	С 10 час. 00 мин. До 18 час. 00 мин.
День 3	<ul style="list-style-type: none"> ▪ Вводная презентация к третьему дню ▪ Отчеты. Создание и настройка отчетов ▪ Создание собственного обработчика журналов ▪ Списки (Watchlists) ▪ Динамические и статичные списки ▪ Управление пользователями ▪ Выполнение лабораторных работ 	С 10 час. 00 мин. До 18 час. 00 мин.

Дополнительная информация

Телефон: +7 (727) 334-15-74

Электронная почта: al@pacifica.kz

Менеджер ТОО «ПАЦИФИКА», Леонтьева Анастасия



ТОО «ПАЦИФИКА»
050060 г. Алматы,
ул. Тимирязева, 42
БЦ «Экспо Сити», Пав.15/7
БИН 080440005514

+7 (727) 334 15 74
+7 (727) 334 15 67
+7 (7172) 28 00 82
info@pacifica.kz
www.pacifica.kz