

Бауманский учебный центр «Специалист»

Программа курса KL 060.4.5: Kaspersky Industrial CyberSecurity Investigation

Код курса: КЛ060

Тема	Ак. часов
Модуль 1. KICS for Networks. Мониторинг сети <ul style="list-style-type: none">Контроль рисков.Информация о сетевых сессиях. Лабораторная работа 1. Настроить интеграцию KICS for Nodes с KICS for Networks. Лабораторная работа 2. Включить обнаружение рисков. Лабораторная работа 3. Включить регистрацию сетевых сессий. <ul style="list-style-type: none">Технологии обнаружения сетевых атак и аномалий.Управление правилами IDS.Обнаружение аномалий в сетевых сессиях.	2
Модуль 2. KICS for Networks. Обнаружение атак и аномалий <ul style="list-style-type: none">Технологии обнаружения.Сценарий возможной атаки.Обнаружение неразрешенных устройств и сетевых взаимодействий.Обнаружение сетевых вторжений (IDS). Лабораторная работа 4. Обнаружить постороннее устройство в сети. Лабораторная работа 5. Обнаружить сканирование сети. Лабораторная работа 6. Обнаружить подбор пароля к сетевому сервису. Лабораторная работа 7. Обнаружить неразрешенное взаимодействие с ПЛК. Лабораторная работа 8. Обнаружить вмешательство в работу ПЛК.	3
Модуль 3. KICS for Networks. Аудит устройств <ul style="list-style-type: none">Контроль конфигурации устройств Windows и Linux. Лабораторная работа 9. Настроить контроль конфигурации устройств. <ul style="list-style-type: none">Обнаружение аномалий с помощью Sigma-правил. Лабораторная работа 10. Настроить обнаружение аномалий с помощью Sigma-правил. <ul style="list-style-type: none">Аудит безопасности устройств по правилам. Лабораторная работа 11. Провести аудит безопасности компьютера SCADA.	2
Модуль 4. KICS for Nodes. Бессигнатурная защита <ul style="list-style-type: none">Защита от эксплойтов.Анализ журналов.	1

Модуль 5. KICS for Nodes. Сигнатурная защита <ul style="list-style-type: none"> Защита файлов. Защита от шифрования. Защита от сетевых угроз. AMSI-защита. Лабораторная работа 12. Настроить защиту узла от программ-вымогателей. Лабораторная работа 13. Настроить защиту узла от сетевых атак. Лабораторная работа 14. Настроить анализ журналов Windows для выявления аномалий в системе.	2
Модуль 6. KICS for Nodes. Портативный сканер	1
Модуль 7. KICS for Nodes. Мониторинг состояния защиты в Kaspersky Security Center <ul style="list-style-type: none"> Формирование отчетов в KSC. 	1
Модуль 8. KICS EDR. Функции и возможности Endpoint Agent <ul style="list-style-type: none"> Функции и возможности Endpoint Agent. Взаимодействия Endpoint Agent. 	1
Модуль 9. KICS EDR. Реагирование на событие обнаружения <ul style="list-style-type: none"> Как реагировать на событие обнаружения? Детали обнаружения. Лабораторная работа 15. Имитировать атаку на сервер SCADA. Лабораторная работа 16. Имитировать атаку на рабочую станцию Admin-ОТ. Лабораторная работа 17. Изучить следы атаки в Kaspersky Security Center. <ul style="list-style-type: none"> Сдерживание угрозы. Проверка компьютеров на наличие индикаторов компрометации. Лабораторная работа 18. Найти индикаторы компрометации. Лабораторная работа 19. Настроить запрет запуска вредоносных скриптов.	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