



Защита виртуальных инфраструктур средствами vGate

Код курса: VG-1

Защита виртуальных инфраструктур средствами vGate

Код курса: VG-1

Длительность	16 ак. часов
Формат	
Разработчик курса	Код безопасности
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс предназначен для изучения работы с сертифицированным программным средством защиты информации vGate и позволяет получить теоретические знания и практические навыки, необходимые для установки и настройки компонентов системы, дальнейшего ее сопровождения, управления политиками безопасности, средствами аудита и мониторинга развернутой в организации виртуальной инфраструктуры.

Подробная информация

Профиль аудитории:

- Данный курс может быть рекомендован системным администраторам и специалистам по информационной безопасности, обеспечивающим развертывание и эксплуатацию виртуальной инфраструктуры и отвечающим за контроль доступа в пределах ее компонентов к конфиденциальной информации.

Предварительные требования:

- Данный курс предполагает наличие у слушателей базовых знаний сетевых технологий, умения работать с серверными платформами Microsoft Windows Server 2008 / 2012, понимания принципов функционирования Microsoft AD, а также базовых навыков развертывания и администрирования виртуальных сред на базе VMWare vSphere 5.x.

По окончании курса слушатели смогут:

- Ознакомиться с особенностями развертывания компонентов vGate, конфигурированием и применением механизмов защиты виртуальных машин, возможностями управления доступом к конфиденциальным ресурсам посредством иерархических и неиерархических меток безопасности.

Программа курса

Модуль 1. Применение vGate для обеспечения информационной безопасности в виртуальной среде.

- Потенциальные угрозы виртуальной инфраструктуры и vGate как актуальное средство защиты
- Архитектура и функциональные возможности vGate
- Особенности развертывания vGate в виртуальной среде: варианты установки и режимы работы системы

Лекция «Потенциальные угрозы виртуальной инфраструктуры и vGate как актуальное средство защиты. Архитектура и функциональные возможности vGate. Особенности развертывания vGate в виртуальной среде: варианты установки и режимы работы системы»

Лабораторный модуль 1. Установка и развертывание компонентов защиты системы vGate. Описание стенда

Лабораторная работа 1. Установка сервера авторизации и компонентов защиты для серверов vCenter, и ESXi

Лабораторная работа 2. Установка и настройка сервера мониторинга

Лабораторная работа 3. Установка агента аутентификации на клиентском компьютере

Модуль 2. Настройка и применение компонентов защиты vGate.

- Применение политик безопасности
- Применение механизма полномочного управления доступом
- Контроль целостности

Лабораторный модуль 2. Настройка конфигурации компонентов защиты системы vGate

Лабораторная работа 1. Добавление на сервере авторизации учетных записей пользователей с разным уровнем доступа к серверу vCenter

Лабораторная работа 2. Настройка и применение политики безопасности, запрещающей прямое подключение к ESXi-серверу

Лабораторная работа 3. Регламентирование доступа к консоли VM. Установка запрета на скачивание файлов VM

Лабораторная работа 4. Настройка контроля целостности виртуальных машин в защищаемом сегменте. Проведение согласования (отклонения) изменений

Лабораторная работа 5. Настройка доступа пользователей к VM в соответствии с уровнем конфиденциальности

Модуль 3. Аудит событий в системе и подготовка отчетов.

- Аудит событий безопасности
- Подготовка и просмотр отчетов

Лабораторный модуль 3. Аудит событий безопасности и подготовка отчетов

Лабораторная работа 1. Настройка перечня регистрируемых в системе событий аудита. Просмотр журнала событий

Лабораторная работа 2. Настройка отправки уведомлений о событиях аудита

Лабораторная работа 3. Генерация отчетов за определенный период по событиям системы vGate

Лабораторная работа 4. Применение утилит командной строки

Модуль 4. Настройка сегментирования и мониторинг событий безопасности.

- Веб-консоль
- Сегментирование
- Мониторинг событий безопасности на объектах виртуальной инфраструктуры

Лабораторный модуль 4. Настройка сегментирования и мониторинг событий безопасности

Лабораторная работа 1. Настройка правил фильтрации трафика в сети виртуальных машин

Лабораторная работа 2. Мониторинг безопасности vGate на объектах виртуальной инфраструктуры

Модуль 5. Некоторые вопросы, связанные с использованием системы vGate.

- Некоторые возможные проблемы при запуске агента аутентификации
- Совместная работа vGate и Secret Net Studio
- Совместная работа vGate и Антивируса Касперского
- Замена основного сервера авторизации vGate в случае сбоя
- Удаление vGate

Лабораторный модуль 5. Уведомления о событиях аудита. Удаление vGate

Лабораторная работа 1. Замена основного сервера авторизации vGate на резервный

Лабораторная работа 2. Удаление vGate

[Посмотреть расписание курса и записаться на обучение](#)

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!



Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline

Вы можете узнать из [профайла](#).