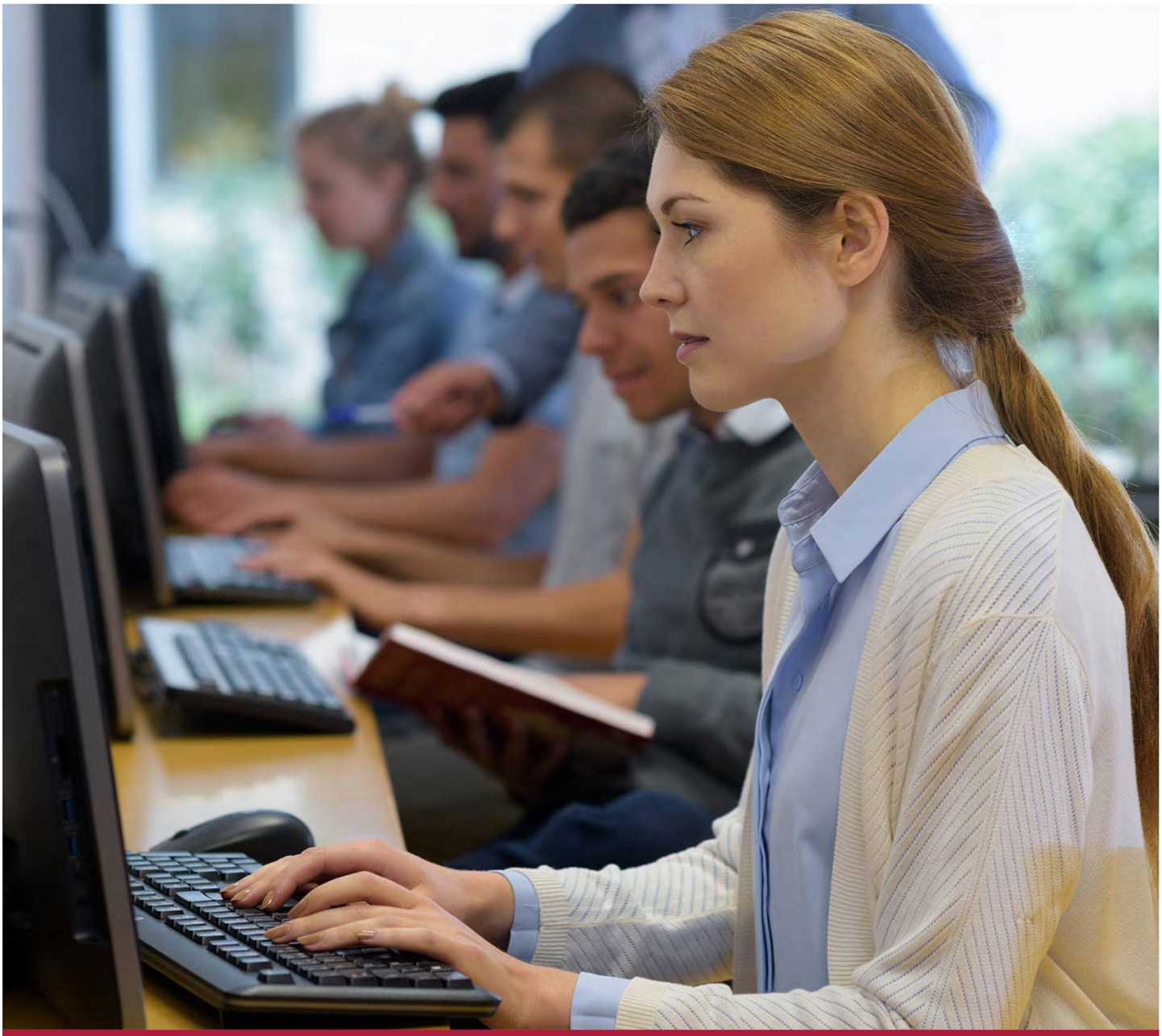
softline®

Учебный центр Softline



# Внедрение ключевых технологий безопасности Cisco (Implementing and Operating Cisco Security Core Technologies)

Код курса: SCOR

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

**Внедрение ключевых технологий безопасности Cisco (Implementing and Operating Cisco Security Core Technologies)**

Код курса: SCOR

| | |
|---|---|
| **Длительность** | 40 ак. часов |
| **Формат** | Очно; Дистанционно |
| **Разработчик курса** | Cisco |
| **Тип** | Учебный курс |
| **Способ обучения** | Под руководством тренера |

## О курсе

Настоящая дополнительная общеобразовательная общеразвивающая программа предназначена для подготовки к внедрению и эксплуатации систем и основных решений в области информационной безопасности корпоративных сетей, а также для подготовки к получению сертификаций Cisco CCNP Security и CCIE Security.

## Подробная информация

**Профиль аудитории:**

- Сетевые администраторы.
- Специалисты систем информационной безопасности, знакомые с функционированием сетей на базе протокола IP и основами работы с сетевым оборудованием CISCO.

**Предварительные требования:**

К освоению программы допускаются лица, обладающие опытом работы с оборудованием CISCO и с доменной инфраструктурой Microsoft Active Directory, имеющими опыт работы с серверными операционными системами и сервисами Microsoft/Linux и опытом эксплуатации, администраторы и инженеры систем информационной безопасности, сетевые инженеры, архитекторы технических решений, специалисты по продаже технических решений Cisco, сетевые интеграторы и партнеры Cisco.

Для успешного прохождения обучения необходимо знать / уметь:

- современные технологии администрирования корпоративных сетей;
- стандарты систем информационной безопасности;
- применять специальные процедуры управления сетевыми устройствами;
- пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;

- применять специальные процедуры установки средств управления сетью;
- настраивать специальные средства управления сетевыми устройствами;
- учитывать и отражать в конфигурации сетевых устройств применяемые стандарты и технологии;
- работать в командной строке с маршрутизаторами и коммутаторами CISCO
- обрабатывать информацию с использованием современных технических средств;
- контролировать качество предоставляемых услуг;
- разбираться в основных концепциях и стандартах, применяемых в современных корпоративных сетях
- использовать программные и технические средства сбора и обработки данных: систем мониторинга оборудования, использовать средства отладки и сбора логирования с оборудования;
- принципы работы основных протоколов коммутации
- принципы работы основных протоколов маршрутизации
- принципах работы платформ виртуализации VMware и Hyper-V
- основные принципы доменной инфраструктуры Microsoft Active Directory
- работать в операционной системе MS Windows
- особенности и отличия принципов работы проводных и беспроводных сетей
- знания и опыт, эквивалентный прохождению курса “Внедрение и администрирование сетевых решений Cisco” (CCNA).

**По окончании курса слушатели смогут:**

- описывать принципы информационной безопасности;
- внедрять контроль доступа на Cisco ASA и Cisco Firepower Next-Generation Firewall;
- внедрять базовые функции безопасности для защиты почтового трафика на Cisco Email Security Appliance;
- внедрять базовые функции безопасности для защиты веб-трафика на Cisco Web Security Appliance;
- разбираться в типах VPN и описывать криптографические алгоритмы, использующиеся в разных системах;
- внедрять решения Cisco для защиты удаленного доступа и настраивать стандарт 802.1X и аутентификацию EAP;
- настраивать механизмы защиты Control, Data и Management Plane на сетевых устройствах
- настраивать механизмы Cisco IOS Software Layer 2 и Layer 3 для защиты Data Plane;
- описывать решения Cisco Stealthwatch Enterprise и Stealthwatch Cloud.

## Программа курса

Модуль 1 «Технологии и решения сетевой безопасности»

- Стратегия Defense-in-Depth
- Сегментация сети и обзор механизмов виртуализации
- Обзор Stateful Firewall и обзор межсетевых экранов нового поколения
- Обзор Security Intelligence
- Стандартизация информации об угрозах
- Обзор сетевой защиты от вредоносного ПО

- Обзор систем предотвращения вторжений
- Обзор Email Content Security
- Обзор Web Content Security
- Обзор Threat Analytic Systems
- Обзор механизмов безопасности DNS
- Аутентификация, авторизация, учет. Управление пользовательскими учетными данными и доступом
- Обзор технологий Virtual Private Network
- Обзор устройств сетевой безопасности

Модуль 2 «Использование межсетевого экрана Cisco ASA»

- Режимы работы Cisco ASA
- Уровни безопасности интерфейсов Cisco ASA
- Объекты и группы объектов в Cisco ASA
- Принцип работы Network Address Translation на Cisco ASA
- Использование ACL на интерфейсах Cisco ASA
- Глобальные ACL на Cisco ASA
- Политики инспектирования Cisco ASA
- Отказоустойчивые топологии Cisco ASA

Модуль 3 «Использование межсетевого экрана Cisco Firepower NGFW»

- Режимы работы Cisco Firepower NGFW
- Процесс обработки пакетов и политики
- Объекты и NAT
- Политики пред-фильтрации
- Политики контроля доступа
- Cisco Firepower NGFW Security Intelligence
- Политики Discovery
- Политики IPS
- Детектирование вредоносного ПО и файловые политики

Модуль 4 «Внедрение Email Content Security (ESA»

- Обзор Cisco Email Content Security
- Обзор SMTP и Email Pipeline
- Public и Private Listeners
- Концепция Host Access Table и Recipient Access Table
- Обзор политик фильтрации почтового трафика
- Защита от Spam и Graymail
- Защита от вирусов и вредоносного ПО
- Фильтры Outbreak
- Фильтрация контента
- Защита от утечки данных
- Шифрование почтового трафика

Модуль 5 «Внедрение Web Content Security (WSA)»

- Обзор решения Cisco Web Content Security, особенности внедрения
- Сетевая аутентификация пользователей
- Расшифровка трафика HTTPS
- Политики доступа и идентификационные политики
- Настройки Acceptable Use Controls
- Защита от вредоносного ПО

Модуль 6 «Описание технологий VPN и криптографические алгоритмы»

- Знакомство с VPN. Типы VPN
- Безопасная передача данных и службы криптографии
- Типы ключей в криптографии
- Обзор инфраструктуры открытых ключей (PKI)

Модуль 7 «Использование Cisco Secure Site-to-Site VPN»

- Технологии Site-to-Site VPN
- Обзор IPsec VPN. IPsec Static Crypto Maps. IPsec Static VTI
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

Модуль 8 «Использование Cisco IOS VTI-Based Point-to-Point»

- Понятие Cisco IOS VTI
- Настройка VTI Point-to-Point IPsec IKEv2 VPN

Модуль 9 «Настройка Point-to-Point IPsec VPN на Cisco ASA и Cisco Firepower NGFW»

- Особенности работы Point-to-Point VPN на Cisco ASA и Cisco Firepower NGFW
- Настройка Cisco ASA Point-to-Point VPN
- Настройка Cisco Firepower NGFW Point-to-Point VPN

Модуль 10 «Настройка удаленного доступа Cisco Secure Remote Access VPN»

- Remote Access VPN. Компоненты и технологии
- Использование SSL для удаленного доступа

Модуль 11 «Настройка удаленного доступа Remote Access SSL VPN на Cisco ASA и Cisco Firepower NGFW»

- Профили подключения и групповые политики удаленного доступа
- Настройки Cisco ASA Remote Access VPN
- Настройки Cisco Firepower NGFW Remote Access VPN

Модуль* «Основные концепции сетевой безопасности»

- Обзор принципов информационной безопасности
- Управление рисками
- Оценка уязвимостей
- Анализ CVSS

Модуль* «Распространенные атаки на протокол TCP/IP»

- Уязвимости стека протоколов TCP/IP
- Уязвимости протоколов 3 уровня
- Уязвимости протоколов 4 уровня
- Векторы атак
- Разведывательные атаки
- Атаки на протоколы доступа
- Атаки вида "Man-In-The-Middle-Attacks"
- Атаки “Denial of Service” и “Distributed Denial of Service”
- Spoofing атаки
- Атаки на DHCP

Модуль* «Распространенные атаки на сетевые приложения»

- Атаки на пароли
- Атаки на сервис DNS
- DNS-туннелирование
- Атаки на веб-сервисы
- Атаки HTTP 302 Cushioning
- Атаки Command Injections
- Атаки SQL Injections
- Атаки Cross-Site Scripting и Request Forgery
- Атаки на протоколы электронной почты

Модуль* «Распространенные атаки на конечные устройства»

- Атаки, связанные с переполнением буфера
- Вредоносное ПО
- Разведка. Получение доступа и контроля
- Настройка маршрутизации голосового вызова через шлюзы и функции доступа к телефонной сети общего пользования.
- Получение доступа с использованием социальной инженерии и атак на веб-трафик
- Exploit Kits, Rootkits, Angler Exploit Kit
- Атаки на повышение привилегий
- Фаза после внедрения

Модуль* «Внедрение Cisco Umbrella»

- Архитектура Cisco Umbrella
- Внедрение Cisco Umbrella
- Cisco Umbrella Roaming Client
- Управление Cisco Umbrella
- Исследование функций Cisco Umbrella

Модуль* «Контроль доступа в сетях Cisco»

- Безопасный доступ к сети
- Сервисы AAA

- Обзор возможностей платформы Cisco Identity Services Engine
- Архитектура Cisco TrustSec

Модуль* «Аутентификация по стандарту 802.1X»

- Доступ к сети с использованием 802.1X и EAP
- Методы EAP
- Роль протокола RADIUS в системе 802.1X
- Использование RADIUS Change of Authorization

Модуль* «Настройка аутентификации 802.1X»

- Настройка 802.1X для проводных сетей на Cisco Catalyst Switch
- Настройка 802.1X для беспроводных сетей на Cisco WLC
- Использование Cisco ISE для аутентификации 802.1X
- Использование Cisco Central Web Authentication

Модуль* «Технологии обеспечения безопасности конечных устройств»

- Межсетевые экраны для конечных устройств
- Антивирусная защита и защита от вредоносного ПО для конечных устройств
- Системы предотвращения вторжений для конечных устройств
- Обзор песочниц
- Белые и черные списки ресурсов на конечных устройствах
- Проверка файлов на конечных устройствах

Модуль* «Использование Cisco AMP for Endpoints»

- Архитектура решения Cisco AMP for Endpoints
- Cisco AMP for Endpoints Engines
- Ретроспективная защита с использованием Cisco AMP
- Построение траекторий файлов с помощью Cisco AMP
- Управление Cisco AMP for Endpoints

Модуль* «Защита сетевой инфраструктуры»

- Плоскости работы сетевого устройства
- Механизмы безопасности Control Plane
- Механизмы безопасности Management Plane
- Телеметрия трафика
- Защита Data Plane на канальном уровне
- Защита Data Plane на сетевом уровне

Модуль* «Внедрение механизмов защиты Control Plane»

- Использование ACL для защиты инфраструктуры
- Политики защиты Control Plane
- Защита Control Plane
- Механизмы защиты протоколов маршрутизации

Модуль* «Внедрение механизмов защиты Data Plane на канальном уровне»

- Обзор механизмов защиты Data Plane
- Защита от атак на VLAN
- Защита от атак на протокол STP
- Защита с использованием Port Security
- Механизм Private VLANs
- Защита от DHCP Snooping
- Механизм ARP Inspection
- Механизм Storm Control
- Технология MACsec

Модуль* «Внедрение механизмов защиты Data Plane на сетевом уровне»

- Защита инфраструктуры Antispoofing ACL
- Использование Unicast Reverse Path Forwarding
- Защита при помощи IP Source Guard

Модуль* «Внедрение механизмов защиты Management Plane»

- Безопасность управления сетевым устройством
- Использование протокола SNMP v3
- Использование AAA для сети управления

Модуль* «Мониторинг сетевого трафика»

- Использование протокола NTP
- Логирование событий на устройствах и экспорт журналов логов
- Мониторинг трафика с использованием Netflow

Модуль* «Использование Cisco Stealthwatch Enterprise»

- Описание системы защиты Cisco Stealthwatch Enterprise
- Используемые сервисы и компоненты Cisco Stealthwatch Enterprise
- Управление потоком данных и мониторинг с использованием Cisco Stealthwatch Enterprise
- Дополнительные возможности и компоненты Cisco Stealthwatch Enterprise
- Интеграция Cisco Stealthwatch Enterprise с платформой Cisco ISE
- Аналитика Cisco Stealthwatch Enterprise
- Шифрование трафика с использованием Cisco Stealthwatch Enterprise
- События, оповещения Cisco Stealthwatch Enterprise
- Хосты, группы хостов, политики по умолчанию Cisco Stealthwatch Enterprise

Модуль* «Облачные сервисы и атаки на облачные ресурсы»

- Облачные сервисы. Основные концепции
- Модели сервисов облачных ресурсов
- Особенности защиты в облачных системах
- Уязвимости в облачных сервисах. Основные проблемы

Модуль* «Безопасность облачных сервисов»

- Использование Cisco Threat-Centric Approach для безопасности сети
- Физическая безопасность облачных ресурсов
- Управление облачными сервисами и защита API интерфейса
- Использование Network Function Virtualization (NFV) и Virtual Network Functions (VNF).
- Мониторинг облачного доступа. Мониторинг защищенности ресурсов
- Использование Cloud Security Broker и Cisco CloudLock
- Понятие OAuth и OAuth Attacks

Модуль* «Использование Cisco Stealthwatch для защиты облачных ресурсов»

- Использование Cisco Stealthwatch для мониторинга Public облачных ресурсов. Возможности
- Использование Cisco Stealthwatch для мониторинга Private облачных ресурсов. Возможности
- Настройки Cisco Stealthwatch для облачных сервисов

Модуль* «Программно - определяемые сети»

- Программно – определяемые сети. Основные концепции
- Автоматизация настроек и сетевое программирование
- API интерфейс для работы с оборудованием Cisco
- Использование скриптов на Python для автоматизации

Примечание: * Модули, предназначенные для самостоятельного изучения

**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 **17 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 Касперсокого, 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 и презентации