Внедрение ключевых технологий безопасности Cisco (SCOR)

ID CI-SCOR **Цена** 195 500,– руб. **Длительность** 5 дней

Кому следует посетить

- Инженерам безопасности
- Сетевым инженерам
- Сетевым дизайнерам
- Сетевым администраторам
- Системным инженерам
- Системным инженерам-консультантам
- Архитекторам технических решений
- Интеграторам / партнерам Cisco
- Сетевым менеджерам

Этот курс является частью следующих программ сертификаций

CCIE Security (CCIE)
Cisco Certified Network Professional Security (CCNP SECURITY)

Предварительные требования

Для прохождения данного курса слушатели должны обладать следующими знаниями и навыками:

- Знания и опыт, эквивалентный прохождению курса Внедрение и администрирование сетевых решений Cisco (CCNA)
- Знания о работе сетей Ethernet и TCP/IP
- Опыт работы с ОС Windows
- Опыт работы с ОС Cisco IOS
- Базовые знания о концепциях сетевой безопасности

Цели курса

После прохождения данного курса слушатели будут уметь:

- Описывать принципы информационной безопасности
- Понимать самые распространенные атаки на сети TCP/IP, сетевые приложения и устройства
- Понимать, как различные технологии сетевой безопасности работаю совместно для защиты от разных типов атак
- 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
- Понимать возможности Cisco Umbrella, схемы внедрения платформы, принципы управления политиками, особенности консоли
- Разбираться в типах VPN и описывать криптографические алгоритмы, использующиеся в разных системах
- Знать, как работают: Cisco site-to-site VPN, Cisco IOS VTI-based point-to-point IPsec VPN, point-to-point IPsec VPN на Cisco ASA и Cisco FirePower NGFW
- Внедрять решения Cisco для защиты удаленного доступа и настраивать стандарт 802.1X и аутентификацию EAP
- Понимать принципы работы решения AMP for Endpoints и как правильно защищать конечные устройства
- Настраивать механизмы для защиты control 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
- Понимать основные принципы защиты облачных инфраструктур от распространенных атак

Содержание курса

- Концепции сетевой безопасности *
- Распространенные атаки на сети TCP/IP *
- Распространенные атаки на сетевые приложения *
- Распространенные атаки на конечные устройства *
- Технологии сетевой безопасности
- Внедрение МСЭ Cisco ASA
- Внедрение МСЭ Cisco Firepower Next-Generation Firewall
- Внедрение решения Email Content Security
- Внедрение решения Web Content Security
- Внедрение решения Cisco Umbrella*
- Изучение технологий VPN и основ криптографической защиты
- Введение в решения Cisco Secure Site-to-Site VPN
- Внедрение Cisco IOS VTI-Based Point-to-Point
- Внедрение Point-to-Point IPsec VPNs на Cisco ASA и Cisco Firepower NGFW
- Введение в решения Cisco Secure Remote Access VPN
- Внедрение Remote Access SSL VPN на Cisco ASA и Cisco Firepower NGFW

- Исследование решений для защиты доступа к сети Cisco Secure Network Access *
- Аутентификация 802.1X *
- Технологии защиты конечных устройств *
- Внедрение Cisco AMP for Endpoints *
- Защита сетевой инфраструктуры *
- Защита Control Plane на сетевых устройствах *
- Защита Layer 2 Data Plane на сетевых устройствах *
- Защита Layer 3 Data Plane на сетевых устройствах *
- Защита Management Plane *
- Traffic Telemetry *
- Внедрение Cisco Stealthwatch Enterprise *
- Распространенные атаки на облачные инфраструктуры *
- Защита облачных инфраструктур *
- Внедрение Cisco Stealthwatch Cloud *
- Введение в SDN *

* Материалы для самостоятельного изучения, которые можно выполнять в своем собственном темпе.

Программа курса

Концепции сетевой безопасности *

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

Распространенные атаки TCP/IP *

- Уязвимости TCP/IP
- Уязвимости сервисов IP
- Уязвимости ICMP
- Уязвимости TCP
- Уязвимости UDP
- Векторы атак
- Разведывательные атаки
- Атаки на протоколы доступа
- Атаки типа "человек по середине"
- Denial of Service и Distributed Denial of Service
- Атаки отражения и усиления
- Атаки типа Spoofing
- Атаки на DHCP

Распространенные атаки на сетевые приложения *

- Атаки на пароли
- Атаки на DNS
- DNS-туннелирование
- Атаки на веб-сервисы
- HTTP 302 Cushioning
- Command Injections
- SQL Injections
- Cross-Site Scripting и Request Forgery
- Атаки на почтовый трафик

Распространенные атаки на конечные устройства *

- Переполнение буфера
- Вредоносное ПО
- Разведка
- Получение доступа и контроля
- Получение доступа с использованием социальной инженерии
- Получение доступа с использованием атак на веб-трафик
- Exploit Kits и Rootkits
- Повышение привилегий
- Фаза после внедрения
- Angler Exploit Kit

Технологии сетевой безопасности

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

Внедрение МСЭ Cisco ASA

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

Внедрение МСЭ нового поколения Cisco Firepower

- Режимы работы Cisco Firepower NGFW
- Процесс обработки пакетов и политики
- Объекты

- NAT
- Политики пред-фильтрации
- Политики контроля доступа
- Cisco Firepower NGFW Security Intelligence
- Политики Discovery
- Политики IPS
- Детектирование вредоносного ПО и файловые политики

Внедрение Email Content Security

- Обзор Cisco Email Content Security
- Обзор SMTP
- Обзор Email Pipeline
- Public и Private Listeners
- Host Access Table
- 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

Внедрение Web Content Security

- Обзор решения Cisco WSA
- Особенности внедрения
- Сетевая аутентификация пользователей
- Расшифровка трафика HTTPS
- Политики доступа и идентификационные политики
- Настройки Acceptable Use Controls
- Защита от вредоносного ПО

Внедрение Cisco Umbrella *

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

Технологии VPN и криптографические алгоритмы

- Знакомство с VPN
- Типы VPN
- Secure Communication and Cryptographic Services
- Типы ключей в криптографии
- Инфраструктура публичных ключей

Cisco Secure Site-to-Site VPN

- Технологии Site-to-Site VPN
- Обзор IPsec VPN
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

Cisco IOS VTI-Based Point-to-Point

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

Point-to-Point IPsec VPNs на Cisco ASA и Cisco Firepower NGFW

- 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

Cisco Secure Remote Access VPN

- Remote Access VPN
- Компоненты и технологии
- Обзор SSL

Remote Access SSL VPN на Cisco ASA и Cisco Firepower NGFW

- Профили подключения
- Групповые политики
- Настройки Cisco ASA Remote Access VPN
- Настройки Cisco Firepower NGFW Remote Access VPN

Контроль доступа в сетях Cisco *

- Безопасный доступ к сети
- Сервисы AAA
- Обзор возможностей платформы Cisco Identity Services Engine
- Архитектура Cisco TrustSec

Аутентификация по стандарту 802.1X *

- 802.1X и EAP
- Методы EAP
- Роль протокола RADIUS в системе 802.1X
- RADIUS Change of Authorization

Конфигурация аутентификации 802.1X *

- Настройки 802.1X на Cisco Catalyst Switch
- Настройки 802.1X на Cisco WLC 802.1X
- Настройки 802.1X на Cisco ISE 802.1X
- Supplicant 802.1x

- Cisco Central Web Authentication

Технологии обеспечения безопасности конечный устройств *

- Хостовые МСЭ
- Хостовые антивирусы
- Хостовые системы предотвращения вторжений
- Белые и черные списки ресурсов на хостах
- Защита от вредносного ПО
- Обзор песочниц
- Проверка файлов

Внедрение Cisco AMP for Endpoints *

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

Защита сетевой инфраструктуры *

- Плоскости работы сетевого устройства
- Механизмы безопасности плоскости контроля
- Механизмы безопасности плоскости управления
- Телеметрия трафика
- Защита плоскости передачи данных на канальном уровне
- Защита плоскости передачи данных на сетевом уровне

Внедрение механизмов защиты плоскости контроля *

- Infrastructure ACLs
- Control Plane Policing
- Control Plane Protection
- Механизмы защиты протоколов маршрутизации

Внедрение механизмов защиты плоскости передачи данных на канальном уровне *

- Обзор механизмов защиты плоскости передачи данных
- Защита от атак на систему VLAN
- Защита от атак на протокол STP
- Port Security
- Private VLANs
- DHCP Snooping
- ARP Inspection
- Storm Control
- Шифрование MACsec

Внедрение механизмов защиты плоскости передачи данных на сетевом уровне *

- Infrastructure Antispoofing ACL
- Unicast Reverse Path Forwarding
- IP Source Guard

Внедрение механизмов защиты Management Plane *

- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Безопасный доступ на устройства Cisco

Телеметрия трафика *

- Network Time Protocol
- Системные события и журналы
- Мониторинг трафика с использованием протокола NetFlow

Внедрение Cisco Stealthwatch Enterprise *

- Обзор решения Cisco Stealthwatch
- Компоненты Cisco Stealthwatch Enterprise
- Flow Stitching и Deduplication

Распространенные атаки на облачные архитектуры *

- История развития облачный вычислений
- Модель облачного сервиса

Механизмы защиты облачной инфраструктуры *

- Подход Cisco Threat-Centric к сетевой безопасности
- Безопасность физической среды облака
- Безопасность приложений и рабочих нагрузок

Внедрение Cisco Stealthwatch Cloud *

- Cisco Stealthwatch Cloud for Public Cloud Monitoring
- Cisco Stealthwatch Cloud for Private Network Monitoring
- Cisco Stealthwatch Cloud Operations

Знакомство с Software-Defined Networking (SDN) *

- Концепции Software-Defined Networking
- Network Programmability and Automation
- Cisco Platforms и APIs

* Данные модули для самостоятельного изучения.