

## Cisco FirePower

### FirePower

اعتبار دهنده: CISCO

پیش نیاز: CCNA&CCNP Security

مدت (ساعت): 70

#### امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
- سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
- مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
- شورای عالی انفورماتیک
- قابلیت ترجمه و تایید قوه قضاییه و امور خارجه
- بهره گیری از لابراتوار سخت افزاری و نرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه های ملی

#### مخاطبان دوره :

- مدیران، کارشناسان و دانشجویان فعال در حوزه فناوری اطلاعات
- مدیران و کارشناسان و فعالان در حوزه امنیت
- کارشناسان بخش SOC سازمان ها

#### معرفی دوره :

در این دوره درباره مبانی فایروال های نسل جدید شرکت سیسکو (Cisco Next Generation Firewalls) خواهیم آموخت و با چگونگی و روش های مختلف راه اندازی و پیاده سازی، پیکربندی و همچنین عیب یابی سرویس های FirePower مربوط به این فایروال ها آشنا خواهیم شد. در بخش دیگری از آموزش های این دوره با سرویس های مختلف امنیتی این نسل از فایروال ها همچون

#### Advanced Malware Protection (AMP)

و سرویس هایی چون WSA و ESA و همچنین ویژگی ها و مشخصات Next Generation IPS آشنا می شویم و نحوه بکار گیری آن را از طریق FirePower Management Center خواهیم آموخت.

در بخشی دیگر از این دوره در مورد

Cisco Firepower Threat Defense و مشخصات و ویژگی های قوی و پیشرفته آن می آموزیم و چگونگی پیاده سازی آن در شبکه های کامپیوتری را بررسی می کنیم.

#### اهداف دوره :

- آشنایی با سرویس FirePower و سخت افزار های مختلفی که قابلیت استفاده از آن را دارند.
- آشنایی با مشخصه های سخت افزاری دستگاه ها و نحوه انتخاب و سفارش آنها و تهیه LOM مناسب.
- آشنایی با لایسنس های مختلف دستگاه ها و مشخصه هر یک از لایسنس های خریداری شده.
- توانایی راه اندازی و مدیریت سرویس های مختلف دستگاه
- توانایی عیب یابی و نگهداری دستگاه ها
- معرفی و پیاده سازی سناریو های متفاوت جهت آشنایی با نحوه عملکرد دستگاه ها در موقعیت های متفاوت



مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزار کننده دوره های آموزشی

Course Outline :	محتوای دوره :
<ul style="list-style-type: none"><li>• Understanding the New Security Threat Landscape and the Attack Continuum</li><li>• Understanding the Cisco ASA Next-Generation Firewalls and the FirePOWER Module</li><li>• Understanding Next-Generation Intrusion Prevention Systems (NGIPS)</li><li>• Understanding Advanced Malware Protection (AMP) for Endpoints and Networks</li><li>• Understanding the Cisco AMP Threat Grid</li><li>• Understanding Cisco Email Security</li><li>• Understanding Cisco Web Security</li><li>• Understanding the Cisco Identity Services Engine (ISE)</li><li>• Understanding the Cisco Meraki Cloud-managed MDM and Security Appliances</li><li>• Understanding Cisco VPN Solutions</li><li>• Introduction to the Cisco Firepower 4100 Series Firewall</li><li>• Cisco Firepower Threat Defense (FTD)</li><li>• Introduction to FX-OS</li><li>• Understanding Inline vs. Promiscuous Mode</li><li>• Understanding Cisco ASA FirePOWER Management Options</li><li>• Understanding Cisco ASA FirePOWER Services Sizing</li><li>• Understanding Cisco ASA FirePOWER Services Licensing</li><li>• Cisco ASA FirePOWER Compatibility with ASA Features</li><li>• Cisco ASA FirePOWER Packet Processing Order of Operations</li><li>• Understanding Cisco ASA FirePOWER Services and High Availability</li><li>• Deploying Cisco ASA FirePOWER Services in the Internet Edge</li><li>• Deploying Cisco ASA FirePOWER Services in VPN Scenarios</li><li>• Deploying Cisco ASA FirePOWER Services in the Data Center</li><li>• Initial Setup of the Cisco ASA FirePOWER Module in Cisco ASA 5585-X Appliances</li><li>• Initial Setup of the Cisco ASA FirePOWER Module in Cisco ASA 5500-X Appliances</li><li>• Configuring the Cisco ASA to Redirect Traffic to the Cisco ASA FirePOWER Module</li><li>• Configuring the Cisco ASA FirePOWER Module Using the (ASDM)</li><li>• Configuring the Cisco ASA FirePOWER Services Module for Firepower Management Center</li><li>• Troubleshooting Cisco ASA with FirePOWER Services</li><li>• Configuring Cisco Firepower Threat Defense</li><li>• Introducing Cisco AMP for Networks</li></ul>	<ul style="list-style-type: none"><li>• Understanding Cisco AMP for Networks Licensing</li><li>• Configuring Cisco AMP for Networks</li><li>• Troubleshooting Cisco AMP for Networks</li><li>• Deploying Cisco AMP for Endpoints</li><li>• Custom Detections</li><li>• Application Control</li><li>• Network IP Blacklists and Whitelists</li><li>• Scheduled Scans</li><li>• Events, File Analysis, Threat Root Cause, and Advanced Reporting</li><li>• Cisco Web Security and AMP</li><li>• Cisco Email Security and AMP</li><li>• Cisco Next-Generation IPS Deployment Scenarios</li><li>• Configuring Cisco Next-Generation IPS Policies and Rules</li><li>• Intrusion Policies Advanced Settings</li><li>• Troubleshooting Cisco Next-Generation IPS Appliances</li><li>• Introduction to the Firepower Management Center</li><li>• FMC Multitenancy and Domains</li><li>• FMC Reporting and Security Operations</li><li>• FTD 6.1 ASA Device Installation</li><li>• FTD 6.1 Firepower Device Manager - Introduction</li><li>• FTD 6.1 Firepower Device Manager - Configuration</li><li>• FTD 6.1 NGFWv and NGIPSv Device Installation</li><li>• FTD 6.1 Device Registration and Smart Licensing</li><li>• FTD 6.1 FMC Web Interface and New Features</li><li>• FTD 6.1 NGIPSv IDS and IPS Modes</li><li>• FTD 6.1 Firewall Mode and Interface Type</li><li>• FTD 6.1 Basic Configuration</li><li>• FTD 6.1 Routing - Static BGP</li><li>• FTD 6.1 Routing - OSPF</li><li>• FTD 6.1 IPv6</li><li>• FTD 6.1 Network Address Translation (NAT)</li><li>• FTD 6.1 Prefilter Policy</li><li>• FTD 6.1 Multicast and QoS</li><li>• FTD 6.1 Safesearch and Youtube EDU</li><li>• FTD 6.1 Inline SGT</li><li>• FTD 6.1 ISE Remediation</li><li>• FTD 6.1 Site-to-Site VPN</li><li>• FTD 6.1 High Availability (HA)</li><li>• FTD 6.1 Conversion to ASA</li></ul>

[www.Cdigit.com](http://www.Cdigit.com)



« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »  
لطفاً در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک 242 تلفن مستقیم آموزش: 88062203، فاکس: 88065222

