

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی  
و برگزار کننده دوره های آموزشی

## CCNA Security & CCNP Security

### Pack CCNA Security & New CCNP Security Part I

اعتبار دهنده: CISCO

پیش نیاز: CCNA

مدت (ساعت): ۷۰

#### امتیازات دوره :

- ▶ اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - سازمان مدیریت و برنامه ریزی کشور ( معلومت 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 لابراتوارسخت افزاری و نرم افزاری مجهز
- ▶ بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه های ملی

#### اهداف دوره :

- ▶ آشنایی با مفاهیم اولیه امنیت شبکه
- ▶ آشنایی با انواع تهدیدات شبکه مانند DOS, Social Engineering
- ▶ آشنایی با متدولوژی AAA و پیاده سازی سامانه ACS
- ▶ آشنایی با امن سازی و پیاده سازی پروتکل های بکار رفته در لایه دو مانند DHCP Snooping, Dynamic Arp Inspection
- ▶ آشنایی و پیاده سازی های اولیه فایروال های ASA
- ▶ آشنایی با سامانه های امنیتی Cisco Prime Infrastructure و GSM
- ▶ آشنایی با پروتکل ۸۰۲.۱x
- ▶ آشنایی با سامانه Cisco ISE و پیاده سازی قابلیت های آن

#### مخاطبان دوره :

- ▶ مدیران، کارشناسان، دانشجویان فعال در حوزه فناوری اطلاعات

#### معرفی دوره :

در بخش اول از امنیت سیسکو بعد از گذراندن چند فصل ابتدایی CCNA Security دو دوره SENSS و SISAS ارائه خواهد شد.

در گذشته مدرک CCNP Security بر اساس تجهیزات امنیتی مانند Firewall و IPS طراحی شده بود اما در ویرایش جدید آن شرکت سیسکو اقدام به طراحی این دوره به تفکیک تکنولوژی های امنیتی بکار رفته در بلاک های مختلف شبکه کرده است.  
این دوره شامل چهار کتاب زیر است:

▶ **SENSS**: در این کتاب افراد با مفاهیم و تکنولوژی های بکار رفته در لبه شبکه شامل DHCP Snooping , Dynamic ARP Inspection و... آشنا خواهند شد. شرکت سیسکو توصیه به گذراندن دوره FIREWALL در حین گذراندن این کتاب کرده است که مطالب آن در این پک گنجانده شده است.

▶ **SISAS**: در این کتاب مفاهیم و تکنولوژی های بکار رفته در بلاک دسترسی شبکه شامل آشنایی با پروتکل 802.1x و با پیاده سازی قابلیت های Cisco ISE آشنا خواهند شد.

▶ **SIMOS**: در این کتاب مفاهیم و تکنولوژی های VPN هم بر روی تجهیز ASA و هم بر روی Router های سیسکو را پوشش خواهد داد. این کتاب ترکیبی از دو کتاب SECURE و FIREWALL است.

▶ **SITCS**: در این کتاب افراد با فایروال های نسل بعدی سیسکو و سرویس های بکار رفته بر روی آن و تجهیز IPS آشنا خواهند شد همچنین با سامانه های امنیتی Cloud Web Security و WSA و ESA آشنا خواهند شد.

این دوره کاملاً بر اساس سرفصلهای ارائه شده توسط شرکت سیسکو طراحی شده است و به صورتی است که افراد پس از گذراندن این دوره توانایی شرکت در آزمون رسمی شرکت سیسکو را خواهند داشت.

www.Cdigit.com



مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزار کننده دوره های آموزشی

Course Outline :	محتوای دوره :
<p><b>CCNA Security 210-260 Part I</b></p> <p><b>Fundamentals of Network Security</b></p> <ul style="list-style-type: none"><li>• Networking Security Concepts</li><li>• Common Security Threats</li></ul> <p><b>Secure Access</b></p> <ul style="list-style-type: none"><li>• Implementing AAA in Cisco IOS</li><li>• Bring Your Own Device (BYOD)</li></ul> <p><b>Secure Routing and Switching</b></p> <ul style="list-style-type: none"><li>• Securing Layer 2 Technologies</li><li>• Network Foundation Protection</li><li>• Securing the Management Plane on Cisco IOS Devices</li><li>• Securing the Data Plane in IPv6</li><li>• Securing Routing Protocols and the Control Plane</li></ul> <p><b>CCNP Security Part I</b></p> <p><b>• Implementing Cisco Edge Network Security Solutions (SENSS 300-206)</b></p> <p><b>Threat Defense</b></p> <ul style="list-style-type: none"><li>• Implement firewall</li><li>• Implement Layer 2 Security</li><li>• Configure device hardening per best practices</li></ul> <p><b>Cisco Security Devices GUIs and Secured CLI Management</b></p> <ul style="list-style-type: none"><li>• Implement SSHv2, HTTPS, and SNMPv3 access on the network devices</li><li>• Implement RBAC on the ASA/IOS using CLI and ASDM</li><li>• Describe Cisco Prime Infrastructure</li><li>• Describe Cisco Security Manager (CSM)</li><li>• Implement Device Managers</li></ul> <p><b>Management Services on Cisco Devices</b></p> <ul style="list-style-type: none"><li>• Configure NetFlow exporter on Cisco Routers, Switches, and ASA</li><li>• Implement SNMPv3</li><li>• Implement logging on Cisco Routers, Switches, and ASA</li><li>• Implement NTP with authentication on Cisco Routers, Switches, and ASA</li><li>• Describe CDP, DNS, SCP, SFTP, and DHCP</li></ul>	<p><b>Troubleshooting, Monitoring and Reporting Tools</b></p> <ul style="list-style-type: none"><li>• Monitor firewall using analysis of packet tracer, packet capture, and syslog</li></ul> <p><b>Threat Defense Architectures</b></p> <ul style="list-style-type: none"><li>• Design a Firewall Solution</li><li>• Layer 2 Security Solutions</li></ul> <p><b>Security Components and Considerations</b></p> <ul style="list-style-type: none"><li>• Describe security operations management architectures</li><li>• Describe Data Center security components and considerations</li><li>• Describe Collaboration security components and considerations</li><li>• Describe common IPv6 security considerations</li></ul> <p><b>• Implementing Cisco Secure Access Solutions (SISAS 300-208)</b></p> <p><b>Identity Management and Secure Access</b></p> <ul style="list-style-type: none"><li>• Implement device administration</li><li>• Describe identity management</li><li>• Implement wired/wireless 802.1X</li><li>• Implement MAB</li><li>• Implement network authorization enforcement</li><li>• Implement Central Web Authentication (CWA)</li><li>• Implement profiling</li><li>• Implement guest services</li><li>• Implement posture services</li><li>• Implement BYOD access</li></ul> <p><b>Threat Defense</b></p> <ul style="list-style-type: none"><li>• Describe TrustSec Architecture</li></ul> <p><b>Troubleshooting, Monitoring, and Reporting Tools</b></p> <ul style="list-style-type: none"><li>• Troubleshoot identity management solutions</li></ul> <p><b>Threat Defense Architectures</b></p> <ul style="list-style-type: none"><li>• Design highly secure wireless solution with ISE</li></ul> <p><b>Design Identity Management Architectures</b></p> <ul style="list-style-type: none"><li>• Device administration</li><li>• Identity Management</li><li>• Profiling</li><li>• Guest Services</li><li>• Posturing Services</li><li>• BYOD Access</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 ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸۸۰۶۵۲۲۲۲ فاکس:

