

Curriculum Overview - Information Security Training for Campus Technical Staff

Course Developed	Course In Development	Course Sheet Completed	Locally-Driven	Cooperatively-Driven	System-Driven
------------------	-----------------------	------------------------	----------------	----------------------	---------------

Information Security <i>Info</i>	Security Management <i>Mgmt</i>	Network <i>Netw</i>	Server <i>Serv</i>	Desktop <i>Desk</i>	Programmer <i>Prog</i>	Database Admin. <i>Data</i>
<i>General</i>	<i>Organizational</i>	<i>Technical</i>			<i>Developer</i>	
101: Information security overview, background, concepts	101: The need for security and the need for security planning	101: Networking concepts and overview			101: Principles of Security in Software Development	
102: The ten domains of information security	102: Establishing, integrating & supporting the information security framework; internal controls & segregation of duties; roles & responsibilities	102: Layers, protocols, topologies and packets			102: How and Why Web Development is Different	
	111: User Provisioning and De-provisioning	111: Network device management - SSH and Central Authentication	111: Data Backups	111: Strong Password Techniques for Users	111: OWASP and the Top Ten Web Application Security Flaws	
201: System Hardening and Documentation	201: Defense in depth: security technologies by layer	201: Segmenting Network Access - Subnets and VLANs	201: Managing Admin Rights and Remote Access	201: Host-based Firewalls	201: Secure Programming Techniques - How to Avoid the Top Ten	201: Managing Database Privileges
202: Change Management	211: Security governance and business alignment, risk analysis & management	211: Hardening network devices	211: Hardening Servers - Windows and Mac/UNIX/LINUX	211: Malware detection/prevention software	211: Software Development Life Cycle	
211: Test Environments	221: Security policies	221: Wireless network management	221: Intrusion Detection, Prevention, and File Integrity Monitoring			
			231: Centralized Logging and Event Monitoring			

Curriculum Overview - Information Security Training for Campus Technical Staff

Information Security <i>Info</i>	Security Management <i>Mgmt</i>	Network <i>Netw</i>	Server <i>Serv</i>	Desktop <i>Desk</i>	Programmer <i>Prog</i>	Database Admin. <i>Data</i>
301: Physical and Environmental Controls	301: Legal and ethical issues in information security	301: Access control lists	301: Server & Workstation Patch Management	301: Desktop Hardening: Running Applications without Administrator Privileges	301: Source Code Security Audits	
	311: Risk Management	321: DMZ	311: Virtualization	311: Malware investigation & removal		
		331: Network Access Controls	321: Advanced Server Management via Scripting and Directory Services			

Curriculum Overview - Information Security Training for Campus Technical Staff

Information Security <i>Info</i>	Continuity of Operations <i>Coop</i>	Incident Response <i>Inci</i>	nCircle IP360 <i>Ncip</i>	Security Event Info. Mgmt. <i>Seim</i>	Mobile Device Encryption <i>Encr</i>	AJAX <i>Ajax</i>
<i>General</i>	<i>Organizational</i>		<i>Technical</i>			<i>Developer</i>
		101: Introduction to Incident Response	101: Introduction to IP360 for Campus Staff			
			201: IP360 Reporting Filters and the Focus Interface		211: Check Point Full Disk Encryption: Administration and Deployment	
			211: Installation and Configuration of a Device Profiler		221: Check Point Media Encryption/Pointsec Protector	
		301: Acquiring Evidence for Incident Response	301: IP360 API Access and Scripting		311: Advanced Check Point Full Disk Encryption: Administration and Support	
			311: VNE Administration - Backups, Repository Access, and Upgrades			
			312: VNE and Device Profiler Troubleshooting			