



InfoSec Academy Incident Handling Track

Fundamental Courses	Foundational Courses	Specialized Courses	Advanced Courses	Certification Preparation Courses
Texas Security & Policy Assurance Soft Skills	Certified Security Sentinel	Certified Information Systems Security Officer	Certified Incident Handling Engineer	N/A Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Certified Information Systems Auditor (CISA) Certified Ethical Hacker (CEH)



InfoSec Academy

Incident Handling Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Texas Security Policy & Assurance Course	Upon successful completion of this course, the participant will be prepared to apply the state rules regarding information security in the state of Texas within their agency.	ISOs & CISOs	Module 1: Texas Rules and Legislation Modules 2: Data Classification Module 3: Security Framework Module 4: Agency Security Plans Modules 5: Reports Modules 6: Security Services
Soft Skills Course (examples): Team Building Without Time Wasting Helping Employees Use Their Time Wisely Everybody Wins: How to Turn Conflict into Collaboration	A variety of soft skills courses are available covering a wide range of topics.	Dependent on the course	N/A



InfoSec Academy

Incident Handling Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Security Sentinel - C)SS	<p>The Certified Security Sentinel certification course is intended for anyone that uses a computer on the internet. Attendees will not only understand security threats and attacks but also be prepared with countermeasures for these attacks. The weakest link in any companies' security program is a poorly trained employee. Once a student understands what can happen, they will know what to look for. And with that understanding, be able to keep the information they have been entrusted with as safe as possible.</p> <p>The social engineering portion of the class is designed to teach the participants the skills used by social engineers to facilitate the extraction of information from an organization using technical and non-technical methods. Computer fraud, black-hat hacking, and cyber-terrorism are all phrases that describe crimes that use over-the-wire technology to attack, steal, and terrorize their victims. The key to most of these over-the-wire attacks being successful is information they receive through social engineering. Does it work? Can smart people be easily deceived? Kevin Mitnick, who served five years in prison for repeated hacking said in testimony before Congress on the subject of Social Engineering: "I was so successful with that attack that I rarely had to resort to a technical attack." If you're afraid of having your identity, credit card credentials, or business information compromised, then this is the training you have been looking for.</p> <p>The Certified Security Sentinel certification course trains students on how attacks are performed, how to identify an attack, and how to secure information. One of the most valuable skill sets of a C)SS is that they understand how to train others on security as well.</p>	Employees who need to learn the basics of security.	Module 1: Basic Computer Security Module 2: User Awareness Module 3: Implementation Countermeasures Module 4: Essential Security Awareness Module 5: Using the Internet at Work Module 6: Accessing the Network Locally Module 7: Accessing the Network Remotely Module 8: Social Engineering Module 9: Understanding and Interacting with our Target Module 10: Researching Our Target Module 11: Methods of Deception



InfoSec Academy

Incident Handling Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Information Systems Security Officer - C)ISSO	<p>The Certified Information Systems Security Officer course is designed for forward-thinking security professionals that want the advanced skillset necessary to manage and consult businesses on information security.</p> <p>The C)ISSO addresses the broad range of industry best practices, knowledge and skills expected of a security leader. The candidate will learn both the theory and the requirements for practical implementation of core security concepts, practices, monitoring and compliance. Through the use of a risk-based approach, a C)ISSO is able to implement and maintain cost-effective security controls that are aligned with business requirements.</p> <p>Whether you are responsible for the management of a Cyber Security team, a Security Officer, an IT auditor or a Business Analyst, the C)ISSO course is the ideal way to increase your knowledge, expertise, skill, and credibility.</p> <p>The C)ISSO program standards are closely aligned with those of the ISO27001, NIST, CISM® and the CISSP® CBK® exam objectives. The C)ISSO excels by providing a well-rounded, comprehensive overview of essential security topics.</p>		Module 1: Risk Management Module 2: Security Management Module 3: Identification and Authentication Module 4: Access Control Module 5: Security Models and Evaluation Criteria Module 6: Operations Security Module 7: Symmetric Cryptography and Hashing Module 8: Asymmetric Cryptography and PKI Module 9: Network Connections Module 10: Network Protocols and Devices Module 11: Telephony, VPNs and Wireless Module 12: Security Architecture and Attacks Module 13: Software Development Security Module 14: Database Security and Development Module 15: Malware and Software Attacks Module 16: Business Continuity Module 17: Disaster Recovery Module 18: Incident Management, Law, and Ethics Module 19: Physical Security



InfoSec Academy

Incident Handling Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Incident Handling Engineer - C IHE	<p>The Certified Incident Handling Engineer course is designed to help incident handlers, system administrators, and general security engineers understand how to plan, create, and utilize their systems in order to prevent, detect, and respond to security breaches. Every business connected to the internet is getting probed by hackers trying to gain access. The ideal situation I to prevent this from happening, but realistically every business needs to know how to detect and resolve security breaches. Certified Incident Handlers are prepared to do handle these situations effectively.</p> <p>Students will learn common attack techniques, vectors, and tools used by hackers, so that they can effectively prevent, detect, and respond against them. This course is ideal for those who lead incident handling teams or are part of an incident handling team.</p> <p>Furthermore, students will enjoy numerous hands-on laboratory exercises that focus on topics, such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, malware and using Netcat plus several additional scenarios for both Windows and Linux systems. The 20 hours of experience in our labs is what will put you ahead of the competition and set you apart as a leader in incident handling.</p>	Security Consultant System Administrator IT Professional Chief Technology Officer	Module 1: Introduction Module 2: Threats, Vulnerabilities, and Exploits Module 3: Identification and Initial Response Module 4: RTIR Module 5: Preliminary Response Module 6: Identification and Initial Response Module 7: Sysinternals Module 8: Containment Module 9: Eradication Module 10: Follow-Up Module 11: Recovery Module 12: Virtual Machine Security Module 13: Malware Incident Response Lab 1: Netcat (Basics of Backdoor Tools) Lab 2: Exploiting and Pivoting our Attack Lab 3: Creating a Trojan Lab 4: Capture FTP Traffic Lab 5: ARP Cache Poisoning Basics Lab 6: ARP Cache Poisoning - RDP Lab 7: Input Manipulation Lab 8: Shoveling a Shell Lab 9: Virus Total Lab 10: Create Malware using SET Lab 11: The Trojans Lab 12: Examine System Active Processes and Running Services Lab 13: Examine Startup Folders Lab 14: The Local Registry Lab 15: The IOC Finder – Collect Lab 16: IOC Finder – Generate Report