Information Security

Information security professionals are responsible for research and analysis of security threats that may affect an organization’s assets, products, or technical specifications. These security professionals will dig deeper into technical protocols and specifications related to security threats than most of their peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

**CORE COURSES**

- **SEC301** Intro to Information Security GSF
- **SEC401** Security Essentials Bootcamp Style GSEC
- **SEC501** Advanced Security Essentials — Enterprise Defender GCED

**TECHNICAL INTRODUCTORY**

- **SEC301** (GISF)
- **SEC401** (GSEC)

**CORE**

- **SEC504** Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

**IN-DEPTH**

- **SEC560** Network Penetration Testing and Ethical Hacking GPEN
- **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GXPN
- **SEC760** Advanced Exploit Development for Penetration Testers

**NETWORK & EXPLOITS**

- **SEC580** Python for Penetration Testers
- **SEC570** Metasploit Kung Fu for Enterprise Pen Testing

**WEB**

- **SEC542** Web App Penetration Testing and Ethical Hacking GWAPT
- **SEC642** Advanced Web App Penetration Testing and Ethical Hacking

**LAB-CENTERED**

- **SEC551** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)
- **SEC561** CyberCity Hands-on Kinetik Cyber Range Exercise

**MOBILE/WIRELESS**

- **SEC575** Mobile Device Security and Ethical Hacking GMOB
- **SEC617** Wireless Ethical Hacking, Penetration Testing & Defenses GAWN

**SPECIALIZATION**

- **SEC583** Penetration Testing and Ethical Hacking GPEN
- **SEC580** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking GXPN
- **SEC780** Advanced Exploit Development for Penetration Testers

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, write modern exploits, and recommend mitigations before those vulnerabilities are exploited by real-world attackers.

**Risk and Compliance/Auditing/Governance**

These experts assess and report risks to the organization by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organization more efficient and profitable through continuous monitoring of risk management.

**SAMPLE JOB TITLES**

- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect

- Penetration tester
- Vulnerability assessor
- Ethical hacker
- Red/Blue team member
- Cyberspace engineer

- Auditor
- Compliance officer
The security-savvy software developer leads all developers in creating secure software and implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.
Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to and mitigate a security incident.

Digital Forensic Investigations and Media Exploitation

With today’s ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. Government organizations also need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.