## COOLEST CAREERS IN CYBER

Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in-demand by employers. Which jobs are the coolest and most in-demand? We know; let us show you the hottest cybersecurity jobs for 2023.

### Curricula:
- Cyber Defense
- Digital Forensics
- Offensive Operations
- Cybersecurity Leadership
- Cloud Security
- Industrial Control Systems
- Purple Team

### Recommended Courses

#### 01 Threat Hunter (Threat/Warning Analyst)
- This role involves identifying potential security threats and warning organizations of potential attacks. Threat hunters investigate suspicious activity, analyze data, and develop strategies to prevent future attacks.
- **Why is this role important?**
  - Threat hunters are crucial in identifying and responding to potential security incidents before they become major threats.
- **Recommended courses**
  - FOR508
  - MGT514
  - GCSA

#### 02 Red Teamer (Adversary Emulation Specialist)
- Red teamers simulate attacks to test the effectiveness of security measures. They aim to find weaknesses in systems and networks and suggest improvements to enhance security.
- **Why is this role important?**
  - Red teaming helps organizations prepare for real-world attacks and improve their security posture.
- **Recommended courses**
  - FOR572
  - MGT553
  - SEC540

#### 03 Digital Forensic Cyber Defense Forensics Analyst
- Digital forensic analysts collect and analyze evidence from digital devices to investigate cyber crimes. They help determine the source and nature of cyber attacks.
- **Why is this role important?**
  - Digital forensics is essential for understanding what happened in a cyber attack and for building cases against attackers.
- **Recommended courses**
  - SEC504
  - GWEB
  - GDCS

#### 04 Purple Teamer
- Purple teamers test the vulnerabilities of a system or network by exploiting security weaknesses. They help organizations prepare for real-world attacks.
- **Why is this role important?**
  - Purple teams provide valuable insights into the weaknesses of a system that can be used to improve security measures.
- **Recommended courses**
  - MGT514
  - GCSA
  - SEC660

#### 05 Malware Analyst
- Malware analysts investigate malicious software to understand how it works and to develop methods to prevent its spread. They are responsible for identifying new malware threats.
- **Why is this role important?**
  - Malware analysts help protect organizations from cyber threats by identifying and mitigating the impact of malware.
- **Recommended courses**
  - FOR508
  - MGT553
  - SEC540

#### 06 Chief Information Security Officer (CISO) (Executive Cyber Leadership)
- The CISO is responsible for setting the overall security strategy and ensuring that it is implemented effectively. They lead a team of security professionals and collaborate with business leaders.
- **Why is this role important?**
  - The CISO plays a critical role in protecting the organization from cyber threats by overseeing the development and implementation of security policies and procedures.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 07 Blue Teamer – All-Around Defender (Cyber Defense Analyst)
- Cyber defense analysts work to protect networks and systems from cyber attacks. They monitor and respond to threats in real-time.
- **Why is this role important?**
  - Cyber defense analysts are crucial in defending against cyber threats and protecting the integrity of the organization's systems.
- **Recommended courses**
  - SEC402
  - GCTD
  - SEC401

#### 08 Security Architect (NICE) and Engineer (Executive Cyber Leadership)
- Security architects design and implement security solutions that meet business needs. They ensure that security is integrated into the overall design of a system or network.
- **Why is this role important?**
  - Security architects are responsible for planning and designing security systems that protect the organization from cyber threats.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 09 Cyber Defense Incident Responder/Law Enforcement Counterintelligence Forensics Analyst
- Cyber defense incident responders investigate security incidents and provide evidence for legal proceedings. They work with law enforcement agencies to combat cyber crime.
- **Why is this role important?**
  - Cyber defense incident responders are essential in gathering evidence and presenting it in court.
- **Recommended courses**
  - FOR508
  - MGT553
  - SEC540

#### 10 Cybersecurity Analyst/Engineer (Systems Security Analyst)
- Systems security analysts ensure that systems are secure and comply with security policies. They work with IT departments to implement preventive measures.
- **Why is this role important?**
  - Systems security analysts help protect the organization's systems from cyber threats by ensuring they are secure and compliant.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 11 OSINT Investigator/Analyst
- OSINT investigators collect open-source intelligence to inform decision-making. They gather information from public sources such as social media to understand potential threats.
- **Why is this role important?**
  - OSINT investigators are crucial in understanding external threats and in developing strategies to mitigate them.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 12 Technical Director (Information Systems Security Manager)
- Technical directors oversee the technical aspects of information security. They work with IT departments to implement security policies and procedures.
- **Why is this role important?**
  - Technical directors are responsible for ensuring that the organization's systems are secure and compliant with industry standards.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 13 Cloud Security Analyst
- Cloud security analysts ensure that cloud-based systems are secure. They work with cloud service providers to implement security measures.
- **Why is this role important?**
  - Cloud security analysts are crucial in protecting the organization's data and systems in the cloud.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 14 Intrusion Detection/SOC Analyst
- Intrusion detection/security operations center (SOC) analysts monitor systems for security threats in real-time. They work with incident responders to manage security incidents.
- **Why is this role important?**
  - Intrusion detection/security analysts are essential in identifying and responding to security incidents in real-time.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 15 Security Awareness Officer (Security Awareness & Communications Manager)
- Security awareness officers educate employees about security best practices. They work with HR to implement security awareness training programs.
- **Why is this role important?**
  - Security awareness officers are crucial in educating employees to prevent security incidents.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 16 Vulnerability Researcher & Exploit Developer (Vulnerability Assessment Analyst)
- Vulnerability researchers develop vulnerability assessment tools. They work with IT departments to identify and exploit security vulnerabilities.
- **Why is this role important?**
  - Vulnerability researchers help identify security weaknesses that can be exploited by attackers.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 17 Application Pen Tester (Secure Software Accessor)
- Application pen testers test the security of software applications. They identify vulnerabilities in the software that could be exploited by attackers.
- **Why is this role important?**
  - Application pen testers help protect the organization from software-based attacks.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 18 ICS/JOT Security Assessment Consultant (ICS/SCADA Security Engineer)
- ICS/JOT security assessment consultants assess the security of industrial control systems. They work with ICS teams to identify and mitigate security risks.
- **Why is this role important?**
  - ICS/JOT security assessment consultants help protect industrial systems from cyber threats.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 19 DevSecOps Engineer (Information Security Systems Developer)
- DevSecOps engineers implement security practices in the development and operations process. They work with development teams to ensure security is integrated into the development process.
- **Why is this role important?**
  - DevSecOps engineers help prevent security incidents by ensuring security is considered at every stage of the development process.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588

#### 20 Media Exploitation Analyst (Cyber Crime Investigator)
- Media exploitation analysts analyze media to extract information. They work with intelligence agencies to identify and track cyber criminals.
- **Why is this role important?**
  - Media exploitation analysts help identify and track cyber criminals by analyzing media.
- **Recommended courses**
  - SEC510
  - GPEN
  - SEC588