Cyber Security Career in 2024

Joas A Santos

https://www.linkedin.com/in/joas-antonio-dos-santos/

GRC Professional (Governance, Risk, and Compliance):

- **Responsibilities**: Develop security policies, monitor compliance with regulations, assess risks, manage audits.
- **Certifications**: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), GRC Professional Certification (GRCP), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Project Management Institute – Risk Management Professional (PMI-RMP), Certification in Risk Management Assurance (CRMA).
- **Training**: Experience in auditing, understanding security regulations.
- **Required Hard Skills**: Knowledge of security regulations, analytical skills, communication ability.
- **Soft Skills**: Teamwork, effective communication, decision-making.

Offensive Security Professional:

- **Responsibilities**: Test systems for vulnerabilities, conduct penetration testing, perform adversary simulation campaigns, social engineering campaigns, red team exercises, and report vulnerabilities.
- **Certifications**: Certified Red Team Operator (CRTO), Certified Red Team Leader (CRTL), Offensive Security Certified Professional (OSCP), Certified Red Team Professional (CRTP), Certified Red Team Expert (CRTE), Certified Red Team Analyst (CRTA), Certified Red Team Specialist (CRTS), Offensive Security Experienced Penetration Tester.
- **Training**: Experience in penetration testing, knowledge of exploits, experience in Red Team, knowledge of social engineering.
- **Required Hard Skills**: Knowledge of penetration testing, programming skills, understanding of exploits, and more.
- **Soft Skills**: Critical thinking, creativity, problem-solving.

Application Security Professional:

- **Responsibilities**: Ensure secure application development, identify code vulnerabilities, conduct security testing.
- **Certifications**: Certified Application Security Tester (CAST), Certified Secure Software Lifecycle Professional (CSSLP), Certified Application Security Engineer (CASE), Certified AppSec Practitioner (CAP), Certified DevSecOps Engineer (ECDE), Offensive Security Web Expert (OSWE), Offensive Security Web Assessor (OSWA).
- **Training**: Experience in secure software development, knowledge of application threats. Tanya Janca Training and OWASP Training
- **Required Hard Skills**: Knowledge of programming languages, understanding of application threats, testing skills.
- **Soft Skills**: Collaboration, communication skills, attention to detail.

vCISO Professional (Chief Information Security Officer Virtual):

- **Responsibilities**: Provide strategic security guidance, lead the security team, assess risks, and mitigation strategies.
- **Certifications**: CISSP, Certified Information Security Manager (CISM), Certified Information Security Manager (CISA), Chief Information Security Officer (CCISO).
- **Training**: Experience in security management, understanding of business.
- **Required Hard Skills**: Leadership, business understanding, risk management.
- **Soft Skills**: Leadership, interpersonal skills, strategic vision.

Data Science with a Focus on Cybersecurity:

- **Responsibilities**: Analyze data to identify threats, develop threat detection models, create security reports.
- **Certifications**: Data Science Certification, Machine Learning Certification.
- **Training**: Programming in Python, data analysis.
- **Required Hard Skills**: Data analysis, machine learning, programming.
- **Soft Skills**: Problem-solving, adaptability, communication.

AI Engineer with a Focus on Cybersecurity:

- **Responsibilities**: Develop AI solutions for detecting cyber threats, automate incident response, enhance security.
- **Certifications**: AWS Machine Learning.
- **Training**: Machine Learning, Neural Networks, AI Security.
- **Required Hard Skills**: Knowledge of AI, machine learning, programming.
- **Soft Skills**: Problem-solving, critical thinking, innovation.

SOC Professional (Security Operations Center):

- **Responsibilities**: Monitor networks and systems, identify real-time threats, coordinate incident responses.
- **Certifications**: CompTIA Security+, Certified Cisco Network Analyst, Network+, Blue Team Labs 1 and 2, eLearnSecurity Certified Threat Hunting, SC-900, Certified SOC Analyst (CSA).
- **Training**: SOC training, Try Hack Me, Blue Team Labs, and Lets Defend.
- **Required Hard Skills**: Security monitoring, log analysis, threat understanding.
- **Soft Skills**: Teamwork, effective communication, time management.

Incident Response Professional:

- **Responsibilities**: Handle security incidents, investigate attacks, coordinate recovery and security improvements.
- **Certifications**: Certified Incident Handler (ECIH), eLearnSecurity Incident Response (eCIR), GIAC Certified Incident Handler (GCIH), Certified Computer Security Incident Handler (CSIH), Certified Incident Handling Engineer (CIHE), Certified Computer Hacking Forensic Investigator (CHFI).
- **Training**: Incident response training, digital forensics. Try Hack Me and Lets Defend.
- **Required Hard Skills**: Incident investigation, digital forensics, knowledge of security tools.
- **Soft Skills**: Decision-making under pressure, communication skills, critical analysis.

Cloud Security Professional:

- **Responsibilities**: Protect data and systems in cloud environments, configure security policies, monitor threats.
- **Certifications**: Certified Cloud Security Professional (CCSP), AWS Certified Security – Specialty, Google Cloud Security Engineer (GCSE), SC-200, SC-900, Certificate of Cloud Security Knowledge (CCSK), CCSP - Certified Cloud Security Professional (CCSP), Hybrid Multi-Cloud Red Team Specialist (CHMRTS), Certified Cloud Security Engineer (CCSE).
- **Training**: Cloud security training, AWS Security.
- **Required Hard Skills**: Knowledge of cloud services, secure configuration, monitoring.
- **Soft Skills**: Project management, adaptability, quick learning.

IAM Security Professional (Identity and Access Management):

- **Responsibilities**: Manage user identities, control system and data access, implement authentication policies.
- **Certifications**: CERTIFIED IDENTITY AND ACCESS MANAGER (CIAM), CERTIFIED ACCESS MANAGEMENT SPECIALIST (CAMS), CERTIFIED IDENTITY GOVERNANCE EXPERT (CIGE), CERTIFIED IDENTITY MANAGEMENT PROFESSIONAL (CIMP), SC-300 Microsoft.
- **Training**: IAM training, identity and product management.
- **Required Hard Skills**: IAM implementation, authentication knowledge, access control, programming.
- **Soft Skills**: Communication, conflict management, teamwork.

Information Security Architect:

- **Responsibilities**: Design the organization's security structure, ensure all security policies and measures are effective.
- **Certifications**: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Defensible Security Architect (GDSA), Advanced Security Practitioner (CASP +), Cloud Security Professional (CCSP), and Certified Network Defender (CND).
- **Training**: Security architecture, security project management.
- **Required Hard Skills**: Security architecture, business understanding, risk analysis.
- **Soft Skills**: Effective communication, leadership, strategic vision.

Cybersecurity Awareness Professional:

- **Responsibilities**: Educate employees and the public on safe cybersecurity practices, create awareness programs.
- **Certifications**: Certified Security Awareness Practitioner (CCAP), SANS Security Awareness (SSAP), NCSC, Security Awareness and Culture Professional SACP.
- **Training**: Development of awareness programs, security training.
- **Required Hard Skills**: Development of awareness programs, security knowledge.
- **Soft Skills**: Communication skills, empathy, creativity.

DevSecOps

- **Responsibilities**: Integrate security into the DevOps process, automate security testing, and ensure security is part of the software development lifecycle.
- **Certifications**: Certified DevSecOps Professional (DevSecOps Institute), Certified DevSecOps Engineer (ISACA), Certified Kubernetes Security Specialist (CKS), Certified DevSecOps Engineer (ECDE)
- **Training**: DevSecOps practices, automation tools, secure coding. HackMD, Try Hack Me, Practical DevSecOps, AppSec Engineer
- **Required Hard Skills**: Automation scripting, knowledge of security tools, software development.
- **Soft Skills**: Collaboration, communication, and problem-solving skills.

ICS/OT Security (Industrial Control Systems/Operational Technology Security)

- **Responsibilities**: Protect critical infrastructure systems, such as power plants and manufacturing facilities, from cyber threats, ensure the reliability and safety of industrial processes.
- **Certifications**: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified SCADA Security Architect (CSSA), Certified Information Systems Auditor (CISA), Certified Automation Professional (CAP).
- **Training**: Understanding of ICS/OT systems, network security, and industrial protocols.
- **Required Hard Skills**: Knowledge of ICS/OT systems, network security, and industrial protocols.
- **Soft Skills**: Analytical thinking, attention to detail, problem-solving, and communication skills.

Threat Hunting and Malware Analysis

- **Responsibilities**: Proactively search for cyber threats within an organization's network, analyze and reverse-engineer malware to understand its behavior.
- **Certifications**: Certified Threat Intelligence Analyst (CTIA), Certified Cyber Threat Hunting Professional (CCTHP), Certified Reverse Engineering Analyst (CREA), Certified Malware Analyst (CMA).
- **Training**: Threat hunting techniques, malware analysis tools, network traffic analysis.
- **Required Hard Skills**: Proficiency in threat hunting tools, malware analysis, network forensics.
- **Soft Skills**: Critical thinking, attention to detail, strong problem-solving abilities, and the ability to think like an attacker.