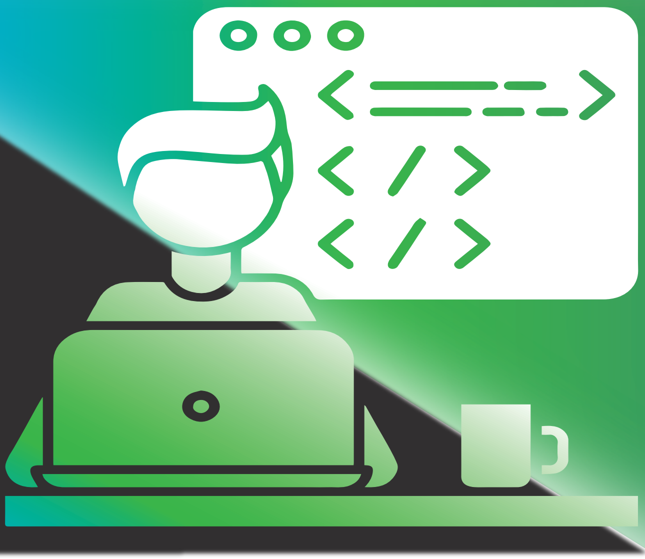
Certified Secure Application Developer



Median Salary

$70,000

Job Growth

24%

Soft Skills

Analytical

Good Communicator

Attention to Detail

Adhere to a Schedule

Common Job Duties

- Develop, create, maintain, and write code for web-based applications
- Design, implement and test software
- Assist in the development of a company-wide software security strategy
- Create new software and forensic tools in compliance with company security strategy
- Participate in the lifecycle development of software systems using different methodologies
- Institute programing techniques that are free from logical design, technical implementation, and security flaws.
- Gain a thorough knowledge of attack vectors that may be used to exploit software
- Support software deployments

Mile2 Cybersecurity Certification's Suggested Course Progression

C)VA	C)PEH	C)PTE	C)SWAE
Vulnerabity Assessor	Professional Ethical Hacker	Penetration Testing Engineer	Secure Web Application Engineer

Person who passes all 4 certification exams in the above progression will earn the Master Cyber Secure Application Developer. This individual will be able to use vulnerability and pentesting assessment skills to discover current threats and then develop secure web applications using the skills that ethical hackers and software developers have in order to create secure programs from the ground up. The Secure Application Developer certificate holder should be able to implement secure programing protocols through each stage of the software development cycle and suggest overal policies and proceedures for secure application development.

Issued by
CERTIFIED
MASTER
SECURE
APPLICATION
DEVELOPER
Mile2 Cybersecurity Certifications

Certified Secure Application Developer

ABILITIES

- Use and understand complex mathematical concepts
- Apply cybersecurity principles to organizational requirements
- Identify critical infrastructure systems with information communication technology that were designed without system security considerations.
- Function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.

KNOWLEDGE

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes (e.g., methods for assessing and mitigating risk).
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cybersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cybersecurity lapses.
- Complex data structures.
- Computer programming principles
- Organization's enterprise information security architecture.
- Organization's evaluation and validation requirements.
- Cybersecurity and privacy principles and methods that apply to software development.
- Cybersecurity and privacy principles and organizational requirements
- Local area and wide area networking principles and concepts including bandwidth management.
- Low-level computer languages (e.g., assembly languages).
- Operating systems.
- Privacy Impact Assessments.
- Programming language structures and logic.
- System and application security threats and vulnerabilities
- Secure configuration management techniques.
- Software debugging principles.
- Software design tools, methods, and techniques.
- Software development models (e.g., Waterfall Model, Spiral Model).
- Software engineering.
- Structured analysis principles and methods.
- System design tools, methods, and techniques, including automated systems analysis and design tools.
- Web services
- Interpreted and compiled computer languages.
- Secure coding techniques.
- Software related information technology (IT) security principles
- Software quality assurance process.
- Supply chain risk management standards, processes, and practices.
- Critical infrastructure systems with information communication technology that were designed without system security considerations.
- Secure software deployment methodologies, tools, and practices.
- Network security architecture concepts including topology, protocols, components, and principles
- Security architecture concepts and enterprise architecture reference models
- Application firewall concepts and functions
- Personally Identifiable Information (PII) data security standards.
- Payment Card Industry (PCI) data security standards.
- Personal Health Information (PHI) data security standards.
- Information technology (IT) risk management policies, requirements, and procedures.
- Embedded systems.
- Penetration testing principles, tools, and techniques.
- Root cause analysis techniques.
- Application Security Risks

SKILLS

- Conducting vulnerability scans and recognizing vulnerabilities in security systems.
- Designing countermeasures to identified security risks.
- Developing and applying security system access controls.
- Discerning the protection needs of information systems and networks.
- Integrating black box security testing tools into quality assurance process of software releases.
- Secure test plan design.
- Using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications
- Using code analysis tools.
- Performing root cause analysis.
- Apply cybersecurity and privacy principles to organizational requirements.

TASKS

- Apply coding and testing standards, apply security testing tools and conduct code reviews.
- Apply secure code documentation.
- Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
- Develop threat model based on customer interviews.
- Consult with engineering staff to evaluate interface between hardware and software.
- Evaluate factors such as reporting formats required, cost constraints, to determine hardware configuration.
- Identify basic common coding flaws at a high level.
- Identify security implications and apply methodologies within centralized and decentralized environments.
- Identify security issues around steady state operation and management of software when a product reaches its end of life.
- Perform integrated quality assurance testing for security functionality.
- Perform risk analysis.
- Address security implications in the software acceptance phase.
- Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
- Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
- Perform penetration testing as required.
- Consult with customers about software system design and maintenance.
- Direct software programming and development of documentation.
- Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
- Analyze and provide information to stakeholders that will support the development of security application or modification of an existing app.
- Analyze security needs and software requirements to determine feasibility of design within time and cost constraints.
- Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
- Develop secure software testing and validation procedures.
- Develop system testing and validation procedures, programming, and documentation.
- Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
- Determine and document software patches or the extent of releases that would leave software vulnerable.

If a person holds the Master Secure Application Developer from Mile2, we certify that they have passed the four certification exams in the role-based progression and thereby has adequate KSA's listed above to complete the applicable tasks required for the job role of Secure Application Developer.