Certified Intrusion Prevention Specialist

Median Salary

$100,000

Job Growth

+20%

Soft Skills

Curiosity & Insight

Strong Communication

Creative Problem Solver

Ability to Write Reports

Capable of Quick Thinking

Common Job Duties

- Perform vulnerability testing, penetration testing, risk analyses and security assessments
- Identify security gaps and suggest improvement plans
- Create new ways to solve existing cybersecurity issues
- Evaluate new technologies and processes that enhance security capabilities
- Draft technical reports following vulnerability and penetration testing activities
- Identify emerging cyber threats and technologies to combat them while enhancing security capabilities
- Advise on and/or build firewalls and intrusion and detection systems
- Create strategies to improve the security of cyber systems

Mile2 Cybersecurity Certification's Suggested Course Progression

C)VA	C)PEH	C)PTE	C)PTC
Vulnerabity Assessor	Professional Ethical Hacker	Penetration Testing Engineer	Penetration Testing Consultant

Person who passes all 4 certification exams in the above progression will earn the Master Intrusion Prevention Specialist certification. This person will be able to assess a company's security posture, perform in-depth penetration testing using a variety of assessment tools, and set up dynamic defenses to prevent intrusion. They will have a firm understanding of cyrptography and various attacks and be able to execute the 5 key elements of a Pen Test; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. They will be able to function within a larger cybersecurity team and protect operating systems from attack.

10213 Wilsky Blvd, Tampa, FL 33625 Phone: +1-813-920-6799 Toll Free: +1 800-816-4532

Certified Intrusion Prevention Specialist

ABILITIES

- Identify systemic security issues based on the analysis of vulnerability and configuration data.
- Communicate complex information, concepts, or ideas in a confident and well-organized manner.
- Apply programming language structures and logic.
- Function effectively in a dynamic, fast-paced environment
- Share meaningful insights about the context of an organization's threat environment that improve its risk management posture.
- Identify intelligence gaps.
- Recognize and mitigate cognitive biases which may affect analysis.
- Recognize and mitigate deception in reporting and analysis.
- Think like threat actors.
- Apply cybersecurity and privacy principles to organizations

KNOWLEDGE

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cbersecurity and privacy principles.
- Cyber threats and vulnerabilities.
- Operational impacts of cybersecurity lapses.
- Application vulnerabilities.
- Cryptography and cryptographic key management concepts
- data backup and recovery.
- Host/network access control mechanisms
- Human-computer interaction principles.
- Cybersecurity and privacy principles and organizational requirements
- Network access, identity, and access management
- Network traffic analysis methods.
- Traffic flows across the network
- Programming language structures and logic.
- System and application security threats and vulnerabilities
- Systems diagnostic tools and fault identification techniques.
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
- Knowledge of interpreted and compiled computer languages.
- Concepts, terminology, and operations of a wide range of communications media
- Physical computer components and architectures, including the functions of various components and peripherals
- Different classes of attacks
- Cyber attackers
- System administration, network, and operating system hardening
- Cyber attack stages
- Network security architecture concepts including topology, protocols, components, and principles
- Security models
- Ethical hacking principles and techniques.
- Data backup and restoration concepts.
- System administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
- Infrastructure supporting information technology (IT) for safety, performance, and reliability.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Packet-level analysis using appropriate tools
- Cryptology.
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Penetration testing principles, tools, and techniques.
- Knowledge of an organization's threat environment.
- Knowledge of website types, administration, functions, and content management system (CMS).
- attack methods and techniques (DDoS, brute force, spoofing, etc.).
- Classification and control markings standards
- Common computer/network infections
- Computer networking fundamentals
- Current computer-based intrusion sets.
- Cyber intelligence/information collection capabilities and repositories.
- Cyber operations terminology/lexicon.
- Data communications terminology
- Encryption algorithms and cyber capabilities/tools
- Evolving/emerging communications technologies.
- Fundamental cyber operations concepts, terminology/lexicon principles, capabilities, limitations, and effects.
- Supervisory control and data acquisition (SCADA) system components.
- Host-based security products and how those products affect exploitation and reduce vulnerability.
- How Internet applications work
- Knowledge of how modern digital and telephony networks impact cyber operations.
- How modern wireless communications systems impact cyber operations.
- How to extract, analyze, and use metadata.
- Intelligence disciplines.
- Intelligence preparation of the environment and similar processes.
- Intelligence support to planning, execution, and assessment.
- Internal tactics to anticipate threat capabilities and actions.
- Internet network addressing
- Knowledge of malware.
- Operations security.
- Organizational hierarchy and cyber decision-making processes.
- Physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
- Telecommunications fundamentals.
- Basic structure, architecture, and design of modern communication
- Basics of network security
- Common networking and routing protocols services and how they interact to provide network communications.
- The ways in which targets or threats use the Internet.
- Threat and/or target systems.
- Virtualization products
- What constitutes a "threat" to a network.
- Wireless technologies to include the basic structure, architecture, and design of modern wireless communications systems.
- Application Security Risks

SKILLS

- Conducting vulnerability scans and recognizing vulnerabilities in security systems.
- Assessing the robustness of security systems and designs.
- Detecting host and network based intrusions
- Mimicking threat behaviors.
- Use of penetration testing tools and techniques.
- Use of social engineering techniques.
- Using network analysis tools to identify vulnerabilities.
- Reviewing logs to identify evidence of past intrusions.
- Conducting application vulnerability assessments.
- Performing impact/risk assessments.
- Conducting non-attributable research.
- Conducting research using deep web.
- Defining and all pertinent aspects of the operational environment.
- recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
- Evaluating information for reliability, validity, and relevance.
- Identifying alternative analytical interpretations to minimize unanticipated outcomes.

If a person holds the Master Cyber Intrusion Prevention 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 Intrusion Prevention Specialist .

Certified Intrusion Prevention Specialist

•Identifying critical target elements, to include critical target elements for the cyber domain.
• Identifying cyber threats which may jeopardize organization and/or partner interests.
• Preparing and presenting briefings.
• Providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.
• Tailoring analysis to the necessary levels.
• Using Boolean operators to construct simple and complex queries.
• Using multiple analytic tools, databases, and techniques.
• Using multiple search engines and tools in conducting open-source searches.
• Utilizing feedback to improve processes, products, and services.
• Utilizing virtual collaborative workspaces and/or tools.
• Writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
• Develop insights about the context of an organization's threat environment
• Apply cybersecurity and privacy principles to organizational requirements.

TASKS

• Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
• Conduct and/or support authorized penetration testing on enterprise network assets.
• Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
• Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
• Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
• Conduct required reviews as appropriate within environment.
• Perform technical and nontechnical risk and vulnerability assessments of relevant technology focus areas.
• Make recommendations regarding the selection of cost-effective security controls to mitigate risk.
• Answer requests for information.
• Provide subject matter expertise to the development of a common operational picture.
• Maintain a common intelligence picture.
• Provide subject matter expertise to the development of cyber operations specific indicators.
• Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
• Assist in the identification of intelligence collection shortfalls.
• Brief threat and/or target current situations.
• Collaborate with intelligence analysts/targeting organizations involved in related areas.
• Conduct in-depth research and analysis.
• Conduct nodal analysis.
• Develop information requirements necessary for answering priority information requests.
• Evaluate threat decision-making processes.
• Identify threats to Blue Force vulnerabilities.
• Generate requests for information.
• Identify threat tactics, and methodologies.
• Identify intelligence gaps and shortfalls.
• Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.
• Monitor and report on validated threat activities.
• Monitor open source websites for hostile content directed towards organizational or partner interests.
• Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.
• Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
• Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
• Provide current intelligence support to critical internal/external stakeholders as appropriate.
• Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
• Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
• Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
• Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
• Report intelligence-derived significant network events and intrusions.
• Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.

If a person holds the Master Cyber Intrusion Prevention 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 Intrusion Prevention Specialist .