Certified Cyber Threat Analyst

Median Salary

$80,000

Job Growth

+20%

Soft Skills

Curiosity & Insight

Strong Communication

Attention to Detail

Ability to Write Reports

Interested in Hacking

Common Job Duties

- Develop cyber indicators to maintain awareness of the status of a dynamic operating environment
- Collect, process, analyze, and disseminate cyber threat/warning assessments
- Create new ways to solve existing cybersecurity issues
- Use manual testing techniques and methods to gain a better understanding of the environment
- Draft technical reports following inspection, forensic investigations, and penetration testing activities
- Compile and track vulnerabilities over time and suggestions and procedures to combat them.
- Advise on and/or build firewalls and intrusion and detection systems
- Suggest strategies to improve the security of cyber systems

Mile2 Cybersecurity Certification's Suggested Course Progression

C)VA	C)PEH	C)TIA	C)CSA
Vulnerabity Assessor	Professional Ethical Hacker	Threat Intelligence Analyst	Cybersecurity Analyst

Person who passes all 4 certification exams in the above progression will earn the Master Cyber Threat Analyst Certification. Persons with this certification have demonstrated the knowledge needed to proactively monitor, detect, prevent, and mitigate threats as they arise in real time. They have also shown that they can set up and deploy analysis tools, intrusion detection tools, syslog servers, SIEMs to find and in many cases, prevent, exploits. They will have demonstrated an ability to detect cyber attacks and deploy blue team tactics to help prevent future attacks. Plus an ability to effectively communicate suggestions and procedures.

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

Certified Cyber Threat Analyst

ABILITIES

- Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Accurately and completely source all data used in intelligence, assessment and/or planning products.
- Clearly articulate intelligence requirements into well-formulated research questions.
- Collaborate via virtual teams.
- Evaluate information for reliability, validity, and relevance
- Evaluate, analyze, and synthesize large quantities of data into high quality, fused tageting/intelligence products.
- Focus research efforts to meet the customer's decision-making needs
- Funtion in a collaborative environment to leverage analytical and technical expertise.
- Identivy intelligence gaps.
- Recognize and mitigate cognitvie biases.
- Think critically.
- Think like threat actors.
- Utilize multiple intelligence sources across all intelligence disciplines.

KNOWLEDGE

- Knowledge of fundamental cyber operations concepts, terminology/lexicon, principles, capabilities, limitations, and effects.
- General 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
- 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 and/or emulate threat capabilities and actions.
- Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
- Knowledge of malware.
- Knowledge of operations security.
- Knowledge of 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 networks.
- Basics of network security
- Common networking and routing protocols, services and how they interact to provide network communications.
- Ways in which targets or threats use the Internet.
- Threat and/or target systems.
- Virtualization products (VMware, Virtual PC).
- What constitutes a "threat" to a network.
- Wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.

SKILLS

- Conducting non-attributable research.
- Conducting research using deep web.
- Defining and characterizing all pertinent aspects of the operational environment.
- Developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
- Ealuating information for reliability, validity, and relevance.
- Identifying alternative analytical interpretations to minimize unanticipated outcomes.
- 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.

TASKS

- 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
- 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.
- 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.
- Provide subject-matter expertise and support to planning/ d evelopmental 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.

If a person holds the Master Cyber Threat Analyst 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 Cyber Threat Analyst.