Cybersecurity Training and Employment Advanced Diploma

Your journey from newbie to cybersecurity pro begins here!

Step into a Security Operations Center (SOC), and you're not just walking into a job, you're stepping into a high-stakes arena where the puzzles are real, complex, and fraught with immediate consequences. This is an environment that buzzes 24/7, where the glow of multiple screens lights up the faces of cybersecurity warriors like you, each one a guardian of the digital realm. Your curiosity isn't just a trait; it's your weapon, constantly driving you to dig deeper into the labyrinthine networks you monitor. Alerts and anomalies are your daily bread, each a riddle begging to be solved: Is that traffic spike an incoming DDoS attack? Is the unusual login from a foreign country a potential breach? Your analytical skills kick into overdrive as you sift through data, chasing down clues and connecting the dots in a race against the clock. In a SOC, you're part Sherlock Holmes, part digital samurai, every moment is a chance to thwart an attack, uncover a hidden vulnerability, or unmask a would-be intruder. It's not just a job; it's a thrilling, never-ending quest to safeguard the digital world, one puzzle at a time.

But where does anybody even begin to learn how to do this? That's where our innovative cybersecurity training enters the picture!

Imagine yourself in a dimly lit room filled with glowing monitors, your fingertips dancing across the keyboard. Something is wrong in the data you've been sifting through, someone is trying to break into your network…and it's *your* job to find and stop them. You dig through event logs, scrutinize packets of data, and piece together the digital puzzle. Just when you hit a roadblock, your mentor is there for you, offering a critical clue that helps you untangle the web of malicious activity.

This isn't just another lecture-driven course, this is an interactive, story-based saga where YOU are the protagonist. *Welcome to the most exhilarating learning experience of your life.*

Who is this course for?

If your curiosity knows no bounds, if you find puzzles not just enticing but essential, if you don't know the term "give up," then you've stumbled upon your next great challenge. You don't need a deep technical background, just a willingness to dive into the nitty-gritty details, a penchant for self-directed learning, and the time, patience, and tenacity to fail, adapt, and succeed. *(Learn more about what it takes to succeed in cybersecurity.)*

What will you do?

- **Analyze a Remote Intrusion Attempt:** Make split-second decisions as you sift through logs originating from a web server under threat. Can you identify if passwords were compromised?
- **Investigate a Watering Hole Attack:** Your mentor guides you through a labyrinthine web where malicious code lurks in the shadows. Do you have what it takes to trace the source?
- **Compile Indicators of Compromise:** Turn into a digital detective, learning how to read the fingerprints to gather evidence for identifying the malware used in a cyberattack.
- **Examine a Compromised Host's Memory:** What crucial secrets are hidden within a powered-on device—vanishing the moment you pull the plug? Can you spot the anomaly where evil lurks?
- **Conduct Forensic Disk Examination:** Tear apart an infected system to find out how it got that way—tracing the roots of the malware attack back to its very source.
- **Close Your Investigation:** Craft an immaculate report that makes sense to both tech geeks and complete novices. Your findings will be the linchpin for fortifying cybersecurity defenses—and preventing future attacks.

As your final “capstone” task in the program, you will study for and then take the CompTIA Security+ Certification exam, an industry-recognized credential for entry-level cybersecurity analysts.

Taken together, the complete sequence of tasks in Cybersecurity Training Advanced Diploma Program gives you the foundational requirements to set you on your career path in the exciting and growing field of cybersecurity. The accelerated pace of skill acquisition enabled by our unique training method prepares you for an entry-level job in a matter of months, instead of the years of study usually required to achieve similar competency in traditional cybersecurity training programs.

Your mentor awaits

You're not alone as you embark on this journey. Your online mentor will offer just-in-time, one-on-one advice, guiding your way but never handing you the answers. Your skills will be tested, your resilience fortified, and your intellectual boundaries pushed.

Are you ready?

This is more than a course; it's a gauntlet thrown at your feet. Do you dare to pick it up? Uncover mysteries, thwart cyber-villains, and emerge as a cybersecurity pro. Your journey starts now. Welcome to learning cybersecurity the CSGA way, where the story is yours to write, but the stakes are very real.

Enroll today and unleash the cyber sleuth in you!

...curiosity piqued?

Discover if you have what it takes to seize this unique opportunity to enter the fast-growing field of cybersecurity! Check out the FAQ below for more information about this exciting certification program.

Frequently Asked Questions

About the program

What courses are involved in this program?

1. Cybersecurity: Immediate Immersion *(8 weeks, 120 hours total)*:

In this introductory cybersecurity course, students immerse themselves in the world of digital defense. Through three engaging tasks, they acquire practical cybersecurity skills. Initially, students identify a vulnerability on a website, exploit it, and subsequently secure the same vulnerability. Next, they assume the role of digital detectives, investigating suspicious user behavior by analyzing network traffic to assess potential threats. Lastly, students explore the field of cyber threat analysis, closely examining malicious network activity.

Immediate Immersion equips students with hands-on experience, preparing them for more significant cybersecurity challenges in NON-118E. By the course's conclusion, students will have gained practical experience with industry-standard tools such as Wireshark, Network Miner, and Burp Suite and will have a clear understanding of whether cybersecurity is the right career path for them.

See FAQ question "What tasks are included in this program?" for a description of the specific tasks included in the NON-108E course.

2. Cybersecurity Defense *(15 weeks, 375 hours total)*:

In this advanced course consisting of six tasks, students embark on a comprehensive journey through real-world cyber threats and defenses. The course begins with the analysis of a possible remote intrusion attempt, challenging students to investigate potential breaches within critical networks. They dive deeper into cyber investigations, exploring "watering hole" attacks, compiling indicators of compromise, and conducting memory and disk forensics. The course culminates in students closing their investigations, crafting polished reports suitable for their portfolios. Throughout, students gain practical experience using industry-standard tools like Splunk, Wireshark, Volatility, Autopsy, Virus Total, Hybrid Analysis, and ANY.RUN.

Upon completing NON-118E, students will have gained practical experience in investigating two different cybersecurity incidents, equipped with the skills and documentation necessary to kickstart their careers in the dynamic field of cybersecurity.

See FAQ question "What tasks are included in this program?" for a description of the specific tasks included in the NON-118E course.

3. CompTIA SECURITY+ Certification Exam *(2–8 weeks; time variable depending on student)*:

BMCC' mentors provide assistance while you prepare for the CompTIA Security+ SY0-601 Certification Exam using Udemy's 21-hour preparation course as well as their Practice Exams. The Security+ certification is an industry-recognized credential that opens the door to entry-level positions as a cybersecurity analyst in a Security Operations Center (SOC).

- See also "What industry-standard certificate do I earn at the end of this program?" for more details about this specific capstone certification.

4. Certified AI Analyst Program (200-hours)

The Certified AI Analyst Program is a practical, workforce-focused training program designed to prepare learners to understand, evaluate, and safely deploy artificial intelligence systems in real-world organizational environments. Delivered through applied, scenario-based learning, the program emphasizes how AI systems are built, trained, governed, and monitored, with a strong focus on data integrity, risk, ethics, and responsible use. Students gain the foundational knowledge needed to assess AI outputs, identify misuse or bias, and support AI-driven decision-making across business, cybersecurity, government, and emerging technology sectors.

Rather than teaching how to simply build AI models, the Certified AI Analyst Program focuses on how AI is used, trusted, secured, and governed in operational settings. Learners work through realistic cases involving AI data pipelines, model behavior, regulatory considerations, and human-AI interaction, supported by expert mentors. Upon completion, graduates are prepared for entry-level AI analyst, AI governance, technology risk, and AI operations support roles, and are equipped with a recognized certification that demonstrates practical readiness in one of the fastest-growing areas of the modern workforce.

5. Certified Cyber Ranges Program (20-hours)

The Certified Cyber Ranges Program is a hands-on, immersive training program designed to prepare learners to operate, analyze, and defend within realistic cyber range environments that mirror real-world enterprise and critical infrastructure networks. The program focuses on practical cyber defense skills, situational awareness, and decision-making under pressure, allowing students to experience live attack and defense scenarios in a controlled, ethical setting. Learners gain direct exposure to how cyber incidents unfold, how defenders respond, and how systems are tested, monitored, and secured across complex digital environments.

Rather than relying on theoretical instruction, the Certified Cyber Ranges Program emphasizes learning by doing through guided simulations, red and blue team exercises, and incident response scenarios supported by expert mentors. Students develop the ability to interpret alerts, analyze adversary behavior, coordinate defensive actions, and evaluate security controls in real time. Upon completion, graduates are prepared for entry-level and intermediate roles in security operations, cyber defense, incident response, and cyber training environments, and earn a recognized certification demonstrating practical readiness to perform in modern cyber operations centers.

What tasks are included in this program?

I. Cybersecurity: Immediate Immersion *(8 weeks, 120 hours total)*:

1. Exploit a Website (and Fix Its Vulnerabilities): A military contractor's website has a critical vulnerability that allows access to sensitive files on the web server. By actively exploiting the vulnerability, you gain access to the webmaster's hashed password, crack it, and then log in to the webserver to address the vulnerability that was just exploited.

2. Insider Threat: Suspicious text was observed on an employee's computer screen. You will analyze a packet capture (PCAP) file of the employee's network traffic to determine whether this person's actions were potentially malicious and assess whether they pose any risk to the company.

3. Analyze Malicious Network Traffic: The security operations center has detected suspicious network traffic associated with a personal laptop used by a military aide. You must analyze a PCAP file of the suspicious network traffic to determine whether it is malicious, identify its source, ascertain whether the aide's computer is infected with malware, and if so, specify the type of malware.

II. Cybersecurity Defense *(15 weeks, 375 hours total)*:

1. Analyze a Remote Intrusion Attempt: A fellow security operations center analyst has detected potential evidence of a brute-force attack within a critical network. Analyze a PCAP file and event logs within a security information and event management system (the Splunk SIEM) to determine if any passwords were compromised and if the network experienced a breach as a consequence.

2. Investigate an Incident Using a SIEM: Analyze a potential "watering hole" attack, where simply visiting a seemingly legitimate website can trigger an exploit kit, resulting in a user's machine being infected with common banking trojan malware.

3. Compile Indicators of Compromise to Guide Forensic Analysis: Leverage the hash of a possibly malicious file to conduct research, utilizing tools like Virus Total, online sandboxes, and open-source intelligence sources. This research aims to identify specific indicators of compromise, which will then guide the forensic analysis of memory and file system images of infected devices.

4. Examine a Compromised Host's Memory: Conduct a forensic examination of a memory image retrieved from a device to identify sophisticated malware that has compromised the system.

5. Conduct a Forensic Disk Examination: Analyze a computer's file system image to find corroborating evidence of the attack and discover new indicators of compromise.

6. Close Your Investigation: Compile a timeline for the attack and write a comprehensive report for technical and non-technical stakeholders.

III. The CompTIA SECURITY+ Certification Exam *(2–8 weeks; time variable depending on student)*:

The SY0-601 CompTIA Security+ Certification Exam consists of 90 questions covering the following domains. To prepare for this exam, you can utilize Udemy's 21-hour preparation course:

- **Threats, Attacks and Vulnerabilities:** Analyze indicators of compromise, determine types of malware, or compare and contrast types of attacks.

- **Identity and Access Management:** Implement identity and access management controls, or differentiate common account management practices.

- **Technologies and Tools:** Troubleshoot common security issues or deploy mobile devices securely.
- **Risk Management:** Explain the importance of policies, plans and procedures related to organizational security.
- **Architecture and Design:** Summarize secure application development, deployment, cloud, and virtualization concepts.
- **Cryptography and PKI:** Compare and contrast basic concepts of cryptography or implement public key infrastructure.
- We recommend that all program graduates take **six (6) practice exams** after familiarizing themselves with the contents of the Udemy course in order to ensure success when sitting for the actual SY0-601 exam.
- See "What industry-standard certificate do I earn at the end of this program?" for more details.

What skills and traits do successful students of this program have?

See FAQ question "Is cybersecurity right for me?"

How are these courses taught?

Cognitive Science research indicates that students learn best by doing; by performing authentic work in the context of realistic tasks and that the best way to teach is via one-on-one mentorship. We call these mentored courses "Story-Centered Curricula" because each course centers on a rich, engaging story, which is closely analogous to situations our students will soon experience in their real-world work. The students play a central role in the story, where they work to achieve one or more significant objectives over a series of tasks. They are given detailed information about the simulated company they are working for together with detailed and authentic projects. Supporting materials and learning resources are provided, and expert mentors are available to provide help, advice, and feedback when needed.

Students who have struggled to achieve in traditional classroom settings, preferring to learn by actually doing tasks instead of passively assimilating through non-interactive lecture-based classes, often excel in this style of training program.

You may also be interested in these related questions:

- *See "Is cybersecurity right for me?" for additional information about what types of people tend to do well in cybersecurity.*

- *See "Who is CSGA, the provider of this innovative training?" for more info about the non-traditional teaching philosophy that drives the successful outcomes in this style of training.*

Which tools will I learn to use during the program?

In the process of doing the tasks required to complete the CTC program, you will gain invaluable, real-world experience using industry-standard tools such as:

- **Splunk:** A popular SIEM used to traverse computer logs from many sources looking for evidence of cyberattacks. The primary tool of many SOC analysts around the world
- **Wireshark:** A DFIR tool for analyzing network traffic from packet captures.
- **Network Miner:** A DFIR tool for analyzing network traffic from packet captures.
- **Volatility:** A CLI DFIR tool for analyzing infected devices from memory images.
- **Autopsy:** A GUI DFIR tool for analyzing infected filesystems from disk images.
- **Burp Suite:** A pentesting tool to identify and exploit website vulnerabilities within a browser.
- **Hybrid Analysis:** A file analysis sandbox tool used by SOCs to help identify malware.
- **Virus Total:** A static file analysis sandbox tool used by SOCs to help identify malware according to detections from dozens of antivirus vendors.
- **ANY.RUN:** A dynamic file analysis sandbox tool used by SOCs to help identify malware by safely detonating suspicious binaries in a virtual machine (VM).

You will NOT need to purchase licenses for any software to complete your work in the CTC program; all tools used in the tasks are free or open-source OR access is provided within the courseware itself and included within the cost of tuition.

What industry-standard certificate do I earn at the end of this program?

After completing the program, you will enroll in a short test-preparation course, offered by Udemy, to prepare you to pass the CompTIA Security+ exam.

How many hours does it take to complete this program?

Our Cybersecurity Training Certification program is an accelerated course of study designed to equip students with a job-ready skillset suitable for entry-level cybersecurity positions in just a matter of months, condensing what other training programs often take years to teach. *(For more information about the innovative teaching methods leveraged to achieve this, see "How are these courses taught?".)*

The complete program of study takes most students 6–7 months, totaling at least ~600 hours to complete. *This estimation includes both NON-108E and NON-118E, as well as passing the CSGA exam to obtain the capstone Security+ certification.*

1. **CYBERSECURITY: IMMEDIATE IMMERSION**

NON-108E takes place over eight (8) weeks, allowing about two and a half (2½) weeks to complete each of the three (3) tasks. You are expected to devote approximately 15 hours a week (~3½ hours a day) to the tasks, totaling about 120 hours of work spread across eight (8) weeks to successfully complete NON-108E.

2. **CYBERSECURITY DEFENSE**

NON-118E takes place over fifteen (15) weeks, providing around two and a half (2½) weeks to complete each of the six (6) tasks. You are expected to devote approximately 25 hours a week (~3½ hours a day) to the tasks, totaling about 375 hours of work spread across fifteen (15) weeks to successfully complete.

3. **COMPTIA SECURITY+ EXAM PREPARATION**

CSGA exam prep involves taking the 21-hour CSGA course as well as several practice exams.

- The time needed to study the material covered in this exam varies significantly from student to student. This variation largely depends on each student's existing familiarity with several IT–related subjects (for instance, networking protocols). *More details about the Security+ certification are described in "What industry-standard certificate do I earn at the end of this program?"*
- A typical program graduate with no prior IT experience usually takes 5–8 weeks of study to pass the SY0-601 exam. However, students with prior IT experience may be able to complete their exam preparations in as few as 1–2 weeks.

4. **CYBERSECURITY ATTACK**

This takes place over fifteen (15) weeks, providing around two and a half (2½) weeks to complete each of the six (6) tasks. You are expected to devote approximately 25 hours a week (~3½ hours a day) to the tasks, totaling about 375 hours of work spread across fifteen (15) weeks to successfully complete.

See also FAQ question "What time commitment is necessary for success?" for more details about how the time commitment is divided in the courses.

IMPORTANT NOTE:

Cybersecurity is a fast-moving and intense field, requiring a significant commitment to “get up to speed” enough to qualify for entry-level positions. This program is designed as an accelerated “fast-track” to acquire the essential skills and knowledge needed to enter the field. It condenses into just a few months what other training programs typically take years to teach. We've noticed that even talented students who couldn't dedicate the required time have struggled to succeed in this program. We *strongly* advise prospective students to take the time estimates provided above very seriously. *Please make necessary arrangements in advance to ensure you can allocate the recommended amount of time to these tasks throughout the program.*

What time commitment is necessary for success?

Mandatory class meetings:

These 60-minute meetings occur once a week for the duration of each course and are mandatory for all students.

- The meeting times are mutually agreed upon by all members of your class during the first week of the course; we endeavor to select a weekly meeting time that works for all participants’ schedules.
- Discussions during this meeting are explicitly relevant to the task you are currently undertaking in the course. Useful hints and walkthroughs are often covered during these meetings.

Self-scheduled coursework:

The remainder of the time you spend on these tasks each week occurs as your schedule permits. Most students must spend at least 24 hours a week (outside of the weekly student meetings described above) to successfully complete each task. We recommend you set aside at least 3–4-hour increments where you can focus exclusively on working on each task; when you schedule these is up to you. Your assigned mentor will be available by chat during most times of day if you get stuck.

See also FAQ question “How many hours does it take to complete this program?” for a detailed breakdown of the differing time commitments for each of the three sections of the program.

Is there any job-placement assistance after program completion?

Yes, there is job placement upon successful completion and final vetting for job placement.

New York City and Toronto are two of the country's cybersecurity hubs and feature many SOCs that may have entry-level job opportunities at the time of your program completion. Particularly motivated graduates may also find entry-level employment at remote, work-from-home job roles at other SOCs or MSSPs located around the country.

See also FAQ question "How many cybersecurity jobs are available?"

Cost

What is the cost of this program?

1. **Cybersecurity: Immediate Immersion *(8 weeks, 120 hours total)*:**

Tuition is **$2,500** USD.

- In addition to the tuition fee, you will be expected to purchase a single textbook (Practical Packet Analysis, 3rd edition [by Chris Sanders]).
- Financial aid is available for eligible students. *See "Is financial assistance available?" for more details.*

2. **Cybersecurity Defense *(15 weeks, 375 hours total)*:**

Tuition is **$6,000** USD.

- There are no additional expenses associated with this course (no textbooks).
- Financial aid is available for eligible students. *See "Is financial assistance available?" for more details.*

3. **CERTIFICATION EXAM: Earning the SECURITY+ credential! *(2–8 weeks; time variable depending on student)*:**

Cost: $500 USD

Access to a self-paced online course walking CTC program participants through the final phase of their training: the process of preparing for the CSGA CompTIA Security+ certification exam. Access to this certificate preparation course (along with access to mentors familiar with the certification process) is provided free of charge to all program graduates. Required "textbooks" include:

- The online CSGA preparation course.
- The online CSGA practice exams. (Each may be taken multiple times.)
- The CompTIA Security+ Certification Exam costs $500 USD to take. Successfully passing this exam is the capstone task of the CTC.

4. **Cybersecurity Attack *(15 weeks, 375 hours total)*:**

Tuition is **$6,000** USD.

- There are no additional expenses associated with this course (no textbooks).
- Financial aid is available for eligible students. *See "Is financial assistance available?" for more details.*

5. **Certified AI Analyst (08 weeks, 200 hours total)**

Tuition is Included $0.00

6. **Certified Cyber Range Program (04 weeks, 20 hours total)**

Tuition is Included $0.00

Is financial assistance available?

Yes!

Email diplomacy@bmcc-cuny.edu for more information.

Enrollment & Registration

Are there any prerequisites before I can enroll?

In order to enroll in our Cybersecurity Training Certification program, you must satisfy at least one (1) of the following prerequisites. Interested students should email dimplomacy@bmcc-cuny.edu with information about which of these prerequisites you have fulfilled in order to obtain permission to enroll. *You need to only fulfill one (1) of these prerequisites, not all!*

Upon approval, you will be provided with a registration link to formally enroll in the Cybersecurity Training Certification program's first set of tasks.

The available options for fulfilling the enrollment prerequisite are:

- IT work experience
- An associate's degree or beyond (in a related field)
- A certification (in a related field)

More details about each prerequisite option are included below:

[OPTION A] IT work experience

You currently (or have recently) held a job role in IT. Some eligible job roles include (but are not limited to):

- Help Desk Technician (providing technical support)
- Customer Service (providing technical support)
- Technical Support Specialist
- Programming and development *(contributions to open-source projects also qualify)*
- Systems Administrator
- Network Engineer
- Database Administrator
- Data Scientist
- Quality Assurance (QA) Tester
- Project Manager (IT)
- Self-directed learning or open-source contributions
- Unsure if your job role qualifies? Contact diplomacy@bmcc.cuny.edu to discuss.

[OPTION B] An associate's degree or beyond (in a related field)

You have an associate's degree or beyond in at least one (1) of the following domains (or their equivalent):

- Computer Science
- Computer Engineering
- Network Technology and Administration
- Computer Information Systems
- Information or Computer Security

[OPTION C] A certificate program (in a related field)

You have completed a certification in at least one (1) of the following programs of study (or their equivalent):

- Computer Support Specialist
- Health IT Support Systems
- IT Support
- Network and Security

IMPORTANT NOTE ABOUT REQUIRED ENGLISH PROFICIENCY:

In addition to satisfying at least one (1) of the prerequisites listed above, we highly recommend that interested students have a strong command of the English language, both orally and in writing.

There are several reasons for this:

- The field of cybersecurity is primarily conducted in English.
- Cybersecurity job roles, even entry-level positions, often involve a significant amount of report writing as part of daily responsibilities. Therefore, it is essential to possess strong English reading comprehension and writing skills to effectively communicate your findings.
- Our CTC program places a strong emphasis on practicing these communication skills, both orally during weekly meetings and in written reports of investigative findings. Students with sufficient English proficiency tend to excel in the program.

Students interested in pursuing a career in cybersecurity but lacking the necessary English proficiency are encouraged to improve their language skills before attempting to enroll.

I am neither a computer expert nor a trained IT professional. Can I still take this program?

Please see the above FAQ question "Are there any prerequisites before I can enroll?" for details about prerequisites that must be satisfied prior to approval to enroll in our Cybersecurity Training Certificate program.

The tasks in both courses (I. Cybersecurity: Immediate Immersion and II. Cybersecurity Defense) are designed to assume students have no advanced technical skills or understanding, but are capable of standard computer usage, such as using a browser and a word processor.

Who is teaching this training?

Interestingly, there is no teacher but only skilled mentors who help you complete each task, tailoring their feedback according to your specific needs. Our partner, BMCC, brings a unique teaching philosophy to their offerings: decades of experience designing learn-by-doing trainings have proven that students learn most effectively *not* within a classroom setting where a single teacher singlehandedly directs each learning experience. Instead, the most effective way to assimilate a new skillset is to work on a series of tasks that actively involve the use of that new skillset with helpful mentors available on the sidelines to assist you if you get stuck or "hit a wall" in your progress on that task.

About Cybersecurity

Is cybersecurity right for me?

People are drawn to cybersecurity for many reasons. Here are some of the most common motivations:

- **A Desire to Protect the Vulnerable:** Many cybersecurity professionals are motivated by a desire to safeguard the vulnerable. Given the complexity of cybersecurity, most internet users are relatively vulnerable. Many individuals in the cybersecurity field aim to create a safer place for everybody to coexist and prevent bad actors from harming innocent people.
- **Love of Mysteries, Puzzles, and Detective Work:** If you have a natural inclination for solving mysteries and enjoy detective work, cybersecurity can be a perfect fit for you. Cybersecurity experts often find themselves in an ongoing battle of wits against cyber threats, working to unravel complex puzzles and expose hidden vulnerabilities.
- **Curiosity:** If you possess a curious mind and enjoy exploring the unknown, cybersecurity offers endless opportunities for exploration. The ever-evolving nature of cyber threats and technologies ensures that there's always something new to discover and understand.
- **Easily Bored:** Cybersecurity is far from dull. It's a dynamic and fast-paced field where new challenges arise daily. If you tend to become bored with routine tasks and seek constant intellectual stimulation, cybersecurity can provide the variety and excitement you crave.
- **A Knack for Dissecting Things:** If you're the type of person who enjoys dismantling and inspecting things to understand their inner workings, you'll find cybersecurity intriguing. In this field, you'll dissect malware, deconstruct cyberattacks, and analyze systems to uncover vulnerabilities.
- **Self-Motivated Learning:** Successful cybersecurity professionals are often self-motivated learners. The field evolves rapidly, and staying updated with the latest threats and defense strategies is imperative. If you have a passion for continuous learning and enjoy staying ahead of the curve, cybersecurity offers a rewarding path.
- **Task Completion Resiliency:** Many successful cybersecurity professionals share the trait of “task completion resiliency” a fancy way of saying they refuse to give up when faced with difficult or confusing problems.

If you can relate to any of the above motivations, there is a good chance that you’ll be able to fit in and succeed in the fascinating field of cybersecurity.

- *You may also be interested in the related question “What skills and traits do successful students of this program have?” as there is significant overlap between a good “personality fit” for cybersecurity and success within the CTC program.*
- *You may also be interested in the information contained in the question “How many cybersecurity jobs are available?”, which discusses why there continues to be a shortage of qualified cybersecurity professionals in spite of years of press coverage regarding the availability of jobs within this growing field.*

What career paths are available within the field of cybersecurity?

While most entry-level cybersecurity jobs are for analysts in a SOC (Security Operations Center), there are many career paths available after a year or two of working in a SOC.

Higher-tier SOC analyst:

Progressing within the SOC hierarchy, higher-tier analysts handle more complex security incidents and investigations, often specializing in specific areas.

Security Engineer:

Security engineers focus on designing, implementing, and managing security solutions and infrastructure, playing an essential role in protecting an organization's digital assets.

Incident Response:

Incident responders are the first line of defense when a security breach occurs, actively mitigating and recovering from cyber attacks to minimize damage.

Digital Forensics (DFIR):

Digital forensics experts specialize in uncovering evidence from digital devices, aiding in investigations, and ensuring the proper handling of digital evidence.

Penetration Tester:

Penetration testers, also known as ethical hackers, assess an organization’s security by attempting to exploit vulnerabilities and identify weaknesses before malicious hackers can.

Compliance:

Professionals in compliance roles ensure that an organization adheres to cybersecurity regulations and standards, helping maintain legal and regulatory compliance.

Chief Information Security Officer (CISO):

CISOs are top-level executives responsible for an organization's overall security strategy, policies, and risk management.

These diverse career paths within cybersecurity provide ample opportunities for specialization and growth, allowing professionals to tailor their careers to their interests and expertise.

What is the average salary of a cybersecurity professional?

All salaries for cybersecurity professionals can vary depending on the region of the country. The following are average salaries typical of the Boston area, one of America's cybersecurity hubs:

- **Entry-level SOC analysts** make on average $69,000—$111,000/year.
- **Higher-tier SOC analysts** make on average $89,000—$150,000/year.
- **Security Engineers** make on average $99,000—$155,000/year.
- **Incident Responders** make on average $53,000—$83,000/year.
- **Digital Forensics** makes on average $77,000—$118,000/year.
- **Penetration Testers** make on average $86,000—$148,000/year.
- **Compliance Officers** make on average $64,000—$125,000/year.
- **Chief Information Security Officers (CISOs)** make on average $217,000—$354,000/year.

The above statistics are provided by Glassdoor.com and are current as of late 2023.

See also the FAQ question "What career paths are available within cybersecurity?" for more details about the above job roles.

How many cybersecurity jobs are available?

Monitoring available cybersecurity job listings over several months in late 2025 on Indeed.com and Glassdoor.com showed anywhere between 35 and 340 available job listings at any given time, with varying degrees of qualifications required.

Graduates of this course of study will qualify for entry-level cybersecurity positions. Mentors will provide graduates with advice on further strengthening their resumes, as well as additional methods for identifying local job opportunities.

Job role availability may differ in other regions of the country.