IT 6200
Cybersecurity Analyst (CySA+)

TUITION	DURATION	TARGET CERTIFICATION	ISSUING AUTHORITIES	REQUIREMENTS
$2,500	2 Weeks	CompTIA CySA+	CompTIA	CompTIA Security+, Network+, or equivalent experience Minimum of 3-4 years of hands-on information security or related experience

MedCerts
A Stride Company
Call us anytime ☎
877. 219. 3306

PROGRAM DETAILS

This program prepares current and future IT professionals for a career in cybersecurity, with a focus on "defensive" strategies to protect an organization from risk. Additionally, students are trained in the proper response to threats and attacks by applying environmental reconnaissance techniques like OS fingerprinting, e-mail harvesting, and social media profiling using tools such as Nmap, Netstat, and syslog. Students also learn to analyze the results of network reconnaissance and recommend or implement countermeasures.

Even the most protected companies are prey to threats, therefore it is important that the cybersecurity professional be trained to properly respond to cyber incidents with a forensics toolkit, maintain the chain of custody, and analyze incident safety. Cybersecurity analysts plan and carry out security measures to protect a company's computer networks and systems. They keep constant tabs on threats and monitor their organization's networks for any breaches in security. This involves installing software and encryption, reporting breaches or weak spots, researching IT trends, educating the rest of the company on security—and even simulating security attacks to find potential vulnerabilities.

CySA+ is the only intermediate high-stakes cybersecurity analyst certification with performance-based questions covering security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing center in a highly secure environment. CySA+ is the most up-to-date security analyst certification that covers advanced persistent threats in a post-2014 cybersecurity environment. Formerly known as CSA+.

Throughout the Cybersecurity Analyst (CySA+) program, students will learn the skills to:

- ✓ Perform data analysis and interpret the results to identify vulnerabilities, threats, and risks to an organization
- ✓ Keep up latest trends in cybersecurity and anticipate new threats
- ✓ Secure and protect applications and systems within an organization
- ✓ Combat malware and advanced persistent threats (APTs)
- ✓ Apply behavior analytics to the IT security of an organization

CAREER SERVICES

For all MedCerts Students that are not affiliated with an employer partner, you also have the added benefit of Job Search Assistance including guidance with resume building, networking, interviewing, and job search tips.

While MedCerts training and related target certifications may be accepted and/or approved by your state of residency, employers reserve the right to dictate pre-requisite education, experience, or certification/licensure requirements for their positions. These requirements may exclude a MedCerts graduate from eligibility. We strongly advise students to research target job posts from area employers and relevant state requirements, barriers or restrictions to ensure eligibility upon graduation.

Some training programs and/or certifications may not be accepted in your state, please review our State Restriction page to confirm eligibility

ATTAINABLE CAREERS

- Cybersecurity Analyst
- Information Security Analyst
- Tier II SOC Analyst
- Vulnerability Analyst
- CyberSecurity Specialist
- Threat Intelligence Analyst

TARGET CERTIFICATIONS

Certifications	Issuing Authority	Exam Details
CompTIA CySA+	Computing Technology Industry Association (CompTIA)	85 multiple choice questions performance-based questions. Time limit: 2 hours 45 minutes

Course Code	Title	Hours	Weeks	Course Materials (Included)
IT-6012	CompTIA CySA+	32	2	None

EXPERIENTIAL/CLINICAL COMPONENT:

Experiential/Clinical Component Requirements (not a requirement for Cybersecurity Analyst (CySA+) program) – Once students complete this program, they will be able to immediately start working with Career Services at MedCerts.

CRIMINAL BACKGROUND CHECKS AND DRUG SCREENING POLICY:

MedCerts does not perform criminal background checks, nor do we test students for illicit drug use. Please be advised that while MedCerts does not perform these checks, the student's drug, criminal, or immunization status may prevent clinical/externship placement and future employment as a healthcare or IT professionals. Externship sites, employers, and State Boards of Pharmacy or other regulatory boards have regulations about immunizations, drug use, and criminal backgrounds. Regulatory boards, externship sites, employers, and other organizations that may require these screenings for placement, and adverse results may prohibit you from moving forward in the program. Candidates with a felony conviction are not eligible to participate in ANY MedCerts program that includes the Pharmacy Technician certification as a primary or secondary certification

The student understands that MedCerts does not hold any control over the drug, immunization, criminal, or background screening processes or policies held by any organization outside of MedCerts.

MedCerts
A Stride Company
medcerts.com

Upon 100% completion of this program, students will receive a "MedCerts Certificate of Completion." This is proof of completion of training but isn't a nationally recognized certification. Students are expected to take and pass the national certification exam through the issuing authority for recognized certification in their field.

Please carefully review the above program specific information and contact your Student Success Advisor if you have any questions or require further clarification of the contents.