

Security+
Fall/Winter 2026/27
Urban League of Greater Pittsburgh
Training Academy

Instructor: Mr. Stephen Deal

Phone:

Email:

The Urban League of Greater Pittsburgh is happy to announce your acceptance into the **Security +** certification course. The technology path you embark on will provide you with superior knowledge and a profitable career path. The Security + certification empowers you to attain employment with a medium pay scale of \$90,000 to \$130,000 annually.

Security+ is a globally recognized, entry-level cybersecurity certification that validates foundational skills for performing core security functions and pursuing an IT security career. It's often considered the first certification IT professionals should earn when entering the cybersecurity field. Included in the course are topics, i.e. social Engineering, Attacks Indicators, Network Attacks, Application Attacks, Secure Protocols, Secure Network Design Authentication, and Authorizations among others.

The course will encompass the following:

1. 16 weeks.
2. Class is offered once a week, on Thursdays from 6:00 – 8:00 pm.
3. All learning materials will be supplied.
4. The Urban League of Greater Pittsburgh covers the financial cost of the exam.
5. **Class Start date: Thursday, November 12, 2026, 6:00 pm – 8:00 pm**

Class Policies

1. You will need a laptop with access to the internet (if you do not have the required technology and cannot attend class via Zoom, you can attend in person at our office in Downtown Pittsburgh).
2. You are expected to attend every class session. Because of the subject matter, missing even one class can have a tremendous impact on your learning process. If you miss a class, it is your responsibility to obtain any notes and information presented in class. If an emergency arises that will leave you unable to attend class (illness, death in family, etc.), please email **your instructor** before or at least within the 24 hours after class.
3. Be on time for class. Situations come up from time to time, however, please try to be on time for class. When you are late, you miss out on important information.

- 3.) Please show your instructor and your classmates the same respect that you want to be shown. Hate speech, harassment, bullying, and any other sort of disruptive behavior will not be tolerated. Additionally, please refrain from using your phone during class.
- 4.) Classes can be taken virtually or in-person. If attending virtually, your camera must always be on, or it will be counted as an absence. Additionally, you must attend at least two classes in person.

Course Calendar

<u>Date</u>	<u>Lesson</u>
Monday, Nov. 2	Orientation
	Part 1 – Threats, Attacks, and Vulnerabilities
Thursday, Nov. 12	Chapter 1: Social Engineering Techniques Chapter 2: Type of Attack Indicators
Thursday, Nov. 19	Chapter 3: Application Attack Indicators Chapter 4: Network Attack Indicators
Thursday, Dec. 3	Chapter 5: Threat Actors, Vectors, and Intelligence Sources Chapter 6: Vulnerabilities
Thursday, Dec. 10	Chapter 7: Security Assessments Chapter 8: Penetration Testing
	Part 2 – Architecture and Design
Thursday, Dec. 17	Chapter 9: Enterprise Security Architecture Chapter 10: Virtualization and Cloud Security
Thursday, Jan. 7	Chapter 11: Secure Application Development, Deployment, and Automation Concepts Chapter 12: Authentication and Authorization
Thursday, Jan. 14	Chapter 13: Cybersecurity Resilience Chapter 14: Embedded and Specialized Systems
Thursday, Jan. 21	Chapter 15: Physical Security Controls Chapter 16: Cryptographic Concepts

	Part 3 - Implementation
Thursday, Jan. 28	Chapter 17: Secure Protocols Chapter 18: Host and Application Security
Thursday, Feb. 4	Chapter 19: Secure Network Design Chapter 20: Wireless Security
Thursday Feb. 11	Chapter 21: Secure Mobile Solutions Chapter 22: Implementing Cloud Security
Thursday, Feb. 18	Chapter 23: Identity and Account Management Controls Chapter 24: Implement Authentication and Authorization
	Part 4 – Operations and Incident Response
Thursday, Feb. 25	Chapter 25: Public Key Infrastructure Chapter 26: Tools/Assess Organization Security
Thursday, March 4	Chapter 27: Incident Response Policies, Processes, and Procedures Chapter 28: Investigations
Thursday, March 11	Chapter 29: Mitigation Techniques and Controls Chapter 30: Digital Forensics
	Part 5 – Governance, Risk, and Compliance
Thursday, March 18	Chapter 31: Security Controls Chapter 32: Regulations, Standards, and Frameworks Chapter 33: Organizational Policies
Thursday, March 25	Chapter 34: Risk Management Chapter 35: Privacy