CYBER BRAIN ACADEMY

1281 9th Ave. Unit 3408
San Diego, CA 92101
(619) 631-3003
learn@cyberbrainacademy.com
cyberbrainacademy.com

Commitment

Impact

Accessibility

CYBER BRAIN ACADEMY

THE CYBER SECURITY TRAINING YOU DESERVE

www.cyberbrainacademy.com

CompTIA Security+

February 22 – February 26, 2021

Training Overview

Table of Contents

1.0 Company Overview

Cyber Brain Academy is a veteran-owned small business headquartered in San Diego, California. We are an experienced IT training company that expertly prepares cyber security professionals for the CompTIA Security+ examination. Cyber Brain Academy is a CompTIA Authorized Training Provider with an exceptional staff of instructors, who are licensed and certified through CompTIA to provide you the Security+ training you deserve.

Cyber Brain Academy is the product of years of research and collaboration with expert cyber security professionals and members of academia. Our team spent over two years working with educators and assessment specialists to design a complete and effective cyber security education experience. Our innovative approach to learning earned us the award of **Most Innovative Cyber Security Training Provider – USA** by Acquisition International in 2020!

As a veteran-owned small business, Cyber Brain Academy proudly supports the Navy SEAL Foundation. We donate 10% of our live-online training session earnings to the Navy SEAL Foundation in support of their mission of service to the Naval Special Warfare community and its families.

2.0 Security+ Training Course

CompTIA Security+ establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them. No other certification that assesses baseline cybersecurity skills has performance-based questions on the exam. Security+ focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection. You will also earn 40 Continuing Education Units (CEUs) for completing Cyber Brain Academy's CompTIA Security+ training session.

2.1 Scope

Cyber Brain Academy will proudly provide you with a five day live-online, instructor-led Security+ training experience. Our Security+ instructor and course materials will provide in-depth, technical Security+ domain knowledge that covers Threats, Attacks, and Vulnerabilities, Technology and Tools, Architecture and Design, Identity and Access Management, Risk Management, and Cryptography and PKI.

2.2 Our Approach to Training

Cyber Brain Academy provides a comprehensive Security+ training experience by conducting our training in three phases – Pre-Training, Live-Online Security+ Training, and Post-Training – to ensure optimum success.

2.2.1 Phase 1: Pre-Training

Phase 1 consists of early access to your Security+ course materials. You will be given access to our digital Security+ courseware 14 days prior to the beginning of your training experience and continued access for six months. This allows for an engaging learning experience and increased competency during Phase 2.

2.2.2 Phase 2: Five Day Live-Online, Instructor-led Security+ Training

Phase 2 consists of comprehensive instruction by our CompTIA authorized instructor. Your five day live-online training session consists of engaging training materials, practice questions, daily-recaps, and question & answer sessions between you and our experienced instructor.

All of our training materials are up to date and cover the latest version of the CompTIA Security+ exam. Please refer to the training schedule highlighted in Appendix A – Schedule of Live-Online Security+ Training for a detailed breakdown of course topics and activities.

2.2.3 Phase 3: Post-Training

Phase 3 consists of reviewing your gained competency through our on-demand Security+ courseware. Our courseware covers 100% of the Security+ exam topics and includes knowledge check questions that assess your understanding of all Security+ domain topics. This advantage allows you to retain knowledge and gain confidence prior to taking the Security+ exam.

Each lesson within Cyber Brain Academy's on-demand Security+ courseware contains a comments section where you can post your questions directly to our Security+ instructor network. This is a feature only provided through Cyber Brain Academy and demonstrates our ongoing commitment to you.

2.2.4 Our Students Say It Best

"I'm a software engineer, with no exposure to IT or Cyber Security field. Despite this obstacle, I successfully passed the CompTIA Security+ exam on my first attempt thanks to the training that I received from Cyber Brain Academy."

- **Kangseon (Alex) Cho, Capital Group**

"I needed to pass the Security+ exam to keep my job as part of DoD 8750. The materials we covered in class followed up with quizzes was effective to maintain knowledge. I passed with a score of 808!"

- **Bobby Andrino, Leidos**

"The Security+ class exceeded my expectations. I passed the exam on my first attempt thanks to the training I received from Cyber Brain Academy."

- **Robert Mills, US Navy 3rd Fleet**

3.0 Our Educators

Cyber Brain Academy provides only highly screened instructors that are licensed and authorized to teach our students. Your Security+ training experience will be conducted by industry experts who are also authorized CompTIA instructors.

4.0 Course Materials

Cyber Brain Academy will provide you with the following course materials for your live-online Security+ training experience:

- CompTIA Authorized Security+ Instructor
- Official CompTIA Security+ Digital Courseware
- Cyber Brain Academy's On-demand Security+ Digital Courseware
- Official CompTIA Security+ Labs
- Official CompTIA Security+ Exam Voucher

5.0 Customer Service

Cyber Brain Academy provides you with a customer engagement specialist throughout the duration of your Security+ training experience, at no additional cost.

Cyber Brain Academy is dedicated to your satisfaction. After you complete your five days of instructor-led training, our engagement specialist will contact you with an optional survey to help us evaluate both our curriculum and our instructors, to ensure that we maintain the highest standard of quality.

Appendix A – Schedule of Live-Online Security+ Training

Schedule	Security+ Domains	Topics Covered
Day 1	Introductions	• Introductions and review of exam objectives
	Threats, Attacks, and Vulnerabilities	• Given a scenario, analyze indicators of compromise and determine the type of malware • Compare and contrast types of attacks • Explain threat actor types and attributes • Explain penetration testing concepts • Explain vulnerability scanning concepts • Explain the impact associated with types of vulnerabilities • Q&A
Day 2	Technology and Tools	• Recap • Install and configure network components, both hardware and software-based, to support organizational security • Given a scenario, use appropriate software tools to assess the security posture of an organization • Given a scenario, troubleshoot common security issues. • Given a scenario, analyze and interpret output from security technologies • Given a scenario, deploy mobile device securely • Given a scenario, implement secure protocols • Q&A
Day 3	Architecture and Design	• Recap • Explain use cases and purpose for frameworks, best practices and secure configuration guides • Given a scenario, implement secure network architecture concepts • Given a scenario, implement secure systems design • Explain the importance of secure staging and deployment concepts • Explain the security implications of embedded systems • Summarize secure application development and deployment concepts • Summarize cloud and virtualization concepts • Explain how resilience and automation strategies reduce risk • Explain the importance of physical security controls • Q&A
Day 4	Identity and Access Management	• Recap • Compare and contrast identity and access management concepts • Given a scenario, install and configure identity and access services • Given a scenario, implement identity and access management controls • Given a scenario, differentiate common account management practices • Q&A
	Risk Management	• Explain the importance of policies, plans and procedures related to organizational security.

		• Summarize business impact analysis concepts. • Explain risk management processes and concepts. • Given a scenario, follow incident response procedures. • Summarize basic concepts of forensics. • Explain disaster recovery and continuity of operations concepts. • Compare and contrast various types of controls. • Given a scenario, carry out data security and privacy practices. • Q&A
Day 5	Cryptography and PKI	• Recap • Compare and contrast basic concepts of cryptography • Explain cryptography algorithms and their basic characteristics. • Given a scenario, install and configure wireless security settings. • Given a scenario, implement public key infrastructure. • Q&A
	Domain Review	• Review of all topics • Final Q&A