Train Smarter

Certify Faster

CompTIA
Security+
CERTIFICATION
Plus Series

Discover the opportunities Security+ creates for your future in cybersecurity.

☎ **cyberbrainacademy.com**
info@cyberbrainacademy

Introduction to the CompTIA Security+ Certification

The CompTIA Security+ certification is one of the most recognized credentials in the field of cybersecurity and serves as a starting point for professionals who want to establish a career in information security. Security+ validates the essential skills required to secure networks, manage risks, respond to incidents, and protect organizations from today's most pressing cyber threats.

CompTIA Security+ is an industry benchmark

Employers, government agencies, and defense contractors frequently list Security+ as a required or preferred qualification for entry-level and mid-level cybersecurity roles. For individuals seeking to enter cybersecurity or IT professionals looking to advance, earning Security+ opens the door to competitive salaries, career mobility, and global recognition as a skilled security practitioner.

Who Should Take the CompTIA Security+ Exam?

The CompTIA Security+ certification is designed for:

Individuals starting a cybersecurity career
Perfect for those with little to no security background who want to gain the essential skills and earn a credential that employers recognize worldwide.

Help desk technicians, system administrators, and network administrators
Provides the bridge into security-focused roles by covering the knowledge needed to secure infrastructure, manage access, and respond to incidents.

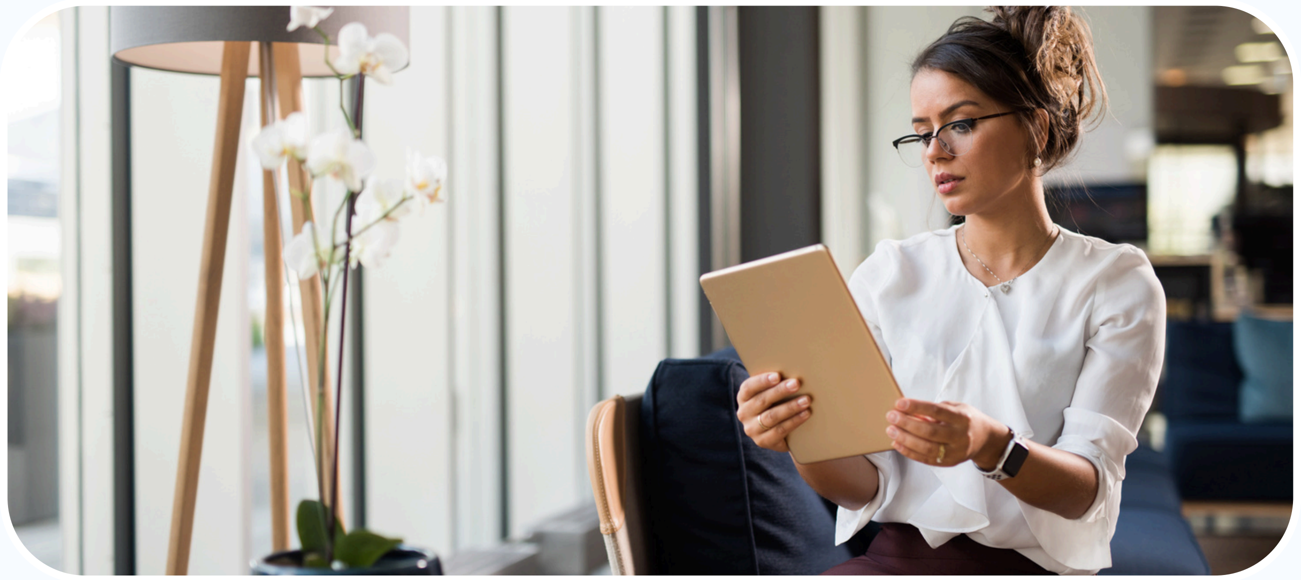
Career changers and students entering the field
A strong foundation for those transitioning from other industries or completing academic programs who want to break into cybersecurity with a respected certification.

Thousands of students around the world have passed Security+ with structured training and dedicated study resources. For many, it has been the first step toward building confidence, earning higher salaries, and starting a career in one of the fastest growing fields today.

Industry Growth and Opportunities

The demand for cybersecurity professionals continues to grow at an unprecedented pace, with millions of open positions projected worldwide in the coming years. Organizations across government, defense, healthcare, finance, and technology are urgently seeking skilled individuals who can protect critical systems and data.

The CompTIA Security+ certification positions candidates to take advantage of this opportunity by qualifying them for roles such as security analyst, systems administrator, SOC analyst, and junior penetration tester. These careers offer competitive salaries, advancement potential, and global recognition, making Security+ a powerful first step into one of the fastest growing and most rewarding industries today.



- Unprecedented demand
- Cross-industry need
- Career pathways
- Competitive advantages

Job Titles and Salaries

Earning the Security+ certification creates opportunities for a variety of roles in the cybersecurity and IT field. Below are three common positions and their average salary ranges in the United States:

Information Security Analyst

$65,000 to $100,000

Focused on monitoring networks, identifying vulnerabilities, and responding to threats.

Systems Administrator

$55,000 to $80,000

Responsible for managing, maintaining, and securing organizational IT systems and networks.

Security Consultant

$85,000 to $120,000

Provides expert advice and strategies to organizations on how to protect their systems and data.

Limits of Traditional Education

Employers are clear about what they need. A degree alone is no longer enough. Our certification programs have become a baseline requirement for many roles, serving as proof that candidates can meet the demands of modern security challenges.

The University Challenge

Where Institutions Struggle

For universities, this creates a difficult reality. While they excel at delivering academic knowledge, many institutions face challenges in offering certification-aligned programs.

Bridging the Academic Gap

Building these programs in-house requires specialized instructors, continuous content updates, and significant financial investment. Without these resources, universities risk falling short of preparing students with the career-ready credentials that employers demand.

Here's What Real Students Are Saying

Google
★★★★★

"I highly recommend"

The instructor was very knowledgeable in the trade and plenty of interaction activities. I to this day still have the study notes and curriculum for personal growth in hopes to pursue this career. I highly recommend this school if you are looking to have a high demand trade.

"One of the best experiences"

I can say that I had one of the best experiences as far as school is concerned. The teacher had a lot of knowledge of the subject, if we needed something, he took the time to explain it to us and he even stayed after my class for people who had questions.

"Well Structured"

I recently completed a security course with Cyber Brian Academy, and I couldn't be more impressed with the experience. The course was thorough, well-structured, and delivered by a knowledgeable instructor who really knew their stuff.

REAL STUDENTS. REAL RESULTS.

Jesse Margarini

"Thanks to Cyber Brain Academy, I was officially able to get certified in Security+."

View Jesse's Testimonial on YouTube

Building the Future **Together**

Train Smarter
Certify Faster

Cyber Brain Academy is the trusted choice for Security+ training. As a CompTIA Platinum Partner with more than seven years of experience, we have helped thousands of students earn certifications and build lasting careers in cybersecurity. Our Security+ program is designed to give you the knowledge, skills, and confidence to master the exam and stand out in the job market.

Our training combines expert instruction, structured lessons, and practical insights that prepare you for real security challenges. Every topic is explained clearly and tied to situations you will encounter on the job, ensuring that what you learn goes beyond theory. We focus on more than passing the test. We prepare you to perform in the field and contribute from day one.

What sets Cyber Brain Academy apart is our commitment to results. We provide flexible learning formats, access to updated materials, and ongoing support that keeps you on track from enrollment to certification. Choosing Cyber Brain Academy means choosing a proven pathway that connects Security+ training directly to career success in one of the fastest growing fields today.

100% Exam Coverage!

A breakdown of the exam domains, their weight in the overall exam, key focus areas, and the corresponding sections that address each topic

Domain	Exam Weight	Key Topics Covered	Days Covered
1. General Security Concepts	12%	Fundamental security principles, risk management strategies, and encryption fundamentals	Days 1-2
2. Threats, Vulnerabilities, and Mitigations	22%	Cyber threats, malware, social engineering tactics, and security control implementations	Days 3-4
3. Security Architecture	18%	Secure network and system design, access control mechanisms, and authentication methods	Days 5-6
4. Security Operations	28%	Incident response procedures, security monitoring, cybersecurity tools, and operational security best practices	Days 6-8
5. Security Program Management & Oversight	20%	Regulatory compliance, security policies, governance structures, and cybersecurity frameworks	Days 9-10

Domain 1: General Security Concepts (Days 1-2)

Core Principles of Security

Domain 1 introduces the foundational principles of cybersecurity and sets the stage for everything that follows in Security+. This domain ensures learners understand the key concepts that form the baseline of security knowledge, including the CIA Triad of confidentiality, integrity, and availability, as well as fundamental security controls and defense strategies.

Building a Foundation for Cybersecurity

By mastering general security concepts, students establish the baseline knowledge required for the rest of the Security+ exam. Domain 1 ensures candidates can identify vulnerabilities, assess risks, and apply appropriate security measures. These skills serve as the foundation for success in both the exam and a future career in cybersecurity.

Domain 2: Threats, Vulnerabilities, and Mitigations (Days 3-4)

Identifying Vulnerabilities

Domain 2 focuses on the weaknesses that attackers exploit in systems, networks, and applications. Learners will study software flaws, misconfigurations, weak access controls, and physical vulnerabilities, as well as the role of unpatched systems in creating opportunities for exploitation. Emphasis is placed on vulnerability management practices and the importance of regular assessments.

Mitigation Strategies and Defensive Measures

The domain explores the strategies to reduce risks and strengthen organizational defenses. Learners will study security controls such as intrusion detection and prevention systems, patch management, network segmentation, and security awareness training. This section emphasizes how layered and proactive defenses reduce the likelihood of successful attacks.

Domain 3: Security Architecture (Days 5-6)

Designing Secure Environments

Domain 3 focuses on the principles of building and maintaining secure systems and networks. Students will learn how security is integrated into infrastructure from the ground up, including the importance of secure design, defense in depth, and system hardening. This section introduces how architecture decisions directly impact the strength of an organization's security posture.

Security Controls and Technologies

Students will learn the tools and mechanisms used to protect information systems. Topics include firewalls, intrusion detection and prevention systems, endpoint security, and encryption. Learners will explore how these controls work together to protect networks, applications, and data, and how to select the right combination of technologies for different environments.

Domain 4: Security Operations (Days 6-8)

Incident Detection and Response

Domain 4 covers the process of recognizing, analyzing, and responding to security incidents. Learners will study incident response plans, containment strategies, and recovery procedures that minimize damage and restore operations. By understanding the phases of incident handling, candidates are better prepared to react quickly and effectively in high-pressure situations.

Automation and Operational Efficiency

As threats grow in scale, organizations rely on automation and orchestration to enhance their operations. Learners will examine the role of automated alerts, security playbooks, and coordinated response systems that speed up detection and reduce human error. Understanding these tools equips candidates to operate effectively in modern security environments.

Domain 5: Security Program Management & Oversight (Days 8-10)

Governance and Policies

Domain 5 introduces the frameworks and policies that guide organizational security programs. Students will learn about governance structures, compliance requirements, and the role of security policies in shaping day-to-day operations. This section highlights how leadership sets the tone for building a culture of security across the organization.

Risk Management and Assessment

Students will learn the process organizations use to understand and control risk. Students will learn how to identify potential threats, evaluate the likelihood and impact of different vulnerabilities, and prioritize risks based on business objectives. Key methods such as qualitative and quantitative risk assessments, risk registers, and cost-benefit analysis are introduced to show how decisions are made in real-world environments.

REAL STUDENTS. REAL RESULTS.

Ibrahim Swaray

"If I'm going to recommend Cyber Brain Academy, I'd put them as top-notch"

View Ibrahim's Testimonial on YouTube

Train Now. Pay Later.

Enroll to our any of our upcoming live training classes for as low as $200 down!

Cyber Brain Academy offers flexible Security+ training packages designed to fit different learning needs and budgets. Each option includes expert-led instruction, structured resources, and ongoing support to help you succeed.

Training Only – $1,299 (Regular $2,000)
Get full access to Security+ training.

- **Finance option: $200 down, $46 per month for 24 months.**

Training + Exam Voucher – $2,000 (Regular $2,499)
Includes Security+ training and the official CompTIA exam voucher.

- **Finance option: $300 down, $71 per month for 24 months.**

Training + Exam Voucher + Training Kit – $2,499 (Regular $2,799)
Complete package with Security+ training, exam voucher, and training kit with additional study resources.

- **Finance option: $500 down, $84 per month for 24 months.**

The World's Most Recognized Credentials

- PMI CAPM® — Certified Associate in Project Management
- PMI PMP® — Project Management Professional
- PMI PMI-RMP® — PMI Risk Management Professional
- PMI PgMP® — Program Management Professional
- PMI PMI-ACP® — PMI Agile Certified Practitioner
- PMI PfMP® — Portfolio Management Professional
- PMI PMI-PBA® — PMI Professional in Business Analysis
- PMI PMI-CP® — PMI Construction Professional

- CompTIA ITF+ CERTIFICATION Plus Series
- CompTIA Tech+ CERTIFICATION Plus Series
- CompTIA A+ CERTIFICATION Plus Series
- CompTIA Network+ CERTIFICATION Plus Series
- CompTIA Security+ CERTIFICATION Plus Series
- CompTIA CySA+ CERTIFICATION Plus Series
- CompTIA Linux+ CERTIFICATION Plus Series
- CompTIA Server+ CERTIFICATION Plus Series
- CompTIA Cloud+ CERTIFICATION Plus Series
- CompTIA PenTest+ CERTIFICATION Plus Series
- CompTIA Project+ CERTIFICATION Plus Series
- CompTIA CASP+ CERTIFICATION Xpert Series

- CCOA. — Certified Cybersecurit Operations Analyst.
- CISA. — Certified Information Systems Auditor.
- CRISC. — Certified in Risk and Information Systems Control.
- CISM. — Certified Information Security Manager.

Cyber Brain Academy

- CDPSE. — Certified Data Privac Solutions Engineer.
- CGEIT. — Certified in the Governance of Enterprise IT.
- C|EH — Certified Ethical Hacker
- C|CISO — Certified Chief Information Security Officer

- CC℠
- SSCP.
- CGRC℠
- CISSP.
- CCSP.
- CSSLP.
- ISSAP.
- ISSEP.

It’s Time To Train Smarter!

Cyber Brain Academy is ready to deliver proven, certification-aligned programs that strengthen outcomes and expand opportunities.

Our team is prepared to show you how Cyber Brain Academy can integrate quickly, scale effectively, and deliver measurable results.

Free 20-Minute Consultation ☎

Explore flexible training formats designed for different schedules and learning styles.

219-641-3851

info@cyberbrainacademy.com