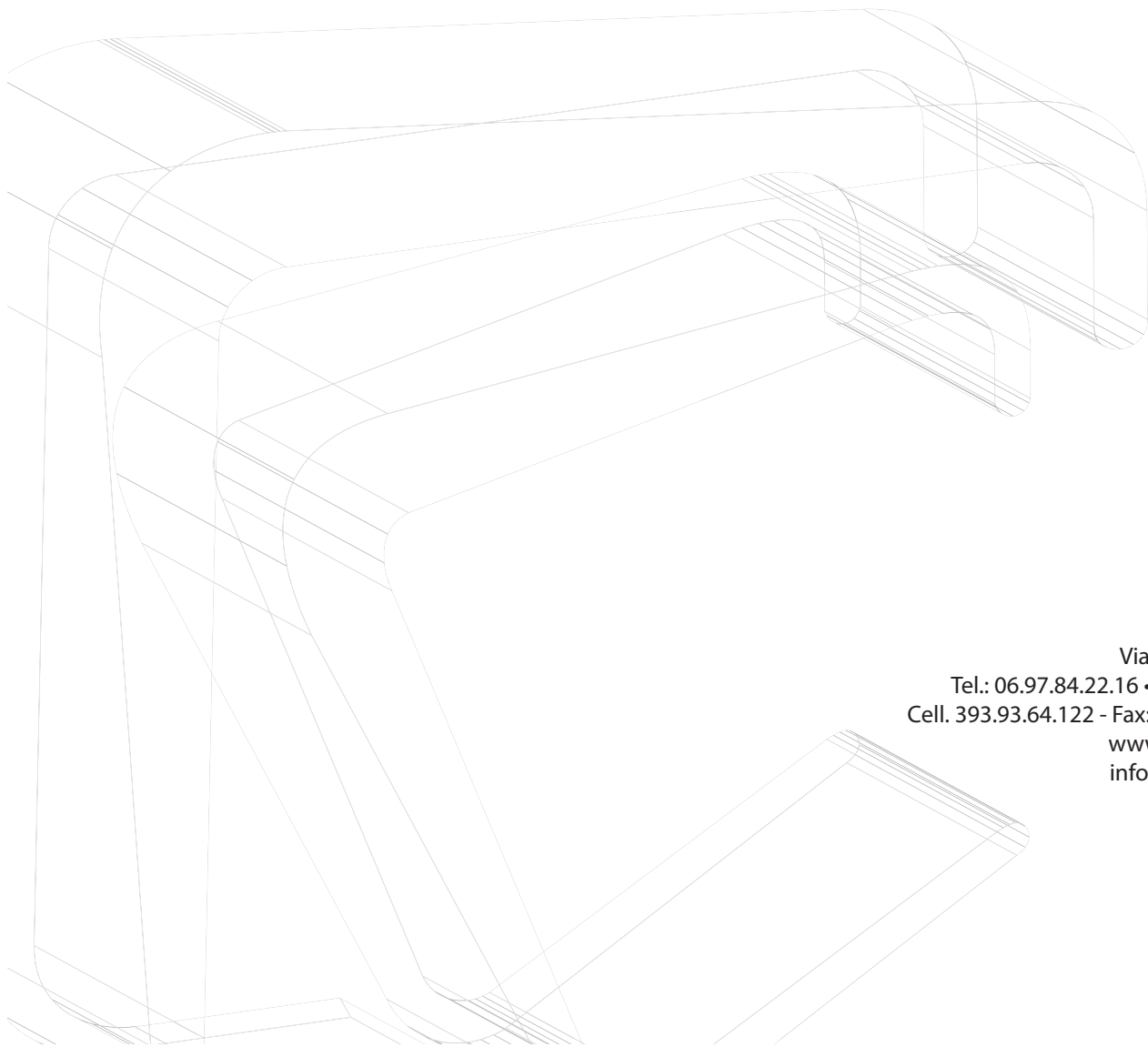




PC ACADEMY

Programma corso Certificazione CompTIA Security+



PCAcademy  
Via Capodistria 12  
Tel.: 06.97.84.22.16 • 06.85.34.44.76  
Cell. 393.93.64.122 - Fax: 06.91.65.92.92  
[www.pcademy.it](http://www.pcademy.it)  
[info@pcacademy.it](mailto:info@pcacademy.it)

### **Informazioni generali**

La certificazione CompTIA Security+ valuta conoscenze nell'ambito di sicurezza dei sistemi, struttura dei network, controllo degli accessi, crittografia e sicurezza delle organizzazioni. Si tratta di una certificazione internazionale, indipendente dal vendor, il cui insegnamento è diffuso in scuole, università e organizzazioni di tutto il mondo.

Anche se non è un requisito obbligatorio, è consigliabile che i candidati alla certificazione CompTIA Security+ abbiano almeno due anni di esperienza pratica nella gestione tecnica dei network, in particolare nell'ambito della sicurezza. Anche la certificazione CompTIA Network+ è consigliata.

Poiché l'errore umano è la causa principale delle falle nei sistemi informatici, la certificazione CompTIA Security+ è ritenuta dalla comunità informatica una credenziale più che valida, in quanto comprova competenze avanzate nella sicurezza delle informazioni.

Alcune tra le maggiori compagnie che impiegano personale certificato CompTIA Security+ sono: Booz Allen Hamilton, Hewlett-Packard, IBM, Motorola, Symantec, Telstra, Hitachi, Ricoh, Lockheed Martin, Unisys, Hilton Hotels Corp., General Mills, U.S. Navy, Army, Air Force e Marines

**Mitigating threats**

- :: Core system maintenance
- :: Virus and spyware management
- :: Browser security
- :: Social engineering threats

**Cryptography**

- :: Symmetric cryptography
- :: Public key cryptography

**Authentication systems**

- :: Authentication
- :: Hashing
- :: Authentication systems

**Messaging security**

- :: E-mail security
- :: Messaging and peer-to-peer security

**User and role based security**

- :: Security policies
- :: Securing file and print resources

**Public key infrastructure**

- :: Key management and life cycle
- :: Setting up a certificate server
- :: Web server security with PKI

**Access security**

- :: Biometric systems
- :: Physical access security
- :: Peripheral and component security
- :: Storage device security

**Ports and protocols**

- :: TCP/IP review
- :: Protocol-based attacks

**Network security**

- :: Common network devices
- :: Secure network topologies
- :: Browser-related network security
- :: Virtualization

**Wireless security**

- :: Wi-Fi network security
- :: Non-PC wireless devices

**Remote access security**

- :: Remote access
- :: Virtual private networks

**Auditing, logging, and monitoring**

- :: System logging
- :: Server monitoring

**Vulnerability testing**

- :: Risk and vulnerability assessment
- :: IDS and IPS
- :: Forensics

**Organizational security**

- :: Organizational policies
- :: Education and training
- :: Disposal and destruction

**Business continuity**

- :: Redundancy planning
- :: Backups
- :: Environmental controls