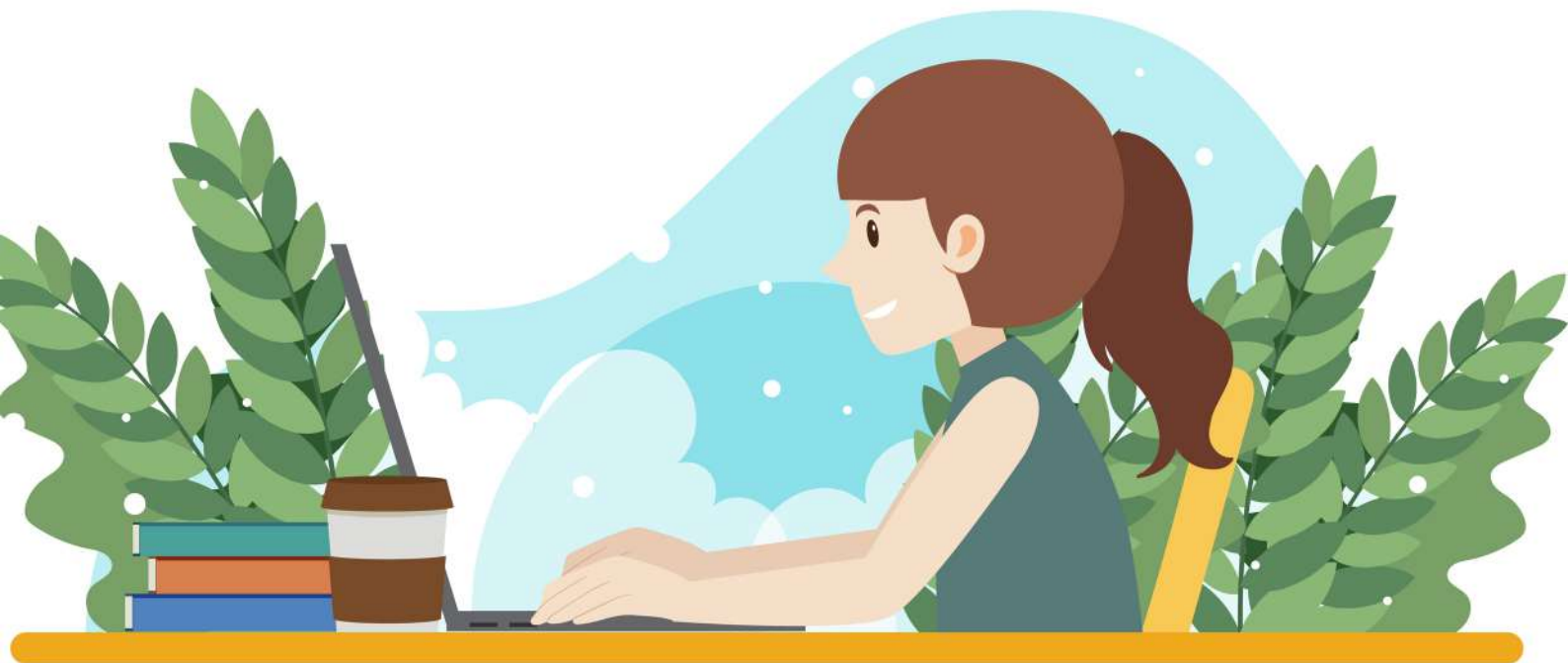


**CompTIA CySA+ (Cybersecurity Analyst+)**



# Online Course

**Learn  
Remotely..!!**

**ZETLAN TECHNOLOGIES**  
**[www.zetlantech.com](http://www.zetlantech.com)**

## Course Modules



### 1. Threat and Vulnerability Management

- Explain the importance of threat data and intelligence
- Threat intelligence to support organizational security
- Perform vulnerability management activities
- The output from common vulnerability assessment tools
- Threats and vulnerabilities associated with specialized tech
- Threats & vulnerabilities associated with operate in the Cloud
- Controls to mitigate attacks and software vulnerabilities

### 2. Software and Systems Security

CompTIA®

- Apply security solutions for infrastructure management
- Explain software assurance best practices
- Hardware assurance best practices
- Security Operations and Monitoring
- Analyse data as part of security monitoring activities
- Configuration changes to existing controls to improve security
- Explain the importance of proactive threat hunting
- Compare and contrast automation concepts and technologies

### 3. Incident Response

- Explain the importance of the incident response process
- Apply the appropriate the incident response procedure
- Analyse potential indicators of compromise
- Utilize basic digital forensic techniques



# CompTIA CySA+ (Cybersecurity Analyst+)

For Enquiry: +91 8680961847

## 4. Compliance and Assessment

- Understand the importance of data privacy and protection
- Security concepts in suprt of organizational risk mitigation
- Importance of frameworks, policies, procedures, and controls

## 5. Afterword

- Recap



Free Advice: +91 9600579474

[www.zetlantech.com](http://www.zetlantech.com)





**LEARN  
REMOTELY!!**

The efficiency of online learning  
in terms of time management,  
flexibility, and the ability  
to access resources anytime,  
anywhere can be compelling.



**ZETLAN TECHNOLOGIES**  
**[www.zetlantech.com](http://www.zetlantech.com)**

**For contact: +91 8680961847  
+91 9600579474**

