CompTIA Security X Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

CompTIA SecurityX is an advanced, hands-on training program designed for experienced**Cyber Security Professionals** who are responsible for designing, implementing, and managing secure enterprise environments. The course prepares learners for the **CompTIA SecurityX Certification Exam** while developing practical expertise in modern security architecture and operations.

Participants will explore **Security Architecture**, **Risk Management**, **Incident Response**, **Cloud Security**, **Artificial Intelligence Security**, and **Threat Intelligence** through a combination of instructor-led sessions, real-world scenarios, and practical lab exercises.

Prerequisites

Participants should have:

- At least **5 years of IT experience**
- Practical exposure to **Cyber Security Operations**

Who Should Attend

This course is ideal for:

- Professionals preparing for the **CompTIA SecurityX Certification**
- **Security Architects**, **Security Engineers**, and **Security Analysts**
- Teams responsible for **Enterprise Risk Management** and **Compliance**
- IT professionals supporting hybrid, cloud, and traditional infrastructures

What You Will Learn

Upon completion of this course, learners will be able to:

- Design resilient **Enterprise Security Architectures**.
- Implement **Risk Management**, **Compliance**, and **Threat Modelling** practices.
- Apply advanced **Cryptography** and **Cloud Security** principles.
- Monitor enterprise systems and automate threat remediation.
- Utilize **Threat Intelligence**, **Incident Response**, and **Root Cause Analysis** methodologies.
- Align security strategies with **Zero Trust**, **Artificial Intelligence**, and modern regulatory requirements.

Outline

CompTIA Security X Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Governance, Risk and Compliance (GRC)

- Security policies, procedures, standards, and governance frameworks
- Security awareness and organisational training programs
- **COBIT**, **ITIL**, and governance methodologies
- Asset lifecycle and **CMDB Management**
- **GRC Tools** and compliance automation
- Data governance practices
- Enterprise **Risk Assessment** methodologies
- Third-party risk management
- **Confidentiality, Integrity, and Availability (CIA)**
- **Threat Modelling** frameworks
- **MITRE ATT&CK**, **CAPEC**, and **STRIDE**
- Attack surface analysis
- **PCI DSS**, **ISO 27001**, and regulatory compliance
- **NIST CSF**, **CSA**, and security frameworks

Security Architecture

- **Cloud Security Architecture**
- **CASB**, Shadow IT detection, and shared responsibility models
- Secure **CI/CD Pipelines**
- Infrastructure automation using **Terraform** and **Ansible**
- Container and Kubernetes security
- Serverless workload protection
- Cloud data security and encryption key management
- Preventive, detective, and corrective security controls
- Network segmentation and micro-segmentation
- Secure VPN and API integrations
- **SASE**, **SD-WAN**, and modern networking strategies
- **Zero Trust Security Models**

Security Engineering

- Automation using **PowerShell**, **Python**, and **Bash**
- **SOAR Platforms** and workflow automation
- Vulnerability assessment and management
- Security scanning and reporting
- **SCAP**, **CVE**, **CVSS**, and OVAL standards
- Advanced cryptographic implementations
- **Post-Quantum Cryptography (PQC)**
- Homomorphic encryption
- Digital signatures and certificate-based authentication
- Tokenization and data protection technologies

Security Operations

- **SIEM Platforms** and security monitoring
- Event analysis and behavioural baselines
- False positive and false negative management
- Correlation and trend analysis
- Attack surface management

CompTIA Security X Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- **Cross-Site Scripting (XSS)** and Injection attacks
- **Defense-in-Depth** strategies
- **Threat Hunting** methodologies
- Internal and external threat intelligence
- **OSINT**, Dark Web, and ISAC intelligence sources
- **STIX**, **TAXII**, **YARA**, **Sigma**, and **Snort**
- Malware analysis and sandboxing
- Reverse engineering techniques
- Data recovery and **Root Cause Analysis**