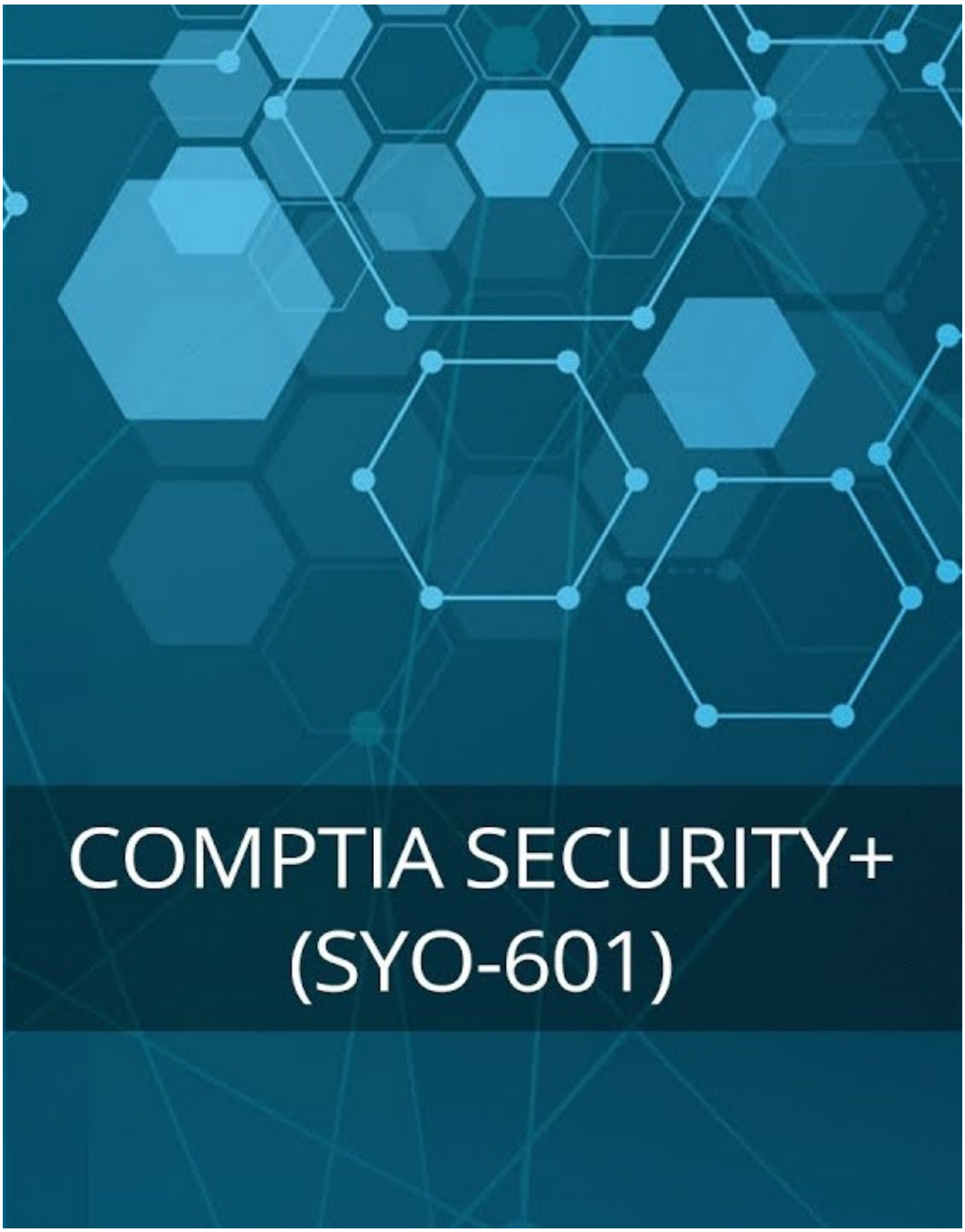
Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

CompTIA-SY0-601-Security+ Certification Training Course



Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Overview

This latest version course expands the coverage of cybersecurity threats, risk management, and IOT threats. This course prepares exam candidates for the first domain of the exam, Threats, Attacks, and Vulnerabilities. By learning about malware, networking and application security exploitations, and social engineering, participants will be prepared to answer questions from the exam and strengthen your own organization's systems and defences.

This CompTIA security+ SYO - 601 course highlights the basic knowledge needed to perform the security functions in IT security. It focuses on the practical skillset required to solve a variety of problems and tackle issues. The course covers the latest updates and market trends on risk management and mitigation, how to respond to threats and treat them, and various auditing and penetration testing opportunities.
Cybersecurity attacks continue to grow. Increasingly, more job roles are tasked with baseline security readiness and Response to address today's threats. Latest Changes in CompTIA security+ certification reflect skills relevant to these job roles and prepare candidates to be more proactive in preventing the next attack.

CompTIA Security 601 Exam Domains

1. Attacks, Threats and Vulnerabilities
2. Architecture and Design
3. Implementation
4. Operations and Incident Response
5. Governance, Risk and Compliance

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 1: Attacks, Threats, and Vulnerabilities

- Different methods of social engineering techniques. Learn about Phishing, Spam, Identity fraud, Hoax, Credential harvesting, etc.
- Learn about potential indicators to determine the type of attack. Get familiar with the Malware, Password attacks, Physical attacks, Cloud-based vs. on-premises attacks, and Adversarial artificial intelligence (AI).
- Analyse potential indicators associated with application attacks. Get a good understanding of Privilege escalation, Cross-site scripting, Injections, Error handling, Replay attack, Application programming interface (API) attacks, Driver manipulation.
- Analyse potential indicators associated with network attacks. Learn about Layer 2 attacks, Domain name system (DNS), Distributed denial-of-service (DDOS), Wireless Attacks, Malicious code, or script execution.
- Explain different threat intelligence sources, actors, and vectors. Learn about Actors and threats, Attributes of actors, Vectors, Threat intelligence sources, Research sources.
- Explain the security concerns associated with different types of vulnerabilities. Get familiar with Cloud-based vs. on-premises vulnerabilities, Zero-day, Weak configurations, Third-party risks, Improper or weak patch management, Legacy platforms, and Impacts.
- Summarize the techniques used in security assessments. Get knowledge about Threat hunting, Vulnerability scans, Syslog/Security information and event management (SIEM), and Security orchestration, automation, and Response (SOAR).
- Explain the techniques used in penetration testing. Learn about Penetration testing, Passive and active reconnaissance, Exercise types.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 2: Architecture and Design

- Explain the importance of security concepts in an enterprise environment. Learn Configuration management, Data sovereignty, Data protection, Geographical considerations, Response and recovery controls, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection, Hashing, API considerations, Site resiliency, and Deception and disruption.
- Summarize virtualization and cloud computing concepts. Learn about Cloud models, Managed service provider (MSP)/ managed security service provider (MSSP), On-premises vs. off-premises, Fog computing, Edge computing, Thin client, Containers, Micro services/API, Infrastructure as code, Server less architecture, Server less architecture, Resource policies, and Virtualization.
- Summarize secure application development, deployment, and automation concepts. Clear your concepts on Environment, Provisioning and de-provisioning, Integrity measurement, Secure coding techniques, Open Web Application Security Project (OWASP), Software diversity, Elasticity, Scalability, and Version control.
- Summarize authentication and authorization design concepts. Learn concepts of Authentication methods, Biometrics, Multifactor authentication (MFA) factors and attributes, And Authentication, authorization, and accounting (AAA).
- Given a scenario, implement cybersecurity resilience. Get to know about Redundancy, Replication, On-premises vs. cloud, Backup types, Non-persistence, High availability, and Restoration order.
- Explain the security implications of embedded and specialized systems. Learn about Embedded systems, Supervisory control and data acquisition(SCADA)/industrial control system (ICS), Internet of Things (IOT), Voice over IP (VoIP), Heating, ventilation, air conditioning (HVAC), Drones, Multifunction printer (MFP), Real-time operating system (RTOS), Surveillance systems, System on a Chip (SOC), Communication considerations.
- Explain the importance of physical security controls. Clear your concepts on Bollards/barricades, Access control vestibules, Badges, Alarms, Signage, Cameras, USB data blocker, Lighting, Fencing, Fire suppression, Sensors, Drones, Visitor logs, Faraday cages, Air gap, Screened subnet (previously known as demilitarized zone), Protected cable distribution, Secure data destruction.
- Summarize the basics of cryptographic concepts. Get to know about Digital signatures, Key length, Key stretching, Salting, Hashing, Key exchange, Elliptic-curve cryptography, Perfect forward secrecy, Quantum, Post-quantum, Ephemeral, Block chain, Symmetric vs. asymmetric, Lightweight cryptography, Steganography, Homomorphic encryption, Common use cases, and Limitations.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 3: Implementation

- Implement secure protocols: Domain Name System Security Extensions (DNSSEC), SSH, Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Real-time Transport Protocol (SRTP), Lightweight Directory Access Protocol Over SSL (LDAPS), File Transfer Protocol, Secure (FTPS), SSH File Transfer Protocol (SFTP), Simple Network Management Protocol, version 3 (SNMPv3), Hypertext transfer protocol over SSL/TLS (HTTPS).
- Implement host or application security solutions. Learn about Endpoint protection, Boot integrity, Database, Application Security, Hardening, Self-encrypting drive (SED)/ full-disk encryption (FDE), Trusted Platform Module (TPM), Hardware root of trust, Sandboxing
- Implement secure network designs. Learn about Load balancing, Network segmentation, Network segmentation, Network access control (NAC), DNS,
- Out-of-band management, Port security, Network appliances, Access control list (ACL), Port spanning/port mirroring, Monitoring services.
- Install and configure wireless security settings. Learn about Cryptographic protocols, Authentication protocols, Installation considerations
- Implement secure mobile solutions. Get to know about Connection methods and receivers, Mobile device management (MDM), Mobile devices, Deployment model, and Enforcement and monitoring of: (Third-party application stores, Rooting/jailbreaking, Side loading, Custom firmware, Carrier unlocking, Firmware over-the-air (OTA) updates).
- Apply cybersecurity solutions to the cloud. Learn about Cloud security controls and Solutions.
- Implement identity and account management controls. Learn concepts like Identity, Account types, and Account policies
- Implement authentication and authorization solutions. Get Knowledge about Authentication management, Authentication/authorization, Access control schemes
- Implement public key infrastructure. Learn about Public key infrastructure (PKI), Types of certificates, Certificate formats, Concepts.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 4: Operations and Incident Response

- Learn how to use the appropriate tool to assess organizational security. Learn Network reconnaissance and discovery, File manipulation, Shell and script environments, Packet capture and replay, Forensics, Exploitation frameworks, Password crackers, Data sanitization.
- Summarize the importance of processes, policies, and procedures for incident response. Learn the concept of Incident response plans, Incident response process, Attack frameworks, Stakeholder management, Communication plan, Continuity of operations planning (COOP), Disaster recovery plan, Business continuity plan, Incident response team.
- Utilizing appropriate data sources to support an investigation. Learn about Vulnerability scan output, SIEM dashboards, Log files, Bandwidth monitors, Metadata, Protocol analyser output, Net flow/slow.
- Use different mitigation techniques or controls to secure an environment. Get familiar with Reconfigure endpoint security solutions, Configuration changes, Isolation, Containment, Segmentation, SOAR.
- Explain the key aspects of digital forensics. Clear your concept on Documentation/evidence, Acquisition, Preservation, E-discovery, Data recovery, Non-repudiation, Strategic intelligence /counterintelligence.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Domain 5: Governance, Risk, and Compliance

- Compare and contrast various types of controls.
- Explain the importance of applicable standards, regulations, or frameworks that impact organizational security posture. Learn about Regulations, standards, and legislation; Key frameworks; Benchmarks /secure configuration guides.
- Explain why policies are important to organizational security. Clear your concept on Organizational policies, Credential policies, Data, Third-party risk management, Diversity of training techniques.
- Summarize risk management processes and concepts. Learn about Risk types, Risk management strategies, Risk analysis, Disasters, Business impact analysis.
- Explain privacy and sensitive data concepts about security. Great to know about Organizational consequences of privacy and data breaches, Notifications of breaches, Data types, Privacy-enhancing technologies, Roles and responsibilities, Information life cycle, Impact assessment, Terms of the agreement Privacy notice.