CompTIA

CompTIA Security+ Certified Professionals Are Trusted Defenders of Digital Environments

The new CompTIA Security+ (SY0-701) has been updated to reflect the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk, and more. Once certified, candidates will understand the core skills needed to succeed on the job – and employers will notice too. Candidates will develop a core foundation of essential skills that pave way for a fulfilling career, which is why more job roles use CompTIA Security+ for baseline cybersecurity skills than any other certification in the industry.

CompTIA Security+ equips candidates with the skills and knowledge necessary to safeguard networks, detect threats, and secure data in roles such as security specialist, systems administrator, and security administrator.

The certification exam covers:

- Assessing the security posture of an enterprise environment and recommending and implementing appropriate security solutions.
- Monitoring and securing hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology (OT).
- Operating with an awareness of applicable regulations and policies, including principles of governance, risk and compliance.
- Identifying, analyzing and responding to security events and incidents.

CompTIA Security+

Exam Objectives Comparison

The following table aligns exam objectives from SY0-701 and SY0-601 for comparison. Skills are aligned by best match.

SY0-701	SY0-601 Equivalent	MAPPING
1.1 Compare and contrast various types of security controls.	5.1 Compare and contrast various types of controls.	Maps
1.2 Summarize fundamental security concepts.	2.1 "Explain the importance of security concepts in an enterprise environment."	Maps
1.2 Summarize fundamental security concepts.	2.7 Explain the importance of physical security controls.	Maps
1.2 Summarize fundamental security concepts.	2.4 Summarize authentication and authorization design concepts.	Maps
1.3 Explain the importance of change management processes and the impact to security.	5.3 Explain the importance of policies to organizational security.	Maps
1.4 Explain the importance of using appropriate cryptographic solutions.	2.8 Summarize the basics of cryptographic concepts.	Maps
2.1 Compare and contrast common threat actors and motivations.	1.5 Explain different threat actors, vectors, and intelligence sources.	Maps
2.2 Explain common threat vectors and attack surfaces.	1.5 Explain different threat actors, vectors, and intelligence sources.	Maps
2.3 Explain various types of vulnerabilities.	1.6 "Explain the security concerns associated with various types of vulnerabilities."	Maps
2.4 Given a scenario, analyze indicators of malicious activity.	1.2 "Given a scenario, analyze potential indicators to determine the type of attack."	Maps
2.4 Given a scenario, analyze indicators of malicious activity.	1.3 Given a scenario, analyze potential indicators associated with application attacks.	Maps
2.4 Given a scenario, analyze indicators of malicious activity.	1.4 "Given a scenario, analyze potential indicators associated with network attacks."	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	4.4 "Given an incident, apply mitigation techniques or controls to secure an environment."	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	3.1 Given a scenario, implement secure protocols.	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	3.2 "Given a scenario, implement host or application security solutions."	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	3.3 Given a scenario, implement secure network designs.	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	3.4 Given a scenario, install and configure wireless security settings.	Maps
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	3.5 Given a scenario, implement secure mobile solutions.	Maps
3.1 Compare and contrast security implications of different architecture models.	2.2 Summarize virtualization and cloud computing concepts.	Maps
3.1 Compare and contrast security implications of different architecture models.	2.6 Explain the security implications of embedded and specialized systems.	Maps
3.1 Compare and contrast security implications of different architecture models.	2.3 "Summarize secure application development, deployment, and automation concepts."	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	2.1 "Explain the importance of security concepts in an enterprise environment."	Gap

SY0-701	SY0-01 Equivalent	MAPPING
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.1 Given a scenario, implement secure protocols.	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.2 "Given a scenario, implement host or application security solutions."	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.3 Given a scenario, implement secure network designs.	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.3 Given a scenario, implement secure network designs.	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.4 Given a scenario, install and configure wireless security settings.	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.5 Given a scenario, implement secure mobile solutions.	Maps
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	3.6 Given a scenario, apply cybersecurity solutions to the cloud.	Maps
3.3 Compare and contrast concepts and strategies to protect data.	5.5 Explain privacy and sensitive data concepts in relation to security.	Maps
3.4 Explain the importance of resilience and recovery in security architecture.	2.5 Given a scenario, implement cybersecurity resilience.	Maps
3.4 Explain the importance of resilience and recovery in security architecture.	2.2 Summarize virtualization and cloud computing concepts.	Maps
4.1 Given a scenario, apply common security techniques to computing resources.	2.6 Explain the security implications of embedded and specialized systems.	Gap
4.1 Given a scenario, apply common security techniques to computing resources.	2.2 Summarize virtualization and cloud computing concepts.	Gap
4.1 Given a scenario, apply common security techniques to computing resources.	3.4 Given a scenario, install and configure wireless security settings.	Maps
4.1 Given a scenario, apply common security techniques to computing resources.	2.3 "Summarize secure application development, deployment, and automation concepts."	Gap
4.1 Given a scenario, apply common security techniques to computing resources.	3.5 Given a scenario, implement secure mobile solutions.	Maps
4.1 Given a scenario, apply common security techniques to computing resources.	3.2 "Given a scenario, implement host or application security solutions."	Maps
4.2 Explain the security implications of proper hardware, software, and data asset management.	2.7 Explain the importance of physical security controls.	Maps
4.2 Explain the security implications of proper hardware, software, and data asset management.	5.3 Explain the importance of policies to organizational security.	Maps
4.2 Explain the security implications of proper hardware, software, and data asset management.	5.5 Explain privacy and sensitive data concepts in relation to security.	Maps
4.3 Explain various activities associated with vulnerability management.	1.6 "Explain the security concerns associated with various types of vulnerabilities."	Maps
4.3 Explain various activities associated with vulnerability management.	1.7 Summarize the techniques used in security assessments.	Maps
4.3 Explain various activities associated with vulnerability management.	1.8 Explain the techniques used in penetration testing.	Maps
4.3 Explain various activities associated with vulnerability management.	4.3 "Given an incident, utilize appropriate data sources to support an investigation."	Maps
4.3 Explain various activities associated with vulnerability management.	3.2 Given a scenario, implement host or application security solutions.	Maps

SY0-701	SY0-601 Equivalent	MAPPING
4.4 Explain security alerting and monitoring concepts and tools.	4.1 "Given a scenario, use the appropriate tool to assess organizational security."	Maps
4.4 Explain security alerting and monitoring concepts and tools.	4.3 "Given an incident, utilize appropriate data sources to support an investigation."	Maps
4.5 Given a scenario, modify enterprise capabilities to enhance security.	3.2 Given a scenario, implement host or application security solutions.	Maps
4.5 Given a scenario, modify enterprise capabilities to enhance security.	4.5 Given a scenario, modify enterprise capabilities to enhance security.	Maps
4.5 Given a scenario, modify enterprise capabilities to enhance security.	4.5 Given a scenario, modify enterprise capabilities to enhance security.	Maps
4.5 Given a scenario, modify enterprise capabilities to enhance security.	4.5 Given a scenario, modify enterprise capabilities to enhance security.	Maps
4.5 Given a scenario, modify enterprise capabilities to enhance security.	4.5 Given a scenario, modify enterprise capabilities to enhance security.	Maps
4.6 Given a scenario, implement and maintain identity and access management.	2.4 Summarize authentication and authorization design concepts.	Gap
4.7 Explain the importance of automation and orchestration related to secure operations.	2.3 "Summarize secure application development, deployment, and automation concepts."	Maps
4.8 Explain appropriate incident response activities.	4.2 Summarize the importance of policies, processes, and procedures for incident response.	Maps
4.8 Explain appropriate incident response activities.	4.5 Explain the key aspects of digital forensics.	Maps
4.9 Given a scenario, use data sources to support an investigation.	4.3 "Given an incident, utilize appropriate data sources to support an investigation."	Maps
5.1 Summarize elements of effective security governance.	4.2 Summarize the importance of policies, processes, and procedures for incident response.	Maps
5.1 Summarize elements of effective security governance.	5.3 Explain the importance of policies to organizational security.	Maps
5.2 Explain elements of the risk management process.	5.4 Summarize risk management processes and concepts.	Maps
5.3 Explain the processes associated with third-party risk assessment and management.	5.3 Explain the importance of policies to organizational security.	Maps
5.3 Explain the processes associated with third-party risk assessment and management.	5.4 Summarize risk management processes and concepts.	Maps
5.4 Summarize elements of effective security compliance.	5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	Maps
5.4 Summarize elements of effective security compliance.	5.5 Explain privacy and sensitive data concepts in relation to security.	Maps
5.5 "Explain types and purposes of audits and assessments."	5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	Maps
5.5 "Explain types and purposes of audits and assessments."	1.8 Explain the techniques used in penetration testing.	Maps
5.6 Given a scenario, implement security awareness practices.	5.3 Explain the importance of policies to organizational security.	Gap

CompTIA