CompTIA

+ means readiness and response

SY0-601 vs SY0-501 Exam Objectives Comparison

As Cybersecurity attacks increase, more job roles are tasked with bridging the gap between improving baseline security readiness and incident response. Updates to Security+ reflect current skills relevant to these job roles and prepare candidates to be more proactive in preventing the next attack.

Security+ SY0-601 has been updated to address the gap between improving the security posture and decreasing cybersecurity risk. It covers the best practices and latest techniques for assessing the security posture of an enterprise, monitoring, and securing various hybrid/cloud environments, complying to IT regulations, managing risk and basic risk assessment, and mitigating security events through incident response.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements

CompTIA Security+

Exam Objectives Comparison

The following table aligns exam objectives from SY0-601 to SY0-501 for comparison. Skills are aligned by best match.

SY0-601	SY0-501
1.1 Compare and contrast different types of social engineering techniques	1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
1.2 Given a scenario, analyze potential indicators to determine the type of attack.	1.2 Compare and contrast types of attacks.
1.3 Given a scenario, analyze potential indicators associated with application attacks.	2.3 Given a scenario, troubleshoot common security issues.
1.4 Given a scenario, analyze potential indicators associated with network attacks.	2.4 Given a scenario, analyze and interpret output from security technologies.
1.5 Explain different threat actors, vectors and intelligence sources.	1.3 Explain threat actor types and attributes.
1.6 Explain the security concerns associated with various types of vulnerabilities.	1.6 Explain the impact associated with types of vulnerabilities.
1.7 Summarize the techniques used in security assessments.	1.4 Explain penetration testing concepts.
1.8 Explain the techniques used in penetration testing.	1.5 Explain vulnerability scanning concepts.
2.1 Explain the importance of security concepts in an enterprise environment.	(The previous exam included fewer enterprise specific topics; no exact match.)
2.2 Summarize virtualization and cloud computing concepts.	3.7 Summarize cloud and virtualization concepts.
2.3 Summarize secure application development, deployment, and automation concepts.	3.4 Explain the importance of secure staging deployment concepts. 3.6 Summarize secure application development and deployment concepts.
2.4 Summarize authentication and authorization design concepts.	4.1 Compare and contrast identity and access management concepts.
2.5 Given a scenario, implement cybersecurity resilience.	3.8 Explain how resiliency and automation strategies reduce risk.
2.6 Explain the security implications of embedded and specialized systems.	3.5 Explain the security implications of embedded systems.
2.7 Explain the importance of physical security controls.	3.9 Explain the importance of physical security controls.
(The previous SY0-501 objective 5.8 was too general; these tasks are now spread throughout SY0-601 objectives.)	5.8 Given a scenario, carry out data security and privacy practices.
2.8 Summarize the basics of cryptographic concepts.	6.1 Compare and contrast basic concepts of cryptography.
(Cryptography is still covered in SY0-601, but algorithms are considered too specialized for most administrators and topic reduced.)	6.2 Explain cryptography algorithms and their basic characteristics.
3.1 Given a scenario, implement secure protocols.	2.6 Given a scenario, implement secure protocols.
3.2 Given a scenario, implement host or application security solutions.	3.2 Given a scenario, implement secure network architecture concepts.

SY0-601	SY0-501
3.3 Given a scenario, implement secure network designs.	3.3 Given a scenario, implement secure systems design.
(The previous SY0-501 objective 2.1 was too general; these tasks are now spread throughout SY0-601 objectives.)	2.1 Install and configure network components, both hardware and software-based, to support organizational security.
3.4 Given a scenario, install and configure wireless security settings.	6.3 Given a scenario, install and configure wireless security settings.
3.5 Given a scenario, implement secure mobile solutions.	2.5 Given, a scenario, deploy mobile devices securely.
3.6 Given a scenario, apply cybersecurity solutions to the cloud.	3.7 Summarize cloud and virtualization concepts.
3.7 Given a scenario, implement identity and account management controls.	4.2 Given a scenario, install and configure identity and access services.
3.8 Given a scenario, implement authentication and authorization solutions.	4.3 Given a scenario, implement identity and access management controls. 4.4 Given a scenario, differentiate common account management practices.
3.9 Given a scenario, implement public key infrastructure.	6.4 Given a scenario, implement public key infrastructure.
4.1 Given a scenario, use the appropriate tool to assess organizational security.	2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
4.2 Summarize the importance of policies, processes, and procedures for incident response. 4.3 Given an incident, utilize appropriate data sources to support an investigation. 4.4 Given an incident, apply mitigation techniques or controls to secure an environment.	5.4 Given a scenario, follow incident response procedures. 5.6 Explain disaster recovery and continuity of operations concepts.
4.5 Explain the key aspects of digital forensics.	5.5 Summarize basic concepts of forensics.
5.1 Compare and contrast various types of controls.	5.7 Compare and contrast various types of controls.
5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.
5.3 Explain the importance of policies to organizational security.	5.1 Explain the importance of policies, plans and procedures related to organizational security.
5.4 Summarize risk management processes and concepts.	5.2 Summarize business impact analysis concepts. 5.3 Explain risk management processes and concepts.
5.5 Explain privacy and sensitive data concepts in relation to security.	3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.