Continue

CompTIA Security+ is amongst the most preferred certifications by major companies than any other IT certification for demonstrating hands-on fundamental cybersecurity abilities. As a result, more IT job positions are turning to CompTIA Security+ to enhance cybersecurity abilities as the demand to safeguard more systems, software, and hardware develops. Keeping all this in mind, CompTIA always keeps its certification exam updated. And, same goes with the CompTIA Secuirty+ certification. To earn this certification, previously you were required to pass CompTIA SY0-501 exam. But, now it has been updated to CompTIA SY0-601 exam. In order to understand the updates and compare the two, in this blog, we will go through the in-depth details of both SY0-501 and SY0-601 for having better clarity! In the enhancement of technology, IT certifications have always illustrated to organizations that candidates possess the necessary knowledge and abilities for the position, as well as assisting IT professionals in their advancement. And, cybersecurity credentials are among the most popular IT qualifications worldwide, since it has become an essential role. In terms of cybersecurity, the CompTIA Security+ certification has been obtained by over 500,000 IT workers, and according to research, it is among the top 10 cybersecurity qualifications. CompTIA Security+ 501 and 601 are two different versions of the CompTIA Security+ certification exam. The Security+ 501 exam was released in 2018 and focuses on basic security concepts, while the Security+ 601 exam, released in 2021, has updated content that reflects the latest advances in cybersecurity and is more comprehensive in scope. Both exams are designed for individuals who are seeking a foundational understanding of security principles, and who want to demonstrate their knowledge and skills in this area. However, the Security+ 601 exam is more current and covers a wider range of topics than the Security+ 501 exam. The CompTIA Security+ 501 exam verifies that the applicant has the necessary knowledge and abilities to: Firstly, installing and configuring systems for securing applications, networks, and devicesSecondly, executing threat analysis and responding with suitable mitigation techniques. Also, be a part of risk mitigation activities.Thirdly, working with a thorough understanding of relevant rules, laws, and regulations Knowledge requirement: The CompTIA Security+ 501 exam is for IT security professionals who have the following skills: Firstly, the experience of a minimum of two years in IT administration with security as the main subject.Secondly, experience in technical information security.Lastly, understanding and familiarity with security concerns and implementation. On October 4, 2017, the CompTIA Security+ SY0-501 exam was released. This exam certifies the successful candidate has the knowledge and skills required for setting up systems to secure applications, networks, and devices, executing threat analysis and responding with suitable mitigation techniques and more. However, this exam had 90 questions of the type multiple choice and performance-based. And, the time duration was of 90 minutes to complete the exam. The exam requires a minimum score of 750 (on a scale of 100-900) to pass, and it can be taken in English, Japanese, Portuguese, or Simplified Chinese. The English exam was retired on July 31, 2021. And, the other languages exam will retire in Q1 2022. But, what are the major changes in the new CompTIA Security+ 601 exam? Let’s find out! CompTIA has always encouraged candidates to use updated exam information for preparation. However, let’s look at or the new CompTIA Security+ (SY0-601) certification exam. CompTIA Security+ SY0-601 is a certification exam that tests individuals’ knowledge and skills in cybersecurity concepts and practices. The exam is designed for IT professionals who have at least two years of experience in IT administration with a focus on security and who are looking to obtain a comprehensive understanding of security principles. The SY0-601 exam covers a range of topics, including: Network securityCompliance and operational securityThreats and vulnerabilitiesApplication, data, and host securityAccess control and identity managementCryptography Further, the CompTIA Security+ 601 exam verifies that the applicant has the necessary knowledge and abilities to: Firstly, examining the security posture of an enterprise environment.Secondly, suggesting and implementing suitable security solutions.Thirdly, monitoring and securing hybrid environments, including cloud, mobile, and IoTThen, operating with an awareness of applicable laws and policies, including:principles of governance, risk, and complianceLastly, identifying, analyzing, and responding to security events and incidents. Knowledge requirement: There has been a bit of change in the knowledge and experience required for the Secuity+ 601 exam. Now, the CompTIA Security+ 601 exam requires the following skills: Firstly, a hands-on experience two years of working in a security/systems administrator job roleSecondly, knowledge and experience in technical information securityLastly, advanced knowledge of security concepts The CompTIA Security+ SY0-601 exam was launched on November 12, 2020. This exam certifies the successful candidate has the knowledge and skills required for examining the security posture of an enterprise environment and suggesting suitable security solutions, checking and securing hybrid environments and more. However, this exam had 90 questions of the type multiple choice and performance-based. And, the time duration was of 90 minutes to complete the exam. The exam requires a minimum score of 750 (on a scale of 100-900) to pass, and it can be given in English and Japanese language. This exam basically retires after three years. And, the cost of taking the exam is $370 USD. Moving on to the major modifications, the exam objectives. Despite the fact that the test objectives paper is longer, the new SY0-601 exam has fewer goals than the old one. However, there are 35 exam objectives on the CompTIA Security+ (SY0-601) exam, compared to 37 on the SY0-501 exam. And, the exam objectives for SY0-601 are different. That is to say, this exam update more examples under each objective. Further, CompTIA has made this update to assist you in better understanding the significance of each exam objective. The more examples and information is there, the more useful the exam objectives are in helping IT professionals prepare for their certification exam and, eventually, the job. But, you need to keep in mind that exam objectives are not exhaustive. That is to say, you may come across additional technologies, procedures, or activities on the exam. The exam questions are focused on the main exam objectives rather than these bulleted samples. And, in order for providing relevancy and exam integrity, CompTIA is regularly evaluating exam material and revising questions. Coming on the objectives! Along with a developing industry job function, the CompTIA Security+ (SY0-601) exam now covers five primary areas instead of six. However, let’s take a look at the changes in the objectives. CompTIA Security+ 501 Exam DomainsNew CompTIA Security+ 601 Exam DomainsThreats, Attacks, and Vulnerabilities (21%)Attacks, Threats, and Vulnerabilities (24%)Technologies and Tools (22%)Architecture and Design (21%)Architecture and Design (15%)Implementation (25%)Identity and Access Management (16%)Operations and Incident Response (16%)Risk Management (14%)Governance, Risk, and Compliance (14%)Cryptography and PKI (12%) But, how CompTIA security+ is ruling the market sector! So, let’s find out the value of Security+ using the updated topics in order to understand more about the SY0-601 exam. CompTIA exam domains must represent what is occurring in the market in a subject like cybersecurity, where the profession is constantly developing. The details below specify why the CompTIA Security+ exam domains were updated and how they relate to job requirements. This area focuses on newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS assaults, and social engineering attacks based on current events, as well as emerging threats, attacks, and vulnerabilities on the Internet. Importance in the job market: 68 percent of corporate leaders believe their cybersecurity risks are growing, according to a source. However, for resisting these new dangers, IT professionals must assist in the detection of cyberattacks and vulnerabilities so that they may be mitigated before they breach information systems. This domain includes enterprise environment coverage and cloud dependency, which is rapidly rising as enterprises shift to hybrid networks. Importance in the job market: IT experts must understand safe virtualization, secure application deployment, and automation ideas for maintaining a solid cybersecurity posture and supporting hybrid environments. This domain broadens to include identity management, access control, public key infrastructure (PKI), fundamental cryptography, wireless, and end-to-end security. Importance in the job market: IT professionals must select and apply the appropriate protocols and encryption for a certain network/cloud design, mobile solution, or wireless scenario, for example, for supporting corporate cybersecurity. This domain includes fundamental threat detection, risk mitigation strategies, security controls, and basic digital forensics, as well as organization security assessment and incident response protocols. Importance in the job market: IT experts are being asked to undertake incident responses early in their careers for supporting operations and the increase of recent attacks. They must be able to defend systems using fundamental mitigation techniques and security controls. This domain grows to support corporate risk management and regulatory compliance, including PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA. Importance in the job market: According to a recent survey, approximately 60% of respondents said compliance activities had increased. IT experts must understand compliance security measures, how they decrease risk, and how to deploy them to improve cybersecurity posture in order to support governance, risk, and compliance. Above we have gone through the major differences and modifications that happened in the CompTIA Security+ exam. Now, in the next section, we will go through the major job role and salaries that you can earn with this certification. As we have understood the new CompTIA Security+ (SY0-601) exam update. Every three years, CompTIA refreshes its certifications to keep up with changing technology, ensuring that your abilities remain current and relevant. Talking about security+, more companies and defense organizations use this certification above any other on the market to confirm baseline security capabilities and meet DoD 8570 compliance. Moreover, the only baseline cybersecurity certification that focuses on hands-on practical skills, ensuring that security professionals have better preparation for dealing with today’s complicated situations. Further, coming on the job roles, for securing networks, software, and hardware, basic cybersecurity skills are relevant across a wider range of today’s job responsibilities. The Security+ exam covers the most basic technical skills in risk assessment and management, incident response, forensics, corporate networks, hybrid/cloud operations, and security policies, all of which are essential for job success. CompTIA Security+ certification is a globally recognized cybersecurity certification that validates the knowledge and skills required to perform security functions in a variety of job roles. Some of the job roles that typically require CompTIA Security+ certification include: Security Analyst: Responsible for monitoring and analyzing security threats, conducting risk assessments, and recommending security measures to protect the organization.Network Administrator: Responsible for maintaining the security of an organization’s network infrastructure, including firewalls, routers, and switches.System Administrator: Responsible for installing, configuring, and maintaining an organization’s computer systems, including ensuring the security of those systems.Security Engineer: Responsible for designing, implementing, and maintaining security systems, including firewalls, intrusion detection systems, and encryption technologies.Information Security Officer (ISO): Responsible for developing and implementing security policies and procedures, conducting risk assessments, and ensuring the organization’s compliance with industry regulations and standards. Contributing organizations to the development of Security+ are: NetflixTargetSplunkJohns Hopkins UniversityGeneral Dynamics IT Above we have gone through the major modifications and differences that have been made for the SY0-501 and SY0-601 exams. CompTIA Security+ exam has already made its position in the cybersecurity sector by gaining the trust of top organizations. So, go through the above information and check out the details to match your skills and experience. And, then start preparing for the updated CompTIA Security+ exam by: Exploring a variety of training options, including study guides, online self-study tools, and instructor-led courses.Then, making use of best practice tests for having a better revision. Further, the CompTIA study resources provide you the confidence to pass your CompTIA certification exam. And, using CompTIA’s online training tools is best for those who are beginning and need comprehensive training for passing the exam. So, start applying your knowledge, practicing, and then earn the certification. CompTIA certifications are globally recognized and highly sought-after credentials, and Security+ is considered by many to be an essential cybersecurity certification. Information technology professionals who earn the CompTIA Security+ certification are in high demand worldwide by many large corporations and organizations. In Washington, D.C., where many businesses are headquartered, there is a huge need for cybersecurity professionals to fill the hundreds of available job roles. Recently, the certification exam for the Security+ credential was updated from exam SYO-501 to SYO-601. You will still be able to take the older version of the exam until July 31, 2021, if you have been studying for it. However, the new version is also available to take as of November of 2020. It's important to understand the changes that CompTIA made to update the Security+ exam when deciding how to proceed with your certification. Why Did CompTIA Update the Security+ Certification Exam? In IT, it's critical that certifications stay relevant to the current state of the industry. As a result, CompTIA and other certifying agencies consistently perform research to determine what needs to be evaluated on certification exams – what set of skills the certification represents. One example related to the Security+ update is CompTIA researchers found that current business leaders are finding their risks of cybersecurity attacks are increasing. That information led to CompTIA placing a higher weight on the exam domain covering attacks, threats, and vulnerabilities. CompTIA Security+ Exam SYO-501 vs. Exam SYO-601 The Security+ certification exam is designed to evaluate your knowledge of the latest cybersecurity trends and techniques. It covers the core concepts and technical skills in risk assessment, risk management, forensics, incident response, security controls, enterprise networks, and hybrid/cloud operations to ensure high job performance levels. You can see some of the changes when looking at the domains that are tested on exam 501 vs. exam 601. The new CompTIA Security+ exam has five domains instead of the previous six, and the weighting of the domains the two tests have in common has been updated. CompTIA Security+ SYO-501 Exam Domains: Technologies and Tools (22%) Threats, Attacks, and Vulnerabilities (21%) Identity and Access Management (16%) Architecture and Design (15%) Risk Management (14%) Cryptography and PKI (12%) CompTIA Security+ SYO-601 Exam Domains: Implementation (25%) Attacks, Threats, and Vulnerabilities (24%) Architecture and Design (21%) Operations and Incident Response (16%) Governance, Risk, and Compliance (14%) Overall, the CompTIA Security+ SYO-601 exam covers the most current skills and knowledge that candidates need to be able for: Assessing the information security posture of enterprise environments Recommending and implementing proper security solutions Monitoring and securing hybrid environments Operating with an awareness of policies and laws that are applicable Identifying, analyzing, and responding to cybersecurity incidents and events The exam objectives document for the SYO-601 exam is longer; however, it consists of fewer objectives. Exam SYO-501 has 37 objectives, while the SYO-601 has 35. The difference lies in the examples that are listed under each objective. The number increased on the SYO-601 by about a quarter. This change was intentional to help candidates better comprehend the meaning of each objective. This is a positive change because the more examples you are given, the easier it is to understand the objective. It is important to note that the list of exam objectives and examples isn't exhaustive. It represents the type of material you need to know that may be included in the exam. However, you may face exam questions pertaining to other processes, technologies, or tasks on your actual test. Questions may not be based solely on the examples but rather on the overall objectives themselves. CompTIA reviews exam content consistently and makes changes as it finds necessary. Training for CompTIA Security+ Certification in Washington, D.C. Now that you understand the significant differences between the outgoing Security+ certification exam and the incoming one, it's time to consider how you will prepare for your test. The Security+ exam covers a lot of critical information that is essential to performing various cybersecurity jobs. At TrainACE, we offer a comprehensive CompTIA Security+ training course covering all the relevant material, exam prep, and practice exams, ensuring that you will be as ready as you can be to take and pass the certification exam. We will continue our training course for SYO-501 until closer to its retirement date this summer. It's important to note that your certification will still be valid for three years if you take and pass SYO-501 before it retires. Let us help you prepare to earn the valuable Security+ credential. It will increase your knowledge and job opportunities to advance your IT career. If you’re considering a career in IT security, you have likely come across the CompTIA Security+ certification. This certification is a highly respected and in-demand credential that validates your knowledge and skills in network security and risk management. However, with the recent release of Security+ 601, you may be wondering which certification is right for you. In this article, we will compare Security+ 501 and 601 from various perspectives to help you make an informed decision. Introduction to CompTIA Security+ Certification CompTIA Security+ is a vendor-neutral certification designed to demonstrate foundational IT security skills and knowledge. The certification covers a broad range of topics, including network security, threats and vulnerabilities, identity management, cryptography, and risk management. This certification is an excellent starting point for anyone looking to launch their career in IT security or professionals seeking to validate their security skills. One of the benefits of obtaining the CompTIA Security+ certification is that it is recognized globally. This means that individuals who hold this certification can work in various countries and industries. Additionally, the certification is accredited by the American National Standards Institute (ANSI) and is compliant with the ISO 17024 standard, which ensures that the certification meets high-quality standards. Another advantage of the CompTIA Security+ certification is that it is a requirement for many IT security positions. Employers often look for candidates who hold this certification as it demonstrates that they have a solid understanding of IT security concepts and can apply them in real-world scenarios. Furthermore, individuals who hold this certification may have a higher earning potential compared to those who do not. Overview of Security+ 501 Exam Security+ 501 is the previous version of the CompTIA Security+ certification exam. The exam includes a maximum of 90 multiple-choice and performance-based questions that tests your knowledge and skills in several areas, such as: Threats, Attacks and Vulnerabilities Technologies and Tools Architectures and Design Identity and Access Management Risk Management The exam has a time limit of 90 minutes and a passing score of 750 points on a scale of 100-900. It is important to note that the Security+ 501 exam is no longer available for new candidates. It has been replaced by the Security+ 601 exam, which covers updated and expanded topics in cybersecurity. However, if you have already passed the Security+ 501 exam, your certification is still valid and does not expire until three years from the date of passing. Overview of Security+ 601 Exam Security+ 601 is the most recent version of the CompTIA Security+ certification exam. The exam includes a maximum of 90 multiple-choice and performance-based questions that are designed to test your knowledge and skills in several areas, such as: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response The exam has a time limit of 90 minutes and a passing score of 750 points on a scale of 100-900. It is important to note that the Security+ 601 exam is recognized globally as a benchmark for cybersecurity knowledge and skills. This certification is highly valued by employers and can lead to various job opportunities in the field of cybersecurity. Additionally, the Security+ 601 certification is valid for three years, after which it can be renewed by passing a renewal exam or earning continuing education units (CEUs). See also Prepare for Your Security+ Exam with a Security+ Boot CampDifferences between Security+ 501 and 601 Exams While both exams cover similar topics, there are some differences between Security+ 501 and 601. Some of the main highlights are: Security+ 601 emphasizes hands-on practical skills, while Security+ 501 focused more on theoretical concepts. The Security+ 601 exam is more scenario-based, whereas Security+ 501 emphasized technical knowledge. Security+ 601 covers emerging technologies like IoT, cloud security, virtualization, and mobile devices in-depth, which Security+ 501 didn’t. The Security+ 601 exam has fewer performance-based questions and more multiple-choice questions compared to the Security+ 501 exam. Another difference between the two exams is the level of difficulty. Security+ 601 is considered to be more challenging than Security+ 501, as it requires a deeper understanding of the concepts and practical skills. Furthermore, Security+ 601 has a greater focus on risk management and mitigation strategies, which are critical for cybersecurity professionals. This includes topics such as threat intelligence, vulnerability assessment, and incident response planning. Which Certification is More Suitable for Beginners? Both exams are suitable for beginners who are looking to start their career in IT security. However, Security+ 601 is more practical and scenario-based, which could be more comfortable for beginners to relate to real-world situations. Security+ 501, on the other hand, has a more theoretical focus, which could be beneficial for candidates looking for a deeper understanding of the concepts. It is important to note that both certifications cover similar topics, such as network security, cryptography, and risk management. However, Security+ 601 also includes new topics such as cloud security and Internet of Things (IoT) security, which are becoming increasingly important in the industry. Therefore, candidates who are interested in these emerging technologies may find Security+ 601 more relevant to their career goals. Which Certification is More Suitable for Experienced Professionals? Security+ 601 is more practical and emphasizes hands-on skills, which could be more suitable for experienced professionals who are looking to validate their skills. In contrast, Security+ 501 is more theoretical, which could be beneficial for experienced professionals who are looking for a deeper understanding of security concepts. However, it is important to note that both certifications are recognized by employers and can lead to career advancement opportunities. Experienced professionals should consider their career goals and the specific skills they want to develop before choosing which certification to pursue. Additionally, Security+ 601 covers more advanced topics such as cloud security and virtualization, which are becoming increasingly important in the industry. This makes it a good choice for experienced professionals who want to stay up-to-date with the latest trends and technologies in the field of cybersecurity. Which Certification is More Popular? Since Security+ 601 is the most recent version of the exam, it has gained more popularity among candidates. However, both exams are widely recognized and highly respected in the IT security industry. It is important to note that the Security+ 501 exam is still valid and available for candidates to take until July 31, 2021. This means that some candidates may still choose to take the 501 exam, especially if they have already been preparing for it or if they prefer the exam format. See also Can I skip Network+ and get security+?Additionally, the popularity of each exam may vary depending on the specific job market and employer preferences. Some employers may prefer candidates with the Security+ 501 certification, while others may prioritize candidates with the Security+ 601 certification. It is important for candidates to research the job market and employer preferences in their specific field before deciding which exam to take. Which Certification is More Difficult? Both exams have the same passing score, time limit, and number of questions. However, Security+ 601 is more scenario-based and practical, which could be more challenging for candidates who don’t have hands-on experience in security. In contrast, Security+ 501 is more theoretical, which could be more challenging for candidates who prefer hands-on and practical experience. Another factor that could make Security+ 601 more difficult is the inclusion of performance-based questions. These questions require candidates to perform specific tasks related to security, such as configuring a firewall or identifying vulnerabilities in a network. This type of question format can be challenging for candidates who are not familiar with the tools and technologies used in security. On the other hand, Security+ 501 may be more difficult for candidates who struggle with memorization and recall. This exam covers a wide range of theoretical concepts, such as cryptography, network architecture, and risk management. Candidates who prefer hands-on experience may find it challenging to remember all the details and concepts required for this exam. Exam Format and Structure for Security+ 501 and 601 Both exams are multiple-choice and performance-based and have the same number of questions, time limit, and passing score. The performance-based questions test your practical skills, while the multiple-choice questions test your theoretical knowledge in IT security. It is important to note that the Security+ 601 exam covers more advanced topics than the Security+ 501 exam. The 601 exam includes additional content on cloud security, IoT security, and other emerging technologies. Therefore, if you are looking to demonstrate a higher level of expertise in IT security, taking the Security+ 601 exam may be the better option. Additionally, both exams require a thorough understanding of the Common Vulnerability Scoring System (CVSS), which is used to assess the severity of security vulnerabilities. It is recommended that you familiarize yourself with the CVSS and its scoring system before taking either exam. Preparing for Security+ 501 and 601 Exams: Tips and Tricks Preparing for either exam requires a combination of theoretical knowledge and practical experience. Some tips and tricks to help you prepare include: Read the official CompTIA study guide for Security+ 501 or 601 to gain a basic understanding of concepts and topics. Practice on real-world scenarios and hands-on labs to gain practical experience. Join an online community or discussion group to share your knowledge and learn from others. Use practice tests and quizzes to test your understanding and identify areas of weakness. Attend training sessions or workshops provided by CompTIA or third-party providers to gain expert insights and tips. See also What is the next certification after SEC+?Another important tip is to stay up-to-date with the latest security trends and technologies. This can be done by reading industry publications, attending conferences, and following thought leaders on social media. It’s also important to develop good study habits and create a study schedule that works for you. This can help you stay on track and avoid cramming at the last minute. Additionally, make sure to take breaks and give yourself time to rest and recharge. Study Materials for Security+ 501 and 601 Exams CompTIA offers several study materials for both exams, including: Official CompTIA study guide Online training courses Practice tests and quizzes CertMaster training tool Additionally, CompTIA offers a variety of resources to help candidates prepare for the exams, such as: Webinars and virtual events Study groups and forums Exam objectives and sample questions Access to certified trainers and mentors These resources can provide valuable insights and support to help candidates succeed in their certification journey. Cost Comparison of Security+ 501 and 601 Exams The cost for either exam is $349 per attempt. However, CompTIA offers bundle packages that include vouchers for both exams at a discounted price. It is important to note that the Security+ 501 exam will retire on July 31, 2021, and will be replaced by the Security+ 601 exam. This means that if you are planning to take the Security+ certification exam, you should consider taking the Security+ 601 exam instead of the Security+ 501 exam. Another factor to consider when comparing the cost of the Security+ 501 and 601 exams is the exam format. The Security+ 501 exam is a traditional multiple-choice exam, while the Security+ 601 exam includes performance-based questions and simulations. This means that the Security+ 601 exam may require more preparation and practice, which could impact the overall cost of taking the exam. Career Opportunities with Security+ Certification Securing a Security+ certification could boost your career prospects in several ways, including: Opening up new job opportunities in IT security field Validating your knowledge and skills in network security Increasing your earning potential Enhancing your credibility and trustworthiness in the field Salary Comparison of Certified Professionals with Security+ 501 and 601 Certifications According to PayScale, a certified IT security specialist with Security+ certification can expect to earn an average annual salary of $74,000. However, the salary varies based on experience, skillset, and location. Conclusion: Which Certification Should You Choose? Choosing between Security+ 501 and 601 depends on your background, interests, and goals. If you’re a beginner looking for a more practical and scenario-based exam, Security+ 601 may be the right choice. If you want a deeper theoretical understanding of security concepts, Security+ 501 may be more suitable. Regardless of which exam you choose, the certification will help validate your knowledge and skills in IT security and open up new career opportunities in the field. As technologies evolve and work environments undergo the next steps in the digital transformation process, information and network security management procedures are more critical today than ever before. This is not limited to large organisations but also affects small businesses. Cybersecurity infrastructure is a leading and growing challenge among several corporate organisations. With the evolution of technology, cyber-attacks are not only increasing but also getting more advanced. By 2020, the average damage per cyberattack was estimated at $150 million. To fight off cybercriminals, discover vulnerabilities in existing security infrastructure and prevent cyberattacks, organisations are increasingly hiring in-house experts with advanced skills in network security. These experts are equipped with the knowledge and credentials needed to protect organisations against malicious third-party hackers. Among the different credentials that network security experts can attain, CompTIA Security+ is one of the highest. It is a vendor-neutral certification program that is often one of the first network security certifications that IT professionals go for. It is also a highly recommended credential among organisations, higher than all other fundamental cybersecurity skill certifications. CompTIA Security+ is a certification program that trains you to locate threats, future threats and vulnerabilities and perform penetration testing. It also teaches you the basic concepts of scanning vulnerabilities and preventing attacks, along with installing, configuring identities, accessing services, managing controls, deploying components, and assessing and troubleshooting problems to improve security measures. You get the skills needed to implement and summarise best practices of risk management, implementation of secure architecture concepts in networks and designing systems. You also attain the knowledge necessary to install, configure security settings and implement the critical infrastructure. Several job roles within an organisation can benefit from a Security+ certification. This includes: Security Administrator Junior IT Auditor Security Engineer Security Consultant Security Specialist Network Administrator Before 2020, professionals only had to pass the Security+ SY0-501 exam. That changed in November 2020, which was when CompTIA introduced the Security+ SY0-601 exam. CompTIA is ready to retire the 501 exams by July 2021, but you can choose which of these exams you wish to take to attain the CompTIA Security+ credential until then. There are several similarities and differences between these organisations. Which one should you choose when you apply for your credential? But first, let's take a quick look at a comprehensive list of all CompTIA certifications. In 1993, CompTIA received the A+ credential. It has issued certifications to more than two million individuals since then. CompTIA has a vendor-neutral certification program recognised as one of the premier ones in the global IT industry. CompTIA launched its 'Infrastructure Career Pathway' in 2018. This comprises various certifications you might or might not have heard of or read about that together form the base of all CompTIA certifications. The new solution track was meant to ensure that the certifications one chooses will align better to real-world situations and role-based skills that professionals might face whenever they work to support or manage an organisation's IT infrastructure. All the CompTIA certifications can be divided into four groups, based on the skill it tests. Every certification is a part of one of these groups. These certifications are aligned to help professionals develop their IT domain's fundamental skills. In this category, CompTIA offers four certifications to choose from. IT Fundamentals+ CompTIA Network+ CompTIA A+ CompTIA Security+ The second category has been created to align with Network+, a networking credential. This group has three certifications. CompTIA Cloud+ CompTIA Server+ CompTIA Linux+ Within this category of certifications, you can choose from three globally renowned credentials designed for cybersecurity aspirants and individuals in the network and information security domain. CompTIA CySA+ CASP+ CompTIA PenTest+ Within this category of certifications, several credentials are not explicitly part of any predefined career path. They include: CompTIA CTT+ CompTIA Cloud Essentials CompTIA Project+ You May Also Like: CompTIA Certification Guide: Overview and Career Paths About the Exam The CompTIA Security+ SY0-501 exam was announced in 2017 and will retire, according to CompTIA, in July 2021. The CompTIA Security+ SY0-601 exam was announced in November 2020 and will be the only exam you will need to pass after July 2021 to earn the Security+ credential. You will get 90 minutes to write the exam, which comprises 90 performance-based and multiple-choice questions. To pass the exam, you need to score 750 marks. There is an exam fee of $349 to be paid. You can give the Security+ exam in Chinese, Japanese, Portuguese and English. As a prerequisite to this exam, you must have a CompTIA Network+ certification, along with work experience in IT administration for at least two years, with security as your focus. Number of Objectives: The SY0-601 has 35 objectives, which is less than the 37 that the SY0-501 has. Examples Given: The SY0-601 has about 25% more examples than the SY0-501 did. Level of Understanding: By having more examples, the SY0-601 becomes much easier to understand than its predecessor, making it easier for you to learn. Number of Domains: The Security+ SY0-501 covered six domains, while the SY0-601 has just five. Different Priorities: The SY0-601 exam has newer priorities when it comes to domains. The 'Attacks, Threats and Vulnerabilities' domain holds 24% weightage, compared to 21% in the SY0-501. Also, the 'Architecture and Design' domain in the SY0-601 carries a 21% weightage, compared to 15% in the SY0-501. New Skills in Focus: The CompTIA Security+ SY0-601 pays more attention to current skills essential to assess the cybersecurity position of a company's infrastructure, recommend and implement corrective measures, monitor and secure hybrid environments and operate while abiding by laws and policies that are in effect. It also places more importance on the identification, analysis and response to cybersecurity situations. Also Read: Spice Up Your Career with CompTIA Project+ Certifications A cyberattack at some point has targeted almost every organisation, but only 38% of organisations are equipped to handle it. According to reports, 85% of professionals with a Security+ credential are more confident in their abilities and have 58% more knowledge than their uncertified peers. Give your career a boost and start training today. Aarav Goel has top education industry knowledge with 4 years of experience. Being a passionate blogger also does blogging on the technology niche. Last Updated on January 30, 2025 NOTE: As of November 2023, the current Security+ exam is 701. This article refers to retired exams 501 and 601. Follow this link for detailed info on the 701 exam. CompTIA Security Plus certification is a widely recognized measure of a person’s competency in network security, compliance, and operational security. The Security+ certification has two exams—the Security+ 501 and the Security+ 601. In this article, we will compare the two exams to help you determine which one is right for you. The Security+ 501 exam covers the fundamentals of security and is intended for those just starting out in the field, while the Security+ 601 exam covers more advanced topics and is intended for those with more experience. 501 Exam The 501 exam covers security fundamentals including cryptography, network security, identity, and access management. It is intended for individuals with at least two years of experience in IT administration with a focus on security. The 501 exam is multiple-choice and performance-based and covers six key domains of knowledge. These include: Threats, attacks, and vulnerabilities (21%) Technologies and tools (22%) Architecture and design (15%) Identity and access management (16%) Risk management (14%) Cryptography and PKI (12%) It is considered more basic than the 601 exam. 601 Exam The CompTIA Security+ 601 exam is the current CompTIA Security+ exam. It’s an updated version of the Security+ 501 exam, and it covers five key domains of knowledge. These are: Attacks, threats, and vulnerabilities (24%) Architecture and design (21%) Implementation (25%) Operations and incident response (16%) Governance, risk, and compliance (14%) The 601 is considered more challenging and in-depth than the 501 exams and places a greater emphasis on hands-on experience and the ability to apply security principles in real-world situations. Eventually, the 601 will be updated as well, so it can be helpful to know when the Security+ exam changes. 501 vs 601 One key change in the 601 exams is the increased emphasis on hands-on experience and the ability to apply security principles in real-world situations. This means that the 601 exam focuses more on practical skills and knowledge than just theoretical concepts. 601 exams also have increased focus on advanced topics, such as cryptography, penetration testing, and incident response. However, they both have much in common. They each: Have ninety questions Has a time limit of ninety minutes Cost $370 Have a passing score of 750 on a scale of 100 to 900 Who Should Take the Security+ 601 Exam? If You’re Already 501 Certified If you are already Security+ certified, you do not need to take the Security+ 601 exam. The Security+ certification is valid for three years, after which you will need to renew your certification by passing the SY0-501 exam or the newer SY0-601 exam. If you are approaching the end of your certification period, you may consider taking the SY0-601 exam to renew your certification. If You’re Prepared for the 501 Exam The Security+ 501 exam covers the same content as the Security+ 601 exam, but the 501 exam has been retired and is no longer available. If you’re preparing for the Security+ 501 exam, it’s recommended that you take the Security+ 601 exam instead. In Summary The 501 and 601 exams are similar, but the Security+ 601 exam requires a combination of hands-on experience and structured learning, meaning passing test-takers will be more prepared for future work in the field. CompTIA Security+ ranks among the top 10 cybersecurity certifications in 2023. See how CompTIA Security+ (SY0-701) compares to SY0-601. IT certifications show employers that candidates have the knowledge and skills they need to do the job, and they help IT pros advance in their careers. As cybersecurity has become a critical function, cybersecurity certifications are among the most popular IT certifications globally.More than 700,000 IT pros have earned CompTIA Security+, and the Skillsoft IT Skills and Salary Report puts CompTIA at #3 of the most widely held security, governance, compliance and/or privacy-related certifications. Plus, CompTIA Security+ is chosen by more employers than any other IT certification to prove hands-on core cybersecurity skills and fulfills U.S. Department of Defense (DoD) 8570 compliance.CompTIA Security+ has recently been updated to reflect skills relevant to job roles tasked with baseline security readiness and response to address today’s threats, and to prepare candidates to be more proactive in preventing the next attack.As the need to secure more systems, software and hardware grows, more IT job roles are now turning to CompTIA Security+ to supplement cybersecurity skills. As cyberattacks continue to grow, more IT job roles are tasked with baseline security readiness and responding to address today’s cyber threats. Updates to CompTIA Security+ (SY0-701) reflect those skills and prepare you to be more proactive in preventing the next cyberattack.The primary CompTIA Security+ job roles include:Security specialistSecurity administrator Systems administratorBut the following IT job roles can also benefit from CompTIA Security+:Security analystSecurity engineerHelp desk analystLearn about the CompTIA Cybersecurity Career Pathway.CompTIA Security+ 601 vs. 701The new CompTIA Security+ (SY0-701) addresses the latest cybersecurity trends and techniques – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations and security controls, ensuring high performance on the job. These skills include:Assessing the security posture of an enterprise environment and recommend and implement 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.And 20% of exam objectives were updated to include:Current trends: The latest trends in threats, attacks, vulnerabilities, automation, zero trust, risk, IoT, OT and cloud environments are emphasized, as well as communication, reporting and teamwork.Hybrid environments: The latest techniques for cybersecurity professionals working in hybrid environments that are located in the cloud and on premises; cybersecurity professionals should be familiar with both worlds.Let’s take a look at the differences between the 601 and 701 exam domains: CompTIA Security+ (SY0-601) Exam Domains CompTIA Security+ (SY0-701) Exam Domains Attacks, Threats and Vulnerabilities (24%)Architecture and Design (21%)Implementation (25%)Operations and Incident Response (16%)Governance, Risk and Compliance (14%) General Security Concepts (12%)Threats, Vulnerabilities and Mitigations (22%)Security Architecture (18%)Security Operations (28%)Security Program Management and Oversight (20%) SY0-701 has the same number of exam domains as SY0-601 but fewer objectives (28 vs. 35) due to a more focused job role in a maturing industry. Several of the exam domains and exam objectives were re-ordered and re-named to address instructional design improvements. Plus, CompTIA is constantly reviewing exam content and updating questions to ensure relevance and exam integrity.How CompTIA Security+ Evolves With the IndustryIn a field like cybersecurity, where the job is continually evolving, CompTIA exam domains need to reflect what’s happening in the industry. The following table explains why we updated the CompTIA Security+ exam domains and how they relate to job requirements. Exam Domain Description How It Applies to IT Jobs General Security Concepts Includes various types of security controls, fundamental security concepts, the importance of change management processes and using cryptographic solutions. Understanding cybersecurity terminology and core concepts are essential to cybersecurity work and provides a common language of communication for cybersecurity industry workers. Threats, Vulnerabilities and Mitigations Includes threat actors and motivations, threat vectors and attack surfaces, types of vulnerabilities, mitigation techniques and indicators of malicious activity. Cybersecurity professionals must be aware of the threats, attacks and vulnerabilities that may impact their networks in order to mitigate them (i.e., reduce the risk, lessen the harm). To prevent data breaches, malicious activity must be identified and analyzed, and mitigation techniques implemented to secure the enterprise. Security Architecture Includes security implications of different architecture models, concepts and strategies to protect data, security principles to secure enterprise infrastructure and the importance of resilience and recovery in security architecture. Cybersecurity professionals must be familiar with different types of security architectures because different techniques are needed to secure them, including on-premises, the cloud and hybrid (on-premises and cloud) networks. Security Operations Includes security techniques, security alerting and monitoring concepts and tools, vulnerability management activities, security implications of proper hardware, software and data asset management, identity and access management, as well as the importance of automation and orchestration and incident response activities.Security operations includes the important day-to-day work that cybersecurity professionals do, such as monitoring systems, finding vulnerabilities, hardening systems and incident response. Incident response is a key function of cybersecurity professionals; skilled employees are needed to implement an effective incident response plan. Security Program Management and OversightIncludes elements of effective security governance, the risk management process (including third-party risk assessment and management), types and purposes of audits and assessments, security awareness practices and elements of effective security compliance. Cybersecurity professionals are responsible for reporting and communicating their activities, such as security incident information, the types of threats, attacks and vulnerabilities found, trends they have encountered, etc.Cybersecurity professionals must learn the latest trends of effective security governance, including third-party risk management concepts, to help with security compliance for an organization. How To Train for CompTIA Security+It may seem like CompTIA Security+ covers a lot of ground, but don’t worry, we’ve got you! CompTIA offers training solutions, including study guides, online self-study tools and instructor-led courses that are designed to cover what you need to know for your CompTIA exam. No other content library covers all exam objectives for all certifications.CompTIA training solutions help you prepare for your CompTIA certification exam with confidence. Whether you are just starting to prepare and need comprehensive training with CompTIA CertMaster Learn, want to apply your knowledge hands-on with CompTIA Labs, need a final review with CompTIA CertMaster Practice or need to renew your certification with CompTIA CertMaster CE, CompTIA's online training tools have you covered.Ready to start studying? Writing out your plan will set you up for success. Download our free training plan worksheet to help get organized and make your dream a reality.Looking for more about CompTIA Security+? Check out these articles: We've said it before: "Cybersecurity is one of the most sought-after competencies for enterprises of all sizes." Employers use security certifications as one way to evaluate the expertise of current and prospective security staff. Faced with the pervasive threat of "bad actors" breaking in, disrupting operations, and stealing valuable information, they need staff at many levels with security expertise.Organizations need expert architects, engineers, and analysts, as well as qualified administrators to handle the day-to-day security activities to protect enterprise

foundational infosec certification, and the new SY0-601 certification exam will further strengthen its perceived value. Earning the certification will help develop the baseline skills needed for a successful career in cybersecurity. Start learning today with CBT Nuggets!