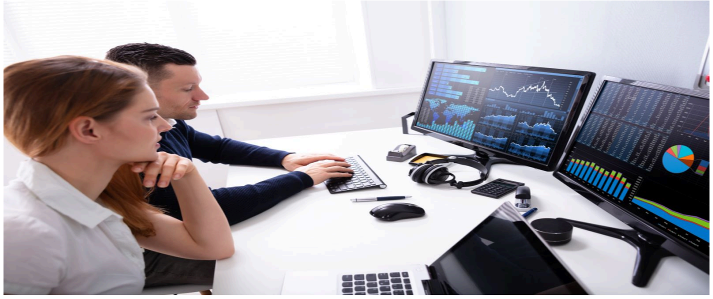
CIT, INFORMATION TECHNOLOGY CYBERSECURITY SPECIALTY, ASSOCIATE OF APPLIED SCIENCE



oVERVIEW

The Cybersecurity Associate of Applied Science (AAS) program is designed to provide students with a comprehensive foundation in the critical field of cybersecurity and network security. As the demand for skilled professionals in cybersecurity continues to grow, this program offers an excellent entry point for those eager to pursue a rewarding career in safeguarding digital infrastructure. The curriculum integrates both theoretical knowledge and practical experience, ensuring that students are well-equipped to defend against the ever-evolving threats in the digital landscape. Students will learn how to identify vulnerabilities, mitigate security risks, and implement security protocols to protect computer systems, networks, and data from various forms of cyberattacks, including hacking, malware, viruses, and other forms of cybercrime. In addition to technical expertise, the program emphasizes the development of problem-solving skills and critical thinking, which are essential for navigating the complex and constantly changing nature of cybersecurity challenges. Through hands-on learning experiences, including labs, simulations, and real-world case studies, students will gain the ability to apply their knowledge in practical settings and prepare for industry certifications that are valued by employers.

Upon completion of the AAS program, graduates will be prepared for various entry-level roles in cybersecurity and network administration, such as security analyst, network security administrator, or IT security specialist. The program also offers the unique advantage of seamless transfer into the Bachelor of Applied Technology (BAT) in Cybersecurity. This pathway allows students to continue their education and further develop their expertise in the field, opening the door to higher-level roles in cybersecurity management, consulting, and advanced technical positions.

Whether students are looking to launch their career in cybersecurity or continue their education toward a Bachelor's degree, the AAS in Cybersecurity provides a strong, supportive foundation for future success in the rapidly expanding cybersecurity sector.

iNDUSTRY cERTIFICATIONS

Students in the Cybersecurity AAS program are equipped with the knowledge and skills to pursue a variety of industry-recognized certifications, which can significantly enhance their qualifications and increase their employability in the cybersecurity field. These certifications serve as a validation of the expertise gained throughout the program, making graduates more competitive in the job market. Certifications may include:

- **CompTIA A+**: A certification focused on IT fundamentals and technical support, including hardware, software, and troubleshooting. While it is often considered an entry-level certification, it provides a critical understanding of IT systems, which is useful for cybersecurity professionals.
- **CompTIA Network+**: A certification that provides a strong foundation in networking, covering topics such as network protocols, infrastructure, security, and troubleshooting. It is essential for those seeking a career in network administration or cybersecurity.
- **CompTIA Security+**: A foundational certification that covers essential cybersecurity concepts such as network security, threats and vulnerabilities, cryptography, and identity management. This is a widely recognized credential for cybersecurity professionals.
- **CompTIA Cloud+**: Focuses on the skills needed to manage and secure cloud-based environments. This certification covers cloud computing principles, implementation, and management, which are crucial as more organizations move to cloud infrastructure.
- **EC-Council Certified Network Defender (CND)**: This certification is designed to train network administrators in advanced network defense concepts, including firewalls, intrusion detection systems, and risk management. It equips professionals to defend against cyber threats and attacks.
- **EC-Council Certified Incident Handler (ECIH)**: Focuses on incident response and handling security incidents efficiently. This certification helps professionals understand how to manage and mitigate damage caused by cybersecurity breaches and how to implement recovery procedures.

These certifications are highly regarded in the cybersecurity industry and are frequently requested by employers looking for qualified professionals to secure their networks, systems, and data. By earning these credentials, graduates not only increase their marketability but also demonstrate a high level of technical proficiency and expertise, ensuring they are well-prepared to meet the demands of the cybersecurity workforce.

Career Opportunities

Graduates of the Cybersecurity AAS program can pursue a wide range of exciting and rewarding careers in cybersecurity, with roles that vary in responsibility, focus, and specialization. Below are some of the most common career paths available to those with a strong foundation in network security and cybersecurity operations:

Security Operations Analyst
This role is focused on maintaining and securing IT networks and ensuring their optimal performance. Security Operations Analysts monitor network traffic, troubleshoot issues, and ensure that systems are running smoothly and securely. They are responsible for configuring and managing network devices, such as routers and firewalls, and implementing security measures to safeguard against unauthorized access and cyber threats. Strong problem-solving skills and in-depth knowledge of network protocols and security best practices are essential for success in this role.

Cybersecurity Analyst

Cybersecurity Analysts play a key role in identifying, analyzing, and responding to cybersecurity incidents. They gather and examine digital evidence, assess the impact of security events, and work with internal IT teams and law enforcement to mitigate the risks associated with breaches or attacks. In this role, professionals must be adept at analyzing data, recognizing security threats, and developing strategies to prevent future incidents. A deep understanding of security tools, incident management, and vulnerability analysis is crucial for those pursuing this career path.

Cybersecurity Consultant
Cybersecurity Consultants evaluate an organization's IT controls and security measures to ensure they are effective and compliant with industry regulations and standards. This role involves conducting audits to assess the security posture of an organization's systems, identifying weaknesses or vulnerabilities, and recommending improvements to mitigate risks. Cybersecurity Consultants need strong analytical skills, a thorough understanding of security frameworks (such as ISO 27001 and NIST), and the ability to communicate findings clearly to management and stakeholders.

As the demand for cybersecurity professionals continues to grow, these roles offer significant opportunities for career advancement, leadership positions, and the ability to contribute to safeguarding organizations against increasingly sophisticated cyber threats. Each position requires a unique set of skills, but all rely on a strong foundation in cybersecurity principles, technical expertise, and problem-solving abilities.

Earning Potential

The field of cybersecurity offers competitive salaries and a wide range of career opportunities. Below are some key positions and their median annual salaries in the Greater Houston Metropolitan Area as of 2025:

Security Operations Analyst: $93,000[1] per year

Cybersecurity Analyst: $96,000[1] per year

Cybersecurity Consultant: $137,000[1] per year

[1] Source: salary.com (http://salary.com/), median salary Greater Houston Metropolitan Area, 2025

For more information about pursuing a career in cybersecurity or the programs at San Jacinto College, students may contact the Senior Director for Cybersecurity Programs, Rizwan Virani. He can be reached by phone at 281-922-3424 or by email at rizwan.virani@sjcd.edu.

Campuses

Central Campus

North Campus

South Campus

San Jac Online

Information

The Cybersecurity Associate of Applied Science (AAS) program is designed for students seeking to develop the critical skills needed to protect and secure digital infrastructures in today's technology-driven world. This degree program can typically be completed in four semesters. For students who already hold relevant industry certifications such as CompTIA Security+, Network+, or other cybersecurity credentials, it may be possible to complete the program in less time. The Cybersecurity AAS program equips students with the technical expertise and hands-on experience needed to protect computer systems, networks, and data from cyber threats. The curriculum is designed to provide both theoretical knowledge and practical skills, enabling students to respond to the growing demand for cybersecurity professionals. This program is perfect for individuals aiming to launch or advance their careers in the cybersecurity field.

After completing foundational courses, students can choose one of three specialized areas to focus their education on and align with their career goals:

- **Security Operations**: Focused on maintaining and securing IT networks by monitoring traffic, troubleshooting issues, and implementing security measures to prevent unauthorized access and cyberattacks.
- **Cybersecurity Analysis**: Emphasizing the identification, analysis, and response to cybersecurity incidents, including gathering evidence, assessing breach impacts, and collaborating with law enforcement and IT teams to mitigate risks.
- **Cybersecurity Consulting**: Specializing in evaluating and improving an organization's security posture, conducting audits, identifying vulnerabilities, and recommending strategies to enhance security and ensure compliance with regulations.

This program places special emphasis on:

- Securing and defending IT systems, networks, and data against a variety of cyber threats such as malware, ransomware, and hackers.
- Developing hands-on experience with monitoring and responding to security incidents in real-time.
- Gaining expertise in risk management, incident response, and vulnerability analysis to protect sensitive information.
- Preparing for industry-recognized certifications, including CompTIA Security+, CompTIA Network+, and Certified Network Defender (CND).

The Cybersecurity AAS degree provides a direct pathway to a variety of cybersecurity careers. Upon completion, students may qualify for positions such as:

- Security Operations Analyst
- Cybersecurity Analyst
- Cybersecurity Consultant

Graduates will find opportunities in industries such as healthcare, finance, government, education, and technology, where the need for cybersecurity professionals continues to grow.

If your selected courses or program of study include clinical, practicum, externship, or cooperative learning components at external sites, you must meet all immunization or policy requirements outlined by the host facility. These requirements are determined by the external site's independent authority rather than by San Jacinto College. Failure to comply with these requirements can prevent you from completing your required external learning experiences and may delay graduation. Students seeking exemptions must address these directly with the external facility, as San Jacinto College does not process immunization exemptions.

By choosing the Cybersecurity Associate of Applied Science program, you are positioning yourself to be part of a fast-growing field that plays a crucial role in protecting sensitive data and securing digital infrastructures. Whether you are starting a new career or building on existing skills, this program provides the foundational knowledge and technical expertise to succeed in the ever-evolving world of cybersecurity.

Program Learning Outcomes

Upon successful completion of this program, graduates will be able to:

1. Utilize network transmission media across various network topologies using a variety of operating systems.
2. Develop a security plan implementing asset risk management.
3. Develop viable solutions to mitigate network security risks to protect assets.
4. Utilize appropriate tools to prevent security threats.
5. Implement and test firewall security system.
6. Deploy countermeasures to minimize the impact of a breach in network security.

Additional Information

For more information about pursuing a career in cybersecurity or the programs at San Jacinto College, students may contact the Senior Director for Cybersecurity Programs, Rizwan Virani. He can be reached by phone at 281-922-3424 or by email at rizwan.virani@sjcd.edu.

Plan of Study

3IT-ITS

First Term		Credits
ITSC 1305	Introduction to PC Operating Systems	3
ITSE 1329	Programming Logic and Design	3
ITNW 1325 or ITCC 1314	Fundamentals of Networking Technologies or CCNA 1: Introduction to Networks	3
ITSY 1342	Information Technology Security	3
ENGL 1301	Composition I	3
	Credits	**15**
Second Term		
ITSC 1316 or ITSC 1307	Linux Installation and Configuration or UNIX Operating System I	3
ITSE 1302	Computer Programming	3
ITSY 2300	Operating System Security	3
ITNW 2353 or ITCC 1444	Advanced Routing and Switching or CCNA 2: Switching, Routing and Wireless Essentials	3
Select one of the following:		3
MATH 1332	Contemporary Mathematics (Quantitative Reasoning)	
MATH 1314	College Algebra	
Life and Physical Science (Natural Science)		
	Credits	**15**
Third Term		
ITNW 1354 or ITNW 1309	Implementing and Supporting Servers or Fundamentals of Cloud Computing	3
ITSY 2301	Firewalls and Network Security	3
ITSY 2341	Security Management Practices	3
Language, Philosophy and Culture (Humanities) or Creative Arts (Fine Arts)		3
Select one of the following:		3
SPCH 1311	Introduction to Speech Communication	
SPCH 1315	Public Speaking	
SPCH 1318	Interpersonal Communication	
SPCH 1321	Business and Professional Speech	
	Credits	**15**
Fourth Term		
ITSY 2342	Incident Response and Handling	3
ITSY 2343	Computer System Forensics	3
ITSY 2345	Network Defense and Countermeasures	3
ENGL 2311 or ENGL 1302	Technical and Business Writing or Composition II	3
Social and Behavioral Sciences or Government/Political Science or American History		3
	Credits	**15**
	Total Credits	**60**

Capstone Experience: ITSY 2345 Network Defense and Countermeasures