CIT, INFORMATION TECHNOLOGY CYBERSECURITY, BACHELOR OF APPLIED TECHNOLOGY

Overview

The cybersecurity program is designed to equip students with essential hand-on technical skills, focusing on critical areas such as network security, security operations, penetration testing, and incident response. A distinctive feature of the program is the opportunity for students to gain real-world experience by working in a student-embedded Security Operations Center (SOC). This hands-on experience allows students to apply their knowledge in a practical setting, dealing with actual cybersecurity challenges.

- **Skill Development:** Emphasis is placed on mastering network security, security operations, penetration testing, and incident response.
- **Practical Training:** Students gain real-world experience working in the student-embedded SOC, using state-of-the-art security tools and technologies.
- **Certification Preparation:** The program guides students towards obtaining industry-recognized certifications such as CompTIA's Security+ and PenTest+, EC Council's CEH and CPENT, and prepares them for higher level certifications such as the ISACA CISA and ISC2 CISSP. These certifications are crucial for validating skills and enhancing job prospects in the competitive cybersecurity landscape.

By combining rigorous coursework with practical experience in the SOC and certification preparation, the program ensures that graduates are fully equipped to enter the cybersecurity workforce and excel in their careers.

Career Opportunities

Graduates of the BAT in Cybersecurity are well-prepared for various high-demand roles across multiple sectors due to the universal need for data protection and threat mitigation. Potential career paths include:

- **Security Operations Center (SOC) Analysts**: Protect organizational information systems from cyber threats.
- **Network Security Engineers**: Design and secure network infrastructures.
- **Information Security Managers**: Oversee and implement organizational security strategies.
- **Penetration Testers**: Identify vulnerabilities before they can be exploited maliciously.

The program's comprehensive approach ensures that graduates can adapt to diverse roles, contributing significantly to safeguarding digital assets in industries such as finance, healthcare, and government.

Emerging Trends in Cybersecurity

The cybersecurity field is rapidly evolving with trends such as the integration of artificial intelligence (AI) and machine learning (ML) into everyday business operations and security practices. These technologies enhance threat detection and response capabilities. Additionally, the rise of ransomware attacks and the proliferation of Internet of Things (IoT) devices present new challenges that cybersecurity professionals must address.

Earning Potential

The cybersecurity field not only offers a wide range of career opportunities but also promises substantial earning potential, reflective of the critical nature of the work and the skills required to perform it. As the volume and sophistication of cyber threats continue to grow, so does the demand for skilled professionals capable of countering these threats. This heightened demand directly translates to competitive compensation packages for cybersecurity professionals. The program's emphasis on current technologies and practices, coupled with preparation for key industry certifications, positions graduates to command higher salaries. Earnings vary based on geographic location, experience, and the specific sector of employment, but the trajectory for career growth and salary advancement in cybersecurity is among the most favorable of all IT disciplines.

Campus

South Campus

Information

The cybersecurity program is structured to develop essential hard skills, emphasizing critical areas such as network security, penetration testing, and incident response. A distinctive feature of the program is the opportunity for students to gain real-world experience by working in a student-embedded Security Operations Center (SOC). This hands-on experience allows students to apply their knowledge in a practical setting, dealing with actual cybersecurity challenges.

Program Highlights

- **Skill Development**: Focus on mastering network security, security operations, penetration testing, and incident response.
- **Practical Training**: Students work in a student-embedded SOC, gaining invaluable real-world experience with state-of-the-art security tools and technologies.
- **Certification Preparation**: The program prepares students for industry-recognized certifications such as CompTIA's Security+ and PenTest+, EC Council's CEH and CPENT, and prepares them for higher level certifications such as the ISACA CISA and ISC2 CISSP.

These certifications are vital for validating skills and enhancing marketability in the competitive cybersecurity job market.

Through a combination of rigorous coursework, hands-on experience in the SOC, and certification preparation, the program ensures that graduates are thoroughly equipped to enter the cybersecurity workforce and excel in their careers.

Admissions Requirements

Prospective students should have:

- An associate degree completed or in the last semester of completion in Information Technology with an emphasis on Cybersecurity or a closely related field from an accredited institution.
- Completed specific cybersecurity coursework to ensure readiness for advanced topics.
- Fulfilled college admission requirements, including submitting official transcripts and attending mandatory orientations.

The program is structured to integrate 60 credit hours from an associate degree with 60 additional credit hours within the BAT curriculum, including 36 upper-level cybersecurity classes.

Application Process

Interested candidates must:

1. Submit official transcripts.
2. Complete college admission requirements.
3. Participate in an information session. Please contact Senior Director of Cybersecurity Programs, Rizwan Virani, at 281-922-3424 or by email at rizwan.virani@sjcd.edu.

ADMISSIONS

San Jacinto College invites applications for its Bachelor of Applied Technology in Cybersecurity (BAT-IT-CYB), designed for individuals aiming to advance their expertise in the dynamic field of cybersecurity. This comprehensive program is tailored for those with an associate degree in Information Technology with an emphasis in Cybersecurity or a closely related field from an accredited institution. Candidates must have completed specific cybersecurity coursework, ensuring readiness for the program's advanced topics.

The application process includes:

- Submitting official transcripts.
- Fulfilling college admission requirements.
- Attending a mandatory orientation.
- Participating in an information session.

Additionally, applicants must undergo a transfer credit evaluation to align previous academic achievements with the BAT-IT-CYB curriculum. The program, encompassing 120 credit hours, integrates 60 credit hours from the associate degree in cybersecurity or closely related information technology program with 60 further credit hours within the BAT program, including 36 upper-level cybersecurity classes.

Prospective students should note the importance of an Ethical Obligation form and the departmental review process, which assesses the applicability of prior coursework. With tuition rates equivalent to associate-level classes, excluding additional fees for materials and certifications, this program offers a valuable opportunity for those seeking to enhance their cybersecurity skills and career prospects. Applicants are encouraged to contact the admissions office directly, the Senior Director of Cybersecurity Programs, or the Dean of Business and Technology at the South campus for the most accurate and up-to-date information.

Plan of Study

BAT-IT-CYB

First Year		
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
MATH 1332 or MATH 1314	Contemporary Mathematics (Quantitative Reasoning) or College Algebra	3
	Credits	**15**
Second Year		
First 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)		3
Component Area Option		3
	Credits	**15**
Second 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		3
	Credits	**15**
Third Year		
First Term		
Life and Physical Science (Natural Science) with lab		4
CYBR 3320	Digital and Device Forensics	3
CSIS 3313	Information Security Standards, Risk Management, and Compliance	3
CSIS 3353	Cyber Law and the Legal System	3

EDUC 1100 or CYBR 3170	Learning Framework or Cybersecurity Pathways and Ethics	1
GOVT 2305	Federal Government (Federal Constitution and Topics)	3
	Credits	**17**
Second Term		
Creative Arts (Fine Arts)		3
CYBR 3340	Cyber Crime	3
ITCS 3350	Project Management for Cybersecurity	3
CYBR 3371	Industrial Control System Security	3
American History		3
	Credits	**15**
Fourth Year		
First Term		
American History		3
ITCS 4315	Cybersecurity Incident Response Team	3
CYBR 4310	Penetration Testing	3
CSIS 4323	IT Security Auditing	3
Life and Physical Science (Natural Science) with lab		4
	Credits	**16**
Second Term		
CYBR 4320	Cyber Defense Operations	3
CYBR 4350	Senior Project	3
CYBR 4330	Virtualization and Cloud Security	3
GOVT 2306	Texas Government (Texas Constitution and Topics)	3
	Credits	**12**
	Total Credits	**120**