CIT, INFORMATION TECHNOLOGY CYBERSECURITY, BACHELOR OF APPLIED TECHNOLOGY

Overview

The Bachelor of Applied Technology (BAT) in Information Technology with an emphasis on Cybersecurity is meticulously crafted to address the escalating complexity and volume of cyber threats in today's digital world. This program not only aims to furnish students with the theoretical underpinnings of cyber security principles but also ensures they acquire hands-on experience in cutting-edge practices and technologies. The curriculum spans from basic IT fundamentals to sophisticated cybersecurity strategies, including ethical hacking, digital forensics, and encryption technologies. Given the program's comprehensive nature, students are uniquely prepared to navigate and mitigate the risks associated with cyber threats, making them invaluable assets to any organization in the digital age. The College plans to begin the BAT in Information Technology with an emphasis on Cybersecurity in fall 2024 pending approval from the Texas Higher Education Coordinating Board (THECB) and the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC).

The cybersecurity domain offers a wide array of career paths due to the universal need for data protection and threat mitigation across various sectors. The program's graduates are primed for success in high-demand roles such as Security Operations Center (SOC) Analysts, who play a crucial role in protecting an organization's information systems and infrastructure from cyber threats; Network Security Engineers, who design secure network infrastructures; Information Security Managers, who oversee organizational security strategies; and Penetration Testers, who identify vulnerabilities before they can be exploited maliciously. The program's broad and in-depth coverage of cyber security concepts ensures that graduates can adapt to various roles, making significant contributions to protecting digital assets in industries ranging from finance and health care to government and beyond. The escalating number of cyber incidents underscores the critical need for skilled professionals, positioning graduates for rapid career advancement and leadership opportunities in cybersecurity.

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

In the cybersecurity field, hard skills are paramount, and the program places a strong emphasis on developing expertise in critical areas such as network security, penetration testing, and incident response. Students gain proficiency in using state-of-the-art security tools and technologies, preparing them for real-world cybersecurity challenges. The program also guides students towards obtaining industry-recognized certifications, including, but not limited to, CISSP, CEH, and CompTIA Security+, which are invaluable for career advancement. These certifications not only validate the skills and knowledge of the graduates but also enhance their marketability in a competitive job landscape. Through a combination of rigorous coursework, practical experience, and certification preparation, the program ensures that graduates are well-equipped to enter the cybersecurity workforce and excel.

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 PSYC 1100	Learning Framework or Learning Framework	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**