# Bachelor of Applied Science in Cyber Defense

**Program Description:**

A Bachelor of Applied Science in Cyber Defense prepares students with the skills to defeat real-world cyber threats and cyberattacks. The curriculum encompasses both defensive and offensive cybersecurity techniques and concepts. Students will develop the knowledge and skills to work in security operations roles.

The program is designed to utilize the foundations of the current A.A.S in Cybersecurity and Data Privacy offered at TMCC. The program ensures that students take the required courses in 8 semesters.

The program has foundations in programming, networking, and cyber security. TMCC's cyber lab will feature current equipment and software to perform ethical hacking and penetration exercises.

Concurrent with the program, students will have the opportunity to prepare for several industry certifications, such as the Palo Alto PCCET & PCNSA, CompTia CySA+ and ComTia Pentest+.

**CIP Code: 43.0401**

**Program Rationale:**

The Bachelor of Applied Science in Cyber Defense program is being developed in conjunction with TMCC's IMPACT: Indigenous Mutual Partnership to Advance Cybersecurity Technology initiative. Through that initiative, TMCC has secured funding and industry partnerships to further develop TMCC's cybersecurity education programs.

**Program Mission:**

The mission of the Bachelor of Applied Science in Cyber Defense degree is to prepare students with the skills and knowledge to become cybersecurity professionals with a curriculum that reflects the Seven Teachings of the Anishinaabe People.

**Program Model:**

The program model for the Cyber Defense degree is based upon the “IAC or CIA triad” and the National Institute of Standards and Technology (NIST) and The Workforce Framework for Cybersecurity known as the “NICE Framework”.   The Seven Teachings of the Anishinaabe People will be reflected in specific exercises included throughout the curriculum.

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

**image courtesy of www.energy.gov*

The three letters of the triad stand for Confidentiality, Integrity, and Availability.  This triad is the standard model that forms the basis for developing security systems and cybersecurity policy.

***Confidentiality***
NIST (National Institute of Standards and Technology) defines confidentiality as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.”

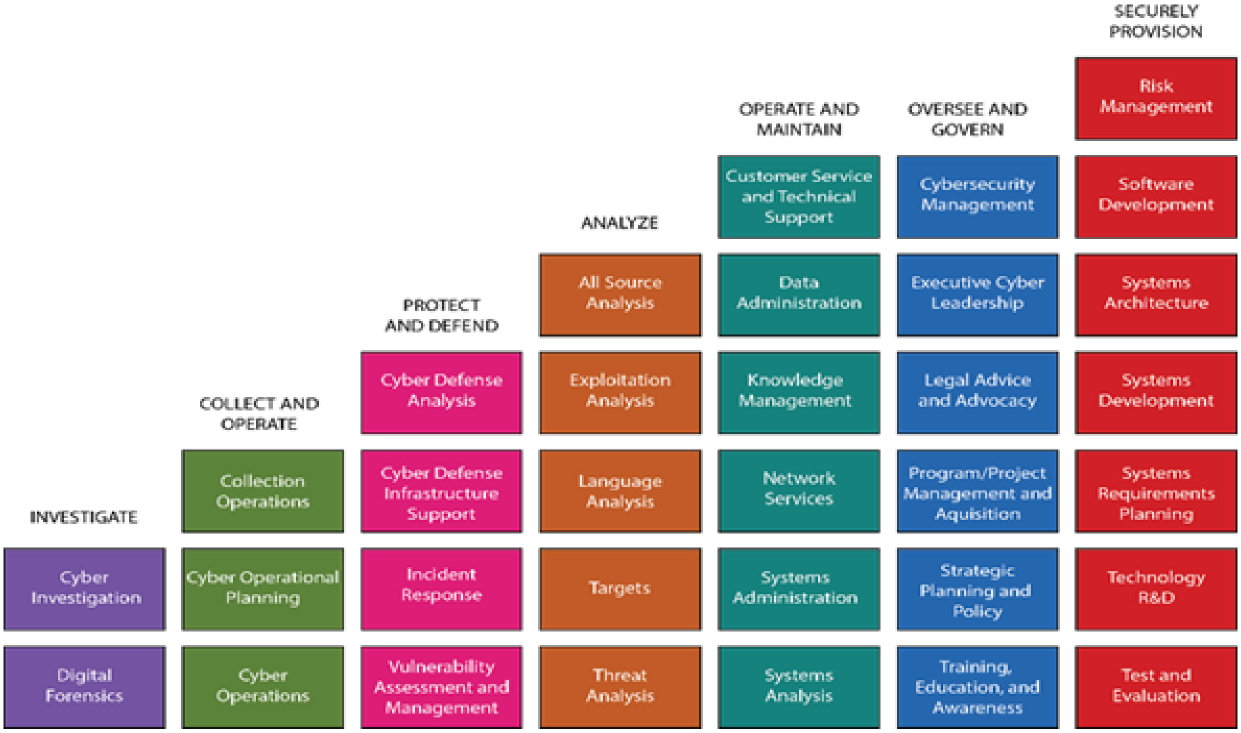
***Integrity***
NIST defines integrity as "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity."

***Availability***
NIST defines availability as "Ensuring timely and reliable access to and use of information.”

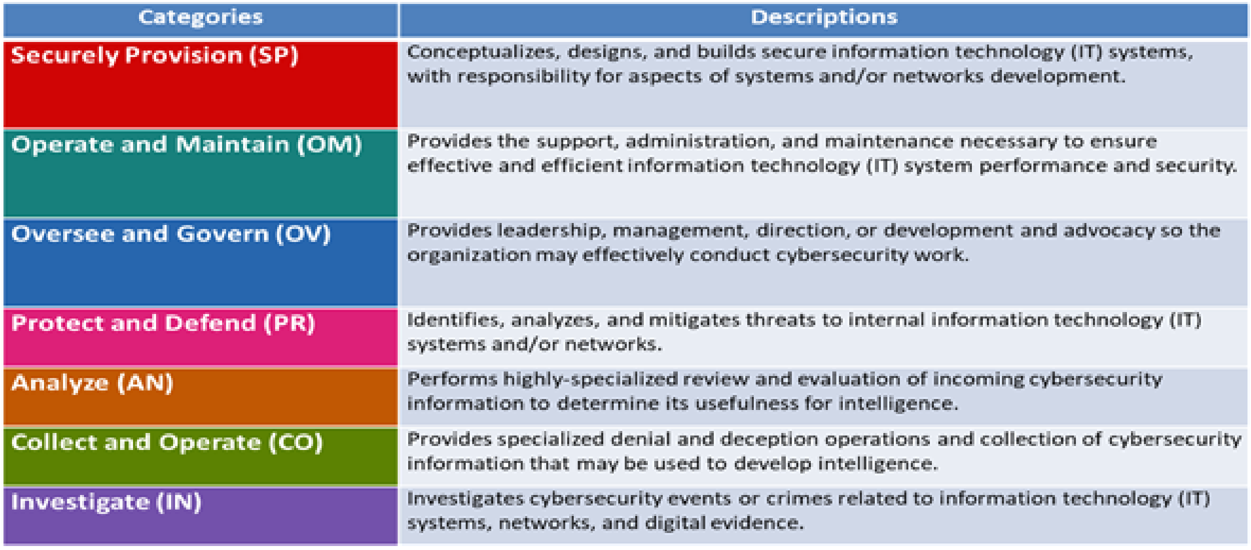
### *NICE Framework*

NIST defines the NICE Framework as “The NICE Framework provides organizations with a common, consistent lexicon that categorizes and describes the cybersecurity work.”  The framework further details the work roles within cybersecurity and the specific knowledge, skills, and abilities (KSAs) required to perform cybersecurity tasks.

NICE Framework Components:



| INVESTIGATE | COLLECT AND OPERATE | PROTECT AND DEFEND | ANALYZE | OPERATE AND MAINTAIN | OVERSEE AND GOVERN | SECURELY PROVISION |
|---|---|---|---|---|---|---|
| | | | | | | Risk Management |
| | | | | Customer Service and Technical Support | Cybersecurity Management | Software Development |
| | | | All Source Analysis | Data Administration | Executive Cyber Leadership | Systems Architecture |
| | | Cyber Defense Analysis | Exploitation Analysis | Knowledge Management | Legal Advice and Advocacy | Systems Development |
| | Collection Operations | Cyber Defense Infrastructure Support | Language Analysis | Network Services | Program/Project Management and Aquisition | Systems Requirements Planning |
| Cyber Investigation | Cyber Operational Planning | Incident Response | Targets | Systems Administration | Strategic Planning and Policy | Technology R&D |
| Digital Forensics | Cyber Operations | Vulnerability Assessment and Management | Threat Analysis | Systems Analysis | Training, Education, and Awareness | Test and Evaluation |



| Categories | Descriptions |
|---|---|
| **Securely Provision (SP)** | Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development. |
| **Operate and Maintain (OM)** | Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security. |
| **Oversee and Govern (OV)** | Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work. |
| **Protect and Defend (PR)** | Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks. |
| **Analyze (AN)** | Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. |
| **Collect and Operate (CO)** | Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. |
| **Investigate (IN)** | Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence. |

*images courtesy of infosecinstitute.com

**Institutional Goals:**

This program is designed to meet TMCC's Institutional Goals which are demonstrated in the curriculum design, program outcomes, and course descriptions. The following table delineates the alignment between the program and TMCC's institutional goals.

| ***TMCC Institutional Goals*** | ***Program Alignment*** |
|---|---|
| 1. A learning environment stressing the application of academic concepts to concrete problems. | All the courses align with this goal. |
| 2. Academic preparation for learning as a life-long process of discovery of knowledge embedded in the intellectual disciplines and the traditions of the tribe. | All the courses align with this goal. |
| 3. In and out of class opportunities to discover the nature of Indian society, its history, variation, current and future patterns, needs to serve as a contributing member toward its maintenance and betterment. | Direct and explicit incorporation of the Seven Teachings of Anishinaabe People in course material and assignments. |
| 4. A curriculum wherein Indian tribal studies are an integral part of all courses offered as well as history, values, methods, and culture of Western society. | The program's general education requirements specify Native American Language and History courses as part of that requirement. |
| 5. Continuous assessment of institutional programs and student academic achievement for the purpose of continuous improvement of student learning. | The curriculum has been and will be reviewed by subject matter experts to keep program material current and relevant. |
| 6. Baccalaureate, Associate of Arts, Associate of Science, Associate of Applied Science degrees and certificate programs of study. | The Cyber Defense Degree Program is a Baccalaureate degree program |
| 7. Cooperation with locally Indian-owned business and | The course "CIS 490 – Capstone Project" will apply student outcomes to real-world scenarios working with local entities. |

| | |
|---|---|
| stimulation of economic development for the service area. | |
| 8. Continued Independent accreditation | |
| 9. Community service and leadership | Students in the program will have the opportunity to assist with summer cyber camps for 7-12 area youth.  Leadership qualities and skills discuss in various courses. |

**Program Outcomes:**

1. Students will be able to deploy and manage practical cyber defense tools and strategies in multiple operating environments.
2. Students will be able to conduct vulnerability tests against computer systems and coordinate and prepare remedies for those vulnerabilities.
3. Students will be able to analyze threats and attacks on computer systems in a security operations center environment.
4. Students will be able to demonstrate and apply the Seven Teachings of the Anishinaabe People to the responsibilities of cybersecurity professionals.

**Requirements:**

| | |
|---|---|
| General Education | 30cr |
| Cybersecurity Foundations | 48cr |
| Cyber Defense Core | 36cr |
| Electives | 6cr |
| Total Program | 120cr |

Students must not receive a grade lower than a “C” in any cybersecurity foundation or cyber defense core course.  Students also must maintain a 2.5 GPA in the Cyber Defense Core courses.

## ***General Education***

English & Communications 9cr

| | | | |
|---|---|---|---|
| ENGL | 110 | College Composition I | 3 |
| ENGL | 120 | College Composition II | 3 |
| COMM | 110 | Fundamentals of Public Speaking | 3 |

Arts & Humanities 9cr (6cr in Native Language)

| | | | |
|---|---|---|---|
| LANG | | Native Language | 3 |
| LANG | | Native Language | 3 |
| HUMS | | Humanities | 3 |

Social Science 6cr (3cr of Native American History)

| | | | |
|---|---|---|---|
| SOCI | | Social Science | 3 |
| SOCI | | Native American History | 3 |

Math & Science 6cr

| | | | |
|---|---|---|---|
| MATH | 103 | College Algebra (Pre-Req for Computer Science II & Cryptography) | 4 |
| | | Science | 2 |
| | | | 30 |

## ***Cybersecurity Foundation Courses***

| | | | |
|---|---|---|---|
| CIS | 141 | Introduction to Cyber Security | 3 |
| CSCI | 160 | Computer Science I | 3 |
| CIS | 161 | Computer Science II | 3 |
| CIS | 162 | Operating Systems | 3 |
| CIS | 165 | Network Fundamentals II | 3 |
| CIS | 168 | Firewalls and Network Security | 3 |
| MATH | 210 | Elementary Statistics | 3 |
| CIS | 223 | Linux System Administration | 3 |
| CIS | 241 | Intro to Digital Forensics | 3 |
| CIS | 245 | Security Operations Fundamentals | 3 |
| CIS | 255 | Cloud Foundations | 3 |
| CIS | 261 | Cyber Law & Ethics | 3 |
| CIS | 264 | Ethical Hacking & Network Defense | 3 |
| CIS | 267 | Intermediate Networking I | 3 |
| CIS | 270 | Cybersecurity Infrastructure Configuration | 3 |
| CIS | 271 | Cybersecurity Prevention and Countermeasures | 3 |
| | | | 48 |

***Cyber Defense Core***

| | | | |
|---|---|---|---|
| CIS | 320 | Information Security Management | 3 |
| CIS | 326 | Database and Application Security | 3 |
| CIS | 365 | Defensive Network Security | 3 |
| CIS | 366 | Security Operations Analysis | 3 |
| CIS | 387 | Cryptography | 3 |
| CIS | 390 | Survey of Critical Infrastructure Security | 3 |
| CIS | 410 | Wireless and Mobile Security | 3 |
| CIS | 418 | Cloud Security Essentials | 3 |
| CIS | 435 | Network Security & Analysis | 3 |
| CIS | 440 | Threat Hunting and Incident Response | 3 |
| CIS | 470 | Penetration Testing | 3 |
| CIS | 490 | Capstone Project/Internship | 3 |
| | | | 36 |
| | | Electives | 6 |
| | | | 12 |
| | | Total Credits | 0 |

## Course Descriptions:

CIS 320 - Information Security Management – 3Cr

This course will examine the framework of policies and controls that systematically manage security and risks across the enterprise environment. Coverage of the foundational and technical components of information security is included to reinforce key concepts. Methods and strategies of security compliance will be examined. **Pre-requisite: CIS 141**

CIS 326 – Database and Application Security– 3Cr

This course will focus on the security vulnerabilities of database and application servers. Methods and best practices for securing against vulnerabilities will be examined. **Pre-requisite: CIS 255**

CIS 365 – Defensive Network Security– 3Cr

This course will examine several different secured access service edge (SASE) technologies such as SD-WAN, next-generation firewalls, and firewalls as a service. Concepts of “network as a service” (NaaS) and zero trust will be covered. Students will get hands-on work in a security operations center environment. **Pre-requisite: CIS 270, CIS 271**

CIS 366 – Security Operations Analysis– 3Cr

This course will examine the application of endpoint protection, security information and event management (SIEM), user and entity behavior analytics, and security orchestration automation and response (SOAR). **Pre-requisite: CIS 365**

CIS 387 – Cryptography– 3Cr

This course will cover the fundamentals of cryptography. Cryptography applications, encryption and decryption, and protocols will be examined. **Pre-requisite: MATH 103**

CIS 390 – Survey of Critical Infrastructure Security

This course will examine critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual are vital to public safety and security. Students will review and discuss regulations and best practices regarding cybersecurity related to those sectors. **Pre-requisite: CIS 320**

CIS 410 – Wireless and Mobile Security– 3Cr

This course focuses on the security and application of wireless communication in networks. Students will gain experience in wireless management systems. Students will also examine the security considerations of mobile devices and Internet of Things (IoT) devices. **Pre-requisite: CIS 164, CIS 165**

CIS 418 – Cloud Security Essentials– 3Cr

This course will equip students to implement appropriate security controls in the cloud. The course will utilize Identity and Access Management (IAM) strategies and practical hands-on exercises relating to different CSP models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Functions as a Service (FaaS).

CIS 435 – Network Security & Analysis– 3Cr

This course will focus on advanced network security aspects and concepts related to data, VoIP, video, and ICS/SCADA networks. Network monitoring and logging tools and strategies will be examined. This course will feature hands-on exercises. **Pre-requisite: CIS 267**

CIS 440 – Threat Hunting and Incident Response– 3Cr

This course will utilize offensive and defensive strategies to identify breaches, compromised network endpoints, and cybersecurity incident management. Students will be exposed to hardware and software solutions for logging and incident response. Incident response plans regarding active events will be developed as well as post-incident review plans. **Pre-requisite: CIS 320**

CIS 470– Penetration Testing– 3Cr

This course will analyze and execute penetration exercises in network and application environments. This course will utilize a hands-on approach to penetration testing using today's latest hardware and software tools. **Pre-requisite: CIS 366**

CIS 490– Capstone Project– 3Cr

This course will require students to demonstrate their cyber defense knowledge and skills. The project will have several deliverables as well as a final presentation. **Pre-requisite: Instructor Approval**