SecuritySkool

mile2 AUTHORIZED TRAINING CENTER
Cyber Security Certifications

Cybersecurity Center of Excellence

Empowering the Future of Cybersecurity Education and Innovation

Presented By Prasanth Konoth & Rajkumar

www.securityskool.com

mile2 SecuritySkool -Cybersecurity Center of Excellence

Abstract

In order to effectively ensure our continued technical advantage and future cybersecurity, we need a technologically skilled and cyber-savvy workforce and an effective pipeline of future employees. Our Government and Governments worldwide has identified Cybersecurity as one of the most serious economic and national security challenges we face as a nation and has earmarked cybersecurity education as a major part of its Comprehensive National Cybersecurity Initiative. By establishing a Cybersecurity Center of Excellence - CCoE as part of our Computer Science-Cybersecurity curriculum, University will be well positioned to train and educate students on this very important National initiative. In addition, we will be providing our students with the skill-sets necessary to become a member of the cybersecurity workforce.

CYBERSECURITY
CENTER OF EXCELLENCE

SecuritySkool

What is Cybersecurity Center of Excellence

Cybersecurity Center of Excellence (CCoE)

- ·**Definition**:

The Cybersecurity Center of Excellence (CCoE) is a state-of-the-art hub dedicated to advancing cybersecurity education, research, and innovation. It serves as a collaborative platform for students, faculty, and industry partners to address the growing challenges of cybersecurity.

- ·**Mission**:

To empower the next generation of cybersecurity professionals through cutting-edge education, hands-on training, and groundbreaking research. To foster innovation and develop solutions to combat evolving cyber threats.

- ·**Vision**:

To become a global leader in cybersecurity education and research, recognized for excellence in preparing skilled professionals and driving technological advancements.

Why the CCoE Matters

- ·**Addressing Critical Needs:**
  - o Cybersecurity is a top priority for governments, businesses, and individuals worldwide.
  - o The CCoE positions the university as a leader in addressing these challenges.
- ·**Benefits to Stakeholders:**
  - o **Students**: Gain practical skills, certifications, and improved job prospects.
  - o **Faculty**: Access to research opportunities and professional development.
  - o **Industry**: A pipeline of skilled graduates and collaborative innovation.

Key Features of the CCoE

1. Advanced Cybersecurity Labs:

- Equipped with cutting-edge tools and technologies for hands-on learning.
- Industry-Recognized Certifications:
- Partnerships with Mile2 to offer certifications like CPTE, CDFE, and CIHE.

2. Comprehensive Course Offerings:

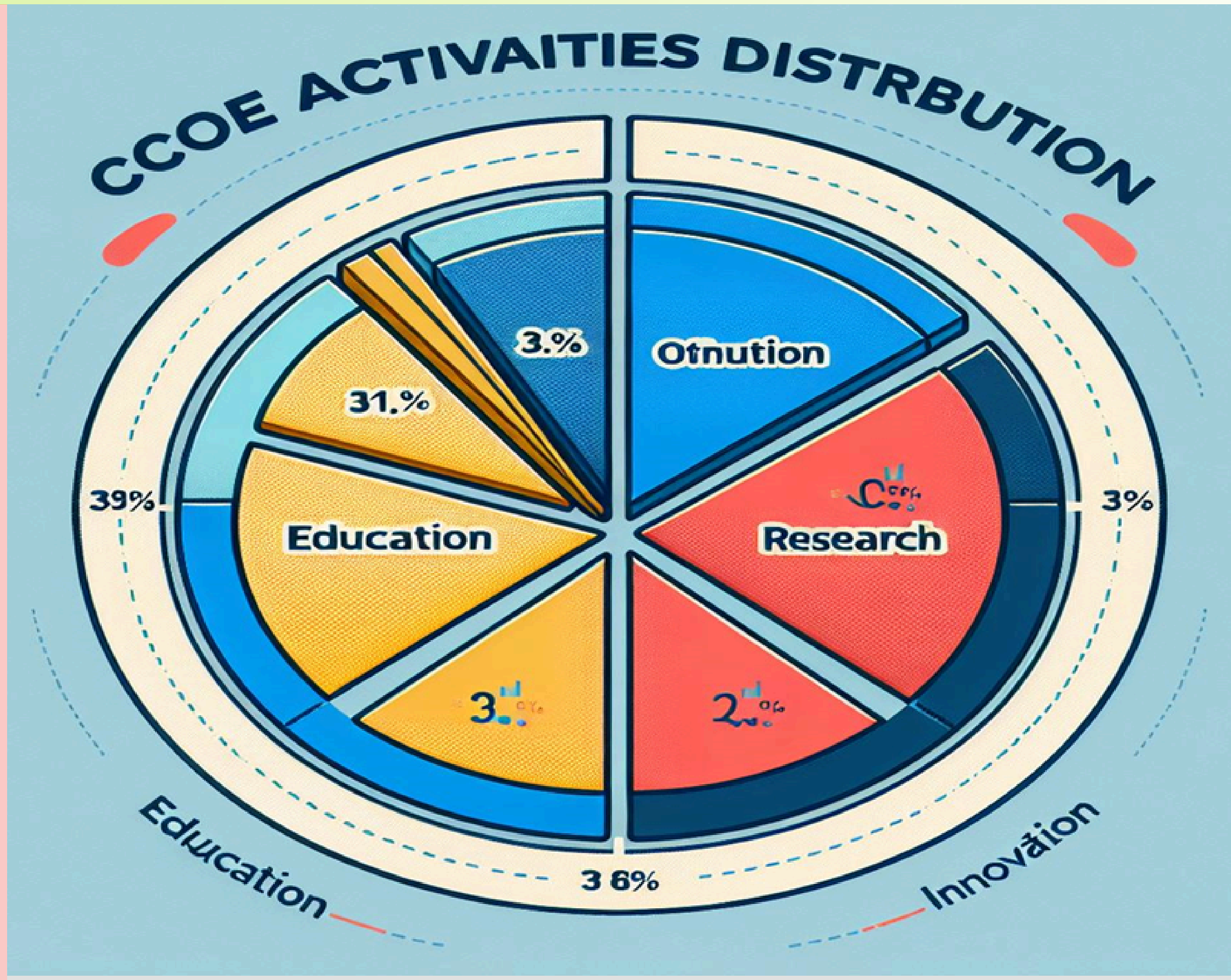
- Undergraduate, graduate, and professional development programs.

Cyber Range:

- A simulated environment for practicing real-world cybersecurity scenarios.

Accreditation:

- Aligned with global standards like the NICE Framework and ISO 27001



Key Takeaways

The CCoE is a cutting-edge initiative to advance cybersecurity education, research, and innovation. It prepares students for high-demand careers, supports faculty in groundbreaking research, and partners with industry to drive innovation. The CCoE is a critical step in addressing the global cybersecurity workforce gap and emerging threats.

CCOE -Addressing the growing demand for skilled cybersecurity professionals

Designed to address the growing demand for skilled cybersecurity professionals.

Global Workforce Gap:

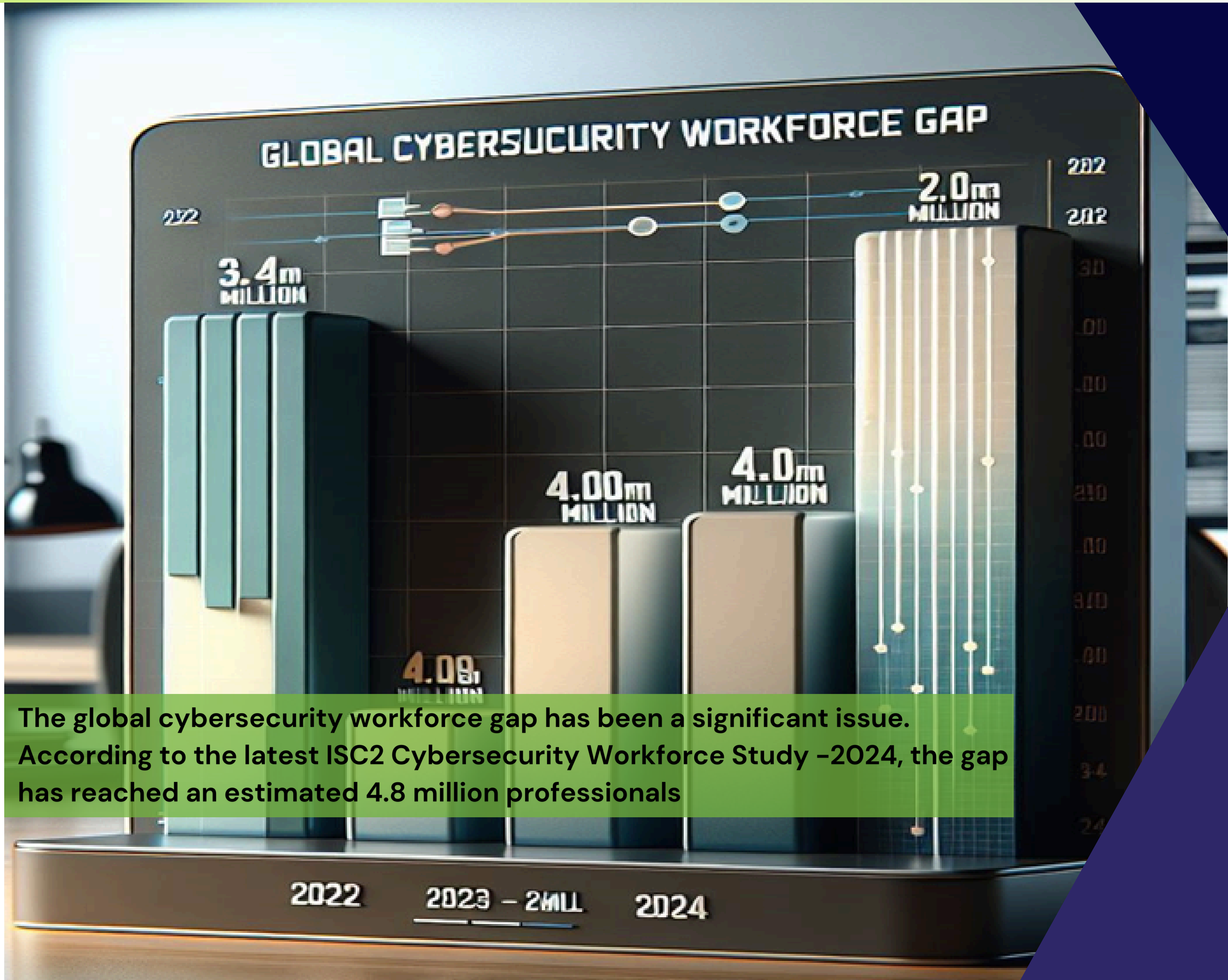
- There are 3.5 million unfilled cybersecurity jobs globally, highlighting the urgent need for skilled professionals.
- The CCoE aims to bridge this gap by producing highly qualified graduates.

Industry-Ready Training:

- Hands-on labs, simulations, and real-world projects ensure students are prepared forthe challenges of the cybersecurity industry.
- Cyber Range for simulating cyberattacks and defense strategies.

Certifications:

- Partnerships with certification bodies like Mile2 provide students with industry-recognized credentials.
- Certified Penetration Testing Engineer (CPTE) , Certified Digital Forensics Examiner (CDFE), Certified Threat Intelligence – CTIA, Certified Incident Handling , SOC – Security Operation centre, Red V/S Blue teaming etc



The global cybersecurity workforce gap has been a significant issue. According to the latest ISC2 Cybersecurity Workforce Study -2024, the gap has reached an estimated 4.8 million professionals

CCOE -A Collaborative Space for Students, Faculty, and Industry Partners

A Collaborative Space for Students, Faculty, and Industry Partners

For Students:

- Access to advanced tools, technologies, and mentorship from industry experts.
- Opportunities to participate in competitions, internships, and research projects
- Example: Annual cybersecurity hackathons and capture-the-flag (CTF) events.

For Faculty:

- A platform to conduct cutting-edge research and collaborate with industry leaders.
- Professional development opportunities through workshops and certifications.
- Example: Faculty-led research on zero-trust architecture.

For Industry Partners:

- A pipeline of skilled graduates ready to join the workforce.
- Opportunities to collaborate on research and innovation projects.
- Example: Industry-sponsored labs and research grants.

SecuritySkool

Mission-Cybersecurity Center of Excellence

The mission of the Cybersecurity Center of Excellence

Advance Cybersecurity Knowledge:

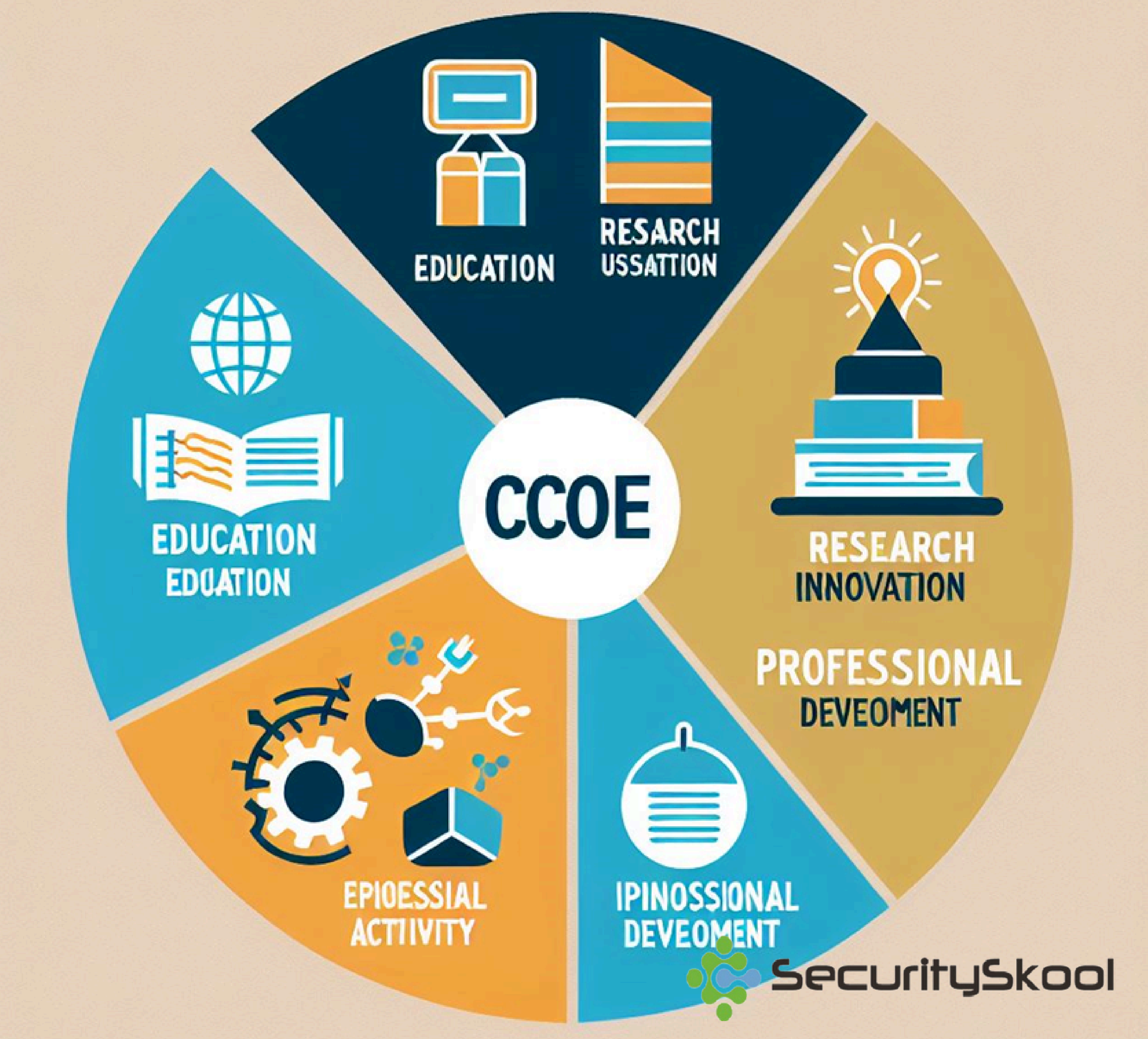
- Develop and disseminate knowledge through academic programs, research publications, and industry partnerships.
- Example: Hosting annual cybersecurity conferences and workshops.

Foster Innovation:

- Create an environment that encourages creativity and the development of new solutions to cybersecurity challenges.
- Example: Innovation grants for student-led cybersecurity projects.

Prepare the Next Generation of Cybersecurity Experts:

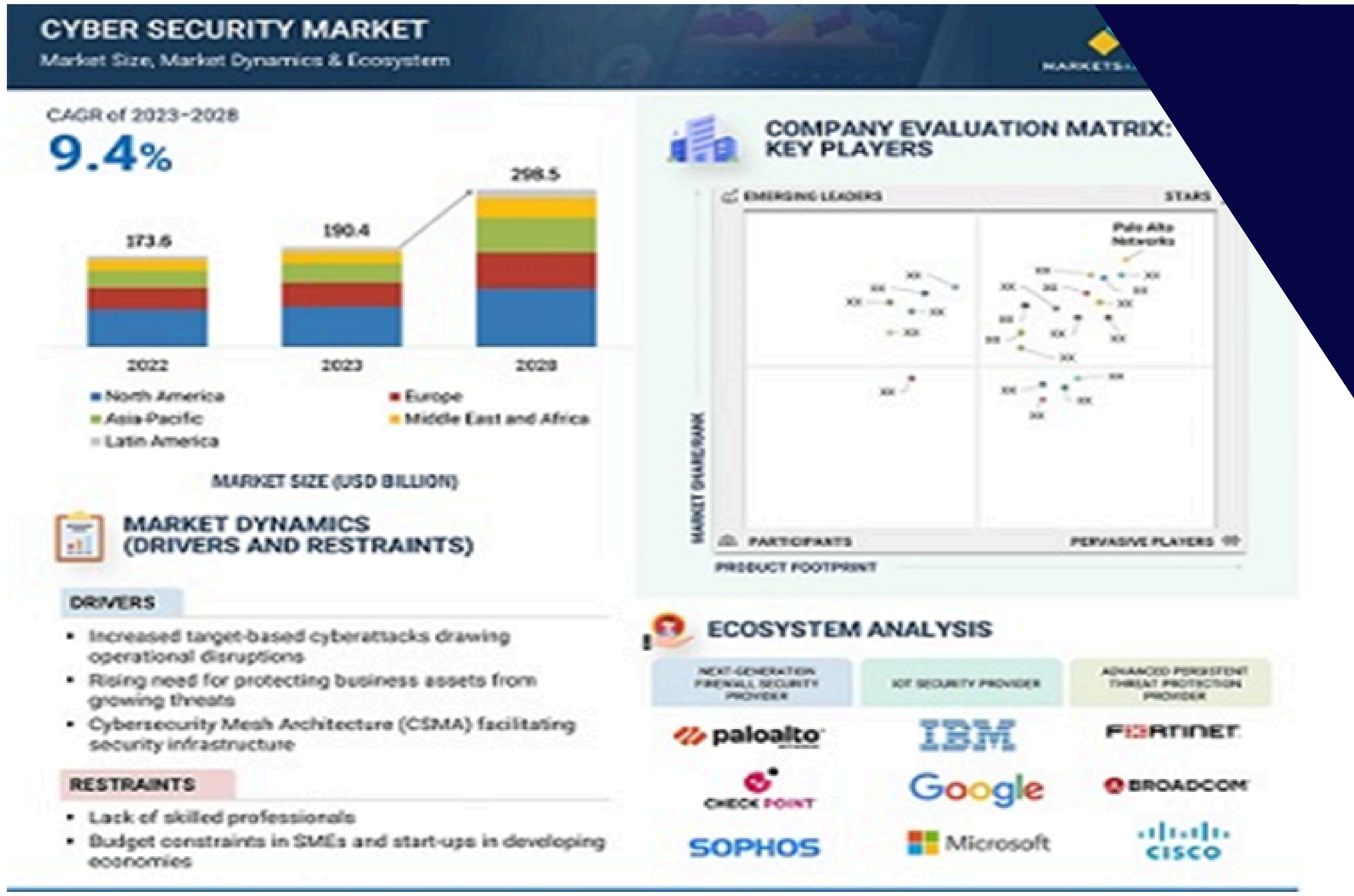
- Equip students with the skills, certifications, and experience needed to excel in the cybersecurity field.
- Example: Job placement programs and partnerships with leading cybersecurity firms.



Market Overview-Global Security Market

Market Growth:

- The global cybersecurity market is projected to grow from 172 billion in 2023 to 267 billion by 2028, at a Compound Annual Growth Rate (CAGR) of 9.2%.
- This growth is driven by the increasing frequency and sophistication of cyberattacks, as well as stricter regulatory requirements.



MARKET DYNAMICS (DRIVERS AND RESTRAINTS)

DRIVERS

- Increased target-based cyberattacks drawing operational disruptions
- Rising need for protecting business assets from growing threats
- Cybersecurity Mesh Architecture (CSMA) facilitating security infrastructure

RESTRAINTS

- Lack of skilled professionals
- Budget constraints in SMEs and start-ups in developing economies

Key Drivers of Growth:

Rising Cyber Threats:

- Cyberattacks such as ransomware, phishing, and data breaches are becoming more frequent and costly.
- Example: The global cost of cybercrime is expected to reach $10.5 trillion annually by 2025.

Digital Transformation:

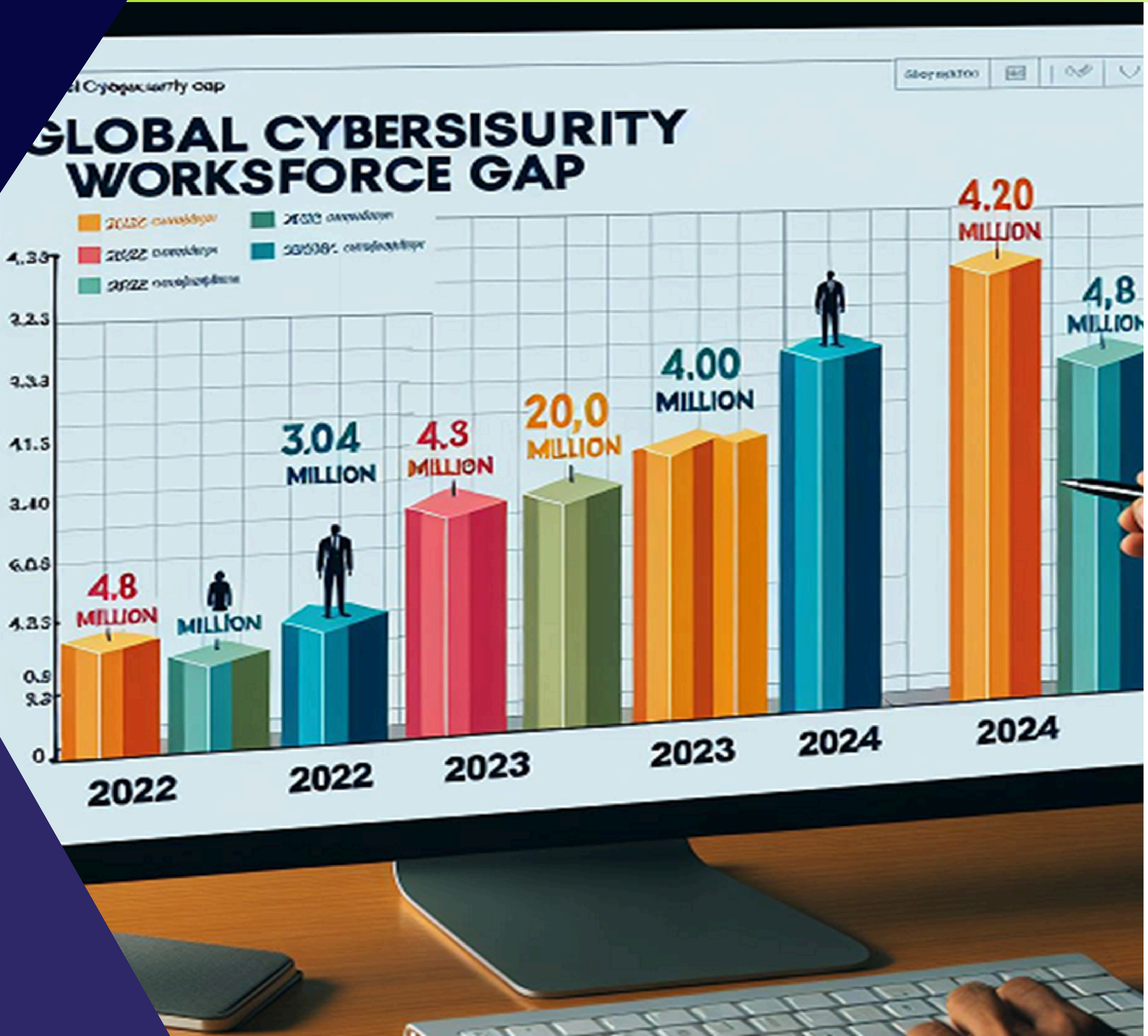
- The shift to cloud computing, IoT, and remote work has expanded the attack surface, increasing the need for robust cybersecurity measures

Regulatory Requirements

- Governments and industries are implementing stricter data protection regulations (e.g., GDPR, CCPA).
- Organizations must invest in cybersecurity to comply with these regulations.

mile2®

Cybersecurity Workforce Gap



Current Workforce Shortage:

- In 2023-24, there are 3.5 to 4 Million unfilled cybersecurity jobs globally.
- This gap is expected to widen as the demand for cybersecurity professionals outpaces supply.

Challenges for Organizations:

- Organizations are struggling to find qualified professionals with the necessary skills and certifications.
- Example: A survey by (ISC)² found that **70% of organizations report a shortage of cybersecurity staff.**
- This shortage leaves businesses vulnerable to cyberattacks and increases the risk of data breaches.

Impact on Industries:

- Critical sectors such as healthcare, finance, and government are particularly affected by the workforce gap.
- Example: The healthcare sector faces increasing cyber threats but lacks the skilled personnel to defend against them

SecuritySkool

Workforce Gap-Opportunity for Universities

Bridging the Skills Gap:

Universities have a unique opportunity to address the cybersecurity workforce shortage by offering **cutting-edge cybersecurity programs.**

- These programs should focus on practical, hands-on training to ensure graduates are job-ready.
- Eg- Courses in ethical hacking, digital forensics, and cloud security..

Partnerships with Industry and Government:

Collaborating with industry leaders and government agencies can enhance the quality and relevance of cybersecurity education.

Benefits of Partnerships:

- Access to real-world case studies and industry-standard tools.
- Opportunities for internships and job placements.
- Funding for research projects and infrastructure development.

Example: A university partnering with a cybersecurity firm to develop a state-of-the-art Cyber Range.

Enhancing Research and Job Placement:

Universities can leverage partnerships to conduct applied research on emerging cybersecurity challenges. Research on AI-driven threat detection or blockchain security Strong industry connections can improve job placement rates for graduates, ensuring they are employed in high-demand roles.

Why the Cybersecurity Center of Excellence?

Bridging the Skills Gap:

Cybersecurity as a Top Priority:

- Governments, businesses, and individuals are increasingly reliant on digital systems, making cybersecurity a critical concern.
- Cyberattacks are becoming more frequent, sophisticated, and costly, with global damages expected to reach $10.5 trillion annually by 2025.

Example: High-profile breaches in healthcare, finance, and government sectors highlight the urgent need for robust cybersecurity measures.

Positioning the University as a Leader:

- The Cybersecurity Center of Excellence (CCoE) will establish the university as a pioneer in cybersecurity education and research.
- By addressing real-world challenges, the CCoE will contribute to national and global cybersecurity efforts.

Example: The university could become a go-to institution for cybersecurity expertise, attracting media attention and government collaboration

Benefits to the University

Attracting Top-Tier Students and Faculty:

- The CCoE will draw high-achieving students and renowned faculty members who are passionate about cybersecurity.

Example: Offering scholarships and research grants to attract talent.

Securing Funding and Partnerships:

- The CCoE will open doors to funding opportunities from government agencies, private sector companies, and grants.
- Partnerships with industry leaders will provide access to resources, tools, and real-world projects.

Example: Collaborating with companies like Cisco, IBM, or Palo Alto Networks for sponsored labs and research initiatives.

Enhancing the University's Reputation:

- The CCoE will elevate the university's profile as an innovation hub and a leader in cutting-edge technology.
- This reputation will attract more applicants, donors, and collaborators.

Example: Being ranked among the top universities for cybersecurity education and research.

Benefits to Students

Hands-On Experience with Real-World Challenges:

Students will gain practical skills by working on real-world cybersecurity scenarios in state-of-the-art labs and cyber ranges.
Example: Simulating cyberattacks and developing defense strategies in a controlled environment.

Access to Industry-Recognized Certifications and Training:

The CCoE will offer certifications from globally recognized bodies like Mile2, CompTIA, and (ISC)².
These certifications will enhance students' resumes and make them more competitive in the job market.
Example: Certifications such as Certified Ethical Hacker (CEH) or Certified Information Systems Security Professional (CISSP).

Improved Job Prospects in a High-Demand Field:

With 3.5 million unfilled cybersecurity jobs globally, graduates of the CCoE will have excellent career opportunities.
The CCoE's industry partnerships will provide students with internships, networking opportunities, and job placements.
Example: Graduates securing roles as cybersecurity analysts, penetration testers, or security architects.

Details of the Cybersecurity Center of Excellence

Key Components:

1. Advanced Cybersecurity Labs
2. Comprehensive Course Offerings
3. Mile2 Certification Programs
4. Cyber Range
5. Accreditation
6. Train The Trainer (TTT Program)
7. Cyber Security Lab (Sample)
8. Mile2 Certificate Road Map

Advanced Cybersecurity Labs

Advanced Cybersecurity Labs

Cutting-Edge Tools and Technologies:

- The labs are equipped with the latest cybersecurity tools and software, such as Wireshark, Metasploit, SIEM platforms, and firewall solutions.
- Students gain hands-on experience with tools used by industry professionals

Simulated Environments for Threat Analysis and Response:

- The labs feature simulated environments that replicate real-world networks and systems.
- Students can practice identifying, analyzing, and responding to cyber threats in a controlled setting.
- Example: Simulating a ransomware attack and developing a response plan

Top 10 Cybersecurity Tools

Dedicated Spaces for Specialized Tasks:

- The labs include specialized areas for -Malware Analysis
- Studying and reverse-engineering malicious software.
- Penetration Testing: Simulating cyberattacks to identify vulnerabilities
- Digital Forensics: Investigating cybercrimes and recovering digital evidence.

Features of Cybersecurity Labs

High-Performance Computing Resources:

- The labs are equipped with powerful servers and workstations capable of handling complex cybersecurity tasks.
- Enables students to run resource-intensive applications like virtual machines, network simulators, and forensic tools.

Access to Industry-Standard Tools:

Students gain hands-on experience with tools used by cybersecurity professionals, including:
Wireshark: For network protocol analysis.
Metasploit: For penetration testing and vulnerability assessment.
SIEM Platforms: For real-time security monitoring and incident response.

Benefits of Cybersecurity Labs

1.Hands-On Learning in a Controlled Environment:

Students can practice cybersecurity techniques in a safe, controlled setting without risking real-world systems.

2.Prepares Students for Real-World Cybersecurity Challenges:

- The labs provide realistic scenarios that mirror the challenges faced by cybersecurity professionals.
- Students develop critical thinking, problem-solving, and technical skills that are directly applicable to their careers.
- Example: Responding to a simulated ransomware attack to develop incident response skills

CCoE- Course Offering

Undergraduate Programs

Bachelor of Science in Cybersecurity:

1. A comprehensive program designed to provide students with a strong foundation in cybersecurity principles and practices.
2. Covers topics such as **network security**, **ethical hacking**, **digital forensics**, and **cyber law**.
3. Prepares students for roles like **cybersecurity analyst**, **penetration tester**, and **security consultant**

Value Added program in Cybersecurity for Non-CS Majors:

1. Allows students from other disciplines (e.g., business, engineering, or law) to gain cybersecurity knowledge.
2. Ideal for professionals seeking to enhance their skill set and understand cybersecurity risks in their field.

Example: A business student learning about cyber risk management to protect organizational assets

Graduate Programs

Master of Science in Cybersecurity:

1. An advanced program for students seeking in-depth knowledge and leadership roles in cybersecurity.
2. Focuses on **advanced threat analysis**, **security architecture**, and **cybersecurity policy.**
3 .Prepares graduates for roles like **chief information security officer** (**CISO**) or **security architect.**

Graduate Certificates in Specialized Areas:

1. Short, focused programs that allow students to specialize in high-demand areas.

Examples:

Cloud Security: Securing cloud-based systems and applications.

IoT Security: Protecting Internet of Things devices and networks.

Ideal for professionals looking to upskill or pivot their careers

CCoE- Course Offering

Professional Development

Short Courses and Workshops for Working Professionals:

- Designed for professionals who want to stay updated on the latest cybersecurity trends and techniques.
- Flexible formats, including weekend workshops, online courses, and bootcamps

Topics Include:

Partnerships with Industry and Government:

- **Ethical Hacking**: Learning to identify and exploit vulnerabilities to improve system security.
- **Risk Management:** Understanding and mitigating cybersecurity risks in organizations.
- **SIEM – SOC Training**
- **Compliance:** Ensuring adherence to regulations like GDPR, HIPAA, and PCI-DSS.

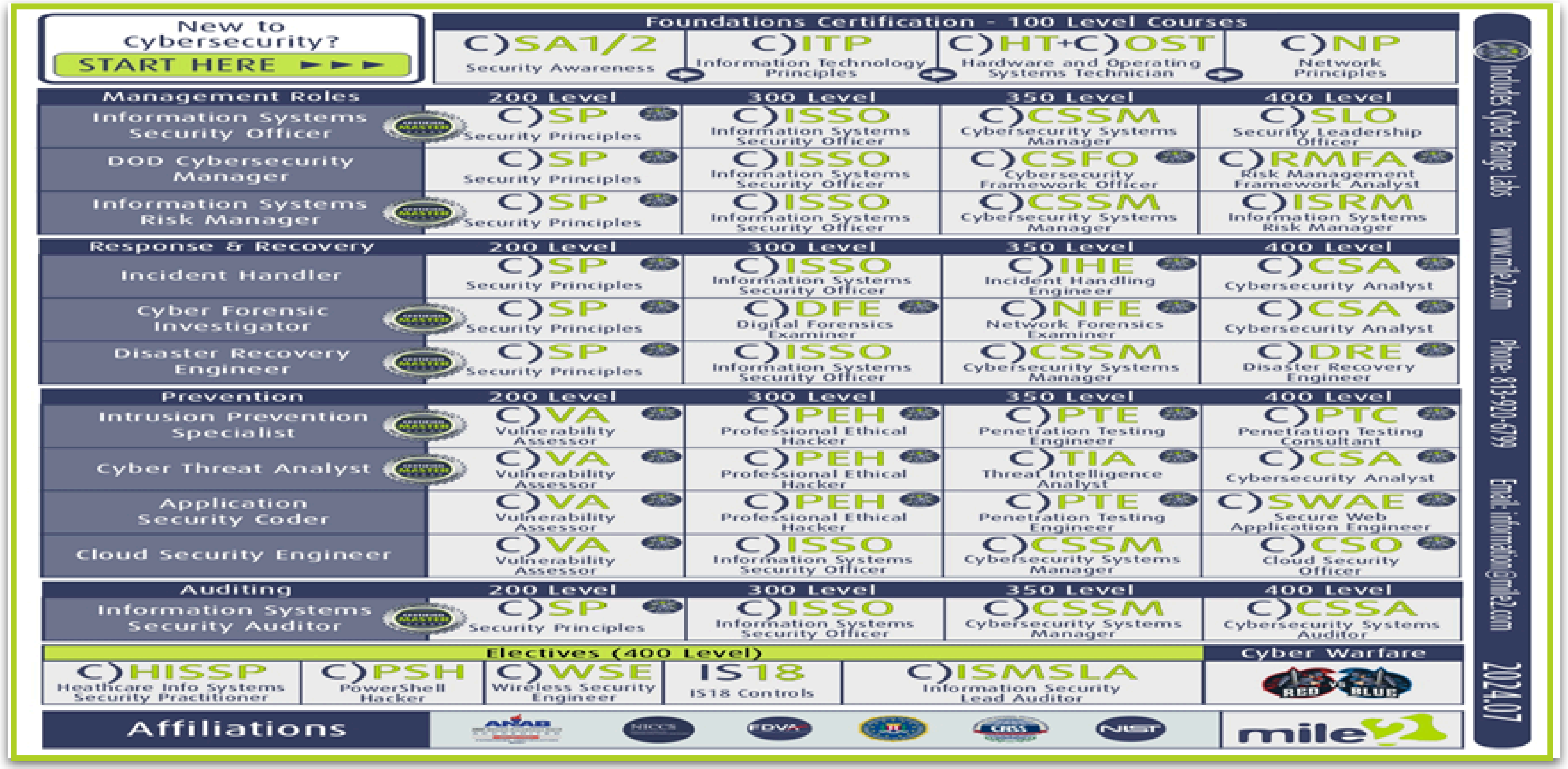
Example: A 2-day workshop on GDPR compliance for IT managers.

Key Takeaways

- ·The **CCoE** offers **undergraduate programs** like a **Bachelor of Science in Cybersecurity** and a **Minor in Cybersecurity for non-CS majors.**
- **Graduate programs** include a **Master of Science in Cybersecurity** and **specialized certificates** in areas like **cloud** and **IoT security**

Professional development courses and workshops provide working professionals with skills in **ethical hacking**, **risk management**, and **compliance**

Mile2 CCoE Certification Programs



New to Cybersecurity?
START HERE ►►►

Foundations Certification - 100 Level Courses			
C)SA1/2 Security Awareness	C)ITP Information Technology Principles	C)HT+C)OST Hardware and Operating Systems Technician	C)NP Network Principles

Management Roles	200 Level	300 Level	350 Level	400 Level
Information Systems Security Officer	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)SLO Security Leadership Officer
DOD Cybersecurity Manager	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSFO Cybersecurity Framework Officer	C)RMFA Risk Management Framework Analyst
Information Systems Risk Manager	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)ISRM Information Systems Risk Manager

Response & Recovery	200 Level	300 Level	350 Level	400 Level
Incident Handler	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)IHE Incident Handling Engineer	C)CSA Cybersecurity Analyst
Cyber Forensic Investigator	C)SP Security Principles	C)DFE Digital Forensics Examiner	C)NFE Network Forensics Examiner	C)CSA Cybersecurity Analyst
Disaster Recovery Engineer	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)DRE Disaster Recovery Engineer

Prevention	200 Level	300 Level	350 Level	400 Level
Intrusion Prevention Specialist	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)PTE Penetration Testing Engineer	C)PTC Penetration Testing Consultant
Cyber Threat Analyst	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)TIA Threat Intelligence Analyst	C)CSA Cybersecurity Analyst
Application Security Coder	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)PTE Penetration Testing Engineer	C)SWAE Secure Web Application Engineer
Cloud Security Engineer	C)VA Vulnerability Assessor	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)CSO Cloud Security Officer

Auditing	200 Level	300 Level	350 Level	400 Level
Information Systems Security Auditor	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)CSSA Cybersecurity Systems Auditor

Electives (400 Level)					Cyber Warfare
C)HISSP Heathcare Info Systems Security Practitioner	C)PSH PowerShell Hacker	C)WSE Wireless Security Engineer	IS18 IS18 Controls	C)ISMSLA Information Security Lead Auditor	RED BLUE

Affiliations

Includes Cyber Range Labs www.mile2.com Phone: 813-920-6799 Email: information@mile2.com 2024.07

Mile2's training program is broken down into 5 key areas in the INFOSEC sector:

- **Management**
- **Recovery**
- **Prevention**
- **Audit**
- **Compliance**

These 4 key areas focus on "Role Based" jobs in over 10 different disciplines (Forensics, IS Management, Pen Testing, Auditing etc.).

Mile2 Certification Programs

Mile2 offers over 32+ certification programs.

- Mile2 as a Globally Recognized Certification Body
- Mile2 is a leading provider of vendor-neutral cybersecurity certifications.
- Known for its practical, hands-on approach to training and certification.

Certifications Align with Industry Standards and Job Roles: Mile2 certifications are designed to meet the NICE Cybersecurity Workforce Framework and other global standards.

Benefits

- Enhances Students' Employability: - Mile2 certifications are recognized by employers worldwide, making graduates more attractive to potential employers.
- Provides a Competitive Edge in the Job Market: Certifications demonstrate practical skills and industry knowledge, setting students apart from their peers.

Key Takeaways

- Mile2 is a globally recognized certification body offering practical, hands-on cybersecurity certifications.
- Key certifications include CPTE, CDFE, and CIHE, which align with industry standards and job roles.
- Mile2 certifications enhance employability and provide a competitive edge in the job market.

Mile2 Cyber Range

What is a Cyber Range?

A Simulated Environment for Practicing Cybersecurity Skills:

- The Cyber Range is a virtualized platform that replicates real-world IT infrastructure, including networks, systems, and applications.
- Provides a safe and controlled environment for hands-on training and experimentation.

Mimics Real-World Networks, Systems, and Threats:

The Cyber Range simulates real-world cyberattacks, such as **ransomware**, **phishing**, and **DDoS attacks**, to provide realistic training scenarios.

Example: Simulating a corporate network under attack to teach incident response strategies.

Features

Scalable and Customizable Scenarios:

- The Cyber Range can be tailored to meet the needs of different users, from beginners to advanced professionals.
- Scenarios can range from basic network defense to complex multi-layered attacks.

Supports Individual and Team-Based Training:

Users can train individually or collaborate in teams to solve complex cybersecurity challenges

Example: A team of students working together to defend against a simulated Advanced Persistent Threat (APT).

Use Cases

Training Students and Professionals:

The **Cyber Range** is an ideal platform for educating students and upskilling professionals in cybersecurity.
Example: A university using the Cyber Range to teach ethical hacking and penetration testing.
Conducting Research on Emerging Threats: Researchers can use the Cyber Range to study new attack vectors, vulnerabilities, and defense mechanisms.

Key Takeaways

- ·The Cyber Range is a simulated environment that mimics real-world networks, systems, and threats.
- ·It offers scalable and customizable scenarios and supports individual and team-based training.
- ·Use cases include training students and professionals, conducting research, and testing security solutions.

mile2®

Mile2 Cyber Range

Importance of Accreditation

1.Ensures Programs Meet Industry and Regulatory Standards:

- Accreditation ensures that the Cybersecurity **Center of Excellence** (CCoE) programs align with global standards and best practices.
- Example: Meeting the **NICE Cybersecurity Workforce Framework** ensures graduates have the skills employers need.

2.Enhances Credibility and Recognition

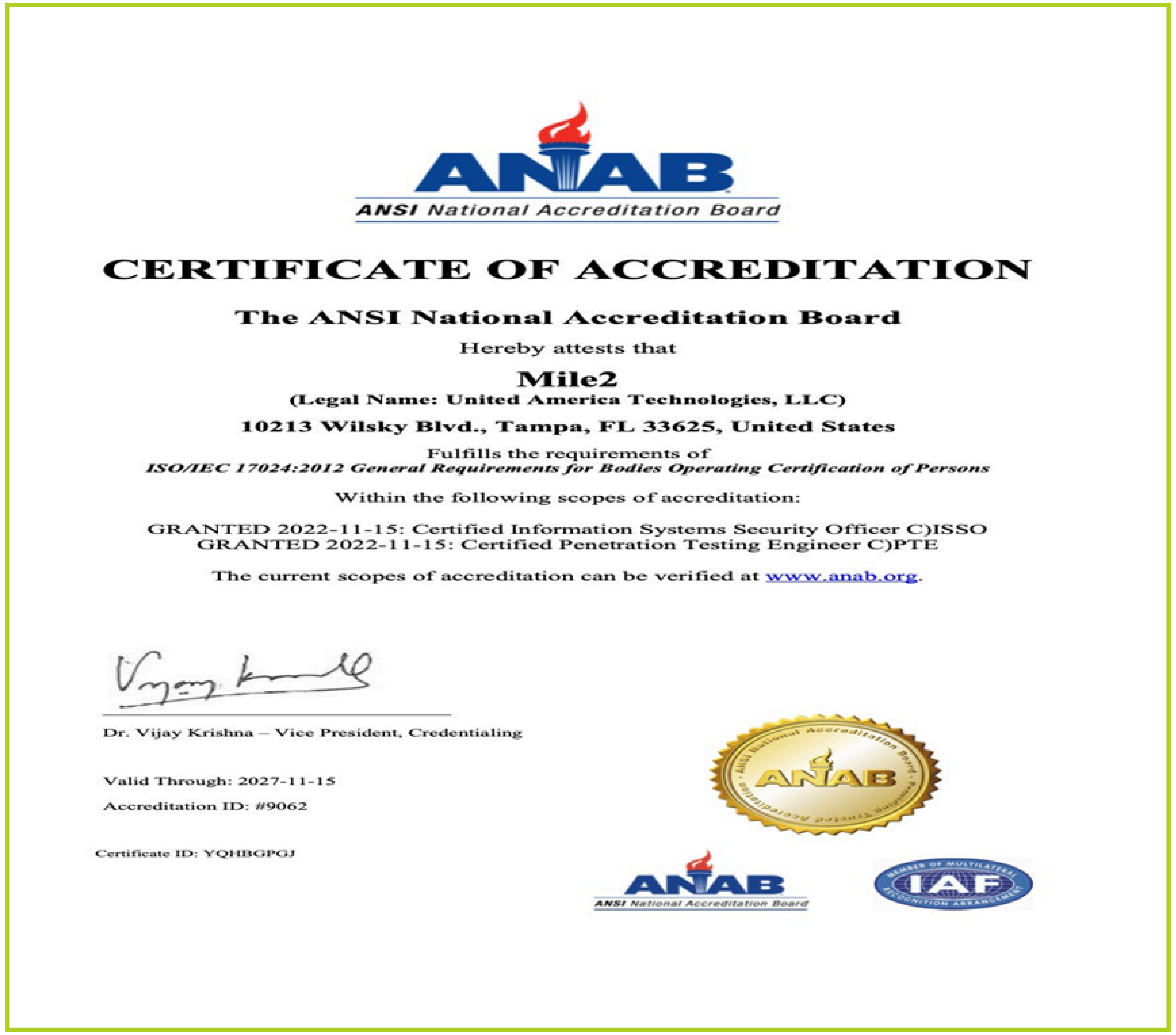
- Accredited programs are recognized by employers, government agencies, and educational institutions worldwide.
- Example: Graduates from an accredited program are more likely to be hired by top-tier organizations.

Accreditation Goals

Align with the NICE Cybersecurity Workforce Framework:

- The CCoE aims to align its programs with the NICE Framework, which defines cybersecurity roles and competencies.
- Ensures graduates are prepared for specific job roles, such as cybersecurity analyst or incident responder.

Achieving this certification will demonstrate the CCoE's commitment to maintaining the highest security standards.



ANAB
ANSI National Accreditation Board

CERTIFICATE OF ACCREDITATION

The ANSI National Accreditation Board

Hereby attests that

Mile2

(Legal Name: United America Technologies, LLC)

10213 Wilsky Blvd., Tampa, FL 33625, United States

Fulfills the requirements of

ISO/IEC 17024:2012 General Requirements for Bodies Operating Certification of Persons

Within the following scopes of accreditation:

GRANTED 2022-11-15: Certified Information Systems Security Officer C)ISSO
GRANTED 2022-11-15: Certified Penetration Testing Engineer C)PTE

The current scopes of accreditation can be verified at www.anab.org.

Dr. Vijay Krishna – Vice President, Credentialing

Valid Through: 2027-11-15

Accreditation ID: #9062

Certificate ID: YQHBGPGJ

ANAB
ANSI National Accreditation Board

IAF

SecuritySkool

Mile2 Cyber Range

APPROVED on the FBI Cybersecurity Certification Requirements (Tier 1-3)

ACCREDITED by the NSA CNSS 4011-4016

MAPPED to NIST/ Homeland Security NICCS's Cybersecurity Workforce Framework.

APPROVED by Florida Department of Veteran's Affairs State Approving Agency

- Florida Department of Veterans Affairs
- National Initiative for Cybersecurity Careers and Studies
- California Specialized Training Institute
- Commission on Peace Officer Standards and Training
- California Office of Emergency Services

Mile2 - CCoE Train the Trainer Program for University Faculty

Overview of the Train the Trainer Program

Purpose:

- The Train the Trainer (TtT) program is designed to equip university faculty with the knowledge and skills to deliver Mile2 certification courses effectively.
- Ensures faculty are proficient in both the theoretical and practical aspects of cybersecurity training.

·Target Audience:

University professors, lecturers, and instructors involved in cybersecurity education

Program Structure

1.Comprehensive Training:

- Faculty undergo intensive training on Mile2 certification courses, including: Certified Penetration Testing Engineer (CPTE)Certified Digital Forensics Examiner (CDFE) Certified Incident Handling Engineer (CIHE)
- Training covers course content, teaching methodologies, and hands-on lab exercises.

2.Hands-On Labs:

- Faculty undergo intensive training on Mile2 certification courses, including: Certified Penetration Testing Engineer (CPTE)Certified Digital Forensics Examiner (CDFE) Certified Incident Handling Engineer (CIHE)
- Training covers course content, teaching methodologies, and hands-on lab exercises.

3. Assessment and Certification:

- Faculty must pass exams and practical assessments to become certified trainers.
- Upon completion, they receive a Mile2 Trainer Certification.

Mile2 - CCoE Train the Trainer Program for University Faculty

Benefits for Faculty

1. **Enhanced Teaching Skills:** Faculty learn advanced teaching techniques and best practices for delivering cybersecurity training

Example: Using real-world scenarios to make lessons more engaging and practical.

2. Access to Mile2 Resources:

Certified trainers gain access to Mile2's training materials, lab environments, and ongoing support.

Professional Development:

The program enhances faculty's expertise and credentials, making them more competitive in academia and industry.

Example: Certified trainers can contribute to research, consultancy, and industry collaborations.

Key Takeaways

- ·The Mile2 Train the Trainer program equips university faculty with the skills to deliver industry-recognized cybersecurity certifications.
- ·Faculty gain enhanced teaching skills, access to Mile2 resources, and professional development opportunities.
- ·The university benefits from high-quality education, increased student employability, and stronger industry partnerships.

Benefits for the University

1. High-Quality Cybersecurity Education:

Certified faculty can deliver **industry-recognized Mile2 certification courses**, enhancing the university's cybersecurity programs.

Example: Offering CPTE and CDFE courses as part of the curriculum.

2. Increased Student Employability

Students trained by certified faculty are better prepared for **high-demand cybersecurity roles.**

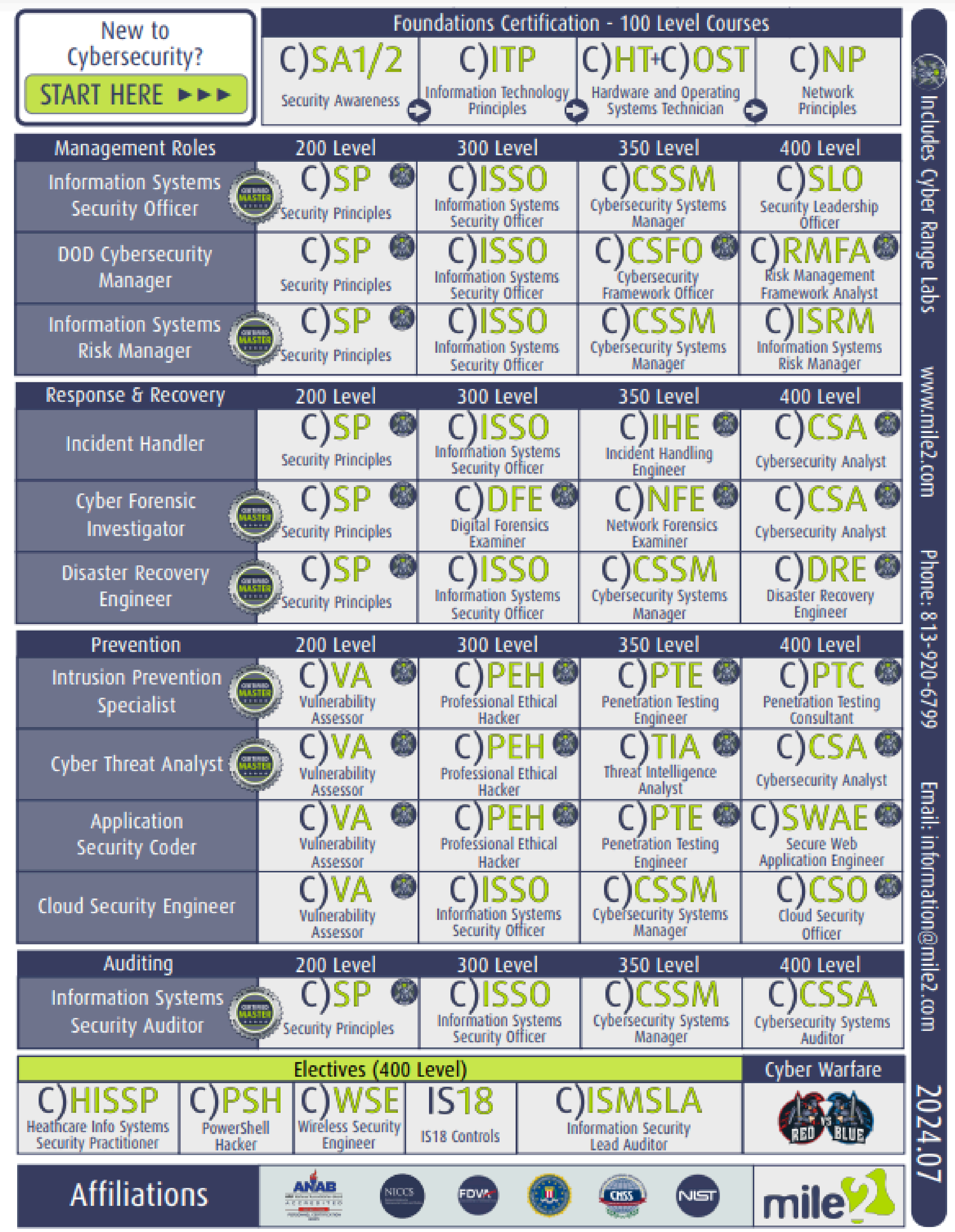
Example: Graduates with Mile2 certifications have a competitive edge in the job market.

3. Strengthened Industry Partnerships:

The university can collaborate with Mile2 and other industry leaders to offer certification programs and research opportunities.

Example: Partnering with Mile2 to host cybersecurity workshops and events

Mile2 Certification Road Map



New to Cybersecurity?
START HERE ▶▶▶

Foundations Certification - 100 Level Courses			
C)SA1/2 Security Awareness	C)ITP Information Technology Principles	C)HT+C)OST Hardware and Operating Systems Technician	C)NP Network Principles

Management Roles	200 Level	300 Level	350 Level	400 Level
Information Systems Security Officer	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)SLO Security Leadership Officer
DOD Cybersecurity Manager	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSFO Cybersecurity Framework Officer	C)RMFA Risk Management Framework Analyst
Information Systems Risk Manager	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)ISRM Information Systems Risk Manager

Response & Recovery	200 Level	300 Level	350 Level	400 Level
Incident Handler	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)IHE Incident Handling Engineer	C)CSA Cybersecurity Analyst
Cyber Forensic Investigator	C)SP Security Principles	C)DFE Digital Forensics Examiner	C)NFE Network Forensics Examiner	C)CSA Cybersecurity Analyst
Disaster Recovery Engineer	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)DRE Disaster Recovery Engineer

Prevention	200 Level	300 Level	350 Level	400 Level
Intrusion Prevention Specialist	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)PTE Penetration Testing Engineer	C)PTC Penetration Testing Consultant
Cyber Threat Analyst	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)TIA Threat Intelligence Analyst	C)CSA Cybersecurity Analyst
Application Security Coder	C)VA Vulnerability Assessor	C)PEH Professional Ethical Hacker	C)PTE Penetration Testing Engineer	C)SWAE Secure Web Application Engineer
Cloud Security Engineer	C)VA Vulnerability Assessor	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)CSO Cloud Security Officer

Auditing	200 Level	300 Level	350 Level	400 Level
Information Systems Security Auditor	C)SP Security Principles	C)ISSO Information Systems Security Officer	C)CSSM Cybersecurity Systems Manager	C)CSSA Cybersecurity Systems Auditor

Electives (400 Level)					Cyber Warfare
C)HISSP Heathcare Info Systems Security Practitioner	C)PSH PowerShell Hacker	C)WSE Wireless Security Engineer	IS18 IS18 Controls	C)ISMSLA Information Security Lead Auditor	RED VS BLUE

Affiliations

Includes Cyber Range Labs

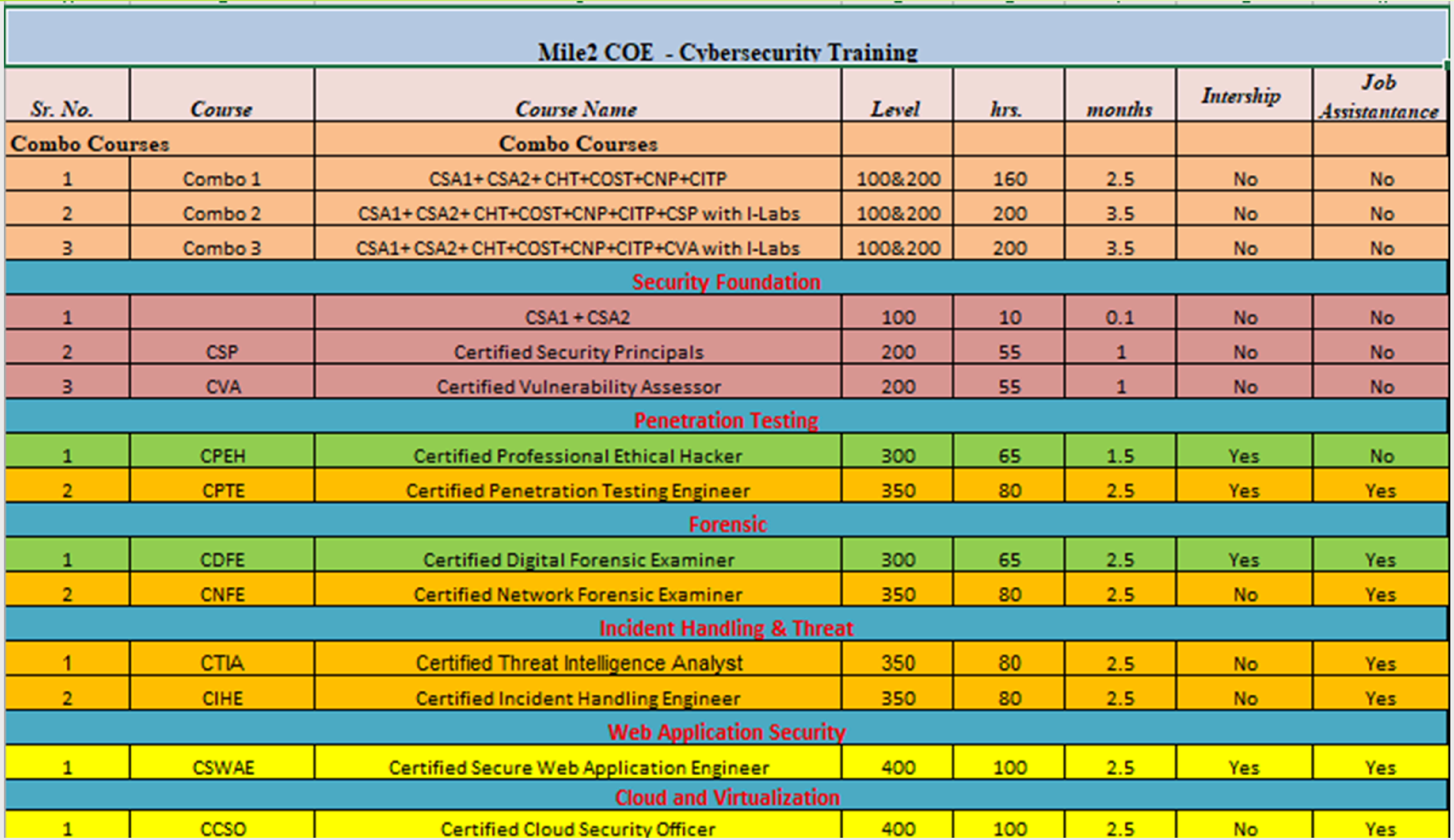
www.mile2.com

Phone: 813-920-6799

Email: information@mile2.com

2024.07

Mile2 Certification Program



Mile2 COE - Cybersecurity Training

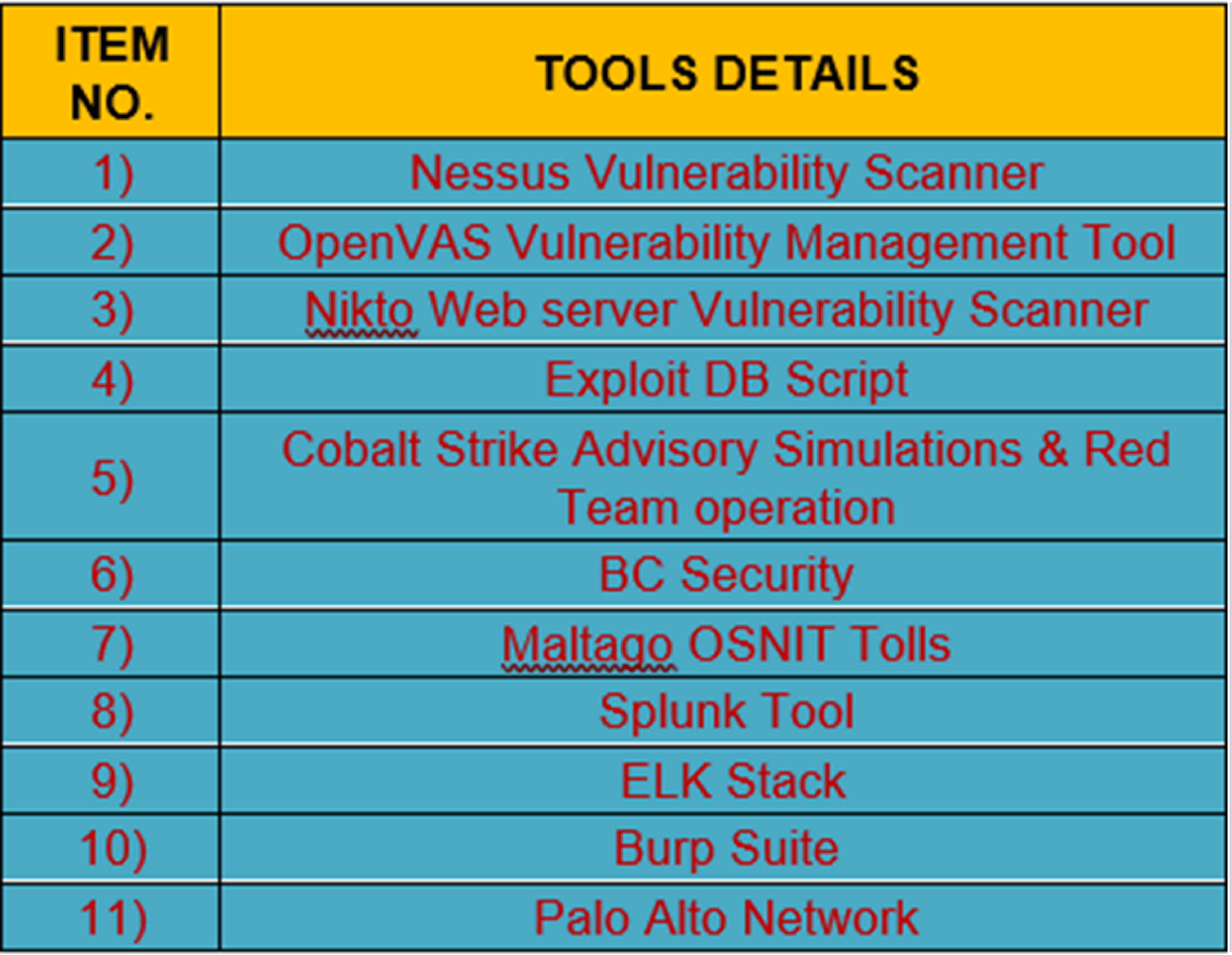
Sr. No.	Course	Course Name	Level	hrs.	months	Intership	Job Assistantance
Combo Courses		Combo Courses					
1	Combo 1	CSA1+ CSA2+ CHT+COST+CNP+CITP	100&200	160	2.5	No	No
2	Combo 2	CSA1+ CSA2+ CHT+COST+CNP+CITP+CSP with I-Labs	100&200	200	3.5	No	No
3	Combo 3	CSA1+ CSA2+ CHT+COST+CNP+CITP+CVA with I-Labs	100&200	200	3.5	No	No
		Security Foundation					
1		CSA1 + CSA2	100	10	0.1	No	No
2	CSP	Certified Security Principals	200	55	1	No	No
3	CVA	Certified Vulnerability Assessor	200	55	1	No	No
		Penetration Testing					
1	CPEH	Certified Professional Ethical Hacker	300	65	1.5	Yes	No
2	CPTE	Certified Penetration Testing Engineer	350	80	2.5	Yes	Yes
		Forensic					
1	CDFE	Certified Digital Forensic Examiner	300	65	2.5	Yes	Yes
2	CNFE	Certified Network Forensic Examiner	350	80	2.5	No	Yes
		Incident Handling & Threat					
1	CTIA	Certified Threat Intelligence Analyst	350	80	2.5	No	Yes
2	CIHE	Certified Incident Handling Engineer	350	80	2.5	No	Yes
		Web Application Security					
1	CSWAE	Certified Secure Web Application Engineer	400	100	2.5	Yes	Yes
		Cloud and Virtualization					
1	CCSO	Certified Cloud Security Officer	400	100	2.5	No	Yes

All course Include

- One Year online Course Access
- Learning Videos
- Lab Guide
- Student Guide
- Exam Prep Guide
- Certification Exam
- Two Exam Pass Attempts

Cybersecurity Lab (Sample)

Lab Setup for Training Ethical Hacking / Penetration Testing / Threat Intelegence / Digital Forensic / Cloud Security / Incident Handling / SIEM



ITEM NO.	TOOLS DETAILS
1)	Nessus Vulnerability Scanner
2)	OpenVAS Vulnerability Management Tool
3)	Nikto Web server Vulnerability Scanner
4)	Exploit DB Script
5)	Cobalt Strike Advisory Simulations & Red Team operation
6)	BC Security
7)	Maltago OSNIT Tolls
8)	Splunk Tool
9)	ELK Stack
10)	Burp Suite
11)	Palo Alto Network

Lab Provision: The university or college must provide one dedicated lab for the setup and operation of the cybersecurity tools and infrastructure.

Tool Installation: SecuritySkool will install all the required tools and software in the designated lab.

Lab Design: SecuritySkool will design and configure the lab according to the specific subject domain and training requirements.

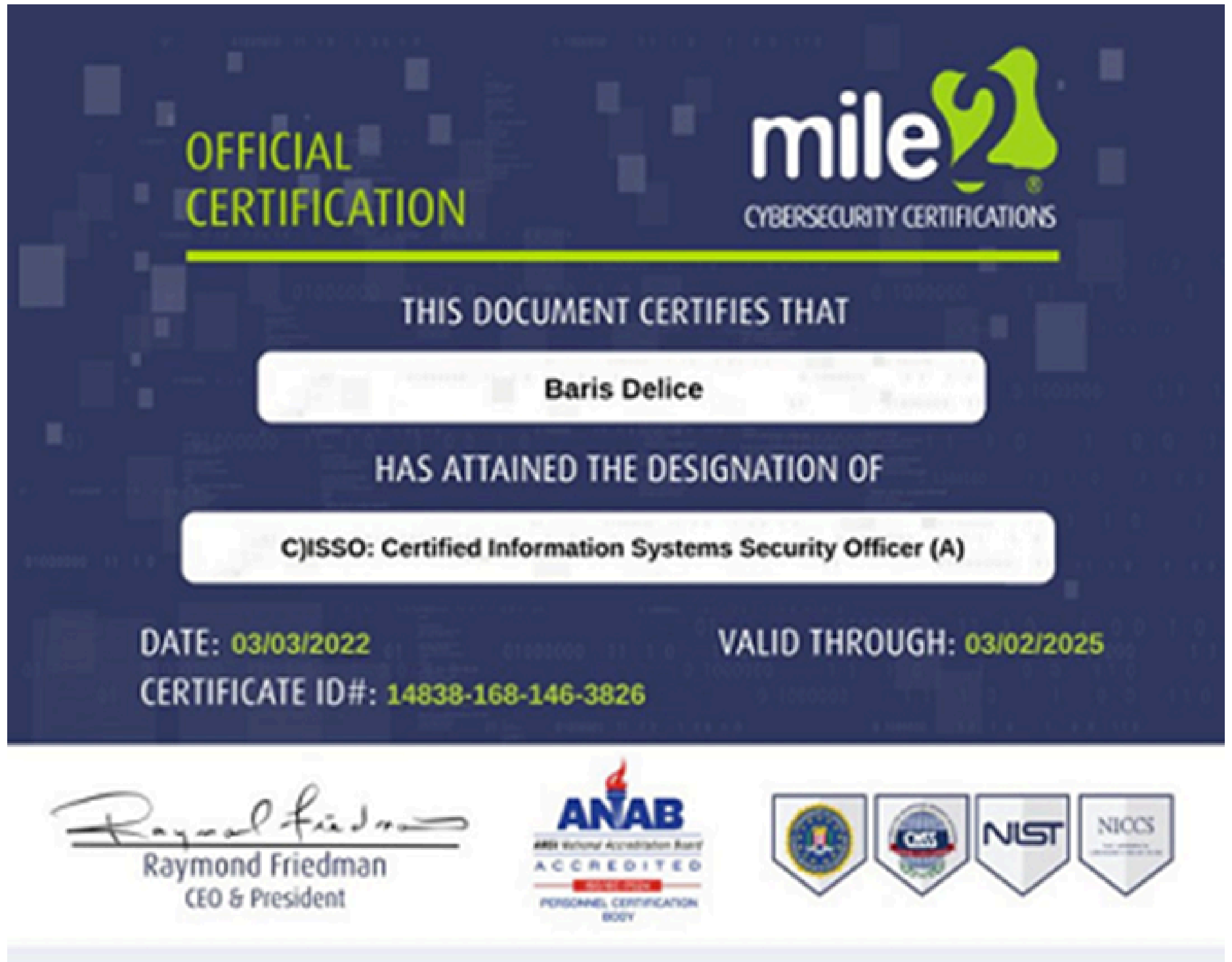
Internet Connectivity: The university must provide a 100 Mbps internet connection to ensure seamless operation of the lab.

Hardware Requirements: The university must supply hardware with the following specifications: Processor: Intel i5, 9th Generation or higher. RAM: 16 GB or higher

Additional Costs: SecuritySkool reserves the right to charge additional fees for any tools, software, or services beyond the initially agreed scope.

Maintenance: SecuritySkool will manage the routine maintenance of the lab to ensure optimal performance and uptime.

Mile2 Sample Certificate



OFFICIAL CERTIFICATION

mile2 CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT

Baris Delice

HAS ATTAINED THE DESIGNATION OF

C)ISSO: Certified Information Systems Security Officer (A)

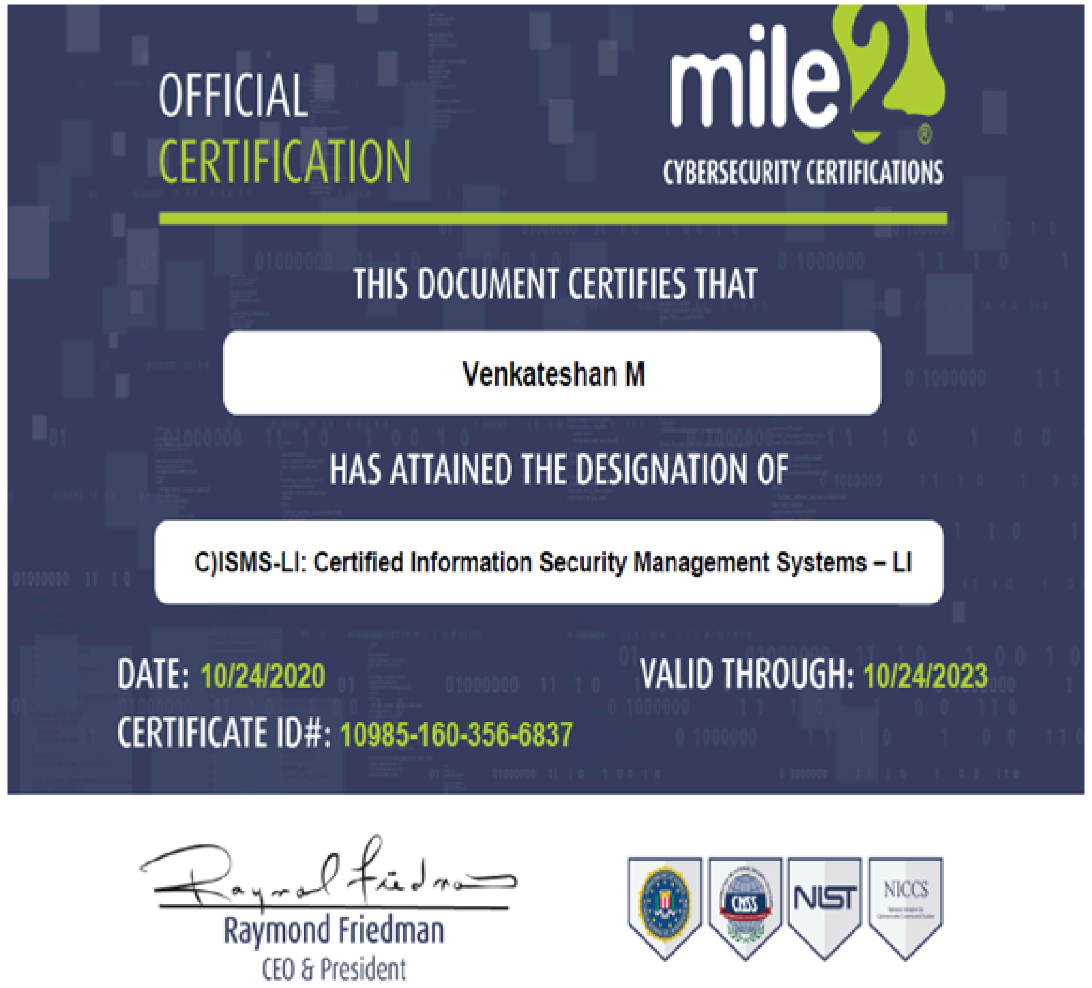
DATE: 03/03/2022 VALID THROUGH: 03/02/2025

CERTIFICATE ID#: 14838-168-146-3826

Raymond Friedman
CEO & President

ANAB ACCREDITED

NIST NICCS



OFFICIAL CERTIFICATION

mile2 CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT

Venkateshan M

HAS ATTAINED THE DESIGNATION OF

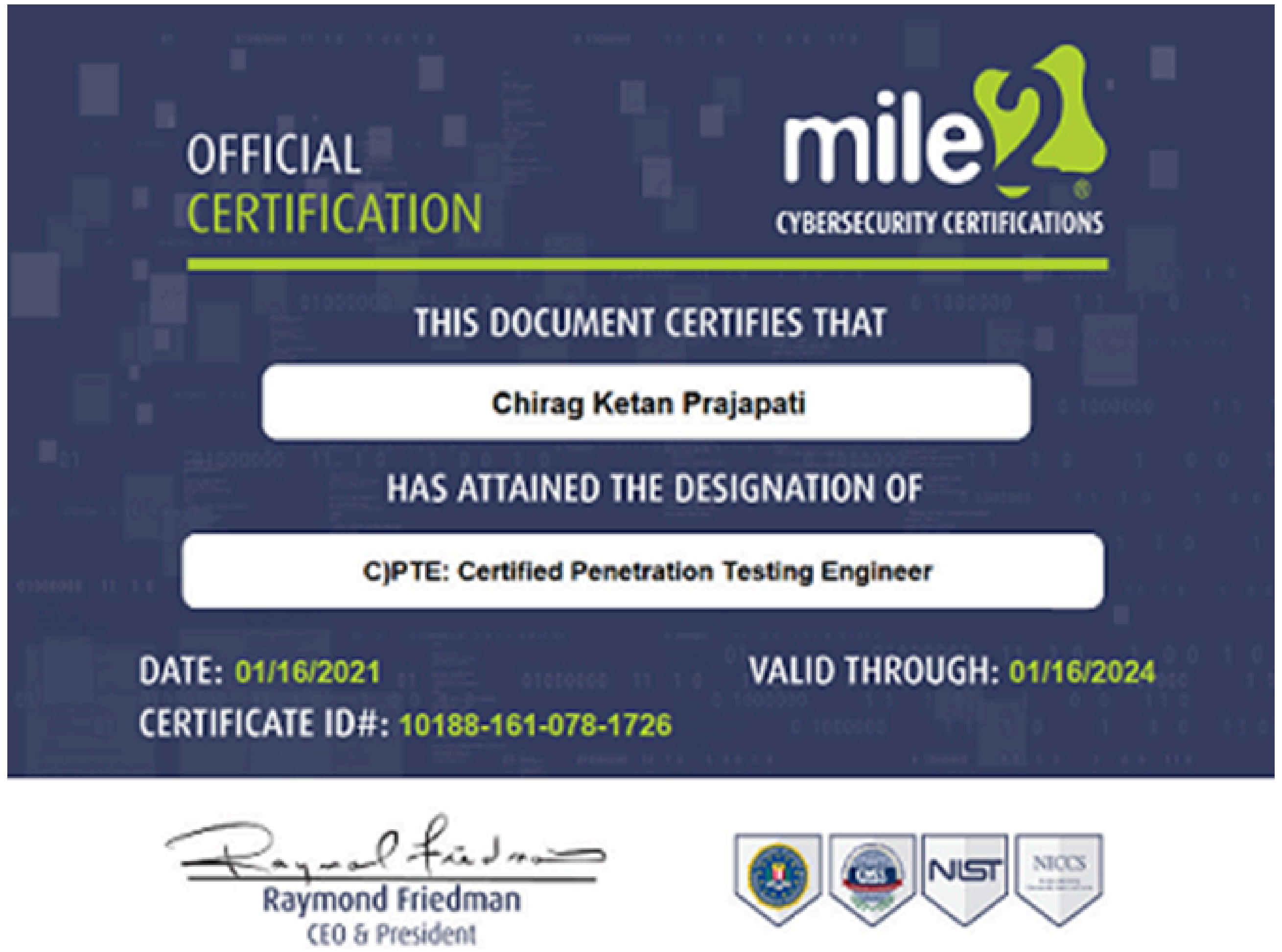
C)ISMS-LI: Certified Information Security Management Systems – LI

DATE: 10/24/2020 VALID THROUGH: 10/24/2023

CERTIFICATE ID#: 10985-160-356-6837

Raymond Friedman
CEO & President

NIST NICCS



OFFICIAL CERTIFICATION

mile2 CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT

Chirag Ketan Prajapati

HAS ATTAINED THE DESIGNATION OF

C)PTE: Certified Penetration Testing Engineer

DATE: 01/16/2021 VALID THROUGH: 01/16/2024

CERTIFICATE ID#: 10188-161-078-1726

Raymond Friedman
CEO & President

NIST NICCS

SecuritySkool

THANK YOU

mile2 AUTHORIZED TRAINING CENTER
Cyber Security Certifications

SecuritySkool