NICE FRAMEWORK SUCCESS STORY
Q-Mission®

The voluntary [Workforce Framework for Cybersecurity](#) (NICE Framework) was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE

Q-Mission® Corp. is a Florida-based, tech innovator that generates cybersecurity readiness for governments and organizations through cybersecurity workforce development.

Q-Mission's unique approach to cybersecurity readiness focuses on the human element of cybersecurity by providing role-based, experiential training in a multipurpose cybersecurity ecosystem where learners can gain the skills and knowledge necessary to be successful in today's ever-changing cybersecurity landscape. This approach has been proven successful in military cyber-force development in Latin America and is now being applied to other industries and organizations in Latin America and the United States.

Q-Mission's primary product is an immersive, experiential education and training platform that provides a safe, realistic environment to conduct exercises, measure skills, and enable continuous learning to develop a more knowledgeable, capable, and confident cybersecurity workforce.

TIE-IN WITH THE NICE FRAMEWORK

The NICE framework's structure and categorization were instrumental in building our role-based training paths. Its granularity provided a comprehensive guide to help identify the specific training and development requirements for each position within a cyber defense team.

This also allowed our training programs to align with international academic mobility education, training, and development frameworks.

DRIVERS

The increasing call for operational cybersecurity talent in the region demanded the development of a performance-based training model to expedite the time to market for students, trainees, and candidates in an environment where:

- Academia-provided talent is scarce,
- Qualified task performance is crucial to operational readiness, and
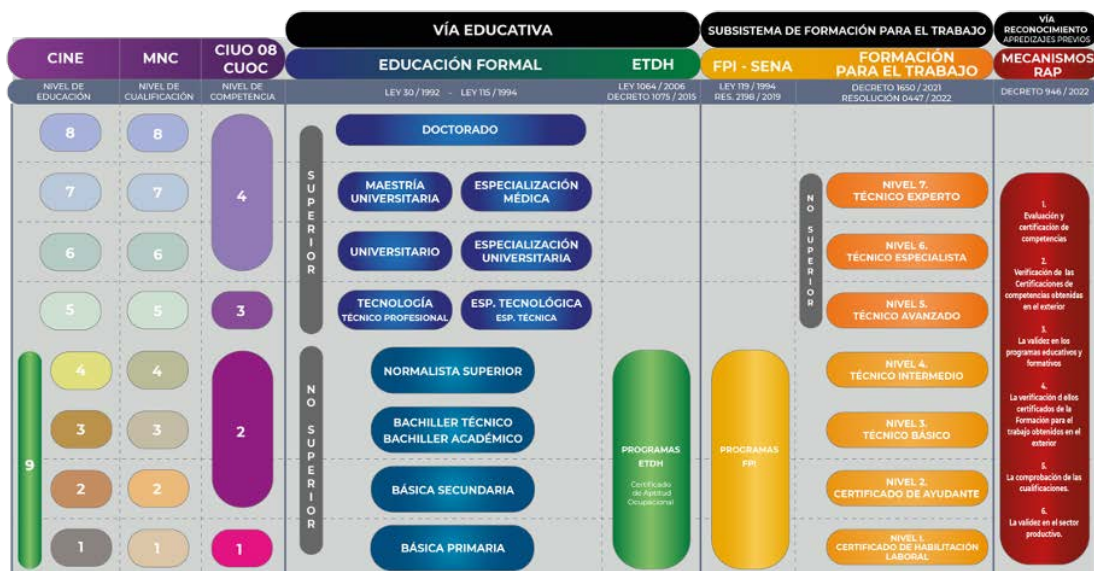- Cybersecurity and defense teams require multidisciplinary role orchestration.

Figure 1: International Qualification Framework

As cybersecurity competence assessment, skilling, re-skilling, and up-skilling have become fundamental for individuals to stay up to date with the rapidly evolving trends and technologies for cybersecurity, our approach ensures that the workforce is equipped with the necessary skills and knowledge to meet the current and future needs of the industry.

PROCESS

We initiated the development of our platform by defining a holistic cyber defense team, as shown in Figure 2.

We extracted core NICE Framework Task statements within the relevant NICE Framework Work Role categories:

- Analyze (Analyst)
- Collect and Operate (Investigator)
- Securely Provision (Hardener)
- Oversee and Govern (Coordinator)
- Investigate (Monitor)
- Investigate (Hunter)

To ensure our platform is comprehensive and practical, we designed our education and training paths to be aligned with the NICE Framework and the Structure of the Observed Learning Outcome (SOLO) taxonomy. This ensures that our platform is comprehensive and effective in providing the necessary cyber defense training.

BENEFITS & IMPACT

As a result of our workforce development experiences, we are seeing positive career impacts, such as higher salaries, promotions, and career advancement. Students who have received certifications through our NICE Framework-aligned courses are able to demonstrate their knowledge to employers in a way that is immediately recognizable.

NICE Framework-aligned training has had a positive impact on the workplace, as well. Operators are better equipped to protect their organizations from cyberattacks and have more confidence in their abilities. In addition, the training has helped employers to identify and recruit top talent for their cybersecurity needs.
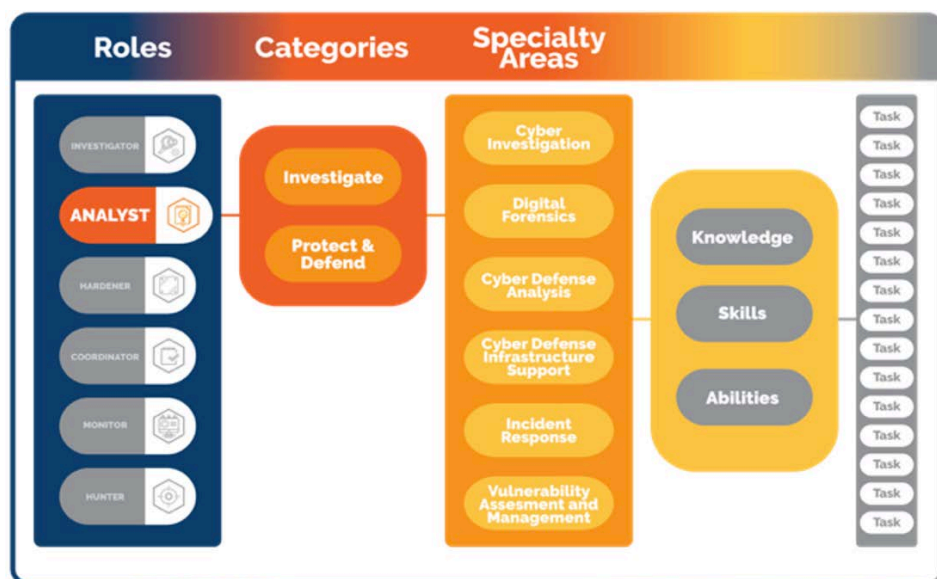

Figure 2: Q-Mission® NICE Framework-Aligned Education and Training

"Human-centric cybersecurity, the right **strategy** executed by the right **people** equipped with the right **tools**."

Alberto L. Roncallo, CEO,
Q-Mission® Corp.

CONTACT INFORMATION & RESOURCES

▸ Alberto L. Roncallo, CEO
alberto.roncallo@qmission.net
▸ www.qmission.net

December 2022