Strategy for Competency-Based Evaluation of Cybersecurity Workforce Proficiency

- Focusing on Cyber Threat Response Personnel -

1. Policy Background and Achievements in Cybersecurity Workforce Development

1.1 2000s: Establishing the Institutional Foundation

In 2000, the **Information Security Industry Promotion Act** was enacted, providing a legal basis for workforce development. Specialized agencies such as KISA and ETRI were designated in 2001, activating education and research programs. A **Comprehensive Plan for Nurturing Information Security Professionals** was established in 2003, supporting the creation of academic programs at universities. By 2003, more than 10 departments had been established, and bachelor's, master's, and doctoral programs were launched, forming a professional education infrastructure and raising awareness in both enterprises and public institutions.

1.2 2010s: Advancing Professional Expertise

In 2011, the National Cyber Security Center (NCSC) expanded training for public-sector professionals. In 2012, cybersecurity graduate schools were established at KAIST, Korea University, and POSTECH to cultivate high-level researchers. In 2014, "Information Security Specialized Universities" were designated, expanding undergraduate-level security education. The **Core Talent Development Program** was launched in 2017 to nurture industry-tailored talent through academia-industry collaboration. Between 2014 and 2019, more than 5,000 graduates were produced, with increasing placement in leading corporations (e.g., Samsung SDS, LG CNS) and government agencies.

1.3 2020s: Focusing on Emerging Technologies

From 2020 onward, programs began training AI, cloud, and OT security specialists. In 2021, the government announced a **"Plan to Train 100,000 Cybersecurity Professionals"**, expanding the number of specialized universities to 13. Additional initiatives included the **Cybersecurity R&D Talent Development Program** (2022) and the **Cybersecurity Career Development Support Program** (2023). Annual graduates from specialized universities exceeded 2,000, and national competitions were expanded to reinforce hands-on skills. The **Cybersecurity Academy** was launched to provide training for SMEs and public institutions, while security-focused startups grew significantly after 2021.

---

2. Current Workforce Development Status and Limitations

2.1 Educational Landscape

- **Secondary Education**: Gifted education centers, specialized high schools

- **Higher Education**: 8 junior colleges (196 students), 44 universities (5,346 students), 49 graduate schools (1,495 students)
- **Public Sector**: KISA, KISIA, CSTEC, and FSEC programs
- **Private Sector**: KITRI BoB, SK Shieldus, KISEC, and 10 other institutions

2.2 Key Limitations

The education system has focused mainly on **quantitative outcomes**, such as the number of graduates and program participants. However, **qualitative outcomes** such as skill proficiency remain unclear. Current curricula emphasize knowledge delivery through lectures, lacking systematic evaluation methods for measuring **real-world competency and proficiency**. A **competency-based and proficiency-oriented framework** is urgently required.

---

3. Competency-Based Cybersecurity Cycle

3.1 Concept

The cycle is structured around **Development** → **Evaluation** → **Management**, ensuring continuous improvement of both technical and role-based competencies.

- **Development**: Customized training programs, hands-on practice, learning content
- **Evaluation**: Competency measurement, diagnostic testing, certification
- **Management**: Performance tracking and improvement methods

3.2 Global Comparison

- **United States**: Since 2010, the NICE Framework has guided federal and private workforce management through integrated policies, laws, and training systems.
- **Europe**: The REWIRE project (since 2021) strengthens ECSF to compete with the U.S. model.
- **Korea**: Currently pursuing K-CSF and K-SDL development (2024–2027) via IITP projects, including cloud-based cyber ranges and training scenario description languages.

---

4. Transition from Knowledge to Skill-Based Development

Cybersecurity personnel must evolve from **knowledge acquisition** to **practical proficiency** through repeated training.

- **Knowledge**: Knowing is insufficient without action.
- **Skills**: Acquired through practice, drills, and simulations.
- **Global Trends**:
  - NICE (2017: T, K, S, A → 2020: T, K, S)
  - ECSF (2022: T, K, S)
    A shift toward **competency and skill-based evaluation** is essential.

---

5. Establishing Professional Competency Standards

5.1 Four Proficiency Levels

- **Basic**: Cybersecurity literacy
- **Low (Entry)**: Ability to perform technical tasks
- **Medium (Intermediate)**: Ability to operate team-level defensive measures
- **High (Advanced)**: Ability to manage organization-wide responses

5.2 Technical Domains

A standardized framework should define 11 domains: **network, security systems, OS security, web security, database security, vulnerability analysis, digital forensics, malware, programming, virtualization, and cloud security**. Training content must be designed for each domain and mapped to proficiency levels.

---

6. Case Study: Proficiency-Based Training and Evaluation

In 2025, KISIA launched an AI security training program with **78 trainees**.

- **Scope**: 15 practice modules across networking, systems, and web security
- **Duration**: 570 minutes total (15 sessions, 30–45 minutes each)
- **Method**: Cloud-based platforms with remote access for exercises and evaluation

Findings revealed **wide differences in learner adaptability and performance**, confirming the feasibility of **proficiency-based competency assessment**.

---

7. Competency Development and Evaluation Framework

7.1 Process

1. **Knowledge Development & Testing**: Online lectures and multiple-choice tests (pre, mid, post)
2. **Skill Development & Testing**: Hands-on training with mission execution and time-based assessment
3. **Certification**: Comprehensive evaluation leading to entry-level professional certification

7.2 Infrastructure

The **K-Cyber Range (K-CR)** system integrates:

- Online learning management (LMS)
- Practice and training scenarios
- Centralized competency measurement and reporting

---

8. Future Directions

- Deliver technical competency reports by domain in a clear, structured format
- Design **customized training pathways** to achieve target proficiency
- Provide **cloud-based evaluation and training services** for individuals and organizations
- Offer **personalized training paths** based on results
- Establish a **quantifiable certification system** recognized by employers and employees, enabling trusted recruitment and workforce mobility

---

Conclusion

Korea’s cybersecurity workforce development has so far prioritized **quantity over quality**, producing graduates but not systematically measuring real-world proficiency. Moving forward, a **competency-based and proficiency-driven model** is needed to enhance national resilience. By leveraging K-CSF and K-CR, Korea can establish a **structured framework for evaluation, certification, and continuous improvement**, ensuring effective preparation against evolving cyber threats.