Cybersecurity Practitioner Badge

The Cybersecurity Practitioner badge recognizes the those with foundational knowledge and hands-on skills in cybersecurity aligned with the CompTIA Security+ certification. It demonstrates that the individuals know how to configure and troubleshoot network protocol issues, analyze and mitigate security threats, perform risk assessments, and apply encryption tools and authentication services commonly used in enterprise environments.

This is a stand-alone foundational badge, serving as an ideal first step for individuals beginning their cybersecurity career pathway. It can also serve as a foundation to more advanced micro-credentials or certifications, such as CompTIA Security+, Cybersecurity Analyst (CySA+), or specialized tracks in network defense, cloud security, and digital forensics.

Competencies below are adapted to explicitly align with NACE Career Readiness Competencies: Critical Thinking, Technology, Professionalism, Teamwork, Equity & Inclusion, Communication, Leadership, and Career & Self-Development. Participants must receive at least 80% passing grades of all assignments or assessments to be eligible for this badge. All competencies must be rated at the Competent level or higher. Any rating at the Basic level will disqualify the participant from earning the badge.

Competency	**Demonstrated Competency**	**Evidence Required**	**Level: Basic (less than 80%)**	**Level: Competent (between 80% – 90%)**	**Level: Accomplished: at least 90%**
Knowledge & Analysis **NACE Alignment:** • **Critical Thinking** (gathering and analyzing information to make informed decisions) • **Technology** (understanding and applying cybersecurity tools and systems)	Explain common network security threats, vulnerabilities, and mitigation strategies	Hands-on assignments, labs, quizzes, or tests	Identifies a few basic types of threats and vulnerabilities but provides limited explanation or examples. Mitigation strategies are vague or incomplete.	Accurately explains common threats, vulnerabilities, and appropriate mitigation techniques with some real-world examples.	Thoroughly explains diverse and evolving network threats, vulnerabilities, and advanced mitigation strategies with clear examples and industry context.
Assessment & Measurement **NACE Alignment:** • **Critical Thinking** (logical evaluation of information; structured reasoning)	Conduct a formal risk assessment to determine an organization's	Hands-on assignments, labs, quizzes, or tests	Demonstrates partial understanding of risk assessment steps but lacks structure or quantification	Applies a standard risk assessment process to identify and rate key risks using recognized frameworks (e.g., likelihood × impact).	Conducts a comprehensive, documented risk assessment using formal methodologies,

• **Professionalism** (accuracy, accountability, high-quality work)	security risk exposure				presenting prioritized, actionable recommendations.
Design & Planning **NACE Alignment:** • **Technology** (selecting and applying security tools and architecture) • **Critical Thinking** (evaluating appropriate design controls) • **Teamwork** (incorporating shared design decisions used in IT environments)	Implement secure network design principles to strengthen organizational security posture	Hands-on assignments, labs, quizzes, or tests	Identifies some security design concepts but lacks practical application or integration into a full network design.	Designs a secure network architecture applying defense-in-depth and segmentation principles for small to medium environments.	Designs and documents an enterprise-level secure network architecture demonstrating layered security, redundancy, and scalability aligned with industry standards.
Implementation & Maintenance **NACE Alignment:** • **Technology** (configuring and troubleshooting systems) • **Professionalism** (accuracy, reliability, quality of work)	Configure and troubleshoot network protocols on devices to resolve issues and enforce security	Hands-on assignments, labs, quizzes, or tests	Configures basic network protocols but has difficulty diagnosing or resolving issues.	Successfully configures and troubleshoots network protocols (TCP/IP, DNS, DHCP, VLANs) to maintain secure connectivity.	Expertly configures, tests, and optimizes network protocols, applying advanced troubleshooting and secure configuration management practices.
Access Control **NACE Alignment:** • **Technology** (secure authentication systems) • **Equity & Inclusion** (ensuring fair, secure access for all users) • **Professionalism** (integrity in handling sensitive credentials)	Select and deploy enterprise authentication services to enforce strict access control	Hands-on assignments, labs, quizzes, or tests	Demonstrates limited understanding of authentication concepts or misapplies tools.	Configures and manages authentication mechanisms (e.g., RADIUS, LDAP, MFA) to enforce access control in a networked environment.	Designs and deploys enterprise-level authentication and authorization systems integrating identity management, zero-trust, and role-based access control.

Data Protection **NACE Alignment:** • **Technology** (managing encryption tools) • **Professionalism** (protecting confidential information) • **Critical Thinking** (choosing appropriate encryption methods)	Apply and manage encryption and decryption methods using current software tools for data protection	Hands-on assignments, labs, quizzes, or tests	Demonstrates minimal understanding of encryption principles or uses tools incorrectly.	Applies symmetric and asymmetric encryption methods using tools (e.g., OpenSSL, GPG, BitLocker) for data protection.	Implements and manages enterprise-grade encryption solutions across devices, ensuring compliance with current standards.