ADVANCED NETWORK SECURITY: MICRO CREDENTIAL

Develop the ability to analyze and apply defense in depth and network security strategies essential for protecting modern enterprise infrastructures. This program equips participants with the critical competencies required to secure networks against unauthorized access while reinforcing organizational resilience.
Through an integrated curriculum grounded in the adversarial mindset, you will explore the foundational principles of network security and systematically apply them to enterprise- level defense strategies. Practical, hands-on Ethical Hacking exercises will reinforce theoretical knowledge, enabling you to critically assess and strengthen system-wide security architectures.

This program offers a structured pathway for individuals aiming to deepen their expertise in network defense and serves as a strong foundation for continued study in either the M.S. in Cybersecurity or the M.S. in Information Technology degree programs. The skillset developed is highly applicable across a wide range of roles, including Network Administrator, IT Analyst, Network Engineer, Penetration Tester, Ethical Hacker, and Cybersecurity Analyst.
Successful completion of this micro-credential formally recognizes your advanced capabilities in network defense making it an asset for industry professionals with a bachelor's degree seeking career progression or leadership roles in cybersecurity and information technology.

The required courses and suggested sequence are as follows:

Code	Title	Credits
INFT 6065	Ethical Hacking and Network Defense	3
INFT 6132	Network Administration	3
INFT 6137	Enterprise Systems Architecture	3
Total Credits		**9**

Upon successful completion of this program, students should be able to:

- Explain the fundamentals of network security.
- Describe the ethical implications of penetration testing and vulnerability analysis.
- Demonstrate network protection strategies and system architectures.