Vulnerability Assessment Analyst

NICE Framework Reference	Protect and Defend, PR-VAM-001, Vulnerability Assessment (VA) Analyst	
Functional Description	Scans applications and operating systems to identify flaws, and vulnerabilities; and conducts and presents vulnerability assessments on an organization's networks and systems.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is often a tier 2 position within a cybersecurity operations environment that is normally preceded by 2-3 years in a network or operational security role. This can lead to increased specialization as a vulnerability analyst, red/blue team leader, penetration tester or management roles.	
Other titles	▪ Vulnerability tester ▪ Vulnerability assessor ▪ Vulnerability assessment manager	
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers	
Tasks	▪ Identify critical flaws in applications and systems that cyber actors could exploit ▪ Conduct vulnerability assessments of relevant technology (e.g., computing environment, network and supporting infrastructure, and applications) ▪ Prepare and present comprehensive vulnerability assessments; ▪ Conduct network security audits and scanning ▪ Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense operations ▪ Prepare audit reports that identify technical and procedural findings, and make recommendations on corrective strategies and solutions ▪ Conduct and/or support authorized penetration testing on organization networks and systems ▪ Define and review requirements for information security solutions ▪ Make recommendations on the selection of cost-effective security controls to mitigate risks ▪ Develop, deliver, and oversee training material and educational efforts	
Required qualifications	Education	Post-secondary education (degree or diploma) in related computer science or IT field.
	Training	Training in cybersecurity systems, vulnerability assessment and analysis. Vendor-based vulnerability system training.
	Work experience	2 – 3 years in a network or cybersecurity operations role.
Tools & Technology	▪ Organizational security policies, procedures and practices ▪ VA tools ▪ Vulnerability management policies, processes and practices	

	▪ Common vulnerability databases
Competencies	KSAs applied at the basic level: ☐ Advanced threat actor tools, techniques and protocols ☐ Penetration testing principles, tools, and techniques ☐ Risk management processes for assessing and mitigating risks ☐ System administration concepts ☐ Cryptography and cryptographic key management concepts ☐ Cryptology ☐ Identifying security issues based on the analysis of vulnerability and configuration data ☐ Vulnerability management policies, processes and practices KSAs applied at an advanced level: ☐ VA planning and scheduling including system risks and mitigations ☐ System and application security threats and vulnerabilities ☐ System administration, network, and operating system hardening techniques ☐ Packet analysis using appropriate tools ☐ Conducting vulnerability scans and recognizing vulnerabilities in security systems ☐ Conducting vulnerability/impact/risk assessments ☐ Reviewing system logs to identify evidence of past intrusions ☐ Using network analysis tools to identify vulnerabilities
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of ‘bring your own device’ (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.