Cybersecurity Operations Technician

NICE Framework Reference	Protect and Defend, PR-INF-001, Cybersecurity Defence Infrastructure Support	
Functional Description	Tests, implements, deploys, maintains, and administers the security operations infrastructure hardware and software.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in security system failure or system compromise which may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is an often an entry-level job to the security domain after gained experience in technical, network administrative, or other similar functions. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Security infrastructure support specialist/technician ▪ Security systems analyst ▪ Security systems technician ▪ Security control analyst	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Actively monitor security system performance, troubleshoot and resolve hardware or software interoperability issues, and system outages and faults ▪ Install, configure, and maintain security system software, hardware, and peripheral equipment ▪ Develop, conduct, and maintain incident reports and vulnerability and impact assessments ▪ Develop and maintain tracking and solution database ▪ Analyze and recommend improvements and changes to support improved security operations ▪ Audit, log and report life-cycle management activities ▪ Administer security system accounts, privileges, and access to systems and equipment ▪ Conduct asset management or inventory control of system and equipment resources ▪ 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, security systems operations and vendor-based tools (e.g. intrusion detection systems, firewalls, anti-virus, incident management, etc.)
	Work experience	2 – 3 years in network operations and security
Tools & Technology	▪ Cybersecurity systems tools, logs, and procedures ▪ Organizational policies and directives ▪ Security event and incident management systems and/or incident reporting systems and networks	

Competencies	KSAs applied at the basic level: ☐ Threats to information systems and their security ☐ Network security architecture concepts, protocols, components, and principles (e.g., application of defense-in-depth). ☐ Basic system, network, and OS hardening techniques. ☐ Transmission records and modes (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)) ☐ Network traffic analysis (tools, methodologies, processes) ☐ Identity, credential and access management architectures and standards ☐ Cybersecurity incident management policy, procedures and practices ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Cybersecurity systems test procedures, principles, and methodologies ☐ Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications ☐ Install, configure, operate, maintain and monitor related applications ☐ Cybersecurity infrastructure troubleshooting, analysis and remediation ☐ Cybersecurity systems policies, account management and controls
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 cybersecurity systems management. ▪ 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 identity and access management processes and the related technical and process changes. ▪ 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 as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.