Cybersecurity Operations Analyst

Note: This role includes the following:

Tier I Analyst - Cybersecurity Operations Analyst

Tier II Analyst - Malware specialist

Tier III Analyst - Threat hunter: management and active defence

NICE Framework Reference	Protect and Defend, Cyber Defence Analyst, PR-CDA-001
Functional Description	Front-line cybersecurity operations center operator responsible for monitoring and maintaining IT security devices and is often responsible for initial detection, incident response and mitigation
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.
Development pathway	This is a common entry-level job within the security operations centre (SOC). With additional training and experience there is potential for more technically or operationally focused roles in cybersecurity operations (e.g. vulnerability assessment & management, digital forensics, threat analytics and malware analysis) as well as management opportunities. Note that Tier II and Tier III roles may require more extensive training and education in addition to relevant experience. Often a computer science or computer engineering degree is a pre-requisite given the level of knowledge and skill required in more complex tasks. However, there are many that have progressed from cybersecurity analyst positions to advanced cybersecurity roles without a related degree.
Other titles	▪ SOC Operator ▪ Cybersecurity Operator ▪ Infrastructure Security Analyst ▪ Network Security Analyst ▪ Network Security Administrator ▪ Data security analyst
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	▪ Identify and analyze technical threats to, and vulnerabilities of, networks ▪ Identify, contain, conduct initial mitigations and report system compromises ▪ Review, analyze, and/or apply internet security protocols, cryptographic algorithms, directory standards, networking protocols, network hardening, technical IT security controls, IT security tools and techniques, OS, intrusion detection/protection systems, firewalls, routers, multiplexers and switches, and wireless devices ▪ Analyze security data and provide alerts, advisories and reports ▪ Install, configure, integrate, adjust, operate, monitor performance, and detect faults on security devices and systems ▪ Conduct impact analysis for new software implementations, major configuration changes and patch management ▪ Develop proof-of-concept models and trials for IT security products and services ▪ Troubleshoot security products and incidents

<table>
<tr><td></td><td colspan="2">▪ Design/develop IT Security protocols
▪ Complete tasks related to authorization and authentication in physical and logical environments
▪ Develop options and solutions to meet the security-related project objectives
▪ Identify the security products and its configuration to meet security-related project objectives
▪ Implement and test configuration specifications
▪ Develop configuration and operational build books
▪ Review, develop and deliver relevant training material</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>College diploma in IT field with specialization in IT/cybersecurity, network security or similar.</td></tr>
<tr><td>Training</td><td>Cybersecurity operations training with industry-level certification in related field (e.g. security operations, network security, threat detection and mitigation, security appliance operations). More advanced training required for Tier II and III analysts.</td></tr>
<tr><td>Work experience</td><td>Initial experiential requirement is to have been successful working in an IT environment and technical team setting.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Incident management processes and procedures
▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
▪ Security event and incident management systems and/or incident reporting systems and networks</td></tr>
<tr><td>Competencies</td><td colspan="2">In larger SOCs there may be the opportunity to progress from Tier 1 to Tier 2 analyst. Tier 3 analysts are rare and almost exclusively employed in national security and military contexts. The required competencies for Tier 1 and 2 are provided below.

For Tier 1 - Cybersecurity Operations Analyst

The following KSA are applied at a basic level:
☐ Network security administration and management
☐ Network security architecture
☐ Hardware and firmware security
☐ Software defined security and application security
☐ Virtualization and Virtual Private Network (VPN) security
☐ Cloud-based security
☐ Wireless/mobile device security
☐ IT security zoning
☐ Encryption and cryptography including key management concepts and principles
☐ Vulnerability scanning and analysis
☐ Vulnerability management tools, processes and procedures
☐ Web application security
☐ Configuration and operational build books
☐ System acquisitions and projects
☐ Legal and ethical responsibilities associated with cybersecurity operations including conduct of investigations, privacy, and preservation of evidence
☐ Writing and briefing on technical matters (e.g. incident reports, technical reports, etc.) for managerial level understanding</td></tr>
</table>

	The following KSA are applied at an advanced level: ☐ Network security appliance concepts, operation and configuration (equipment specific based on role - network, server and desktop cyber defence systems and/or appliances) ☐ Types of intrusions and indicators of compromise (IoCs) ☐ Sources of threat information ☐ Common threat actor tactics, techniques, and procedures (TTPs) ☐ Incident management processes, responsibilities and authorities ☐ Intrusion detection and prevention methodologies, tools and systems ☐ Intrusion analysis and mitigation techniques ☐ Basic malware analysis **For Tier II Analyst - Malware specialist** The following KSA are applied at an advanced level. All of the above plus: ☐ Persistent and sophisticated threat TTPs ☐ Cyber defence tools, techniques and procedures ☐ Development and testing of network security appliances (including scripts and coding). ☐ Advanced malware analysis and reverse malware engineering ☐ Implementing advance security controls in response to advanced persistent threats ☐ Advanced incident response and recovery activities **For Tier III Analyst - Threat hunter: management and active defence** The following KSA are applied at an advanced level: ☐ Advanced threat management ☐ Advanced threat actor TTPs including specialization of persistent threat actors (e.g. nation state, organized crime) ☐ Interpreting/synthesizing classified / sensitive threat intelligence from multiple sources ☐ Legal and ethical responsibilities associated with active defence techniques ☐ Exploitation analysis ☐ Threat hunting and active defence frameworks ☐ Developing complex courses of action including risk assessment and mitigation plan ☐ Active defence tactics, tools and procedures including advanced threat countermeasures and counter-countermeasures ☐ Adversarial thinking ☐ Developing, testing and deploying technical tools within an active defence framework to protect organizational information and systems at risk
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 as well as threat actor tools, techniques and protocols related to quantum computing attacks and how to defend against them.