Cybersecurity Incident Responder

OT incident responder

NICE Framework Reference	Protect and Defend, Cyber Defence Incident Responder, PR-CIR-001
Functional Description	Provides immediate and detailed response activities to mitigate or limit unauthorized cybersecurity threats and incidents within an organization. This includes planning and developing courses of action; prioritizing activities; and supporting recovery operations and post-incident analysis.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in catastrophic failure of organizational IT and data systems and associated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 such as vulnerability assessment & management, digital forensics, threat analytics and malware analysis.) as well as management opportunities.
Other titles	▪ Cybersecurity incident responder ▪ Security Operations Centre - Incident handler ▪ Cybersecurity first responder ▪ Operational technology security incident responder
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers
Tasks	These tasks apply equally to IT and OT systems. ▪ Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) ▪ Conduct security triage to identify and analyze cyber incidents and threats ▪ Actively monitor networks and systems for cyber incidents and threats ▪ Conduct risk analysis and security reviews of system logs to identify possible cyber threats ▪ Conduct analysis and review, and/or apply network scanners, vulnerability assessment tools, network protocols, internet security protocols, intrusion detection systems, firewalls, content checkers and endpoint software ▪ Collect and analyze data to identify cybersecurity flaws and vulnerabilities and make recommendations that enable prompt remediation ▪ Develop and prepare cyber defence incident analysis and reporting ▪ Define and maintain tool sets and procedures ▪ Develop, implement, and evaluate prevention and incident response plans and activities, and adapt to contain, mitigate or eradicate effects of cybersecurity incident ▪ Provide incident analysis support on response plans and activities ▪ Conduct research and development on cybersecurity incidents and mitigations ▪ Create a program development plan that includes security gap assessments, policies, procedures, playbooks, and training manuals ▪ Review, develop and deliver relevant training material

<table>
<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).

Specialized training required for Operational Technology and related systems.</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">Cybersecurity Incident Responder
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 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
☐ Business continuity and disaster response basics

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
☐ Cybersecurity investigations and evidence preservation</td></tr>
</table>

	For Operational Technology Incident Responder In addition to the relevant KSAs above, the follow applied at the basic level: ☐ OT systems software and hardware, programmable logic controllers, and digital and analog relaying ☐ Threat and risk assessment to internet connected OT (including implications and assessment of IoT devices) ☐ Legal and compliance requirements including organizational responsibilities for workplace and public safety related to OT/ production ☐ Telemetry systems, data communications, data acquisition and process control ☐ Operating systems, networking, and communications systems concepts ☐ Electrical distribution networks, power system equipment, transformer station operation and electrical theory ☐ Database management systems and applications ☐ Measures or indicators of OT system performance, availability, capacity, or configuration problems ☐ Analysis tools and network protocols ☐ Diagnostic tools and fault identification techniques
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.