Security Automation Engineer/Analyst

NOTE: *This is an emerging work role. There are limited samples of this work role and subject matter expert tasks and activities vary based on organizational requirements. Accordingly, the information below is based upon current representations based on demand driven requirements and an understanding of artificial intelligence, machine learning and data science requirements to support automated process engineering and analysis. It is anticipated that this will evolve significantly over the next years.*

NICE Framework Reference	None.
Functional Description	Given references, organizational security documentation, IT security guidance and required tools and resources researches and defines the business needs for security, identifies requirements for and engineers automated solutions that support organizational security.
Consequence of error or risk	Error, neglect, outdated information or failure to account for organizational requirements, business needs and threats could result in poor systems design and/or integration of systems/devices that create exploitable vulnerabilities which can have significant implications to organizational objectives including the potential for catastrophic systems failure.
Development pathway	Typically follows formal education and 5-10 years' experience in related IT engineering, systems design, or systems integration functions. Additional training, education and/or experience in process automation and related artificial intelligence/machine learning engineering activities.
Other titles	▪ Systems automation engineer ▪ Automated systems designer ▪ Security automation and controls engineer
Related NOCs	2133 Electrical and electronics engineers 2147 Computer engineers (except software engineers and designers) 2173 Software engineers and designers 2241 Electrical and electronics engineering technologists and technician
Tasks	▪ Research, develop, integrate, test and implement security automation solutions for cloud or systems ▪ Scope and plan out automation work to meet timelines ▪ Manage/monitor automated security solution activities including fixes, updates and related processes ▪ Develop and maintain tools and processes to support security automation activities ▪ Review and test security automation scripting prior to implementation ▪ Troubleshoot any issues that arise during testing, production or use ▪ Create, use and maintain resource documentation for reference ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support security automation activities ▪ Review, approve, and oversee changes on cybersecurity policies and controls and their implication for automated activities ▪ Schedule and oversee security assessments and audits ▪ Oversee and manage vendor relations related to acquired IT security products and services ▪ Ensure security requirements are identified for all IT systems throughout their life cycle

<table>
<tr><td></td><td colspan="2">▪ Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
▪ Assess threats and develop countermeasures and risk mitigation strategies against automated system vulnerabilities
▪ Perform risk analysis and testing whenever an automated system undergoes a change
▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Relevant engineering or computer science degree with post graduate training or equivalent in systems automation, artificial learning or machine learning.</td></tr>
<tr><td>Training</td><td>Relevant cybersecurity training to support functions as a security engineer.</td></tr>
<tr><td>Work experience</td><td>Moderate experience (3-5 years) in security and associated systems design, integration, testing and support. Experience in programming and application testing. 2-3 years practical experience in automating system processes.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Threat and risk assessment tools and methodologies
▪ Protective and 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
▪ Authentication software and systems
▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used
▪ Security services provided if applicable
▪ Security testing and evaluation tools and techniques
▪ Process automation tools, techniques and procedures
▪ Applicable programming languages</td></tr>
<tr><td>Competencies</td><td colspan="2">Advanced level of application of the following KSAs:
☐ Process automation within a security setting
☐ API, automation and scripting languages
☐ SDN, NFV, and VNF functions
☐ Security engineering models
☐ Defining and communicating security approaches that support organizational requirements
☐ International security standards and compliance
☐ Security architecture concepts and enterprise architecture reference models
☐ Systems security during integration and configuration
☐ Security assessment and authorization processes
☐ Security testing and evaluation methodologies and processes
☐ Security across the system / software development lifecycle
☐ Vulnerability assessment and penetration testing methodologies and applications
☐ Systems and software testing and evaluation methodologies
☐ Evidence-based security design
☐ Developing and testing threat models
☐ Project management and security assessment throughout the project lifecycle
☐ Procurement processes and supply chain integrity assessments</td></tr>
</table>

	☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)
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 cybersecurity responsibilities relative to organizational cybersecurity risks. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ If automated security tools will be used, testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised / trained on the resulting process and procedural changes. Additionally, as the potential technical lead for security automation, there may be a requirement to educate organizational leaders on the benefits and risks of automation and any change management required. ▪ 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 a significantly better appreciation of threat actor capabilities and potential countermeasures. ▪ 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 be a need for increased understanding of organizational risks posed 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 and understanding of the implications on AI-enabled security mechanisms.