Identity Management & Authentication Support Specialist

NICE Framework Role	None.	
Functional Description	Provides ongoing support to identity, credentials, access and authentication management in support of organizational IT security.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a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 with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials and access management (ICAM) specialist	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Identify client requirements and propose technical solutions ▪ Model and map users to resources (e.g. role based) ▪ Install, configure, operate, maintain and monitor related applications ▪ Deploy, configure and manage user provisioning including identity synchronization, auto-provisioning and automatic access deactivation, self-service security request approvals workflow and consolidated reporting ▪ Configure and manage enterprise and web-based access management solutions (single sign on, password management, authentication & authorization, delegated administration) ▪ Analyze patterns or trends in incidents for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	College diploma in IT field.
	Training	Training in relevant identity, credentials, access management and authentication policies, protocols, tools and procedures. Developing and applying user credential management system.
	Work experience	Experience in managing directory services and working in a security environment.

Tools & Technology	▪ Identity and access management systems ▪ Directory services ▪ Authentication tools and services ▪ Security event and incident management systems and/or incident reporting systems and networks
Competencies	KSAs applied at the basic level: ☐ Identity, credential and access management architectures and standards ☐ Related application life-cycle processes ☐ Mapping and modeling credentials ☐ Policy-based and risk-adaptive access controls ☐ Developing and applying user credential management system ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution KSAs applied at an advanced level: ☐ Network access, identity, and access management protocols, tools and procedures ☐ Authentication, authorization, and access control methods ☐ Install, configure, operate, maintain and monitor related applications ☐ Developing and applying security system access controls. ☐ Maintaining directory services ☐ Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
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 a deep understanding of the implications to authentication protocols and how to defend against potential quantum computing threats.