

Role Description

Lead Cyber Intelligence Analyst

Cluster	Education
Agency	NSW Department of Education
Division/Branch/Unit	Information Technology Directorate
Role number	236764
Classification/Grade/Band	Clerk Grade 9/10
Senior executive work level standards	Not Applicable
ANZSCO Code	223111
PCAT Code	2224992
Date of Approval	February 2022
Agency Website	https://education.nsw.gov.au/

Agency overview

The NSW Department of Education serves the community by providing world-class education for students of all ages. We ensure young children get the best start in life by supporting and regulating the early childhood education sector. We are the largest provider of public education in Australia with responsibility for delivering high-quality public education to two-thirds of the NSW student population. We are committed to fostering vibrant, sustainable and high-performing vocational and higher education sectors.

We are responsible for enacting NSW Government policy, driving improvement in education, and overseeing policy, funding and compliance issues relating to non-government schools. We respect and value Aboriginal and Torres Strait Islander people as First Peoples of Australia.

Primary purpose of the role

The Lead Cyber Intelligence Analyst is responsible for leading the intelligence methodologies to monitor, assess and report on the cyber threat landscape. The role supports the Department's response to cyber security issues and contributes to strengthening the Department's cyber security posture through the provision of advice on IT security, information security threats, risks and information security incidents.

Key accountabilities

- Lead the creation of actionable intelligence reports for audiences across technical, risk and business leadership, informing them of the risk to the organisation.
- Use analysis tactics, techniques and procedures (TTPs) of threats to the government to determine attribution, motivation and capability.
- Prepare Indicators of Compromise (IoC) reports, detailing new and modified TTPs being used, what IoCs exist and recommendations to ITD teams to reduce the likelihood of attacks.
- Respond to requests for ad-hoc reporting and research topics from management and analysts as required.
- Identify gaps in available intelligence information and engages with leadership on strategies to meet intelligence requirements through Intelligence collection processes.

- Work collaboratively with internal and external stakeholders and vendors to monitor, detect, report and share cyber vulnerabilities, incidents, threats and trends.
- Contribute technical expertise and knowledge to reporting on current and emerging cyber security risks and trends.

Key challenges

- Maintaining up-to-date knowledge and understanding of current and the future NSW cyber security environment including threats and vulnerabilities to information, assets and services.
- Developing and maintaining positive stakeholder relationships to ensure oversight and value to cluster agencies from a cyber-security perspective.
- Delivering multiple cyber intelligence assessments, in line with agreed standards and objectives, given tight deadlines and competing demands and priorities

Key relationships

Who	Why
Internal	
Manager	<ul style="list-style-type: none"> • Escalate issues, keep informed, advise and receive instructions • Report on projects, issues, products and systems
Work team	<ul style="list-style-type: none"> • Work collaboratively to achieve the organisation's business goals • Participate in meetings to obtain the work group perspective and share information
Clients/ customers	<ul style="list-style-type: none"> • Resolve and provide solutions to issues • Guide and inform user population regarding relevant security practices and processes
External	
Stakeholders/ Industry Professionals	<ul style="list-style-type: none"> • Develop and maintain effective working relationships and open channels of communication to ensure relevant information is shared • Consult, provide and obtain information to stay informed on developing industry trends • Address/respond to queries where possible, or redirect relevant party for review and resolution • Manage the flow of information, seek clarification and provide advice and responses to ensure prompt resolution of issues • Participate in forums, groups to represent the agency and share information • Participate in discussions regarding innovation and best practice
Vendors/Service Providers	<ul style="list-style-type: none"> • Assist in the management of contracts and monitor provision of service to ensure compliance with contracts and service arrangements • Contact to provide and gather information and resolve routine issues

Role dimensions

Decision making

This role is responsible for delivering intelligence and reporting on cyber security threats that are under their direct control and leading the triage of incoming requests. They refer to their Manager, decisions that require significant change to program outcomes or time frames or are likely to escalate or require submission to a higher level of management.

Reporting line

Manager Service Monitoring & Events

Direct reports

This role will have up to 5 direct reports

Budget/Expenditure

Nil

Key knowledge and experience

- Lead the alert detection capabilities from a Security Information and Event Management (SIEM) Splunk Enterprise Security (ES).
- Ability to communicate technical information in a non-technical way to brief senior personnel and executives on threats, vulnerabilities and cyber security breaches
- Strong understanding of threat analysis and enterprise level, mitigation strategies.
- Knowledge of, and commitment to implementing the Department's Aboriginal Education Policy and upholding the Department's Partnership Agreement with the NSW AECG and to ensure quality outcomes for Aboriginal people.

Essential requirements

- The successful applicant may be required to undergo a security clearance to the level of Negative Vetting 1 (NV1)

Capabilities for the role

The [NSW public sector capability framework](#) describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for roles with managerial responsibilities. These groups, combined with capabilities drawn from occupation-specific capability sets where relevant, work together to provide an understanding of the capabilities needed for the role.

The capabilities are separated into **focus capabilities** and **complementary capabilities**.

Focus capabilities

Focus capabilities are the capabilities considered the most important for effective performance of the role. These capabilities will be assessed at recruitment.

The focus capabilities for this role are shown below with a brief explanation of what each capability covers and the indicators describing the types of behaviours expected at each level.

FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
 Personal Attributes	Display Resilience and Courage Be open and honest, prepared to express your views, and willing to accept and commit to change	<ul style="list-style-type: none"> • Be flexible and adaptable and respond quickly when situations change • Offer own opinion and raise challenging issues • Listen when ideas are challenged and respond appropriately • Work through challenges • Remain calm and focused in challenging situations 	Intermediate
 Relationships	Commit to Customer Service Provide customer-focused services in line with public sector and organisational objectives	<ul style="list-style-type: none"> • Focus on providing a positive customer experience • Support a customer-focused culture in the organisation • Demonstrate a thorough knowledge of the services provided and relay this knowledge to customers • Identify and respond quickly to customer needs • Consider customer service requirements and develop solutions to meet needs • Resolve complex customer issues and needs • Cooperate across work areas to improve outcomes for customers 	Intermediate
 Results	Think and Solve Problems Think, analyse and consider the broader context to develop practical solutions	<ul style="list-style-type: none"> • Research and apply critical-thinking techniques in analysing information, identify interrelationships and make recommendations based on relevant evidence • Anticipate, identify and address issues and potential problems that may have an impact on organisational objectives and the user experience • Apply creative-thinking techniques to generate new ideas and options to address issues and improve the user experience • Seek contributions and ideas from people with diverse backgrounds and experience • Participate in and contribute to team or unit initiatives to resolve common issues or barriers to effectiveness • Identify and share business process improvements to enhance effectiveness 	Adept
	Technology Understand and use available technologies to maximise efficiencies and effectiveness	<ul style="list-style-type: none"> • Identify opportunities to use a broad range of technologies to collaborate • Monitor compliance with cyber security and the use of technology policies 	Adept



- Identify ways to maximise the value of available technology to achieve business strategies and outcomes
- Monitor compliance with the organisation's records, information and knowledge management requirements


Project Management

Understand and apply effective planning, coordination and control methods

- Perform basic research and analysis to inform and support the achievement of project deliverables
- Contribute to developing project documentation and resource estimates
- Contribute to reviews of progress, outcomes and future improvements
- Identify and escalate possible variances from project plans

Intermediate

Occupation specific capability set



Category	sub-category and skill	Level and Code
	Strategy & Architecture	Information Strategy: Information Security
	Relationships & Engagement	Stakeholder Mgmt: Relationship Management
	Strategy & Architecture	Business Strategy & Planning: Demand Management
		Level 6 - SCTY
		Level 6 - RLMT
		Level 6 - DEMM



Complementary capabilities

Complementary capabilities are also identified from the Capability Framework and relevant occupation-specific capability sets. They are important to identifying performance required for the role and development opportunities.

Note: capabilities listed as 'not essential' for this role are not relevant for recruitment purposes however may be relevant for future career development.

COMPLEMENTARY CAPABILITIES

Capability group/sets	Capability name	Description	Level
 Personal Attributes	Act with Integrity	Be ethical and professional, and uphold and promote the public sector values	Intermediate
	Manage Self	Show drive and motivation, an ability to self-reflect and a commitment to learning	Advanced
	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Adept
 Relationships	Communicate Effectively	Communicate clearly, actively listen to others, and respond with understanding and respect	Adept
	Work Collaboratively	Collaborate with others and value their contribution	Advanced
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Intermediate

	Deliver Results	Achieve results through the efficient use of resources and a commitment to quality outcomes	Intermediate
	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Intermediate
	Demonstrate Accountability	Be proactive and responsible for own actions, and adhere to legislation, policy and guidelines	Adept
	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Intermediate
	Procurement and Contract Management	Understand and apply procurement processes to ensure effective purchasing and contract performance	Intermediate

Occupation specific capability set (Skills Framework for the Information Age – SFIA)

Category and Sub-category		Level and Code	Level descriptions
Strategy and Architecture – Information Strategy – Information Security		SCTY – Level 6	Develops and communicates corporate information security policy, standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks. Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with experts in other functions e.g. legal, technical support. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines.
	Relationships & Engagement - Stakeholder Mgmt - Relationship Management	RLMT – Level 6	Builds long-term, strategic relationships with senior stakeholders in the largest client organisations (internal or external). Acts as a single point of contact and facilitates access to colleagues and subject experts. Maintains a strong understanding of clients' industry and business, assists clients in the formation of IT strategies, and acts to ensure that they are offered products and services aligned to these strategies. Negotiates at senior level on technical and commercial issues. Influences the development and enhancement of services, products and systems, and oversees the management and planning of business opportunities. Oversees monitoring of relationships and acts on relevant feedback.
	Strategy and Architecture – Business Strategy & Planning - Demand Management	DEMM – Level 6	Defines the approach and sets policies for the discovery, analysis, planning, controlling and documentation of demand for services and products. Organises scoping and business priority setting for strategic business changes involving business policy-makers and direction setters. Engages with and influences senior stakeholders to improve the business value to be delivered from new or existing services and products. Leads the development of demand management capabilities and ensures decision making is informed by robust scenario planning and what-if analysis. Leads the integration of demand management with complementary strategic, operational and change management processes.