|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Operations and User Support | | | | | |
| **TSC Title** | Threat Intelligence and Detection | | | | | |
| **TSC Description** | Monitor intelligence-gathering and anticipate potential threats to an ICT system proactively. This involves the pre-emptive analysis of potential perpetrators, anomalous activities and evidence-based knowledge and inferences on perpetrators' motivations and tactics | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  | **ICT-OUS-2015-1.1** | **ICT-OUS-3015-1.1** | **ICT-OUS-4015-1.1** | **ICT-OUS-5015-1.1** | **ICT-OUS-6015-1.1** |
|  | Install security applications and interpret logs to detect anomalous activity, intrusions and threats | Implement intrusion detection technology and analyse multi-source information to identify vulnerabilities, potential exploits, methods, motives, and capabilities | Develop strategies to monitor threats and project future technical cyber threat scenarios and present mission reports to key stakeholders | Establish a threat intelligence strategy and direct analysis and integration across various sources to present a robust view on threats, perpetrators, motivations and modus operandi | Anticipate evolving trends and threats in the operating environment, and redefine threat intelligence strategies, methodologies and tactics to predict and mitigate threats |
| **Knowledge** |  | * Methods and tools for monitoring network activities, systems and mechanisms * Intrusion detection techniques, software, and their functions * Types of security threats and intrusions * Security protocols, standards and data encryption * Indicators of attacks * Attack patterns and threat vectors * Techniques, methods and technologies in threat data collection | * Range of intrusion detection and monitoring technologies * Applied principles and tools of information security * Techniques for analysis and integration of threat data * Relevant data sources of threat intelligence in the form of firewall logs, intrusion detection system logs, open source internet searches, honeypots * Types and features of exploits and malware | * Mechanisms for threat detection and monitoring * Advanced statistical and trend analysis techniques * Emerging trends and developments in cyber security * Impact analysis of cyber threats * Range of possible tactics, techniques and procedures used for security attacks * Key components and objectives of intelligence products and mission reports | * Multiple fields in cyber intelligence, including intelligence collection operations and cyber counter-intelligence * Emerging threats, perpetrators, doctrines and methods of operation * Wider business and financial impact of cybersecurity threats | * Long-term trends and evolution of the operating environment * Principles underlying threat intelligence and detection strategies and methodologies |
| **Abilities** |  | * Install security applications and appliances for detecting intrusions and guarding against attacks * Monitor access control mechanisms, network activities and operating systems * Interpret information from logs and scanners to detect threats and intrusion attempts * Apply detection technologies, checks and techniques to identify anomalous activity and patterns * Recognise indicators of attacks during the detection process * Follow-up with relevant parties on any security threats or intrusions detected * Use technologies, methods and tradecraft to retrieve and organize threat data or information | * Identify resources and technologies required for intrusion detection according to technical and cost guidelines * Implement intrusion detection and analysis based on key objectives and stakeholders' requirements * Analyse collected information to identify vulnerabilities and potential for exploitation * Review multiple sources of data and intelligence feeds * Conduct intelligence analysis of cyber activities to identify entities of interest, potential methods, motives, and capabilities * Present contextual information to place cyber attacks in context * Integrate information to support the creation of internal cyber threat intelligence products | * Develop strategies for threat monitoring and tracking efforts across enterprise systems * Perform advanced trend, pattern and statistical analysis to project future technical cyber threat scenarios * Synthesise multiple information sources and analysis reports into a holistic view of potential threats * Draw insights about the potential impact of estimated cyber threat scenarios * Develop mission reports and threat intelligence products that leverage so as to present analysis of threat data to key stakeholders * Lead comprehensive evaluation of the capabilities and activities of cyber criminals, foreign intelligence entities or perpetrators * Conduct in-depth research into cyber security issues of industry-wide or nation-wide significance * Produce findings to help initialise or support law enforcement and counterintelligence investigations or activities | * Develop an overarching threat intelligence strategy * Manage the research, analysis, and data integration across a wide variety of information sources * Determine the tactics, techniques and procedures used for intrusions and attacks * Present an informed and robust point of view on both current and anticipated threats, perpetrators, motivations, doctrine and modus operandi * Articulate significance of evolving cyber security threats to critical decision-makers and senior management in the organisation * Present policy recommendations and impact assessments to critical industry stakeholders and leaders | * Chart direction to anticipate trends, changes and evolution of cybersecurity threats in the operating environment * Redefine threat intelligence strategy in anticipation of evolving operating environment * Employ new methodologies and tactics to anticipate and detect threats |
| **Range of Application** |  | | | | | |