

All-Source Analyst

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Category: Analyze

Specialty Area: All-Source Analysis

Tasks

T0569:	Answer requests for information.
T0582:	Provide expertise to course of action development.
T0583:	Provide subject matter expertise to the development of a common operational picture.
T0584:	Maintain a common intelligence picture.
T0585:	Provide subject matter expertise to the development of cyber operations specific indicators.
T0586:	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
T0589:	Assist in the identification of intelligence collection shortfalls.
T0593:	Brief threat and/or target current situations.
T0597:	Collaborate with intelligence analysts/targeting organizations involved in related areas.
T0615:	Conduct in-depth research and analysis.
T0617:	Conduct nodal analysis.
T0642:	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.
T0660:	Develop information requirements necessary for answering priority information requests.
T0678:	Engage customers to understand customers' intelligence needs and wants.
T0685:	Evaluate threat decision-making processes.
T0686:	Identify threat vulnerabilities.
T0687:	Identify threats to Blue Force vulnerabilities.
T0707:	Generate requests for information.
T0708:	Identify threat tactics, and methodologies.
T0710:	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
T0713:	Identify and submit intelligence requirements for the purposes of designating priority information requirements.
T0718:	Identify intelligence gaps and shortfalls.
T0748:	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.
T0749:	Monitor and report on validated threat activities.

All-Source Analyst

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Category: Analyze

Specialty Area: All-Source Analysis

Tasks

T0751:	Monitor open source websites for hostile content directed towards organizational or partner interests.
T0752:	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.
T0758:	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
T0761:	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
T0771:	Provide subject matter expertise to website characterizations.
T0782:	Provide analyses and support for effectiveness assessment.
T0783:	Provide current intelligence support to critical internal/external stakeholders as appropriate.
T0785:	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
T0786:	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
T0788:	Provide input and assist in post-action effectiveness assessments.
T0789:	Provide input and assist in the development of plans and guidance.
T0792:	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
T0797:	Provide target recommendations which meet leadership objectives.
T0800:	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
T0805:	Report intelligence-derived significant network events and intrusions.
T0834:	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.