the ThreatLab
Integrating Research Into Practice

# Counter-Insider Threat (C-InT) Analyst Professionalization Road Map

Lorien Megill
Mario Ruiz
*Northrop Grumman Defense Systems*

Caitlyn Foley
Amanda Boelke
Slaton Lucero
Marisa Peyton
*Global Skills X-Change*

Stephanie Jaros
Leissa Nelson
*Defense Personnel and Security Research Center*

PERSEREC PA 21 13 | OPA Report No. 2021 063

## Sponsors

The Defense Personnel and Security Research Center (PERSEREC) is a Department of Defense (DoD) entity dedicated to improving the effectiveness, efficiency, and fairness of DoD personnel suitability, security, and reliability systems. PERSEREC is part of the Office of People Analytics (OPA), which is a component of the Defense Human Resources Activity under the Office of the Under Secretary of Defense (Personnel and Readiness).

The primary mission of the National Insider Threat Task Force is to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies.

The DoD Counter-Insider Threat Program provides leadership, management, and oversight of the policy, resources, and operational capabilities to prevent, detect, deter, and mitigate the threat posed by an insider. As part of this, the program works to ensure a well-equipped, trained, and vigilant workforce and a program/capabilities informed by social and behavioral science research.

## Introduction

As the Counter-Insider Threat (C-InT) mission space continues to evolve, there is a need for a comprehensive professionalization program to better equip the C-InT workforce with the necessary skillsets to deter, detect, and mitigate the threats trusted insiders pose to national security, critical infrastructure, and our private sector partners.

To support this effort, the National Insider Threat Task Force (NITTF) asked The Threat Lab, a division of the Defense Personnel and Security Research Center (PERSEREC), to create a professionalization Road Map for C-InT Analysts that will help elevate the role from a series of tasks to a profession of its own.

The finished Road Map is designed to:

1. Define the role of the C-InT Analyst in a C-InT Hub;
2. Define a core knowledge base that support's an organization's understanding of the C-InT Analyst's role; and
3. Establish expectations for foundational knowledge and professional advancement.

## Method

We developed and validated the content of this Road Map by reviewing existing policy and professionalization materials and conducting interviews with Subject Matter Experts (SMEs) from organizations across the Federal Government and cleared industry partners. We began our research by reviewing publicly-available C-InT policies and program documentation published by the United States Government.

Second, we held nine focus groups with 19 SMEs in March 2021. These focus groups included government and private sector SMEs from nine organizations identified as model programs by the OUSD(I&S) DoD Counter-Insider Threat Program. OUSD(I&S) defined model programs as those with advanced capabilities in one or more C-InT lines of effort (i.e., pillars) and/or fully operational programs with more structured systems for training and developing C-InT Analysts. To maximize candor, we promised SMEs we would not reference their names or organizations in the final deliverable. Focus groups lasted up to one hour and focused on a list of brainstorming questions that we sent SMEs ahead of time. We provided field notes to each SME after the focus group for review and revision to ensure accuracy.

We used the results of the document review and SME interviews to 1) refine the key tasks and competencies, 2) define the roles and responsibilities of three levels of C-InT Analyst, and 3) identify the education/training, experience, and exposure required to advance from one level to the next. We used the following definitions for these requirements:

- **Education/Training**: Learning opportunities, such as on-the-job training (OJT) or formal/classroom training, that teach C-InT Analysts the necessary knowledge and skills to fulfill their role
- **Experience:** The suggested amount of time it takes an individual working in a C-InT Program to learn how to successfully perform the tasks needed to transition to the next level of C-InT Analyst and the type of tasks performed during that time
- **Exposure:** Activities or opportunities that provide C-InT Analysts the chance to learn about the full breadth of the C-InT mission space including inquiry types, fields related to C-InT, and inquiry study outcomes

In addition to the focus groups, we conducted semi-structured interviews. These interviews were intended to refine the education, experience, and exposure identified in the early phases of the work and to define the minimum proficiency levels (i.e., level of performance) at which C-InT Analysts must perform each key C-InT Analyst task and understand each key C-InT competency. We conducted the interviews with five individuals from the initial nine model programs. Telephone interviews lasted up to ninety minutes. After each interview, we provided field notes to the SMEs for review and revision to ensure accuracy. We then aggregated and analyzed those field notes.

## Results

Using the results of the document review, focus groups, and interviews, we developed a list of high-level, overarching functions meant to cover the majority of a C-InT Analyst's position, which we identified as the key C-InT Analyst tasks. We also developed a list of high-level, overarching competencies meant to cover the majority of the knowledge and skills needed by C-InT Analysts, which we identified as key Analyst competencies. The knowledge and skill areas that make up each competency are shown in Table 1.

**Table 1: Seven C-InT Analyst Key Competencies**

| Competency | Knowledge and/or Skill Areas |
|---|---|
| **1. C-InT Fundamentals** | • C-InT Policies and Directives<br>• Privacy and Civil Liberties Protections<br>• Risk Management Framework (RMF)<br>• C-InT pillars<br>• C-InT Program/Hub mission, resources, and policies |
| **2. Information Collection & Validation** | • Building collaborative relationships with pillar experts or outside experts<br>• Source identification<br>• Information source research<br>• Evaluation and guidance of information collection<br>• Data collection strategies<br>• Outreach strategies<br>• Identifying gaps in data<br>• Databases and data feeds<br>• Information requests<br>• Data validation/evaluation<br>• Referral triage<br>• Monitoring and tracking data feeds |
| **3. Data Integration & Analysis** | • Data aggregation<br>• Data normalization<br>• Baseline identification<br>• Contextualizing behavior to form a baseline<br>• Risk-scoring technologies<br>• Anomalous behavior identification<br>• Whether anomalous behavior meets thresholds/indicators<br>• Longitudinal analysis<br>• Identifying gaps in data |
| **4. Critical Thinking** | • Intellectual Standards (Interpreting, Analyzing, etc.)<br>• Analytic methodologies and tools<br>• Identifying cognitive limitations (e.g., cognitive biases)<br>• Discernment of biases<br>• Proposing alternative hypotheses |
| **5. Insider Threat Response & Mitigation** | • Individual mitigation strategies<br>• Organizational mitigation strategies<br>• Procedures for determining/conducting insider threat response actions<br>• Measures used to reduce unauthorized disclosure |
| **6. Inquiry Management & Information Protection** | • Inquiry lifecycle<br>• Investigative and operational viability<br>• Information protection/safeguarding information<br>• Documenting insider threat matters<br>• Digital asset records management<br>• Investigative referral requirements; development of referrals to other departments/agencies<br>• Case management tools used to ensure the integrity and effectiveness of the inquiry and response processes<br>• Understanding the appropriate officials to consult for authoritative compliance (e.g., legal, privacy and civil liberties, agency policy, etc.) |
| **7. Information Dissemination & Sharing** | • Developing reports following analytic tradecraft standards<br>• Intelligence Community analytic standards<br>• Demonstrating customer relevance and addressing implications<br>• Requesting/responding to customer feedback |

We also identified the education, experience, and exposure needed to progress from one level of C-InT Analyst to the next and identified existing available training and resources.

In addition to the information included in the Road Map, we used the review of references and the focus groups to develop definitions for three levels of Analyst: Beginner, Intermediate, and Advanced. Beginner Analysts can perform specific, defined tasks autonomously, while more Intermediate and Advanced Analysts review and supervise all of their work. Intermediate Analysts can work most inquiries autonomously and follow the inquiries management process. Intermediate Analysts may require some assistance from Advanced Analysts to complete more novel or complex inquiries. Advanced Analysts provide oversight and/or guidance to other C-InT Analysts, perform strategic analyses, and manage both internal and external data sources to complete analyses. Full definitions of each level of C-InT Analyst are shown in Table 2.

**Table 2: C-InT Analyst Definitions**

| Title | Knowledge and/or Skill Areas |
|---|---|
| **Beginner Analyst** | Beginner Analysts have previous experience in a C-InT-related field (e.g., Human Resources, Counterintelligence, Security, etc.) or have applied the C-InT Analyst core competencies in a different role/job setting. These individuals may have minimal experience working directly in or in support of a C-InT Program. These individuals are focused on: learning the inquiry management process, how and when to use available databases, and specific organizational procedures through on-the-job training (OJT); completing analysis courses; and practicing writing and briefing skills. These individuals collaborate with more experienced Analysts to learn the process and develop the foundational knowledge needed to lead an inquiry. These individuals triage reports/tips, begin collecting information from data sources, and begin the initial data analysis to form the big picture. These individuals are able to perform specific, defined tasks autonomously, but Intermediate and Advanced Analysts review and supervise all of their work. |
| **Intermediate Analyst** | Intermediate Analysts have experience working directly in a C-InT Program. These individuals have received formal training in C-InT analysis and have received on-the-job training (OJT) to grow their knowledge and understanding of the various disciplines that make up the C-InT mission. These individuals use their knowledge to collect, validate, and aggregate data to provide stakeholders with a holistic perspective of a subject’s potential risk indicators (PRIs). These individuals work collaboratively with all other team members to identify and fill gaps in their work product. While able to work most inquiries autonomously and follow the inquiry management process, these individuals may require some assistance from advanced C-InT Analysts to complete more novel or complex inquiries. These individuals are beginning to learn how to develop mitigation recommendations. |
| **Advanced Analyst** | Advanced Analysts have extensive experience working directly in a C-InT Program. These individuals have received formal training in C-InT analysis, are responsible for the most complex or high threat inquiries, work closely with other Analysts to assist as needed, collaborate with various stakeholders, and draw connections between seemingly disparate information. These individuals have a deeper understanding of the tools, techniques, and processes utilized by experts in related fields (e.g., psychology, threat assessment, counterintelligence) and when to involve those experts. They take a more proactive approach to identify new alerts/flags and develop mitigation responses to their inquiries. Work activities for these individuals may include: providing oversight and/or guidance to other C-InT Analysts, performing strategic analyses, and managing both internal and external data sources to complete analyses. These individuals may provide mitigation recommendations to internal and external stakeholders and leadership in a way that makes sense to non-C-InT professionals or, in rare inquiries involving imminent danger, take action to implement some mitigation responses. |

The information and definitions depicted in the Road Map represent the aggregated results of the policy review and SME interviews. We present three data visualizations, described as follows.

1. **Overview of Key C-InT Analyst Tasks and Competencies –** This visualization describes the key tasks and competencies and shows how the competencies are linked to each task.
2. **Expected Proficiency of Each Competency at Each Level of a C-InT Analyst's Career –** This visualization rates each competency for the Beginner, Intermediate, and Advanced Analyst using a five-point proficiency scale.
3. **How to Transition from Beginner to Intermediate Analyst and Intermediate to Advanced Analyst –** This visualization lists the education/training, experience, and exposure that help an Analyst advance along their career path.

Taken together, we encourage C-InT professionals to use these data visualizations to target areas for advancement and development; we encourage C-InT programs to use these data visualizations to determine selection criteria, to advance their people, and to identify relevant training.

# Key C-InT Analyst Tasks and Competencies

## TASKS

**Task 1**
Comply with and stay current on relevant C-InT and other regulations, laws, policies and directives.

**Task 2**
Apply C-InT Discipline Knowledge to the analytic process to contextualize behavior and identify concerning behavior.

**Task 3**
Apply agency and organizational potential risk indicators and/or reporting thresholds to all analytic and inquiry management processes.

**Task 4**
Establish collaborative relationships with internal/external partners and stakeholders to facilitate information gathering and inquiry/investigation processes, mitigate bias, and support the overall C-InT mission.

**Task 5**
Receive and/or validate potential InT information to identify resource needs for collection.

**Task 6**
Gather information relevant to the potential risk indicators presented by an individual using multiple data sources.

**Task 7**
Identify gaps in the content of gathered information and determine any gaps in information sources.

**Task 8**
Integrate collected information to identify a baseline set of behaviors for an individual.

**Task 9**
Identify and flag anomalous activity using data integration methodologies and advanced analytics to contextualize an individual's behavior.

**Task 10**
Evaluate, integrate, analyze, and interpret information using structured analytic techniques.

**Task 11**
Evaluate and prioritize alternatives and assess similarities and differences in data to develop findings and conclusions.

**Task 12**
Determine whether an individual is a potential insider threat and, if applicable, recommend tailored mitigation strategies, either individual or organizational.

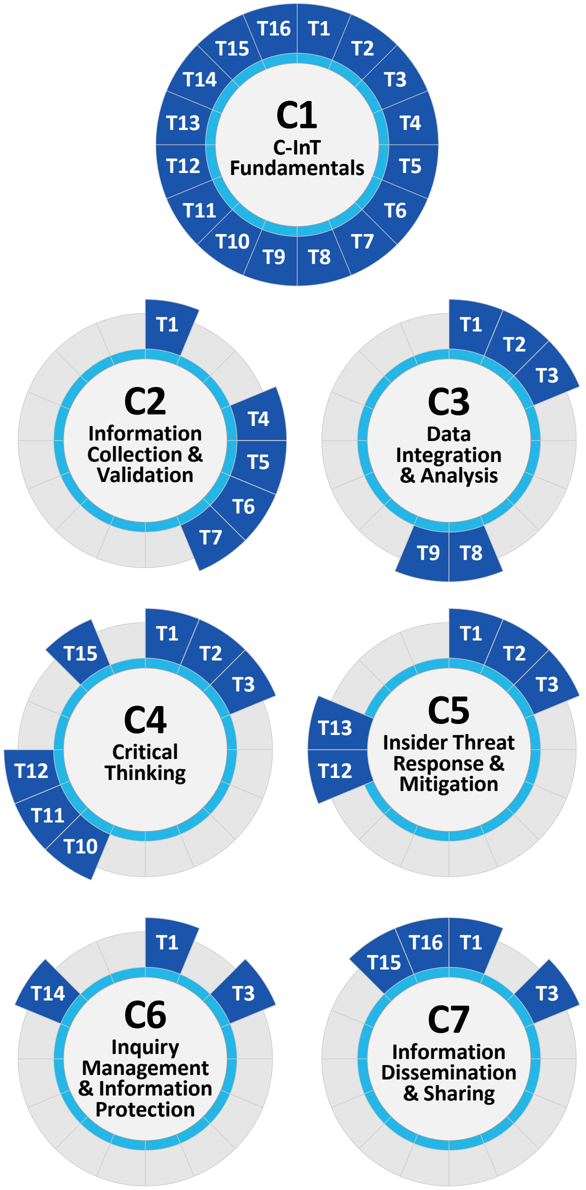
**Task 13**
Review insider threat indicators and recommend updates to organizational trigger policies based on environmental and/or situational changes, as needed.

**Task 14**
Employ case management principles and tools to ensure the integrity and effectiveness of the insider threat inquiry and response processes.

**Task 15**
Report and brief findings to internal/external leadership, and ensure reporting follows analytic standards, demonstrates stakeholder relevance, and addresses implications.

**Task 16**
Request and respond to stakeholder comments and/or feedback.

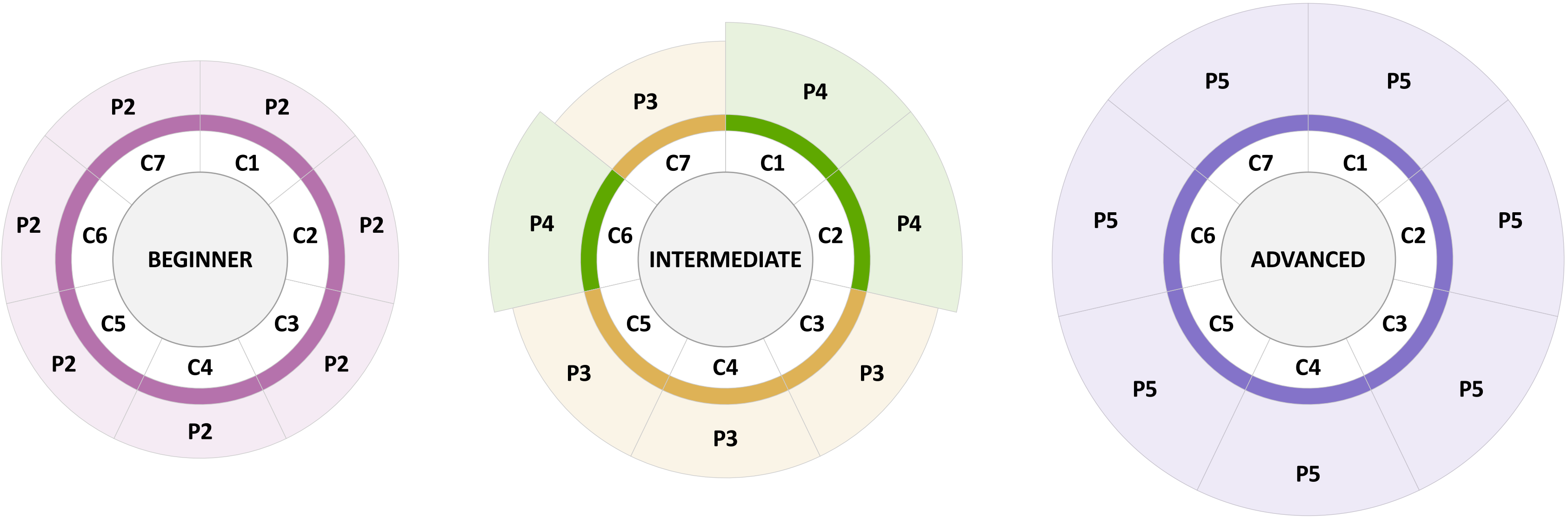
## COMPETENCIES


C1
C-InT Fundamentals
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
T15
T16
C2
Information Collection & Validation
T1
T4
T5
T6
T7
C3
Data Integration & Analysis
T1
T2
T3
T9
T8
C4
Critical Thinking
T15
T1
T2
T3
T12
T11
T10
C5
Insider Threat Response & Mitigation
T1
T2
T3
T13
T12
C6
Inquiry Management & Information Protection
T14
T1
T3
C7
Information Dissemination & Sharing
T15
T16
T1
T3

# Expected Proficiency of Each Competency at Each Level of a C-InT Analyst's Career

**C1:** C-InT Fundamentals
**C2:** Information Collection & Validation
**C3:** Data Integration & Analysis
**C4:** Critical Thinking

**C5:** Insider Threat Response & Mitigation
**C6:** Inquiry Management & Information Protection
**C7:** Information Dissemination & Sharing



## P1[1]

### Fundamental Awareness

(basic knowledge)

**FOCUS:**

- Learning

**INDIVIDUALS AT THIS LEVEL:**

- Have a common knowledge or understanding of the basics

## P2

### Novice

(limited experience)

**FOCUS:**

- Development through training

**INDIVIDUALS AT THIS LEVEL:**

- Understand relevant terminology, concepts, principles, and issues
- Are expected to need help completing work

## P3

### Intermediate

(practical application)

**FOCUS:**

- Application and enhancement

**INDIVIDUALS AT THIS LEVEL:**

- Understand the application of and implication of changes to relevant processes, policies, and procedures

## P4

### Advanced

(applied theory)

**FOCUS:**

- Coaching others

**INDIVIDUALS AT THIS LEVEL:**

- Are "People to ask" when difficult questions arise
- Offer practical ideas on process improvements
- Develop reference and resource materials

## P5

### Expert

(recognized authority)

**FOCUS:**

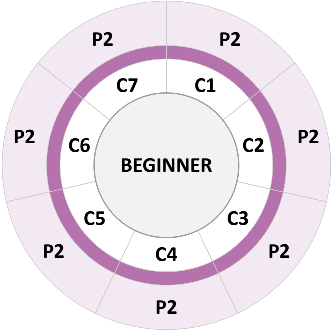
- C-InT Program strategy and development

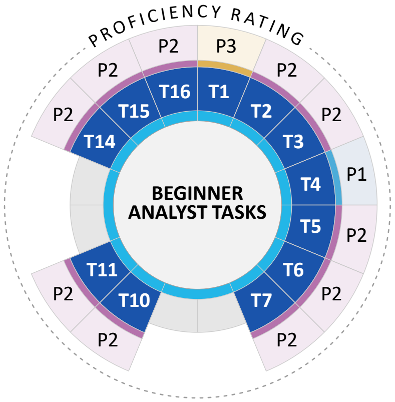
**INDIVIDUALS AT THIS LEVEL:**

- Provide guidance, troubleshoot, and answer general and specific C-InT questions
- Are able to present relevant process elements and issues in relation to organizational issues and trends

[1] The scale provided to the SMEs included P1, but their average ratings did not identify P1 for any competencies, indicating that even Beginner Analysts enter the field with some relevant background knowledge.

# How to Transition from Beginner to Intermediate Analyst





## Education/Training:

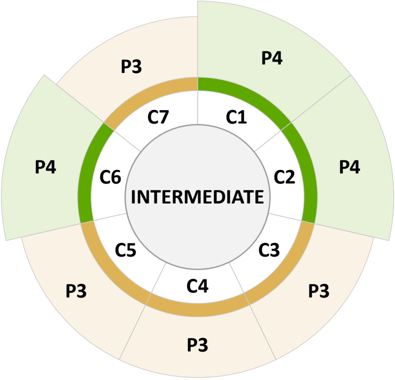
- 40 hours of hybrid C-InT Program training; formats may include formal training and on-the-job training (OJT), covering:
  - C-InT 101 (e.g., what is C-InT, what is a hub, pathway of an insider threat, C-InT pillars)
  - Policy & directives
  - Organizational hub/program structure & procedures
  - Social & behavioral science fundamentals
  - C-InT research, information collection, & validation
  - Vulnerabilities assessment & management
- 100 hours of OJT, topics may include:
  - Holistic, whole-person perspective
  - Organizational policies, procedures, and positioning
  - Organization-specific data sources and pulling data for inquiries
  - Inquiry management knowledge
  - InT terminology
  - Writing and briefing standards
- Additional formal training—examples listed below

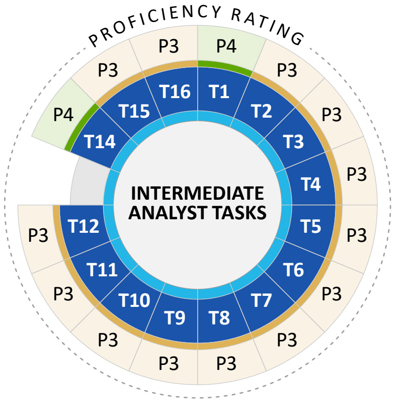
## Experience:

- Experience working in a C-InT Program performing tasks such as:
  - Triaging reports/alerts/tips
  - Managing autonomously the lifecycle of three or more common inquiries types (e.g., low threat, low risk)
  - Identifying connections between inquiries and new information
  - Identifying information gaps and data collection needs

## Exposure:

- Collaborate with Intermediate and Advanced Analysts to learn the holistic perspective and how to develop mitigation responses
- Establish collaborative relationships with internal and external partners, stakeholders, & subject matter experts (e.g., behavioral psychologists and data scientists)
- Review case studies covering the breadth of InT event types

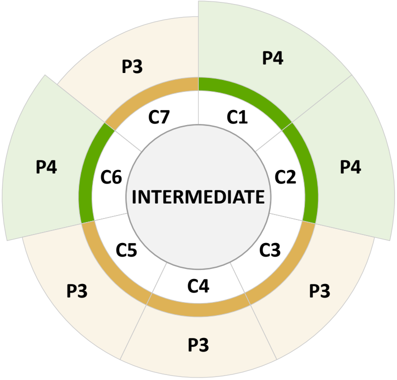


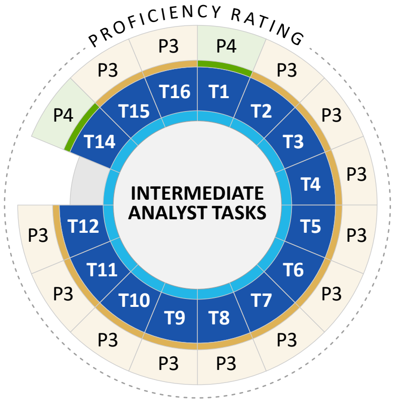


## TRAINING/RESOURCES TO HELP TRANSITION FROM **BEGINNER TO INTERMEDIATE**

- CDSE: Insider Threat Program Operations Personnel Program INT311.CU
- CDSE: Insider Threat Awareness Course INT101.16
- CDSE: Insider Threat Basic Hub Operations INT240.16
- CDSE: Critical Thinking for Insider Threat Analysts INT250.16
- CDSE: Insider Threat Privacy and Civil Liberties INT260.16
- CDSE: Insider Threat Program Operations Personnel Program INT311.CU
- CDSE: Insider Threat Resources (e.g., Job Aids, Webinars)
- Certified Counter-Insider Threat Professional-Fundamentals (CCITP-F) Certification
- Counter-Insider Threat Analyst Basic Tradecraft Primer
- Insider Threat Detection Analysis Course (ITDAC)
- Insider Threat Analyst Workbook
- Insider Threat Mitigation Guide (https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf)
- NITTF: Additional Insider Threat Resources
- NITTF: Directives & Advisories
- 2017 NITTF Insider Threat Guide
- Insider Threat Training Module (External Learning) https://www.dni.gov/ncsc/Insider-Threat/index.html
- NITTF: Maturity Framework
- The Threat Lab: Introduction to Behavioral Threat Assessment
- Threat Assessment Glossary (University of Nebraska, Lincoln https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1122&context=publicpolicypublications)
- A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf)

# How to Transition from Intermediate to Advanced Analyst





### Education/Training:

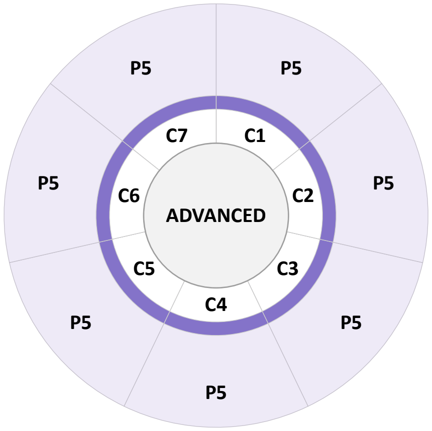
- 40+ hours of training in C-InT Analytic Methodology and Techniques; topics may include:
  - Identifying relevant events & connections
  - Autonomously writing concise analytic finding reports
  - Identifying which events/triggers require immediate action & which allow more time for research
  - Introducing creativity into the analysis process (e.g., developing new intelligence, identifying previously unused information, imagining previously unidentified threats, introducing new tools & techniques)
- Discipline-specific training (e.g., UAM, law enforcement, social and behavioral science, human resources)
  - Note: The exact number of hours required per discipline is dependent on the individual InT Program's needs and environment
- On-the-job training in program management
- Additional formal training— examples listed below

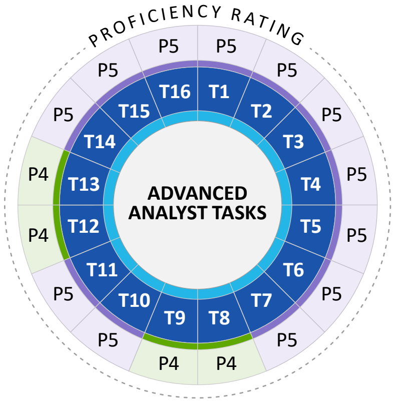
### Experience:

- Experience working in a C-InT Program performing tasks such as:
  - Using internal and external data sources to assess threats
  - Writing and briefing inquiry analysis, results, and mitigation responses to higher level officials
  - Mentoring other C-InT Analysts
  - Applying the holistic perspective to inquiries
  - Modifying existing flags/alerts to better identify "true" threats

### Exposure:

- Brief case studies covering the breadth of InT event types
- Obtain C-InT discipline-specific certifications based on work (e.g., Senior Cybersecurity certification, Personnel Security certifications, Certified Threat Manager certification)
- Work to obtain SEI CERT Insider Threat Program Manager certificate





## TRAINING/RESOURCES TO HELP TRANSITION FROM **INTERMEDIATE TO ADVANCED**

- CDSE: Behavioral Science in Insider Threat INT290.16
- CDSE: Cyber Insider Threat INT280.16
- CDSE: Developing a Multidisciplinary Insider Threat Capability INT201.16
- CDSE: Establishing an Insider Threat Program for Your Organization INT122.16
- CDSE: Insider Threat Mitigation Responses INT210.16
- CDSE: Insider Threat Program Management Personnel Curriculum INT312.CU
- CDSE: Preserving Investigative and Operational Viability in Insider Threat INT220.16
- Certified Counter-Insider Threat Professional-Analysis (CCITP-A) Certification
- Cyber Intelligence Tradecraft Report (Carnegie Mellon University https://apps.dtic.mil/sti/pdfs/AD1090501.pdf)
- NITTF: Additional Insider Threat Resources
- NITTF: Directives & Advisories
- Privacy & Civil Liberties Refresher Training
- Structured Professional Judgment (SPJ) Tools: A Reference Guide for Counter-Insider Threat (C-InT) Hubs