CTI Analyst Core Competencies Checklist

Based on Mandiant's CTI Analyst Core Competencies Framework:
https://www.mandiant.com/sites/default/files/2022-05/cti-analyst-core-competencies-framework-v1.pdf

PROBLEM SOLVING

Critical Thinking

- [ ] Apply the intelligence lifecycle to analysis tasks
- [ ] Identify first, second, and third order effects of cyber events
- [ ] Evaluate intelligence source credibility based on:
  - [ ] Reliability
  - [ ] Level of access
  - [ ] Placement
- [ ] Apply inductive and deductive reasoning to data sets and vendor reports
- [ ] Use structured analytic techniques (SATs) to mitigate cognitive biases
- [ ] Create and evaluate alternative competing hypotheses
- [ ] Develop creative solutions for research challenges
- [ ] Create analytic frameworks for data collection
- [ ] Conduct trend forecasting

Research and Analysis

- [ ] Capture and prioritize stakeholder intelligence requirements
- [ ] Work with different types of indicators of compromise (IOCs):
  - [ ] Atomic indicators
  - [ ] Computed indicators
  - [ ] Behavioral indicators

  Analyze various data types:
  - [ ] Malware samples
  - [ ] Network traffic
  - [ ] Log events
- [ ] Use key research tools and data sources:
  - [ ] Passive DNS records
  - [ ] Netflow data
  - [ ] Internet scan data
  - [ ] Malware analysis platforms
  - [ ] Network packet captures
  - [ ] Sandbox environments
  - [ ] System event logs
- [ ] Apply statistical reasoning skills:
  - [ ] Hypothesis testing
  - [ ] Statistical significance
  - [ ] Conditional probability
  - [ ] Sampling methodologies

- [ ] Bias identification
- [ ] Use technical tools:
  - [ ] Python scripting
  - [ ] SQL queries
  - [ ] Jupyter/Zeppelin notebooks
  - [ ] Data visualization tools

Investigative Mindset

- [ ] Understand complex cyber threat actor TTPs
- [ ] Apply CTI frameworks to investigations
- [ ] Identify when existing tools/frameworks need updates
- [ ] Develop new analytical approaches for emerging threats
- [ ] Identify meaningful signals in noisy data
- [ ] Account for and overcome cognitive biases

PROFESSIONAL EFFECTIVENESS

Communication

- [ ] Create various intelligence products:
  - [ ] Written FINTEL reports
  - [ ] Slide presentations
  - [ ] Email briefings
  - [ ] Internal documentation
  - [ ] Technical bulletins
- [ ] Adapt communication style for different audiences:
  - [ ] Executive leadership
  - [ ] Technical practitioners
  - [ ] Media contacts
  - [ ] External partners
- [ ] Use CTI frameworks to represent:
  - [ ] Organizational threat models
  - [ ] Intrusion activities
  - [ ] Adversary workflows
  - [ ] Technical relationships
- [ ] Apply information sharing standards:
  - [ ] STIX
  - [ ] TAXII
  - [ ] JSON
- [ ] Use probabilistic language for assessments
- [ ] Apply storytelling frameworks (AIMS)

Teamwork and Emotional Intelligence

- [ ] Build collaborative relationships across teams

- [ ] Provide peer mentoring
- [ ] Share knowledge effectively
- [ ] Practice core emotional intelligence skills:
    - [ ] Self-awareness
    - [ ] Self-control
    - [ ] Social awareness
    - [ ] Relationship management
    - [ ] Elicit information from stakeholders
    - [ ] Navigate organizational dynamics

Business Acumen

- [ ] Understand organizational mission and goals
- [ ] Evaluate cyber risk implications of business decisions
- [ ] Assess impact of strategic changes on threat landscape
- [ ] Communicate findings in business context
- [ ] Demonstrate ROI for security measures
- [ ] Align intelligence activities with business objectives
- [ ] Navigate organizational politics
- [ ] Speak stakeholder language/terminology

TECHNICAL LITERACY

Enterprise IT Networks

- [ ] Understand operating system principles:
    - [ ] System architecture
    - [ ] Identity management
    - [ ] Access control
    - [ ] Event logging
    - [ ] Network protocols
- [ ] Comprehend enterprise network design:
    - [ ] Virtualization concepts
    - [ ] Cloud computing implications
    - [ ] Operating system selection rationale
    - [ ] Network perimeter considerations

Cyber Security Ecosystem

- [ ] Know core security concepts:
    - [ ] Access control
    - [ ] Identity management
    - [ ] Authentication methods
    - [ ] Network segmentation
    - [ ] Cryptography basics
- [ ] Understand security technologies:

- [ ] Network security tools
- [ ] Endpoint protection
- [ ] Log collection systems
- [ ] Detection tools
- [ ] Apply security frameworks (NIST CSF)

- [ ] Know key security processes:
  - [ ] Business continuity
  - [ ] Disaster recovery
  - [ ] Incident response
  - [ ] Threat hunting

Cyber Security Roles

- [ ] Understand various security functions:
  - [ ] SOC roles (Tiers 1-3)
  - [ ] Forensics
  - [ ] Reverse engineering
  - [ ] Security architecture
  - [ ] Red/Blue/Purple teams
  - [ ] GRC
  - [ ] Know role interactions and dependencies
  - [ ] Apply RACI matrices
  - [ ] Work within established SLAs

CYBER THREAT PROFICIENCY

Drivers of Offensive Operations

- [ ] Understand offensive cyber program organization
- [ ] Identify nation-state motivations
- [ ] Analyze criminal motivations
- [ ] Assess ideological motivations
- [ ] Evaluate resource allocation decisions
- [ ] Track evolution of adversary operations
- [ ] Forecast targeting based on objectives

Threat Concepts and Frameworks

- [ ] Work with vulnerability concepts:
  - [ ] CVSS scoring
  - [ ] CVE system
  - [ ] Exploit development
  - [ ] Zero-day vs. n-day
- [ ] Understand malware concepts:
  - [ ] Execution chains
  - [ ] Command and control

- [ ] Communication methods
- [ ] Malware-as-a-service

- [ ] Apply CTI frameworks:
  - [ ] FAIR
  - [ ] Kill Chain models
  - [ ] Diamond Model
  - [ ] MITRE ATT&CK

Threat Actors and TTPs

- [ ] Track threat actor naming conventions
- [ ] Identify nation-state affiliations
- [ ] Analyze criminal group operations
- [ ] Document actor TTPs:
  - [ ] Initial access methods
  - [ ] Reconnaissance techniques
  - [ ] Lateral movement
  - [ ] Command and control
  - [ ] Data exfiltration
  - [ ] Understand anti-forensic techniques
  - [ ] Track infrastructure preferences
  - [ ] Monitor operational workflows