DATA SHEET

The Treadstone 71 Cyber Intelligence Tradecraft Framework for Cyber Threat Intelligence Programs

HIGHLIGHTS

- We apply actual tactics, techniques, and methods learned from cyber operations.
- Students learn and apply standards and directs from the intelligence community.
- We ensure students more than a baseline knowledge of intelligence but a full scope, strategic, operational, tactical and technical hands-on education..

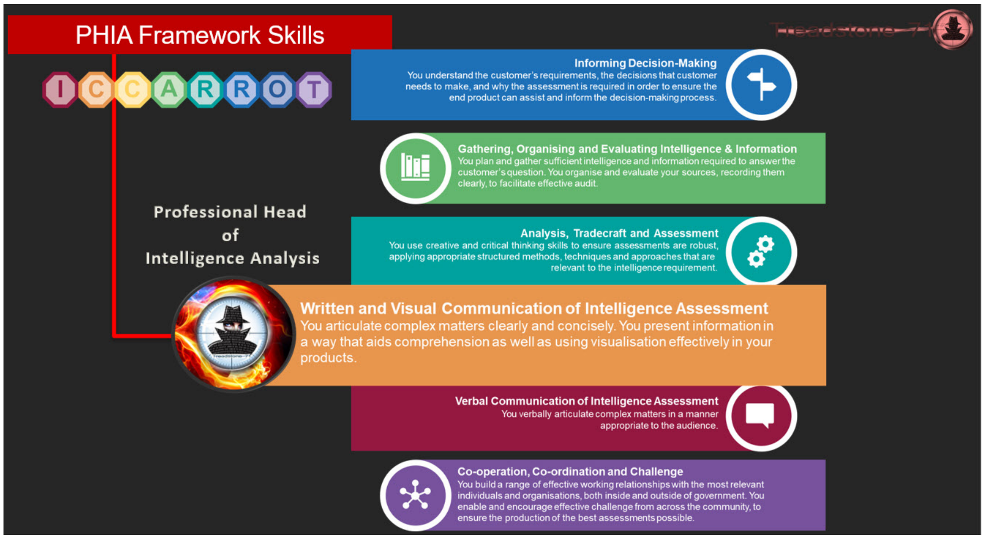
The baseline Cyber Intelligence training derives directly from standards. Standards used in the intelligence community directly applied to the cyber arena. Treadstone 71 started teaching intelligence courses at the master's level in 2008 developing cyber intelligence, cyber counterintelligence, and cybercrime courses for Utica College of Syracuse University. We continue to maintain pace with the changing standards and directives of the community leading the way with applications to the cyber world. We stay well ahead of the pack with our own forecasting of courses providing students with the skills that drives intelligence collection and analysis excellence. What we do that no one else does is take our operational expertise gained performing research, cyber operations, cyber counterintelligence actions, both passive and active collections, and apply these learnings directly into our courses. Students learn the standards, integrate the directives, and apply the hands-on successes learned on the cyber battlefield.

The Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft training course follows the iterative processes of the intelligence lifecycle while covering non-inclusively. This course follows the International Association for Intelligence Education Standards for Intelligence Analyst Initial Training incorporating intelligence community member validated content, intelligence community directives and hands-on experience in the cyber environment since 2004. We adapted all that was physically oriented. The model follows the International Association for Intelligence Education Standards for Intelligence Analyst Initial Training (IAFIE), the United Kingdom Professional Head of Intelligence

Analysis Framework (PHIA), combined with operational cyber and threat intelligence tradecraft built from the Treadstone 71 Cyber Intelligence Common Body of Knowledge. The International Association for Intelligence Education Standards for Intelligence Analyst Initial Training:

I. Introduction to Intelligence
II. Critical Thinking
III. Analytic Writing
IV. Creative Thinking
V. Analytic Briefing
VI. Structured Analytic Techniques.
VII. Analytic Issues
VIII. Argument Mapping
IX. Case Studies

The PHIA Professional Head of Intelligence Analysis framework:



PHIA Framework Skills

Professional Head of Intelligence Analysis

Informing Decision-Making
You understand the customer's requirements, the decisions that customer needs to make, and why the assessment is required in order to ensure the end product can assist and inform the decision-making process.

Gathering, Organising and Evaluating Intelligence & Information
You plan and gather sufficient intelligence and information required to answer the customer's question. You organise and evaluate your sources, recording them clearly, to facilitate effective audit.

Analysis, Tradecraft and Assessment
You use creative and critical thinking skills to ensure assessments are robust, applying appropriate structured methods, techniques and approaches that are relevant to the intelligence requirement.

Written and Visual Communication of Intelligence Assessment
You articulate complex matters clearly and concisely. You present information in a way that aids comprehension as well as using visualisation effectively in your products.

Verbal Communication of Intelligence Assessment
You verbally articulate complex matters in a manner appropriate to the audience.

Co-operation, Co-ordination and Challenge
You build a range of effective working relationships with the most relevant individuals and organisations, both inside and outside of government. You enable and encourage effective challenge from across the community, to ensure the production of the best assessments possible.

Figure 1 PHIA Framewore

Introduction to Intelligence

Intelligence Cycle: Discuss the intelligence cycle or process and how its components interrelate.

Intelligence Community Directives: Describe the intelligence community directives (ICD) as they apply to the cyber world.

Intelligence Planning - *The process of defining an intelligence organization's strategy or direction, including making decisions on allocating its resources to pursue this strategy.*

Demonstrate knowledge of intelligence activities, including intelligence collection, counterintelligence, and covert action.

Demonstrate knowledge of appropriate strategies and plans, including their interrelationships, similarities, and differences.

Explain the strategic planning interfaces between various levels of information security, SOC, Incident Response, Red, Blue, Purple Teams, and cyber threat intelligence.

Employ the latest in strategic and organizational management, organizational behavior, leadership, organizational operations, and information sharing procedures used in the intelligence functions across the organization (business, competitive, cyber).

Explain the intelligence resource management process.

Create intelligence requirements from stakeholders prioritizing them as a precursor to collection planning.

Author collection plans describing resource and mission management. Define initial OSINT tools to be used.

Demonstrate the preparation and presentation of intelligence management written and oral communications.

Appraise the use of the "Intelligence Cycle" as a framework for understanding intelligence activities.

Intelligence Collection – The process of collecting, processing, and exploiting information used in intelligence products.

Discuss processes for prioritizing and tasking the employment of collection assets to support strategic, operational, tactical, and technical intelligence analysis.

Explain the organization, capabilities, limitations, exploitation, and issues in Cyber Human Intelligence collection operations, both overt and covert.

Explain the organization, collection platforms, capabilities, limitations, exploitation, and issues in Open Source Intelligence (OSINT) collection operations.

Explain the organization, collection platforms, capabilities, limitations, exploitation, and issues in online Geospatial Intelligence (GEOINT) (imagery-mapping) collection operations.

Explain the organization, collection platforms, capabilities, limitations, exploitation, and issues in online Measurement and Signature Intelligence (MASINT) (other technical) collection operations.

Discuss the contributions, limitations, and issues related to the collaboration of information and intelligence sharing obtained through adversary targeting.

Describe the issues and challenges in coordinating intelligence collection from multiple sources.

Use open-source tools, techniques, and methods for data collection.

Structured Analytic Techniques

Data Exploitation/Collation: Understand the need to organize data effectively to analyze it properly.

Issue/Problem Development Techniques:

Issue Restatement: Understand how to paraphrase an issue for more effective problem-solving.

Evidence Evaluation: Explain when and how to weigh evidence and demonstrate proficiency in doing so.

Assumptions Check: Describe the nature of assumptions, their impact on decision-making, and why we need to identify and explicitly state them.

Denial and Deception Check: Describe the elements of denial and deception and their impact on analysis.

Visualization Techniques

Link Analysis: Describe the nature of associations and how analyzing these can provide evidence or leads in conspiratorial operations.

Pattern Analysis: Understand the types of patterns that may occur and why or how these patterns may assist in developing indicators and warnings.

Trend Analysis, Tendency Analysis, Semiotic Analysis, Aggregation Analysis, Link analysis/network charts:

Timeline/Chronology

Network Analysis

Brainstorming

Structured Brainstorming

Virtual Brainstorming
Nominal Group Technique
Starbursting
Cross-Impact Matrix
Morphological Analysis
Quadrant Crunching
Scenario Analysis
Alternative Futures Analysis
Indicators
Indicators Validator
Hypothesis Generation
The Multiple Hypotheses Generator
Diagnostic Reasoning
Devil's Advocacy
Force Field Analysis
Storyboards

Analysis of Competing Hypotheses
Argument Mapping
Deception Detection
Key Assumptions Check
Maps
Flow Charts
Frequency Charts
Maps
Outside in Thinking
Pre-Mortem Assessment
What If? Analysis
High Impact, Low Probability

Timeline and Chronology Analysis:

Demonstrate the utility of timelines as a marshaling tool.

Commodity Flow Analysis: Demonstrate the efficacy of following movements of things concerning covert activities.

Demonstrate procedures for modeling and hypothesis generation.

Alternative Analysis Techniques:

What If? Discuss how unlikely events which may have a significant impact should be considered.

Analysis of Competing Hypotheses: Have an understanding of the ability to use Analysis of Competing Hypotheses as an analytic method. Full use of the toolset is required

Devil's Advocacy:

Describe how Devil's Advocacy can be used to uncover analytic alternatives.

Denial and Deception through MOM, POP, MOSES, and EVE.

Intelligence Analysis

The process where information is analyzed, and intelligence products are developed and provided to strategic, operational, and tactical consumers.

Formulate analyzable questions through de-construction of the intelligence tasking or problem.

Review, understand, and use the following types of analysis:

Decomposition
Link Analysis
Pattern Analysis
Trend Analysis
Technical Baseline
Functional Baseline
Cultural Baseline
Tendency Analysis
Cultural Analysis
Anomaly analysis
Semiotic Analysis
Anticipatory Analysis
Recomposition
Synthesis

Locate and search available databases and other sources to gather existing information and intelligence products, including Open Source Intelligence (OSINT) (publicly available information), and identify information gaps.

Assess the validity of cyber human, tactical, and technical information through vetting procedures designed to detect misinterpretations, fabrications, deliberate deceptions, and unacknowledged biases.

Explain the challenges of tasking multi-source collection assets to fill identified information gaps.

Select appropriate procedures for group analytic efforts (brainstorming, Red Team analysis, Team A/B).

Employ qualitative and quantitative analysis procedures to test hypotheses and develop analytic findings.

Demonstrate the ability to present complex data and findings in meaningful ways (e.g., maps, charts, tables, graphs).

Critical Thinking

Critical Thinking Defined: Explain what critical thinking is and its importance to intelligence analysis and the problem-solving process.

Eight Elements of Thought: Apply Paul and Elder (or other recognized critical thinking) model using the

Eight Elements of Thought (or related structure).

Intellectual Standards: Describe the Paul & Elder intellectual standards (or another set of intellectual standards) and how they apply to intelligence analysis.

Creative Thinking

Brainstorming: Expand their view of possible alternatives.

Rethinking: Challenge their assumptions and cognitive illusions.

Lateral Thinking: Provide alternative thinking modes.

Red Teaming: Think from the adversary's point of view.

Analytic Issues

Collector/Analyst Integration: Explain the role of collectors; how to identify gaps in evidence and work with a collector to close gaps.

Cognitive Bias, fallacies, pitfalls, and methods to identify bias in the collection, analysis, and writing.

Analytic Software: Describe available analytic software and demonstrate how to use the software.

Analytic Outreach and Resources: Describe varied ways in which analytic outreach can be affected, including resources available in open source.

Customer Engagement: Understand the importance of knowing the customer and ascertaining his/her needs.

Analytic Pitfalls: Describe examples of historic pitfalls in analytic thinking and suggest methods to avoid these.

Analytic Writing

Create written and oral reports to convey analytic findings to superiors and customers.

Products Overview: Identify the traits of effective IC products.

Tradecraft Standards: Relate analytic tradecraft standards to clear writing.

Sourcing Standards: Practice writing in compliance with sourcing standards.

Writing for Release: Demonstrate writing for release.

Practical Exercises: Review and practice critical thinking skills in writing appropriate intelligence documents.

Types of Reports

Warning, Basic/Research, Estimates/Forecasts, Advisories, Current, Summaries, and Technical

Product Line Mapping – aligning products, timeliness, editing cycles, serialization, with the audience, their knowledge, attitude, needs, and methods of receiving intelligence

Analytic Briefing

Briefing Fundamentals: Describe the fundamentals of briefing.

Briefing Formulation: Formulate a briefing based on those fundamentals.

Exercise: Provide a short briefing on an intelligence topic – present analytic results orally effectively.

Open Source and Vendor Intelligence Tools and Methods

Tool Selection Methods

- RFPs, kickoff meeting setup, use cases, selection criteria and scoring, proof of concept, cost model comparisons, vendor scoring analysis, tool use process flows and procedures, approval letters to leadership

Adversary Targeting – ATT&CK – Threat Hunting High Level Outline

- Tactics, Techniques, Procedures, Software, Tools
  - ATT&CK Navigator
  - ATT&CK Examples
- Chronology and Timelines
  - ATT&CK Chronology
  - Comparing past and present
  - Comparing and contrasting different threat groups
- Estimative ATT&CK
- Adversary Targeting – Threat Profiling
  - Primary Threats
    - Nation state
    - Foreign intelligence services
    - Military cyber units
    - Threat groups and proxies
    - Cyber criminals
    - Others
  - Target centric approach
    - Adversary targeting you
    - Verticals – common industries
    - Critical infrastructures
  - Adversary skills
  - Adversary maliciousness
  - Interest in your organization
  - Motivation – objective – conditions
    - Opportunity
    - Triggers
    - Course(s) of action
    - Capabilities
  - Level of automation
  - Potential impact
- Establish priorities Iterative Approaches and Feedback Loop
- RACIs – who does what
- Tactical Intelligence Risk
- Situational Awareness
  - Emerging threats
  - Coordination with other groups
  - Likely adversary courses of action
- Source Validation Credibility
- Evidence Types
- Confidence Levels
- Intake Forms
  - Request for Information (RFI)
  - Responding to RFIs
- What can CTI do and what can they not do
- Indicators Cyber DECIDE, DETECT, DELIVER and ASSESS (D3A) framework

Specific information requirements Cyber FIND, FIX, FINISH, EXPLOIT, ANALYZE and DISSEMINATE (F3EAD) methodology as part of the intelligence lifecycle

Mission and Requirements Management

Priority Intelligence Requirements

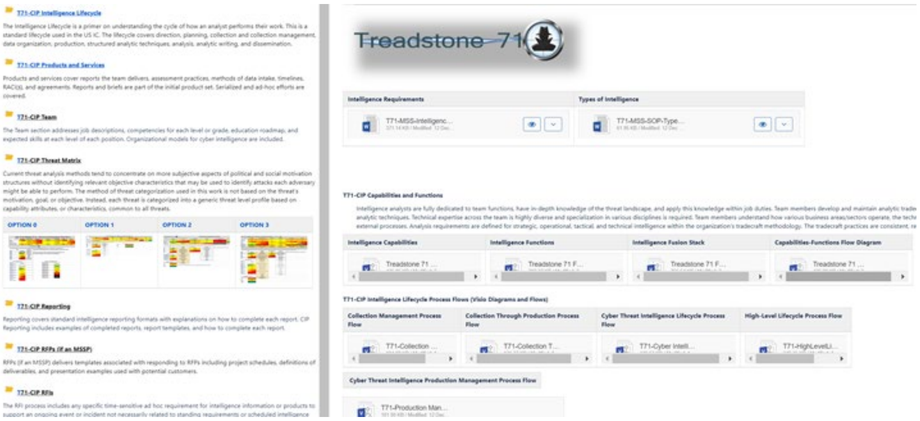
Intelligence Requirements

Prioritization and ranking, Indicators, SIRs

CyberIntellipedia

Cyber Intelligence wiki includes knowledge gained over years of cyber and threat intelligence program builds, targeted adversary research, and intelligence community-driven cyber intelligence training courses. CyberIntellipedia consists of documents defining (non-inclusively) (https://www.treadstone71.com/index.php/products/cyberintellipedia):

- Cyber Intelligence (CI) Strategic Planning, CI Team Capabilities, job Descriptions, Organization Charts, Training Plans, Team Accountabilities and Competency Levels
- Threat Matrices with Mitre ATT&CK inclusion
- Collection Management and Planning Methods
- CI Capability Maturity Model and Measuring Tools
- Cyber and Threat Intelligence Production Procedures
- Stakeholder Analysis, Checklists, Activities, and Tracking Modules
- Intelligence Requirements, Priority Intelligence Requirements, Indicators, and Specific Information Requirements



T71-CIP Intelligence Lifecycle

The Intelligence Lifecycle is a primer on understanding the cycle of how an analyst performs their work. This is a standard lifecycle used in the US IC. The lifecycle covers direction, planning, collection and collection management, data organization, production, structured analytic techniques, analysis, analytic writing, and dissemination.

T71-CIP Products and Services

Products and services cover reports the team delivers, assessment practices, methods of data intake, timelines, RACI(I), and agreements. Reports and briefs are part of the initial product set. Serialized and ad-hoc efforts are covered.

T71-CIP Team

The Team section addresses job descriptions, competencies for each level or grade, education roadmap, and expected skills at each level of each position. Organizational models for cyber intelligence are included.

T71-CIP Threat Matrix

Current threat analysis methods tend to concentrate on more subjective aspects of political and social motivation structures without identifying relevant objective characteristics that may be used to identify attacks each adversary might be able to perform. The method of threat categorization used in this work is not based on the threat's motivation, goal, or objective. Instead, each threat is categorized into a generic threat level profile based on capability attributes, or characteristics, common to all threats.

OPTION 0	OPTION 1	OPTION 2	OPTION 3

T71-CIP Reporting

Reporting covers standard intelligence reporting formats with explanations on how to complete each report. CIP Reporting includes examples of completed reports, report templates, and how to complete each report.

T71-CIP RFPs (If an MSSP)

RFPs (if an MSSP) delivers templates associated with responding to RFPs including project schedules, definitions of deliverables, and presentation examples used with potential customers.

T71-CIP RFIs

The RFI process includes any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing event or incident not necessarily related to standing requirements or scheduled intelligence

Intelligence Requirements	Types of Intelligence
T71-MSS-Intelligenc...	T71-MSS-SOP-Type...

T71-CIP Capabilities and Functions

Intelligence analysts are fully dedicated to team functions, have in-depth knowledge of the threat landscape, and apply this knowledge within job duties. Team members develop and maintain analytic trade analytic techniques. Technical expertise across the team is highly diverse and specialization in various disciplines is required. Team members understand how various business areas/sectors operate, the techn external processes. Analysis requirements are defined for strategic, operational, tactical, and technical intelligence within the organization's tradecraft methodology. The tradecraft practices are consistent, re

Intelligence Capabilities	Intelligence Functions	Intelligence Fusion Stack	Capabilities-Functions Flow Diagram
Treadstone 71 ...	Treadstone 71 F...	Treadstone 71 F...	Treadstone 71 ...

T71-CIP Intelligence Lifecycle Process Flows (Visio Diagrams and Flows)

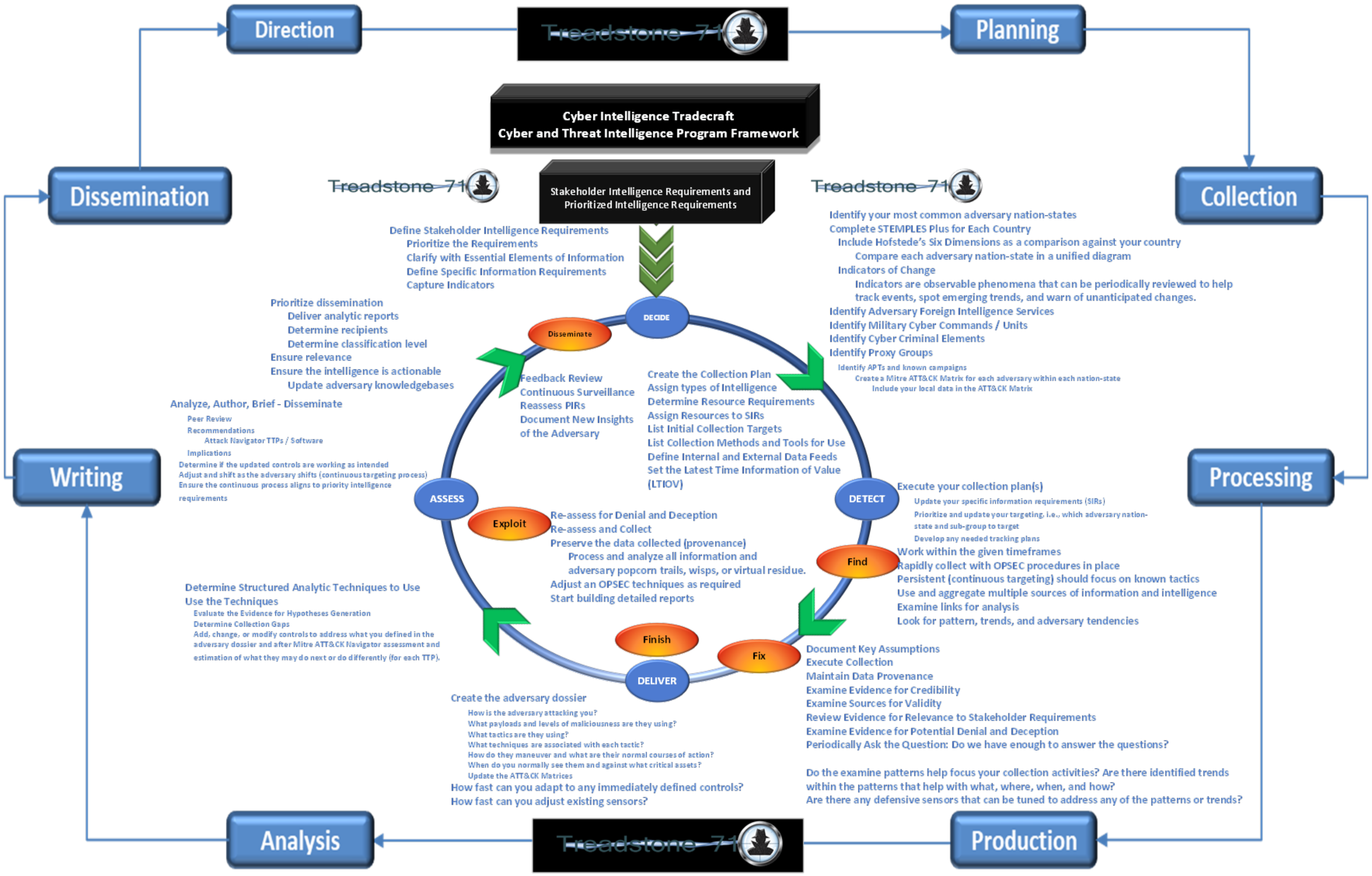
Collection Management Process Flow	Collection Through Production Process Flow	Cyber Threat Intelligence Lifecycle Process Flow	High-Level Lifecycle Process Flow
T71-Collection ...	T71-Collection T...	T71-Cyber Intell...	T71-HighLevelLi...

Cyber Threat Intelligence Production Management Process Flow
T71-Production Man...

- Structured Analytic Techniques Methods
- Types of Analysis Policies, Procedures, and Templates
- Complete end-to-end Cyber and Threat Intelligence Lifecycle with Iterative Feedback Loops
- Open Source and Vendor Intelligence Tools and Methods
    - Tool Selection Methods
        - RFPs, kickoff meeting setup, use cases, selection criteria and scoring, proof of concept, cost model comparisons, vendor scoring analysis, tool use process flows and procedures, approval letters to leadership
- Reporting and Dissemination Types Procedures and Templates
- Warning, Estimative, Baseline, Advisory and other report examples
- Threat Intelligence Platform (TIP) RFP Templates, Project Schedule and Selection Process
- TIP Rollout Schedule, Scrum Process, Deployment Methods, Use Cases, Questionnaires, Data Feed Selection
- Targeted Adversary Knowledgebase with Campaigns
- Online OPSEC Tools and Methods
- Evidence Validation Methods and Scoring
- Communities of Interest and Information Sharing

CyberIntellipedia consists of multiple sections covering strategic planning, policies, procedures, templates, taxonomy, examples, dossiers, finished intelligence, estimative intelligence, open-source tools, adversary research, process flow diagrams, reporting, analytic tools and methods, and threat intelligence TTPs, non-inclusively. CyberIntellipedia delivers the tools necessary to build a sustainable program. The wiki gives users access to twelve years of effort demonstrating proven success for cyber threat intelligence strategies, operational efficiencies, tactical methods, and technical alignment. Organizations pay hundreds of thousands of dollars over years of labor to establish what is in the Cyber & Threat Intelligence Wiki - CyberIntellipedia. With guidance and time-based direction, clients can build a complete intelligence program, educate stakeholders, staff, and leadership, without the usual massive outlay for time and materials, and commitment to constant consultant change orders.

Treadstone 71



Cyber Intelligence Tradecraft
Cyber and Threat Intelligence Program Framework

Stakeholder Intelligence Requirements and
Prioritized Intelligence Requirements

Define Stakeholder Intelligence Requirements
Prioritize the Requirements
Clarify with Essential Elements of Information
Define Specific Information Requirements
Capture Indicators

Identify your most common adversary nation-states
Complete STEMPLES Plus for Each Country
Include Hofstede's Six Dimensions as a comparison against your country
Compare each adversary nation-state in a unified diagram
Indicators of Change
Indicators are observable phenomena that can be periodically reviewed to help track events, spot emerging trends, and warn of unanticipated changes.
Identify Adversary Foreign Intelligence Services
Identify Military Cyber Commands / Units
Identify Cyber Criminal Elements
Identify Proxy Groups
Identify APTs and known campaigns
Create a Mitre ATT&CK Matrix for each adversary within each nation-state
Include your local data in the ATT&CK Matrix

Create the Collection Plan
Assign types of Intelligence
Determine Resource Requirements
Assign Resources to SIRs
List Initial Collection Targets
List Collection Methods and Tools for Use
Define Internal and External Data Feeds
Set the Latest Time Information of Value (LTIOV)

Execute your collection plan(s)
Update your specific information requirements (SIRs)
Prioritize and update your targeting, i.e., which adversary nation-state and sub-group to target
Develop any needed tracking plans
Work within the given timeframes
Rapidly collect with OPSEC procedures in place
Persistent (continuous targeting) should focus on known tactics
Use and aggregate multiple sources of information and intelligence
Examine links for analysis
Look for pattern, trends, and adversary tendencies

Document Key Assumptions
Execute Collection
Maintain Data Provenance
Examine Evidence for Credibility
Examine Sources for Validity
Review Evidence for Relevance to Stakeholder Requirements
Examine Evidence for Potential Denial and Deception
Periodically Ask the Question: Do we have enough to answer the questions?

Do the examine patterns help focus your collection activities? Are there identified trends within the patterns that help with what, where, when, and how?
Are there any defensive sensors that can be tuned to address any of the patterns or trends?

Re-assess for Denial and Deception
Re-assess and Collect
Preserve the data collected (provenance)
Process and analyze all information and adversary popcorn trails, wisps, or virtual residue.
Adjust an OPSEC techniques as required
Start building detailed reports

Create the adversary dossier
How is the adversary attacking you?
What payloads and levels of maliciousness are they using?
What tactics are they using?
What techniques are associated with each tactic?
How do they maneuver and what are their normal courses of action?
When do you normally see them and against what critical assets?
Update the ATT&CK Matrices
How fast can you adapt to any immediately defined controls?
How fast can you adjust existing sensors?

Determine Structured Analytic Techniques to Use
Use the Techniques
Evaluate the Evidence for Hypotheses Generation
Determine Collection Gaps
Add, change, or modify controls to address what you defined in the adversary dossier and after Mitre ATT&CK Navigator assessment and estimation of what they may do next or do differently (for each TTP).

Analyze, Author, Brief - Disseminate
Peer Review
Recommendations
Attack Navigator TTPs / Software
Implications
Determine if the updated controls are working as intended
Adjust and shift as the adversary shifts (continuous targeting process)
Ensure the continuous process aligns to priority intelligence requirements

Prioritize dissemination
Deliver analytic reports
Determine recipients
Determine classification level
Ensure relevance
Ensure the intelligence is actionable
Update adversary knowledgebases

Feedback Review
Continuous Surveillance
Reassess PIRs
Document New Insights of the Adversary

888.714.0071 ☎

Info AT treadstone71 DOT com ✉

www.treadstone71.com

To learn more about Treadstone 71, visit, www.Treadstone71.com

Since 2002, Treadstone 71 delivers intelligence training, strategic, operational, and tactical intelligence consulting, and research. We provide a seamless extension of your organization efficiently and effectively moving your organization to cyber intelligence program maturity. Our training, established in 2009, follows intelligence community standards as applied to the ever-changing threat environment delivering forecasts and estimates as intelligence intends. From baseline research to adversary targeted advisories and dossiers, Treadstone 71 products align to intelligence requirements. We do not follow the create once and delivery many model. We contextually tie our products to your needs. Intelligence is our only business.

888.714.0071 ☎
Info AT treadstone71 DOT com ✉
www.treadstone71.com 🌐