

Cyber Intelligence Tradecraft Subscription Model from Treadstone 71 Announced

HALF MOON BAY, Calif., June 23, 2020 (SEND2PRESS NEWSWIRE) – Treadstone 71, the leading pure-play cyber intelligence and counterintelligence firm announced the release of a new subscription model. The new model not only includes online, in-depth, standard-based intelligence training, but offers access to CyberIntellipedia and up to four weeks of consulting time.

T71-CIP Issues Tracker
CIP Issues Tracker provides a running ticketing system for RFIs, tasks, project schedule issues and other possible trackable items. Jira may be enabled for this section.

T71-CIP Analysis
We cover several different types of analysis, multiple structured analytic techniques, analysis of competing hypotheses, reasoning, critical thinking, and cognitive bias non-inclusively.

T71-CIP Collections and Research
Collection Management is the set of procedures that drives the team to focus the intelligence effort in support of organizational operations, mission and leadership requirements. The collection manager acquires information to satisfy priority intelligence requirements (PIRS) within the timelines that support operational decisions. Initial collection activity is based upon information requirements and key assumptions check. Collection planning and management guide research activities including basic, estimative, and warning intelligence.

T71-CIP Threat Intelligence Platform (TIP)
The TIP section includes the TIP selection process, questionnaires responses, use cases, kick-off plan, and decks, tracking of use case process, selection process, and executive justification letter non-IP process. Has been used multiple times in TIP selection. This study is

CONSULTING
Cyber Intelligence Maturity Assessment
Analysis as a Service
Targeted Research
Cyber Intelligence Program Build - Strategy
Intelligence Requirements
Collection Management
Cyber Intelligence Organizational Structure
– Job Descriptions – Competency Model
And more ...

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

T71-CIP RFPs
The RFP process includes any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing effort or project and response to standard requirements or ad-hoc intelligence

T71-CIP Types of Analysis
T71-CIP Analytic Writing Rhythm T71-CIP Analytic Writing T71-CIP Peer Review Rubric T71-CIP Report Templates T71-CIP Templates T71-CIP Analytic Writing Style Guide T71-CIP ATT&CK Model Analysis T71-CIP Report Editing Cycle

T71-CIP Analysis of Competing Hypotheses (ACH)
T71-CIP ACH Examples
T71-CIP ACH Instructions

T71-CIP Collections and Research - Daily Activities
T71-CIP Collections Management T71-CIP Confidence Levels T71-CIP Requirements and Mission Management T71-CIP Adm T71-CIP Rules of Engagement T71-CIP Evidence Relevance T71-CIP OPSEC Setup Options

T71-CIP RFP Process
T71-CIP TIP Proof of Concept Kickoff
T71-CIP TIP Overview T71-CIP TIP Use Cases
T71-CIP TIP Tagging T71-CIP TIP Questionnaires

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 CIP. 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, RACIS, 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.

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

T71-CIP RFPs
The RFP process includes any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing effort or project and response to standard requirements or ad-hoc intelligence

TRAINING AND WEBINARS
Analytic Writing
Adversary Targeting – Threat Matrices, Intelligence Requirements, Stakeholder Management, STEMPLES Plus Indicators of Change, Collection Management
Collection Manager's Course
Cyber Counterintelligence Tradecraft - Certified Threat Counterintelligence Analyst
Cyber Intelligence Tradecraft - Certified Threat Intelligence Analyst
Intelligence for the C-Suite
Strategic Intelligence Analysis, Forecasting, Estimative and Warning Intelligence
Structured Analytic Techniques

Treadstone 71

Treadstone 71

Intelligence Requirements
Types of Intelligence

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 tradecraft 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 full 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

T71-CIP Intelligence Lifecycle Process Flows (Main Diagrams and Flows)
Collection Management Process Flow
Collection Through Production Process Flow
Cyber Threat Intelligence Lifecycle Process Flow
High-Level Lifecycle Process Flow

Cyber Threat Intelligence Production Management Process Flow

SEND2PRESS.COM

The two-year subscription trains your staff, drives education across internal boundaries, gives access to years of cyber intelligence program information while providing four weeks access to Treadstone 71 expertise.

“We supplement our training with proven strategies, processes, procedures, and methods through our online knowledgebase wiki,” stated Jeff Bardin, Chief Intelligence Officer for Treadstone 71. “Organizations need more than a training class to mature their cyber and threat intelligence programs. Our new subscription model gives organizations the keys to the kingdom to build their own teams efficiently and quickly.”

Based on terms and conditions, the program can include unlimited online training for employees for two years. Online courses and webinars available are:

- Analytic Writing

- Adversary Targeting
- Collection Management
- Collection Manager's Course
- Cyber CounterIntelligence Tradecraft – Certified Threat CounterIntelligence Analyst
- Cyber Intelligence Tradecraft – Certified Threat Intelligence Analyst
- Intelligence for the C-Suite
- Intelligence Requirements
- Open Source Intelligence
- Stakeholder Management
- STEMPLES Plus – Indicators of Change
- Strategic Intelligence Analysis, Forecasting, Estimative and Warning Intelligence
- Structured Analytic Techniques

The training is directly supported with artifacts from CyberIntellipedia

The subscription model has a few levels from unlimited training courses, download and licensing of CyberIntellipedia and four weeks consulting over two years, designed to fit your budget and timeline. Treadstone 71's efforts to educate staff targets not only intelligence professionals, but incident responders, SOC personnel, information security staff, risk, governance, and audit staff as well as competitive and physical intel and security groups.

"When you have the training, are given a knowledgebase of targeted artifacts, and have direct access to the source for four weeks, you have everything you need to rapidly build your cyber and threat intelligence program," continued Bardin.

The program includes:

- Any-time access for two years.
- Developed and delivered by Intelligence Community professionals.
- Instructor office hours, access via Slack, questions via online comments, direct access to secure methods of communication to the instructor.
- Two-year unlimited number of students' access to all Treadstone 71 online courses.
- Students also receive course books via the Kindle App (for courses with books), two-year VPN access, two-year access to Hunchly, and lifetime access to Start.me and the Hemingway Editor.
- TERMS AND CONDITIONS APPLY

About Treadstone 71:

Treadstone 71's Certified Threat Intelligence and CounterIntelligence Analyst training are the gold standard in the industry today derived from both academia, the intelligence community, and from Treadstone 71's experience in building cyber and threat intelligence programs at Fortune 500 organizations worldwide. Treadstone 71 offers training, consulting, CyberIntellipedia (knowledgebase wiki), Conscientia (cyber intelligence lifecycle management), and intelligence team program builds and assessments.

Information: <https://www.treadstone71.com/index.php/products/subscription>

MEDIA CONTACT:

Jeff Bardin
Treadstone 71
info@treadstone71.com
888.714.0071

*VIDEO (YouTube): <https://youtu.be/HVXfNXeZRdA>

*IMAGE link for media:

<https://www.Send2Press.com/300dpi/20-0623s2p-t71-wikiconsulting-300dpi.jpg>