MANDIANT

WHITE PAPER

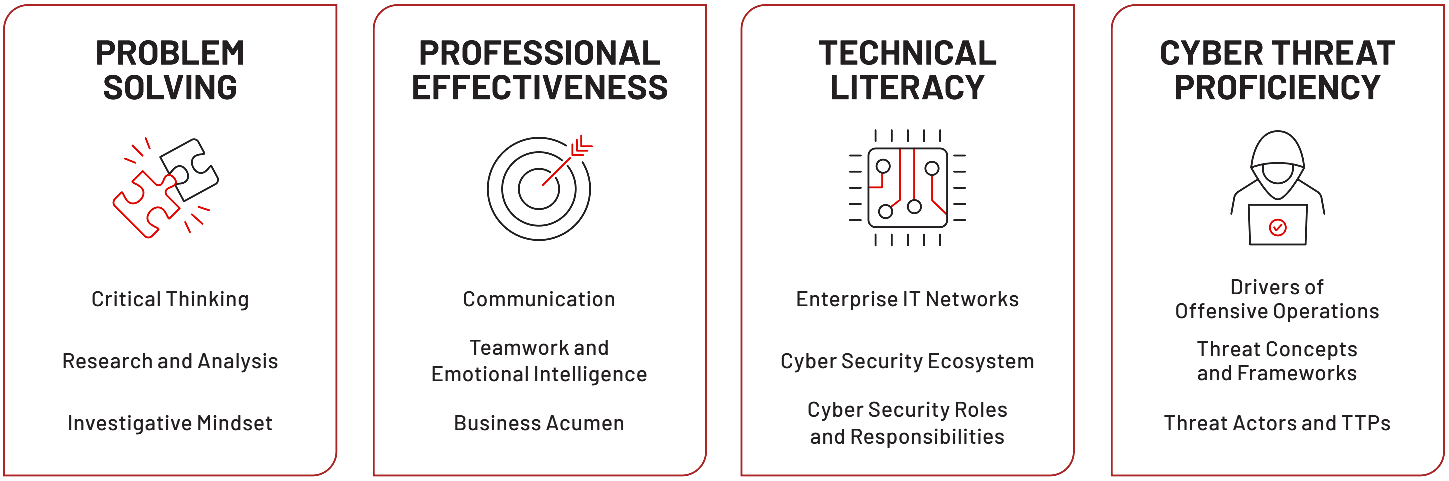
THE MANDIANT CYBER THREAT INTELLIGENCE (CTI) ANALYST CORE COMPETENCIES FRAMEWORK

Mandiant has developed a comprehensive Cyber Threat Intelligence (CTI) Analyst Core Competencies Framework as a guide for the CTI discipline to identify, build, foster, and retain talent. The Intelligence and National Security Alliance (INSA) in 2015[1] and Carnegie Mellon University in 2012 attempted to develop similar frameworks to identify the underpinning knowledge, skills and abilities (KSAs) requirements for CTI analysts.[2] However, the CTI discipline has evolved considerably since then, increasing the scope and scale of KSAs. Additional KSAs are the result of advancements in the information and communication technology field, such as the adoption of cloud computing and hybrid environments, the evolution of cyber security technologies and the subsequent shift in cyber adversaries' operational tradecraft.

Organizations can elect to use this Framework to identify areas for team or individual growth, determine appropriate developmental roadmaps and align internal, external or on-the-job training opportunities to support CTI skills progression. Some competencies take longer time to develop than others because of prerequisite KSAs. In this Framework, each competency includes a description that covers KSA requirements. If a competency represents more generalist skills, specific language covers the CTI use cases.

The Framework groups individual competencies into four pillars: problem solving, professional effectiveness, technical literacy and cyber threat proficiency.

Cyber Threat Intelligence (CTI) Analyst Core Competencies Framework



PROBLEM SOLVING

Critical Thinking

Research and Analysis

Investigative Mindset

PROFESSIONAL EFFECTIVENESS

Communication

Teamwork and Emotional Intelligence

Business Acumen

TECHNICAL LITERACY

Enterprise IT Networks

Cyber Security Ecosystem

Cyber Security Roles and Responsibilities

CYBER THREAT PROFICIENCY

Drivers of Offensive Operations

Threat Concepts and Frameworks

Threat Actors and TTPs

FIGURE 1. CTI pillars and core competencies.

This Framework was developed with input from several Mandiant and non-Mandiant CTI professionals, who reviewed it to ensure that content presented represents the realities of the CTI workforce. It is current as of May 2022.

[1] Intelligence and National Security Alliance (September 2015). Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats.

[2] Melissa Ludwick, Jay McAllister, Andrew O. Mellinger, Kathryn Ambrose Sereno, Troy Townsend (2013). Cyber Intelligence Tradecraft Project: Summary of Key Findings.

Problem Solving

Critical Thinking

The ability to conceptualize, identify, evaluate and synthesize information to formulate unbiased judgements, analytic lines and relevant recommendations. These judgements should be based on one's understanding of an organization's cyber threat realities, cyber security posture and alignment to an organization's mission, vision and goals. Analysts should be able to:

- Employ the intelligence lifecycle
- Identify first, second and third order effects
- Evaluate the credibility of intelligence sources based on reliability, level of access and placement
- Approach data sets and vendor reports using inductive and deductive reasoning
- Apply structured analytic techniques (SATs)[3] and peer review to mitigate inherent cognitive biases
- Ability to create and evaluate alternative competing hypotheses

Critical thinking also encompasses the ability to think outside-of-the-box to devise creative solutions and analytic frameworks for research, data collection and effective communication. Critical thinking is a fundamental prerequisite for innovation and trend forecasting.

Research and Analysis

The ability to capture stakeholder needs in the form of intelligence requirements and prioritize data sets and tooling against them in a collections management framework. Research uses logic and sound reasoning to investigate technical and non-technical data sources to uncover new leads, identify new connections, and reach clear analytic conclusions. CTI research can range from extracting indicators of compromise to identifying files that share similar characteristics to finding associated malicious infrastructure used by a cyber threat group. Analysis involves interpreting and synthesizing the results of research.

- Understanding the utility and limitations of various type of indicators of compromise (IOCs)—atomic, computed, and behavioral
- Identifying what data is needed to enrich existing data sets, where to procure it and how to integrate it.
- Ability to analyze malware, inspect network traffic, and triage log events data

Research skills include the ability to mine, interpret, extract, store, and pivot on relevant content found in the following types of internal, commercial, and open source data sets to enrich existing intelligence collection and understanding of cyber threat groups:

- Passive DNS (pDNS) records. Example: PassiveTotal/RiskIQ and Domain Tools
- Netflow data. Example: Team Cymru Augury
- Internet scan data. Example: Shodan and Censys.io
- Malware zoos. Example: VirusTotal, HybridAnalysis, and any.run
- Network traffic. Example: Packet captures (PCAP)
- Sandbox submissions
- Host-based system event logs

Analytic skills include the ability to query data sets, develop logical data schema and tagging, normalize and apply structure to unstructured data and interpret findings to identify trends and patterns over time. Research and analysis skills also include the ability to examine technical artifacts whether or not they are host-based (such as scripts and compiled malware) or network-based (such as infrastructure relationships and domain name structure). Research and analysis are significantly aided by familiarity with scripting languages such as Python, SQL for interacting with datasets, execution environment such as Jupyter or Zeppelin notebooks, visualization tools like Tableau or PowerBI, and other tools to quickly manipulate data sets. Strong statistical reasoning skills are also critical and includes concepts such as hypothesis testing, statistical significance, conditional probability, sampling and bias.

Research and analysis also benefits from linguistic capability, cultural background and regional familiarity.

Investigative Mindset

The ability to understand complex challenges and develop out-of-the-box solutions to solve them. The investigative mindset requires a thorough understanding of cyber threat actors and their tactics, techniques and procedures (TTPs) as well as existing CTI frameworks, CTI tools, and IT systems. The investigative mindset involves maintaining an open mind to determine whether existing constructs, frameworks or tools require uplift, or if there is the need to develop new ones in response to innovations in adversary tradecraft or technologies. The investigative mindset also allows analysts to develop intuition and identify signals in noise. The investigative mindset is different than critical thinking and blends research and analysis with identifying and accounting for cognitive and logical biases and employing SATs to overcome them.

[3] Richards Heuer (1999). The Psychology of Intelligence Analysis.

Professional Effectiveness

Communication

The ability to present analytic conclusions, research and methodologies to various audiences in an effective manner through written finished intelligence (FINTEL) products, slide decks, emails, Confluence or SharePoint pages, internal tickets and briefings. The Bottom-Line Up-Front (BLUF) and an executive summary are two effective methods for presenting analytic findings.

A core tenet is the ability to identify and adapt communication style. This covers medium, language, message, cadence and preference for different audiences, ranging from the strategic, executive level to highly technical practitioners, such as detection engineers and security architects. This also includes working with the media and external liaison partners. Existing CTI frameworks can be used to graphically represent organizational threat models, intrusion activities, adversary operational workflows and the relationship between technical and non-technical adversary artifacts. Examples include:

- Organizational threat realities modeled in a cyber threat profile
- Adversary operational tradecraft using a CTI-centric kill chain
- Clustering intrusion activity to define an intrusion set or activity group
- Adversary workflows, playbooks, and hunt packages using standardized vernacular
- Connections between adversary tools, infrastructures, personas and suspected affiliation using Maltego, MISP or other link analysis tools, workbenches or hypergraphs

It is important to have the ability to clearly convey judgements using probabilistic language so judgements can be uncoupled from facts and direct observations. Of related importance is the ability to use precise language to ensure the intended message is properly conveyed and does not prompt unnecessary alarm. Employing storytelling frameworks such as AIMS—audience, intent, message and story—helps analysts convey assessments.

Finally, awareness of information sharing standards and communities of interest is critical. This includes technology standards such as Structured Threat Information Expression (STIX)[4] or JavaScript Object Notation (JSON) to share information between machines using Trusted Automated eXchange of Intelligence Information (TAXII)[5] or other conduits, industry specific information sharing groups and private-public Information Sharing and Analysis Centers and Organizations (ISACs and ISAOs).[6] Familiarity with cyber policy and law enforcement mechanisms used to counter cyber actions to include takedowns, sanctions, indictments, raids, and public awareness and advisory campaigns.

Teamwork and Emotional Intelligence

The ability to interact effectively with peers and leadership to build a collaborative culture that embraces diversity in backgrounds, skills, knowledge, and experiences to identify and answer key intelligence questions (KIQs). Drawing on individuals' unique characteristics helps teams provide peer mentoring and learning opportunities to fill knowledge and skills gaps while building a culture of cohesion and trust. Being able to work with stakeholders to elicit information about business operations, information shortfalls and decision-making processes can inform threat intelligence processes and improve success.

Emotional intelligence includes fostering good judgement and situational awareness to understand when and how to engage peers, leadership, or clients while understanding the organizational impacts of adverse behaviors. Four core skills of emotional intelligence are self-awareness, self-control, social awareness and relationship management.

Business Acumen

The ability to understand an organization's mission, vision, goals and how business decisions could influence an organization's cyber risk exposure. Examples of such decisions include prospective mergers and acquisitions or expanded operational footprint into a new geography. Shifts in strategic direction may prompt an organization to re-evaluate risks to trade secrets and intellectual property. Cyber threat analysts may be required to provide a net assessment on change in risk exposure and revisit cyber groups that have the intentions, capability and opportunity to threaten the organization. Public commentary by an organization's leadership may also have cyber risk implications. CTI analysts should be able to understand and evaluate outcomes for threat intelligence in terms of demonstrable value to the business.

It is important to be aware of how organizational structure and internal politics within an organization's construct affect cyber security collaboration and decisions. Business acumen includes understanding the lexicon, terminology and frame of reference used by various organizational elements. It allows analysts to articulate findings to better resonate with stakeholders, which may include conveying threat in the context of risk, expressing return on investment for implementing certain cyber security measures or conveying budgetary needs. Ideally, keen business acumen translates to finding alignment opportunities within each phase of the Intelligence Lifecycle.

[4] Sean Barnum (2012). Structured Threat Information eXpression (STIX).
[5] Julie Connolly, Mark Davidson, Matt Richard, and Clement Skorupka (2012). The Trusted Automated Exchange of Indicator Information (TAXII).
[6] Cybersecurity & Infrastructure Security Agency (CISA) (February 22, 2022). Information Sharing and Awareness.

Technical Literacy

Enterprise IT Networks

The ability to understand operating systems principles, which include:

- Design decisions inherent to system architecture and implications on file storage, memory management and network connections
- How identities, access and authorization are administered, provisioned and managed on internal and domain-connected workstations and servers
- How security roles and attributes are assigned to user accounts and processes
- Information stored natively in the operating system's event logs
- How user credentials, remote connections, and shared drive mappings are stored
- Role the kernel plays in security policy enforcement
- How systems communicate with one another and the protocols used for certain types of communication. Examples include RDP, SSH, SMB, FTP, DNS and HTTP(S)
- Functionality to forward events to a centralized logging platform

The ability to understand business decisions around enterprise network design:

- Why enterprise networks often use a virtualized environments over physical workstations and servers
- Why certain operating systems are preferred over others to meet business needs
- How technology advancements and adoption of cloud computing service offerings augment business functionality and the security implications of an expanded network perimeter

Cyber Security Ecosystem

The ability to identify the core concepts, components and conventions associated with cyber defensive measures and cyber security processes, technologies and job roles. A core tenet is knowledge of industry best practices and frameworks such as the National Institute of Science and Technology's (NIST) Cyber Security Framework (CSF)[7] and how defensive approaches and technology align to at least one of the five cyber defense phases (identify, protect, detect, respond and recover).

Key concepts:

- Access control
- Identity and access management
- Multifactor authentication
- Need-to-know
- Network segmentation
- Public Key Infrastructure (PKI)
- Symmetric and asymmetric cryptography use cases
- Signature-based and behavior-based detection. Examples: Yara and Snort
- Fuzzy hashing algorithms. Examples: SSDeep
- Threat hunting and incident response
- Red team, purple team and proactive cyber defense
- Zero Trust Architecture

Key plans, processes, and policy documents

- Business continuity plan (BCP)
- Disaster recovery plan (DRP)
- Incident response (IR) plan

System profiling, standardization and account management:

- IT asset inventory management
- Configuration management and golden images
- Privileged account management

[7] The National Institute of Standards and Technology (NIST) (2018). The Cybersecurity Framework.

Security-centric technologies:

- Network and boundary devices
  - Firewalls
  - Email inspection and sandboxing
  - Intrusion detection and prevention systems (IDS/IPS)
  - Netflow collectors
- Endpoint
  - Antivirus
  - Endpoint detection and response (EDR)
  - Extended detection and response (XDR)
- Centralized log collection and related technologies
  - Security incident and event management (SIEM) systems
  - User entity behavior analytics (UEBA)
  - Security orchestration, automation and response (SOAR)

Organizational Cyber Security Roles and Responsibilities

The ability to understand cyber security and cyber security-adjacent job roles, responsibilities, and the interplay between the various functions within an organization

- Security operations center (SOC) Tier 1 watch floor analyst
- SOC Tier 2 analyst and incident responder
- SOC Tier 3 analyst and team lead
- Forensic analyst
- Reverse engineer
- Vulnerability analyst
- Security architect
- Detection engineer
- Red team
- Blue team
- Purple team
- Governance, risk management and compliance (GRC)
- Chief privacy officer
- IT support and help desk

For analysts, an established RACI (responsible, accountable, consulted and informed) matrix and service level agreements (SLAs) can clarify the expectations and responsibilities for peer review, intelligence product development and requests for additional information with the cross-functional cyber defense partners.

Cyber Threat Proficiency

Drivers of Offensive Operations

The ability to characterize the organizational composition of an offensive cyber program, its constituent job functions, and operational decisions that affect capability development and potential impact on achieving mission objectives. Such decision points include allocating finite resources to outsource elements of the cyber program to purchase operational tools, enlist contractor support, or purchase criminal capabilities. Additional decision points include coercing individuals and companies to support such programs based on legal authorities and creating operational front companies.

The secondary tenet of this competencies is to identify the underpinning motivations behind why nation-state, criminal, and ideologically motivated hackers conduct cyber operations, their historic context, and associated significance. This includes nation-states using cyber operations as a tool of statecraft to achieve geopolitical objectives, ranging from conducting espionage to steal diplomatic or military information on an enemy's bilateral or multilateral position in anticipation of negotiations to cyber-enabled influence operations to disruptive attacks in the lead up to and during a military action.

A keen understanding of acceptable operations undertaken during peace time and how this shift during a war time is critical. Additionally, analysts should be able to identify operations that throttle the line of acceptable use and push existing norms to include operations undertaken such as those that impact water purification ability in a water-scarce region of the world.

Similarly, a key tenet in this competency is the ability to recount the history and evolution of adversary operations and tradecraft per cyber threat groups. A large base of historical examples can help chart the evolution of the use and drivers of cyber operations, allowing analysts to identify trend lines and deviations between threat groups. This also includes the ability to forecast targeting efforts based on relation to national, enduring objectives or in response to tactical situations versus identifying potential targets of opportunity.

Threat Concepts and Frameworks

The ability to identify and apply appropriate CTI terms and frameworks to track and communicate adversary capabilities or activities. This competency also includes understanding the evolution of cyber threat terms, reasoning behind the development of various CTI frameworks and what problems they helped the CTI community overcome. Cyber threats are defined as a function of actor intention/motivation, capabilities and opportunity. This competency focuses heavily on threat actor capabilities.

- Vulnerabilities and exploits
  - The Common Vulnerability Scoring System (CVSS)[8]
  - Common Vulnerability and Exposure (CVE)[9] system
  - Software vulnerability categories
  - Not all vulnerabilities can be exploited
  - Zero-day and n-day vulnerabilities
  - Exploit development and vulnerability weaponization
  - Exploit and infection chains
  - The patch management lifecycle
  - Exploit procurement gray market
  - Role of bug bounty programs
- Malware
  - Ability to explain a malware execution chain from stage 1 droppers to launchers to post-exploitation tools
  - Ability to explain how adversaries interact with malware through command and control (C2) servers
  - Ability to explain how malware communicates with C2 servers
  - Ability to explain the differences in the utility of using scripts compared to compiled malware
  - Ability to identify modular malware or use of builders
  - Malware-as-a-service marketplaces

[8] The National Institute of Standards and Technology (NIST) (1999). The National Vulnerability Database Common Vulnerability Scoring System (CVSS).
[9] David Mann and Steven Christey (1999). Towards a Common Enumeration of Vulnerabilities.

- Infrastructure
  - Differences in infrastructure used for malware and exploit delivery compared to C2 and data exfiltration
  - Selection and preference of hosting services
  - Privacy protections offered by hosting providers or based on EU Privacy Directives
  - Dynamic DNS
- Attribution, intrusion clustering, and naming conventions
  - Characteristics of intrusion activity
  - Creating intrusion set clusters to characterize activity types
  - Ability to identify and differentiate unique, novel attributes of intrusion activity and common ones as anchoring functions to support attribution and clustering efforts
  - Vendor naming convention for intrusion activities of cyber groups and why vendors do not often borrow existing names from one another
  - How to map various vendor names to identify similar cyber threat group threat activities
- CTI Frameworks
  - Factor Analysis of Information Risk (FAIR)[10] or Vocabulary for Event Recording and Incident Sharing (VERIS)[11] for threat modeling
  - The Lockheed Martin Cyber Kill Chain, Mandiant Targeted Attack Lifecycle, or the Unified Cyber Kill Chain to visually depict the discreet phases of an adversary's operation
  - The Diamond Model of Intrusion Analysis to cluster, track, and group intrusion activities
  - The MITRE ATT&CK framework of adversary operational TTPs
  - MITRE ATT&CK Navigator to create time delimited playbooks of adversary TTPs

Threat Actors and TTPs

The ability to discern vendor naming convention used across cyber threat groups, their nation-state or criminal affiliation, and an understanding of the tactics, techniques, and procedures (TTPs) certain groups employ during cyber operations. A critical tenet in this competency is for analysts to be able to identify key indicators across a cyber kill chain to determine adversary operational workflows and preferences. Such preferences also account for hosting provider selection for operational infrastructure and network anonymization technologies.

Analysts should be able to enumerate the range of initial access vectors and identify how various threat groups exhibit operational preference ranging from spearphishing to using compromised websites for payload delivery to conducting close-access operations in the vicinity of a target's physical location. Likewise, analysts should understand common internal reconnaissance commands adversaries use to perform system, network, and file discovery. This includes understanding lateral movement techniques such as using proxy chains, modifying IP tables, or port or reverse forwarding to include pros and cons of each.

Analysts should be able to explain why threat groups often only maintain a few footholds into a victim's network, rely almost exclusively on a singular system in a victim's network for data staging, and employ different command and control servers across exploitation, beaconing, interactive operations, and exfiltration. Similarly, analysts should be versed in the reasoning behind why a cyber operator would prefer to employ malware instead of interacting directly with a remote shell. Lastly, analysts should be able to explain why and how threat groups employ network-based obfuscation such as protocol tunneling, host-based anti-forensic techniques, and host-based obfuscation inside of malware.

[10] Risk Management Insight LLC (2006). An Introduction to Factor Analysis of Information Risk (FAIR).
[11] Verizon (2010). Vocabulary for Event Recording and Incident Sharing (VERIS) Project.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT