Cyber Threat Intelligence Analysts and You:

Understanding the Discipline to Optimize Cyber Defense Collaboration

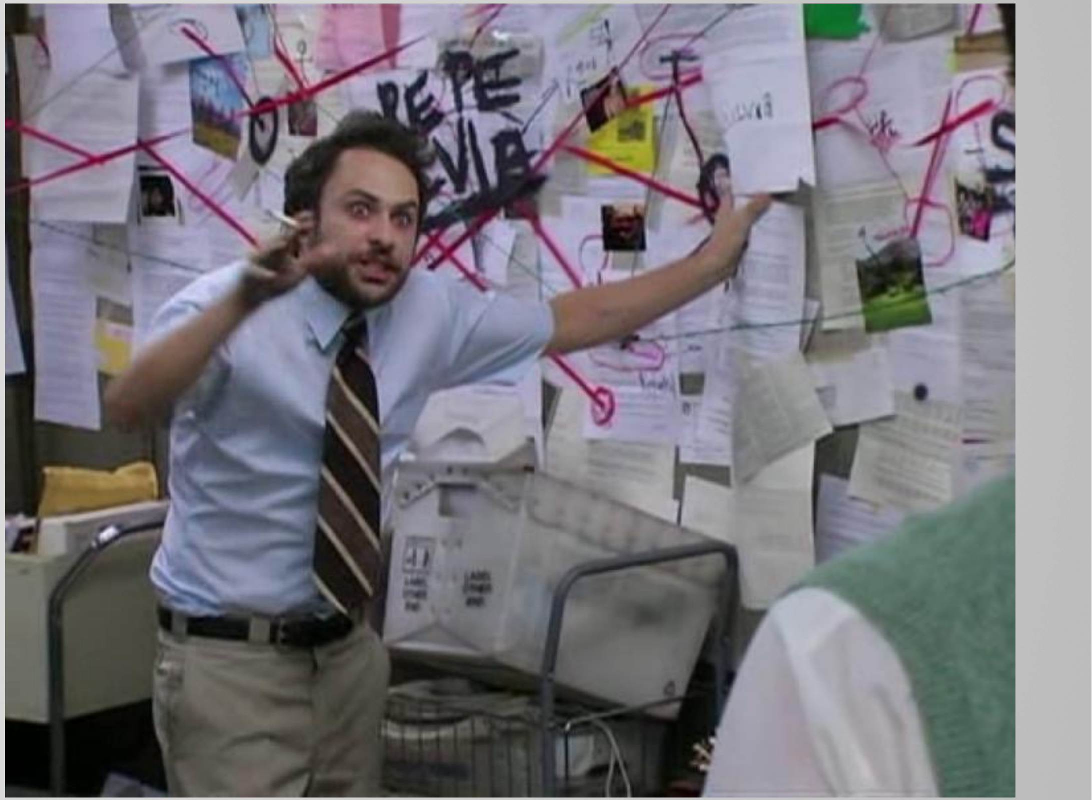
John Doyle

Foreword

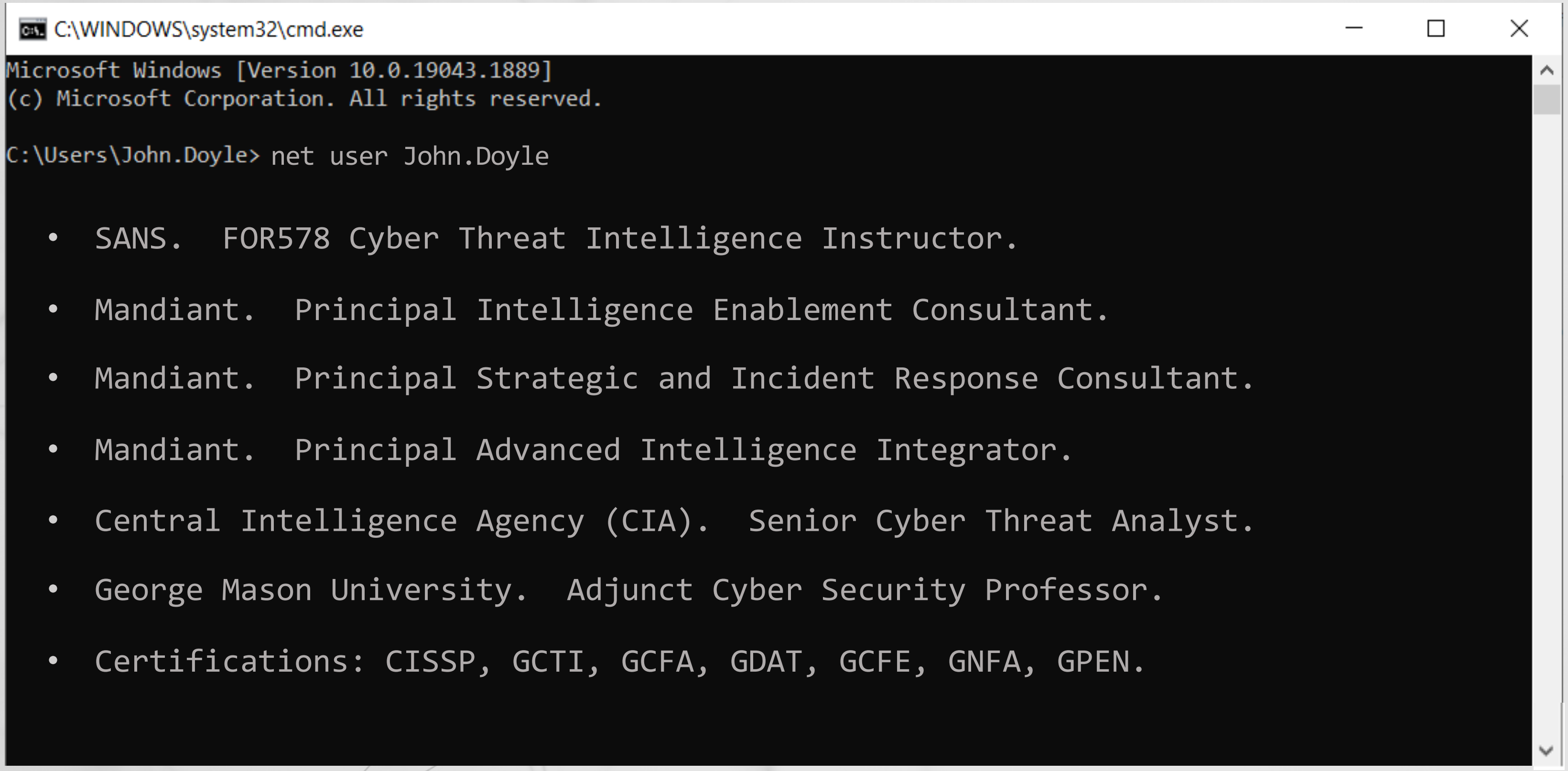
- All views represented in this presentation reflect my own and do not represent those of my employer.

Agenda

- Introduction
- Sharing a Common Frame of Reference
- CTI Support and Stakeholders
- CTI Analyst Core Competencies
- Parting Thoughts
- Q&A



whoami



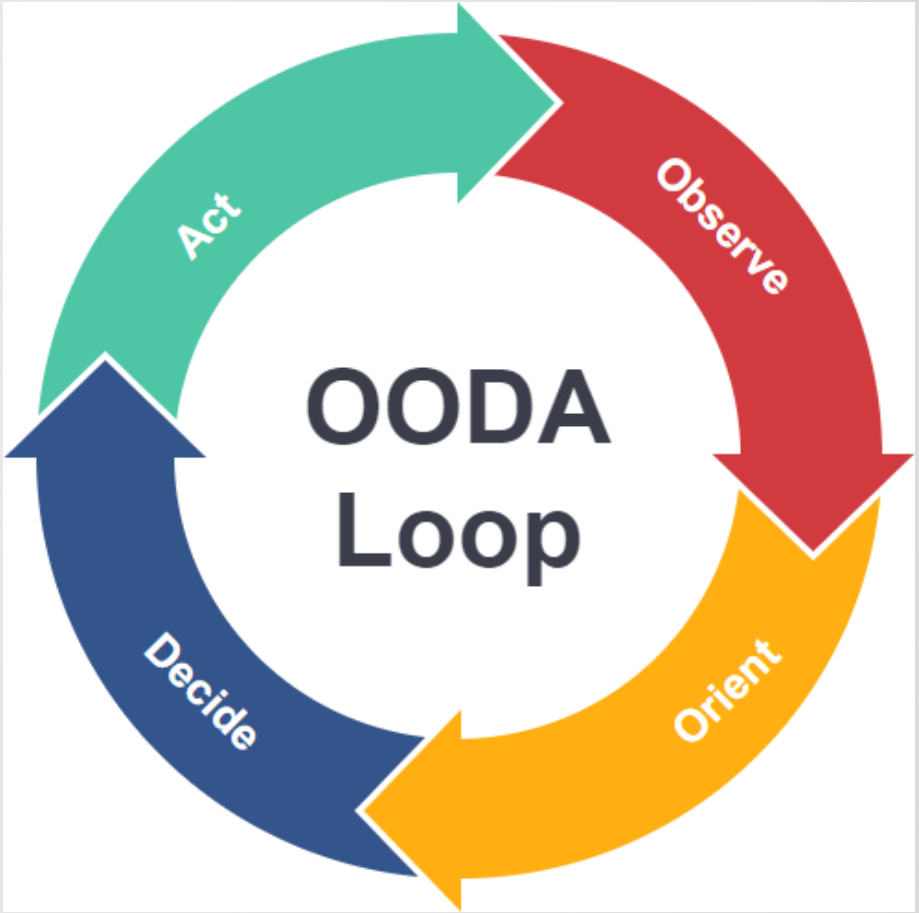
```
Microsoft Windows [Version 10.0.19043.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\John.Doyle> net user John.Doyle
```

- SANS. FOR578 Cyber Threat Intelligence Instructor.
- Mandiant. Principal Intelligence Enablement Consultant.
- Mandiant. Principal Strategic and Incident Response Consultant.
- Mandiant. Principal Advanced Intelligence Integrator.
- Central Intelligence Agency (CIA). Senior Cyber Threat Analyst.
- George Mason University. Adjunct Cyber Security Professor.
- Certifications: CISSP, GCTI, GCFA, GDAT, GCFE, GNFA, GPEN.

Sharing a Common Frame of Reference

./synergy.sh

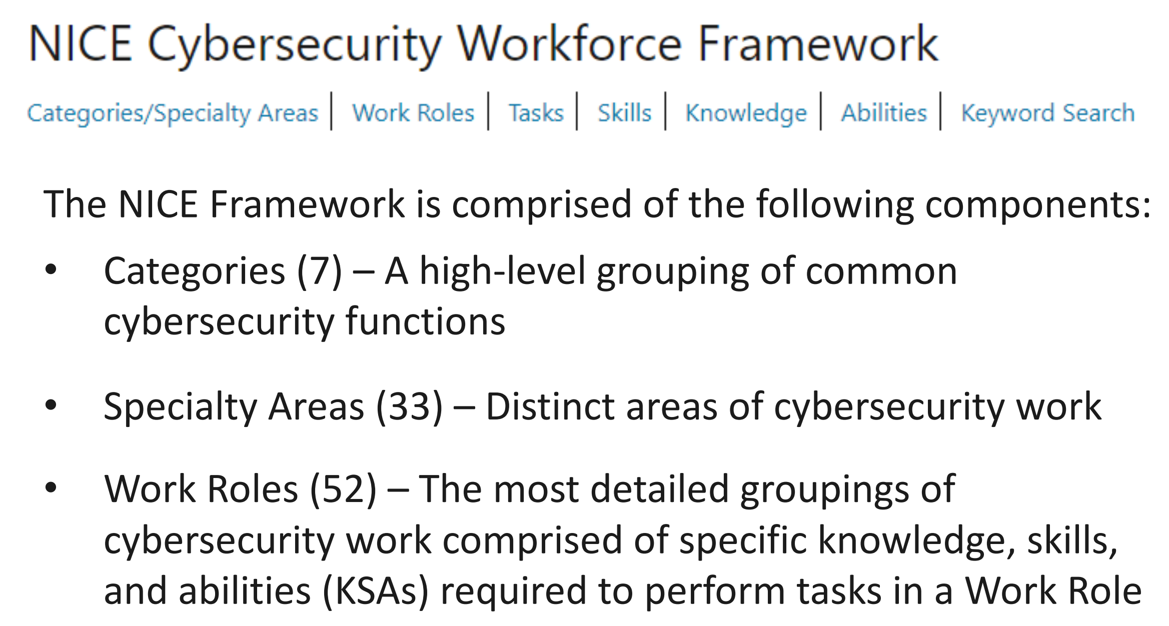
- Differential equations and race conditions are real in cyber security
- Defenders and attackers operate at various speeds to complete objectives
- Intelligence speeds up how quickly we can complete the defender’s OODA loop
- But first, we need a common operating picture of what everyone’s role is and how we contribute



Sharing a Common Frame of Reference

./synergy.sh

- Collaboration is most effective when we understand what each other do.

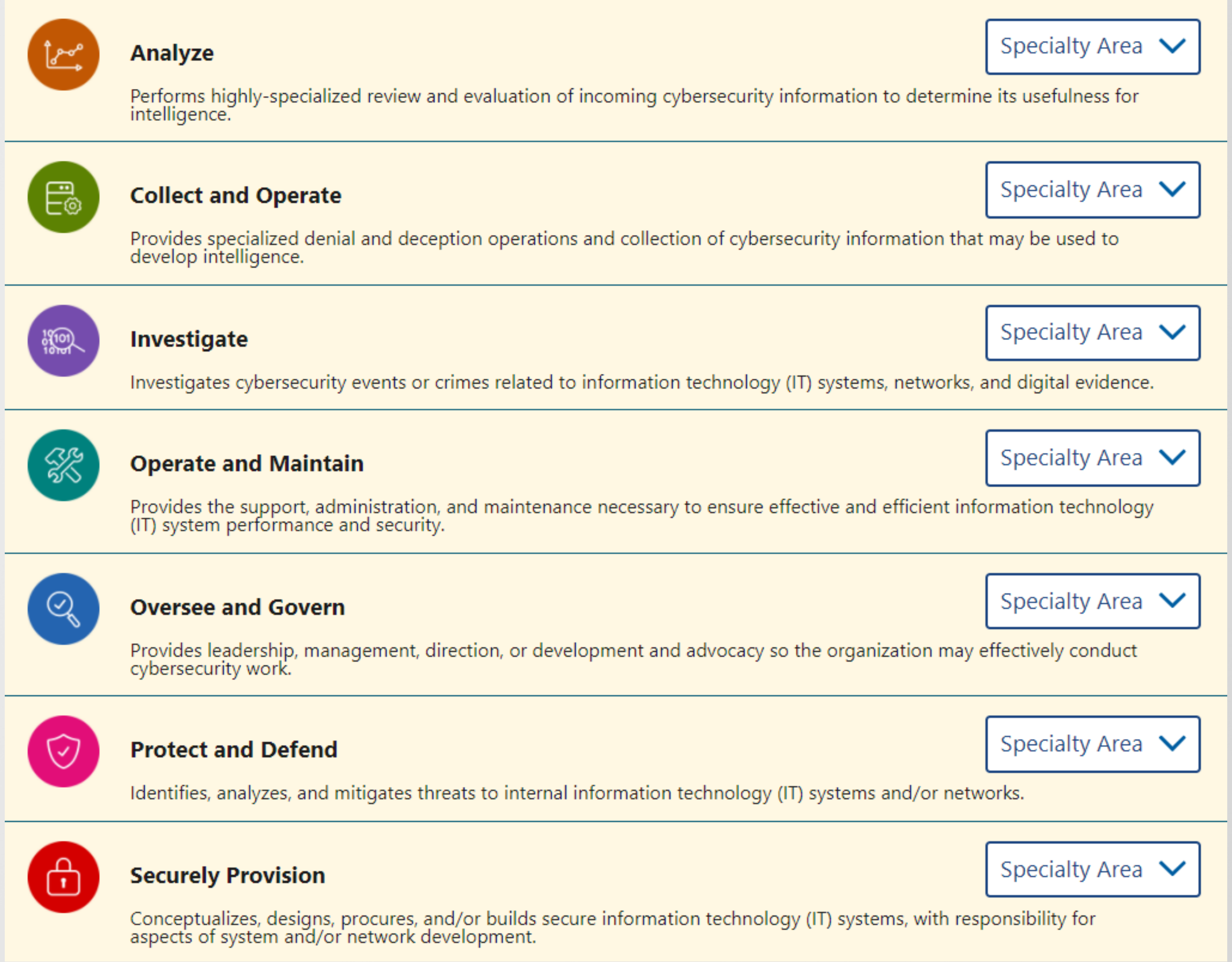


NICE Cybersecurity Workforce Framework

Categories/Specialty Areas | Work Roles | Tasks | Skills | Knowledge | Abilities | Keyword Search

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role



Analyze

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Investigate

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Protect and Defend

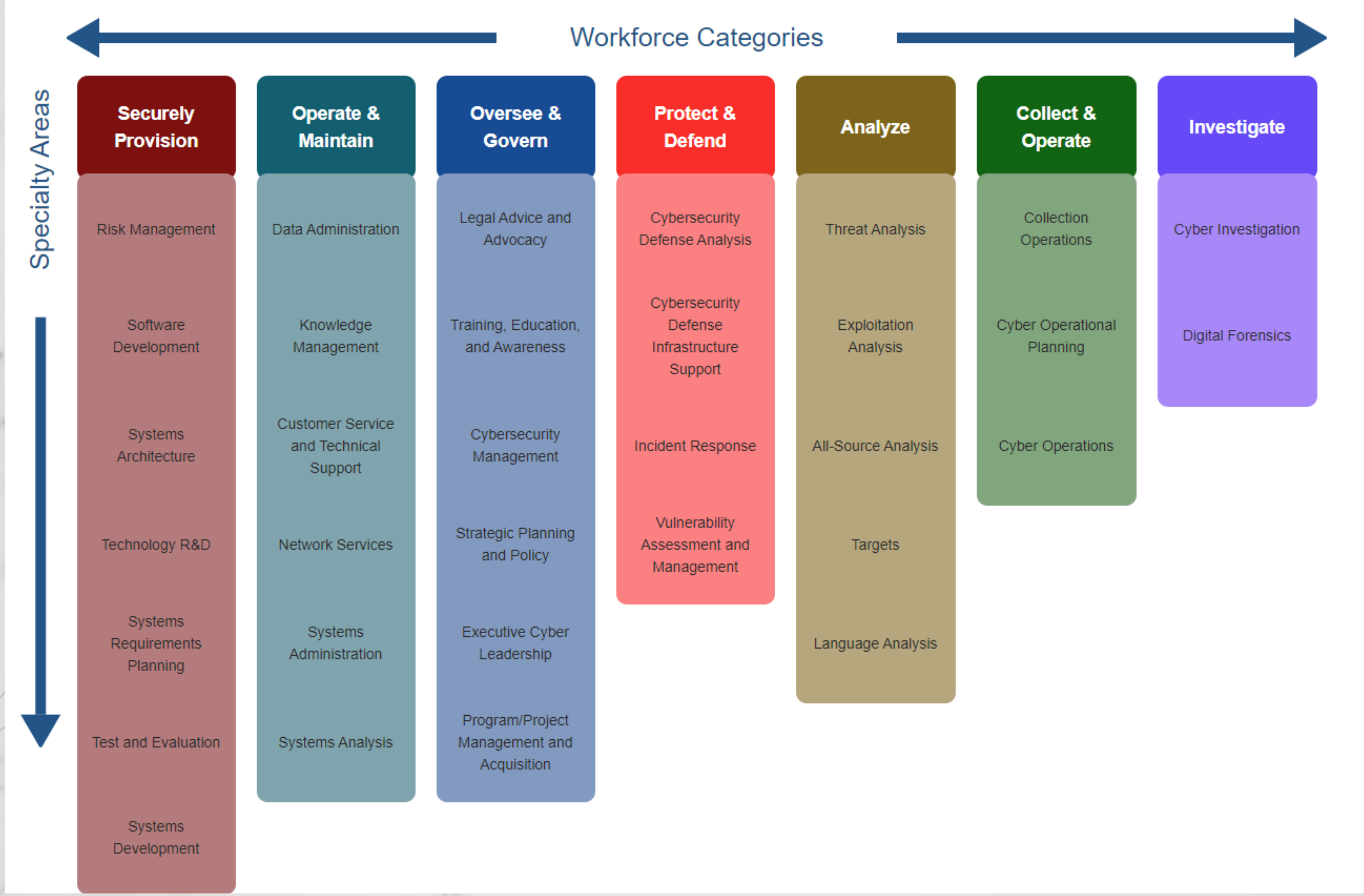
Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

Sharing a Common Frame of Reference

./synergy.sh



Workforce Categories

Specialty Areas

Securely Provision
- Risk Management
- Software Development
- Systems Architecture
- Technology R&D
- Systems Requirements Planning
- Test and Evaluation
- Systems Development

Operate & Maintain
- Data Administration
- Knowledge Management
- Customer Service and Technical Support
- Network Services
- Systems Administration
- Systems Analysis

Oversee & Govern
- Legal Advice and Advocacy
- Training, Education, and Awareness
- Cybersecurity Management
- Strategic Planning and Policy
- Executive Cyber Leadership
- Program/Project Management and Acquisition

Protect & Defend
- Cybersecurity Defense Analysis
- Cybersecurity Defense Infrastructure Support
- Incident Response
- Vulnerability Assessment and Management

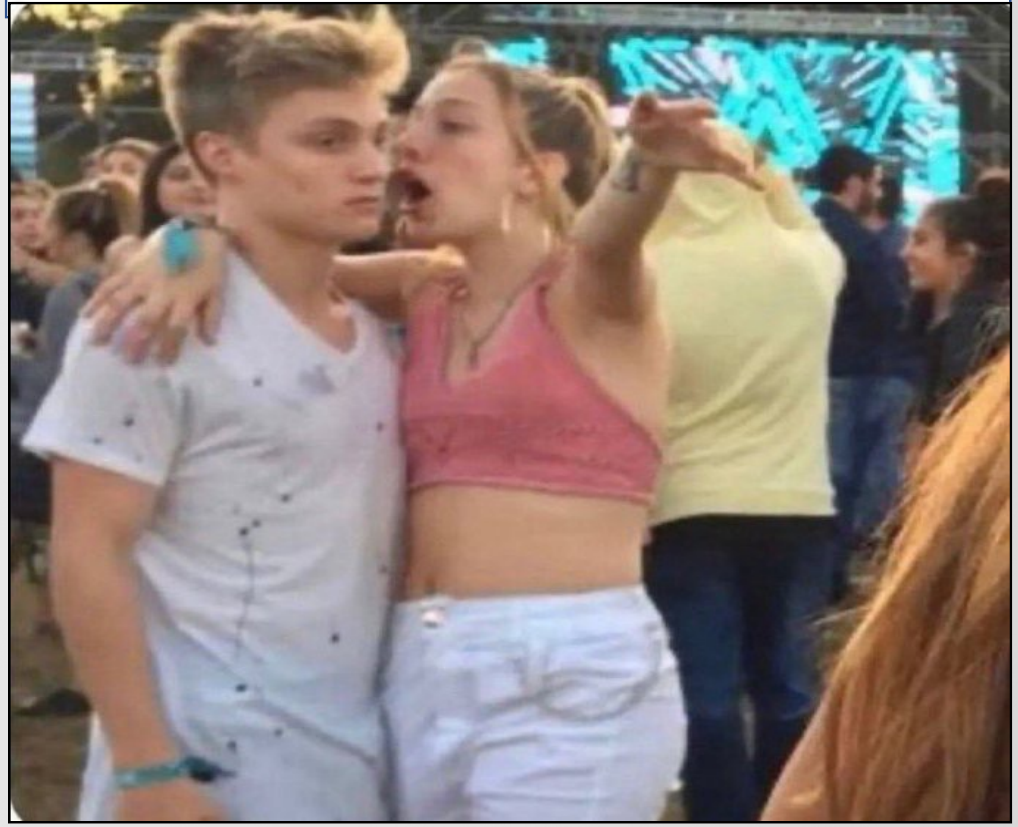
Analyze
- Threat Analysis
- Exploitation Analysis
- All-Source Analysis
- Targets
- Language Analysis

Collect & Operate
- Collection Operations
- Cyber Operational Planning
- Cyber Operations

Investigate
- Cyber Investigation
- Digital Forensics

CTI Support and Stakeholders

A CTI ANALYST PROVIDES TIMELY, RELEVANT, ACTIONABLE INSIGHTS ON THREAT ACTORS, CAPABILITIES, MOTIVATIONS, AND THE THREAT LANDSCAPE TO INFORM RISK EXPOSURE DECISIONS AND CYBER DEFENSE ACTIONS



CTI Support and Stakeholders

Audience Type:	Strategic	Operational	Tactical
Customer Roles:	• Chief Information Security • Security Management • Risk Management and Analysts	• Incident Response Team • Vulnerability Management Team • Forensics Team • Red Team • Purple Team	• Security Operations Center • Network Operations Center
Customer Tasks:	• Allocate resources • Communicate with executives	• Determine attack vectors • Patch systems • Remediate • Hunt for breaches	• Indicators to security tools
Problems They Face:	• No clear investment priorities • Executives are not technical	• Event reconstruction tedious • Difficult to identify damage • Difficult to prioritize patches	• False positives • Alert overload
Value-add from CTI:	• Demystify threats • Prioritize based on business risk	• Add context to reconstruction • Prioritize patches • Focus in on potential targets	• Validate and prioritize indicators • Prioritize alerts

CTI Support and Stakeholders

1 role to rule them all…

Strategic threat analyst

Cyber espionage analyst

Hunt analyst

Technical threat analyst

Threat researcher

Vulnerability intelligence analyst

Threat context analyst

Intrusion analyst

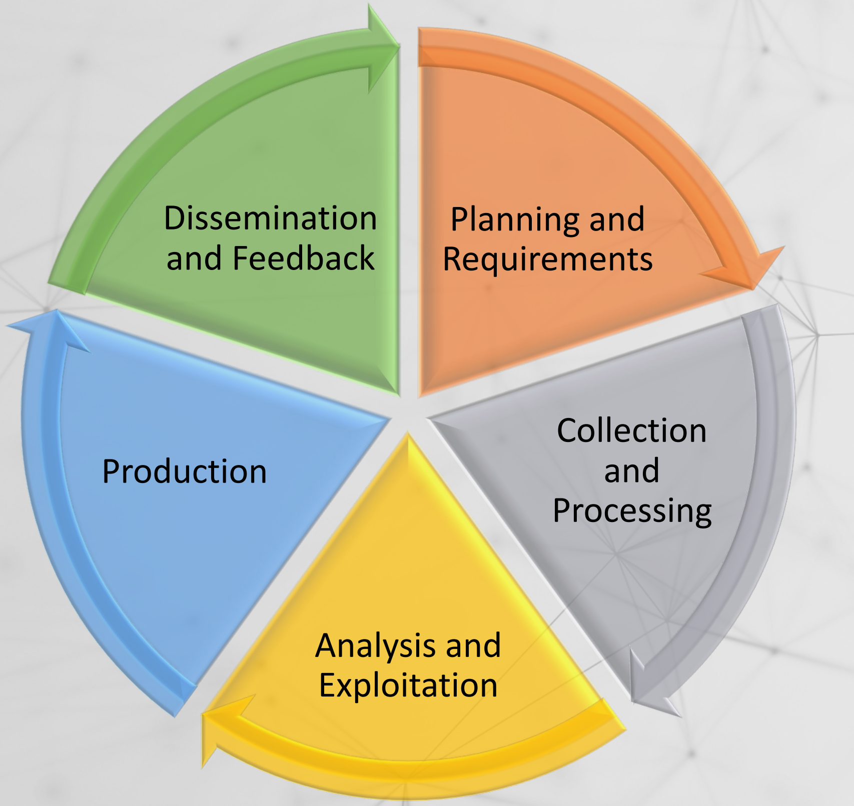
Intelligence engineer

eCrime analyst

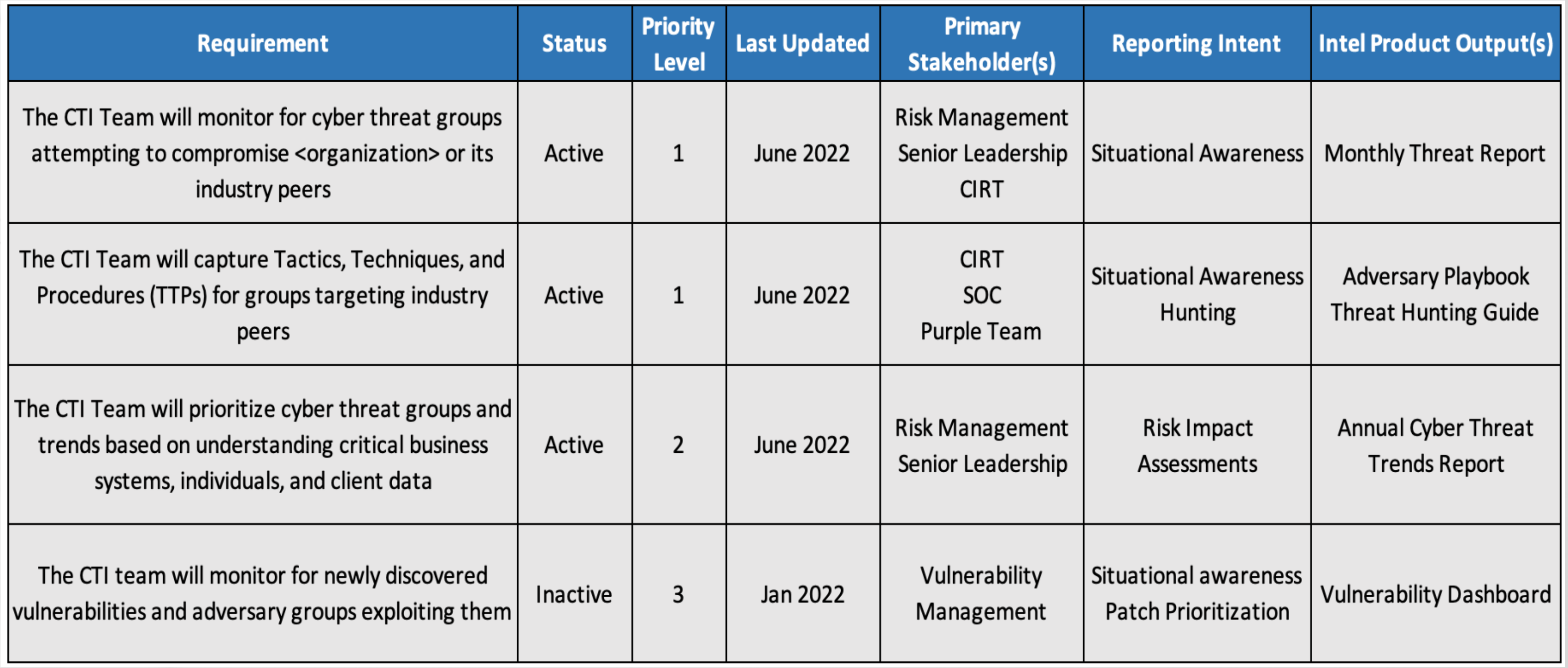
Threat hunter

Detection engineer

CTI Support and Stakeholders


Planning and Requirements
Collection and Processing
Analysis and Exploitation
Production
Dissemination and Feedback

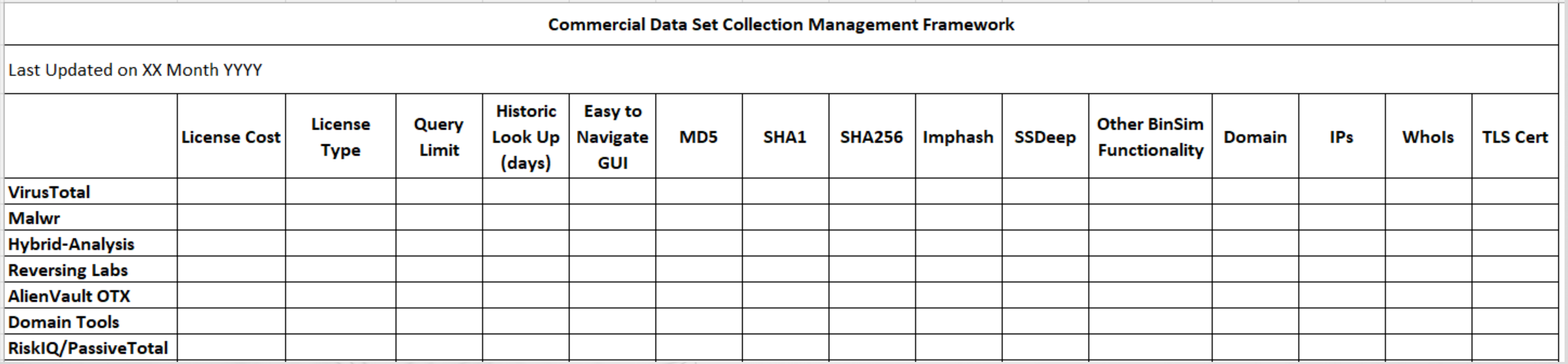
Intelligence Requirements Framework



Requirement	Status	Priority Level	Last Updated	Primary Stakeholder(s)	Reporting Intent	Intel Product Output(s)
The CTI Team will monitor for cyber threat groups attempting to compromise <organization> or its industry peers	Active	1	June 2022	Risk Management Senior Leadership CIRT	Situational Awareness	Monthly Threat Report
The CTI Team will capture Tactics, Techniques, and Procedures (TTPs) for groups targeting industry peers	Active	1	June 2022	CIRT SOC Purple Team	Situational Awareness Hunting	Adversary Playbook Threat Hunting Guide
The CTI Team will prioritize cyber threat groups and trends based on understanding critical business systems, individuals, and client data	Active	2	June 2022	Risk Management Senior Leadership	Risk Impact Assessments	Annual Cyber Threat Trends Report
The CTI team will monitor for newly discovered vulnerabilities and adversary groups exploiting them	Inactive	3	Jan 2022	Vulnerability Management	Situational awareness Patch Prioritization	Vulnerability Dashboard

CTI Support and Stakeholders

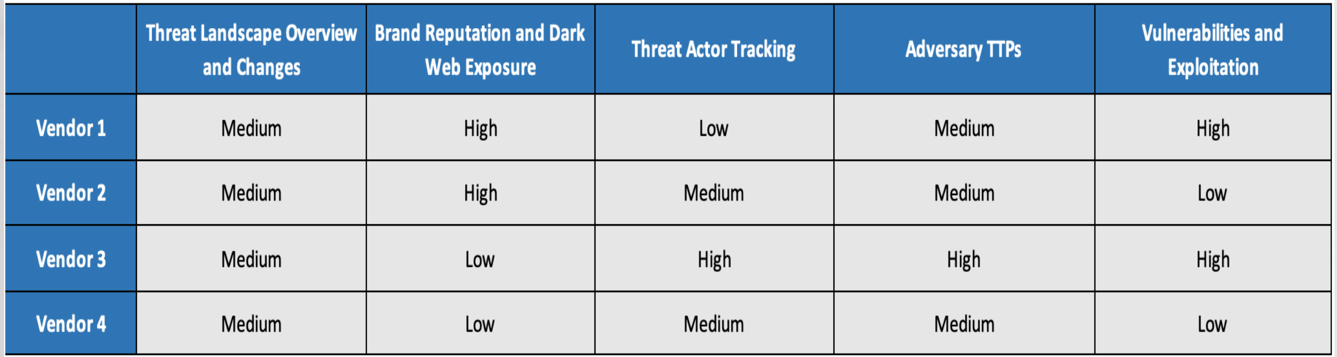
Collection Management Framework/Plan



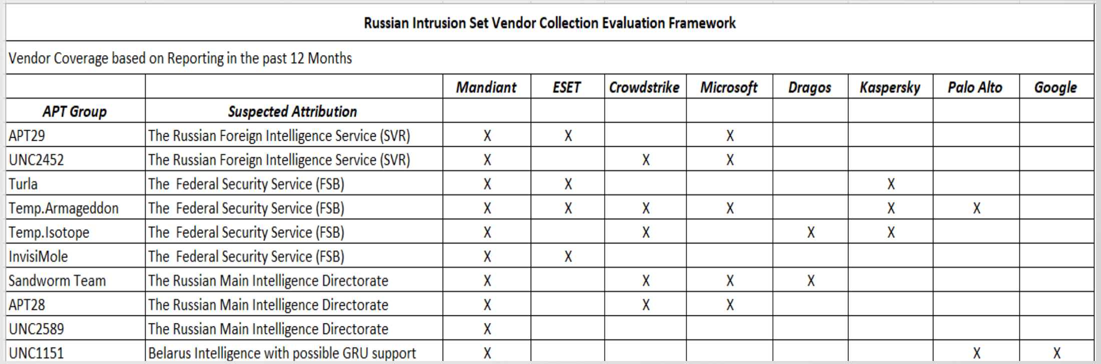
Commercial Data Set Collection Management Framework

Last Updated on XX Month YYYY

	License Cost	License Type	Query Limit	Historic Look Up (days)	Easy to Navigate GUI	MD5	SHA1	SHA256	Imphash	SSDeep	Other BinSim Functionality	Domain	IPs	WhoIs	TLS Cert
VirusTotal															
Malwr															
Hybrid-Analysis															
Reversing Labs															
AlienVault OTX															
Domain Tools															
RiskIQ/PassiveTotal															



	Threat Landscape Overview and Changes	Brand Reputation and Dark Web Exposure	Threat Actor Tracking	Adversary TTPs	Vulnerabilities and Exploitation
Vendor 1	Medium	High	Low	Medium	High
Vendor 2	Medium	High	Medium	Medium	Low
Vendor 3	Medium	Low	High	High	High
Vendor 4	Medium	Low	Medium	Medium	Low



Russian Intrusion Set Vendor Collection Evaluation Framework

Vendor Coverage based on Reporting in the past 12 Months

		Mandiant	*ESET*	*Crowdstrike*	*Microsoft*	*Dragos*	*Kaspersky*	*Palo Alto*	*Google*
APT Group	***Suspected Attribution***								
APT29	The Russian Foreign Intelligence Service (SVR)	X	X		X				
UNC2452	The Russian Foreign Intelligence Service (SVR)	X		X	X				
Turla	The Federal Security Service (FSB)	X	X				X		
Temp.Armageddon	The Federal Security Service (FSB)	X	X	X	X		X	X	
Temp.Isotope	The Federal Security Service (FSB)	X		X		X	X		
InvisiMole	The Federal Security Service (FSB)	X	X						
Sandworm Team	The Russian Main Intelligence Directorate	X		X	X	X			
APT28	The Russian Main Intelligence Directorate	X		X	X				
UNC2589	The Russian Main Intelligence Directorate	X							
UNC1151	Belarus Intelligence with possible GRU support	X						X	X

CTI Analyst Core Competencies

Intelligence Analysts

- Generalists
- Able to quickly understand content and apply context
- Communicates effectively
- Understand human biases in cognition and logic
- Introspects frequently, using system 1 thinking
- Regularly asks what are we missing and identifies strategies to fill existing gaps

IT/Information Security Practitioners

- Deep technical expertise
- Leverages intuition, understands interconnections and next steps
- Understands technologies and their limitations
- Understands system security
- Understands information security roles and responsibilities
- Aware of when to leverage other teams
- Not usually excited about, prefer, or desire to document, write reports, or communicate

Cyber Threat Intelligence Analysts

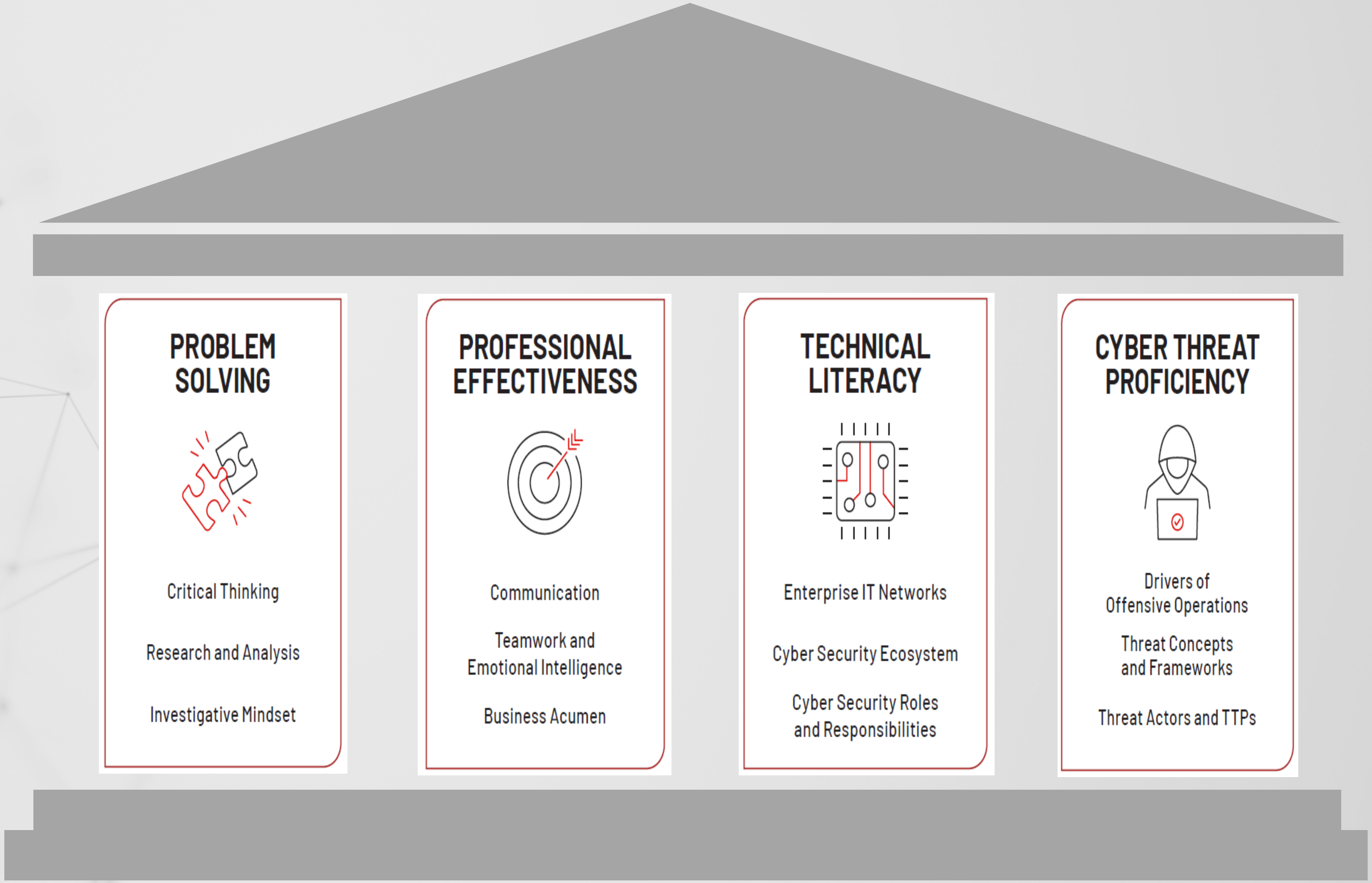
CTI Analyst Core Competencies

Cyber Threat Intelligence Analysts

- Translation layer, able to tell compelling stories
- Able to contextualize technical and non-technical content
- Deep understanding of cyber intrusions and actor motivations
- Driven by passion and intellectual curiosity
- Ability to aggregate, synthesize, and draw insights and trends from data sets
- Considers realm of possible before arriving at decisions
- Ability to enrich existing data while understanding tool and data set limitations
- …and more!

CTI Analyst Core Competencies

- “Mandiant Cyber Threat Intelligence Analyst Core Competencies Framework” published in May 2022
- Helps solve 3 problems:
  - Empower analyst growth pathways
  - Provide aspirant analysts developmental guideposts
  - **Raise awareness of CTI roles and responsibilities to cyber security partners**
- Broken into 4 pillars with 12 competency areas with 178 defined KSAs
- Thanks to James Sadowski, Kelli Vanderlee, Steve Stone, Jeff Compton, Joe Slowik, and Jake Williams for helping develop this 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

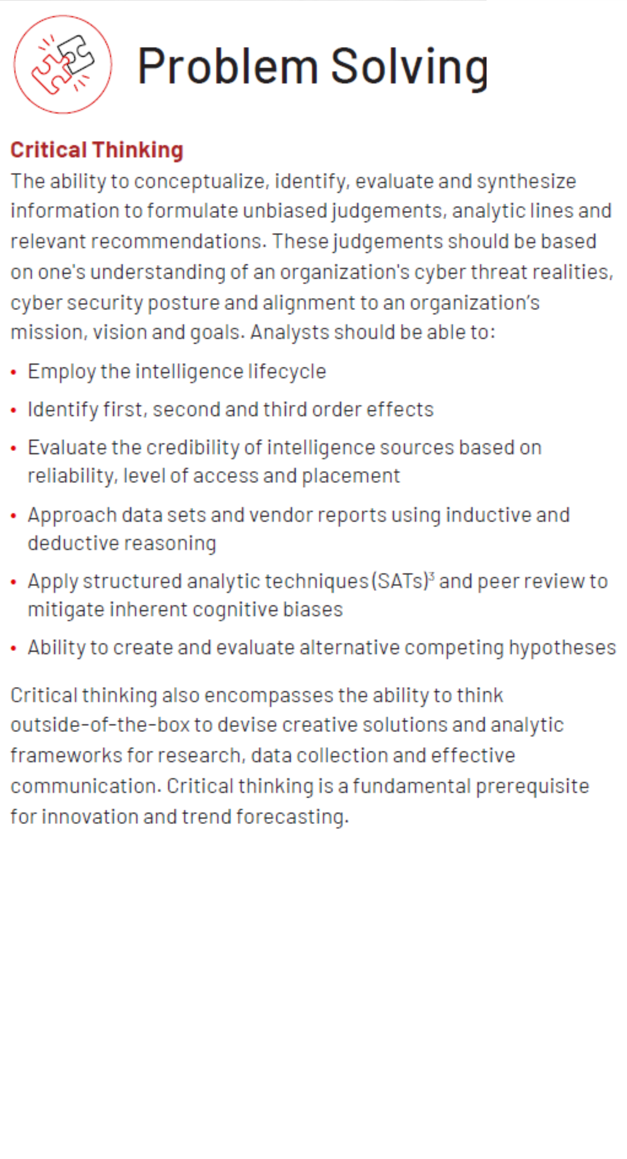
CYBER THREAT PROFICIENCY

Drivers of Offensive Operations

Threat Concepts and Frameworks

Threat Actors and TTPs

CTI Analyst Core Competencies



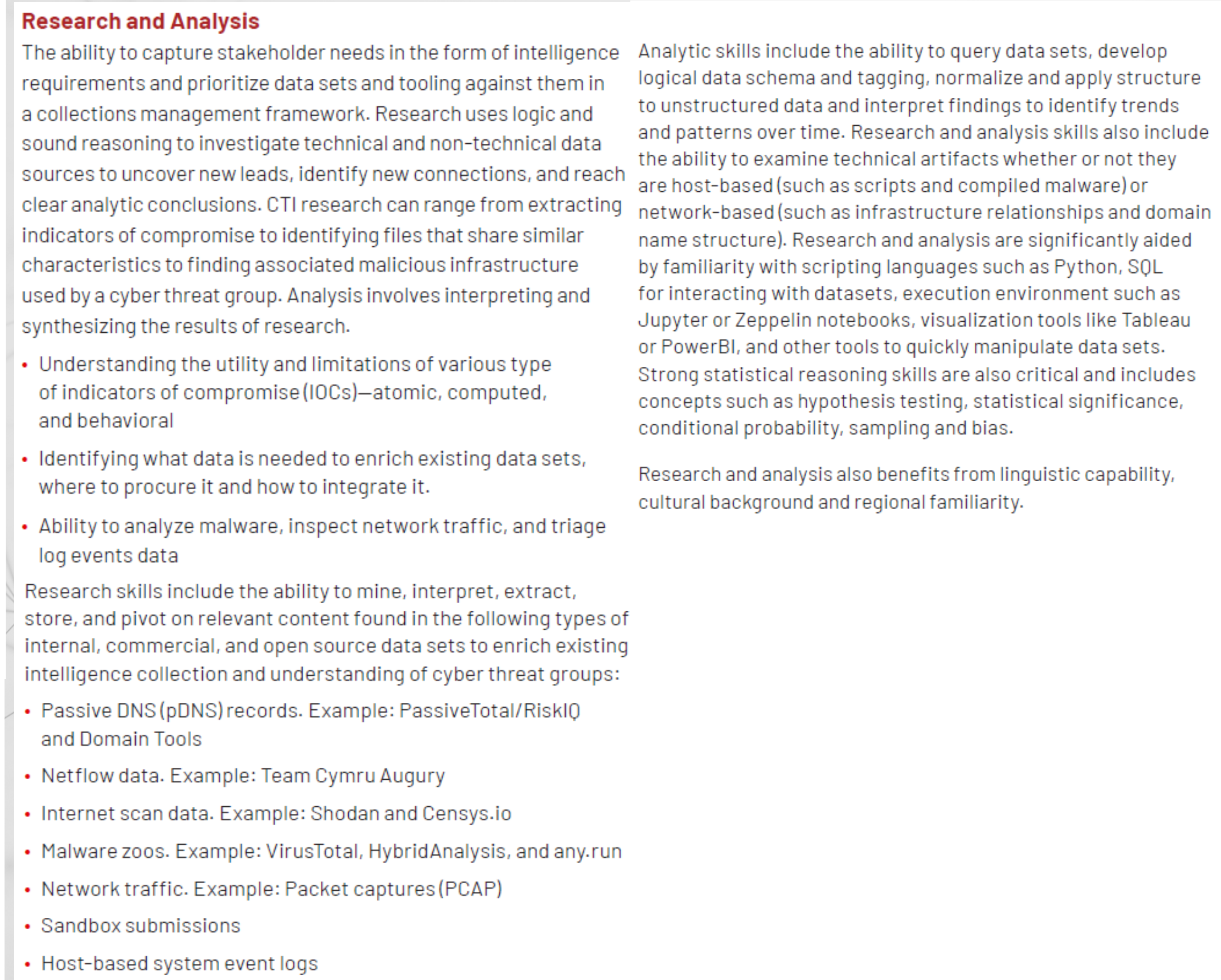
Problem Solving

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.

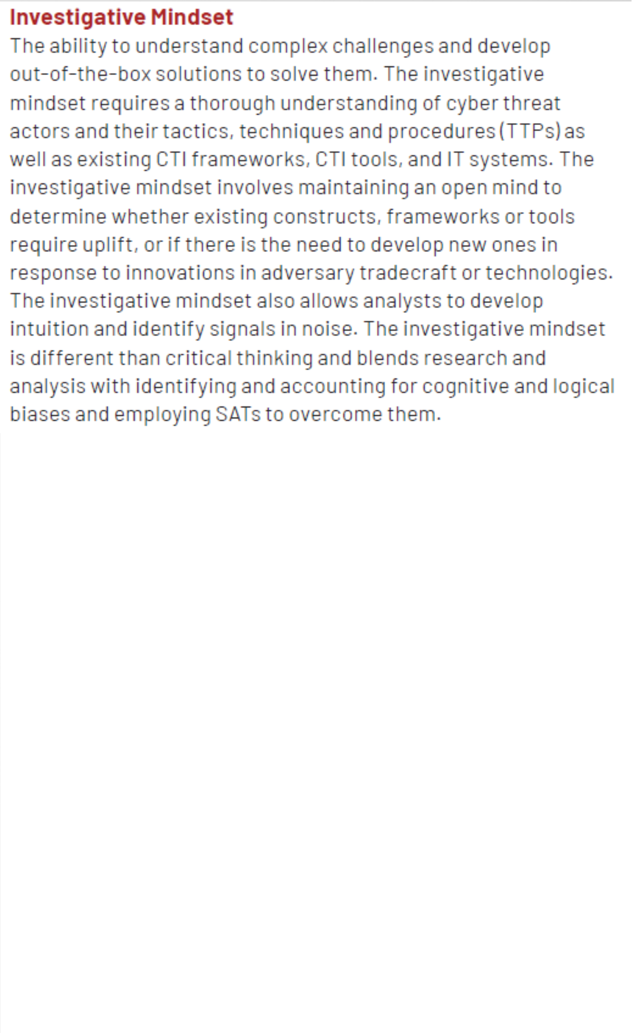
- Understanding the utility and limitations of various type of indicators of compromise (IOCs)—atomic, computed, and behavioral
- Identifying what data is needed to enrich existing data sets, where to procure it and how to integrate it.
- Ability to analyze malware, inspect network traffic, and triage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

CTI Analyst Core Competencies

Problem Solving

Critical Thinking

- Apply logic and reasoning
- Undertake efforts that align with the business
- Considers current and future needs
- Deep knowledge on industry construct and trends
- Ability to devise out-of-the-box solutions

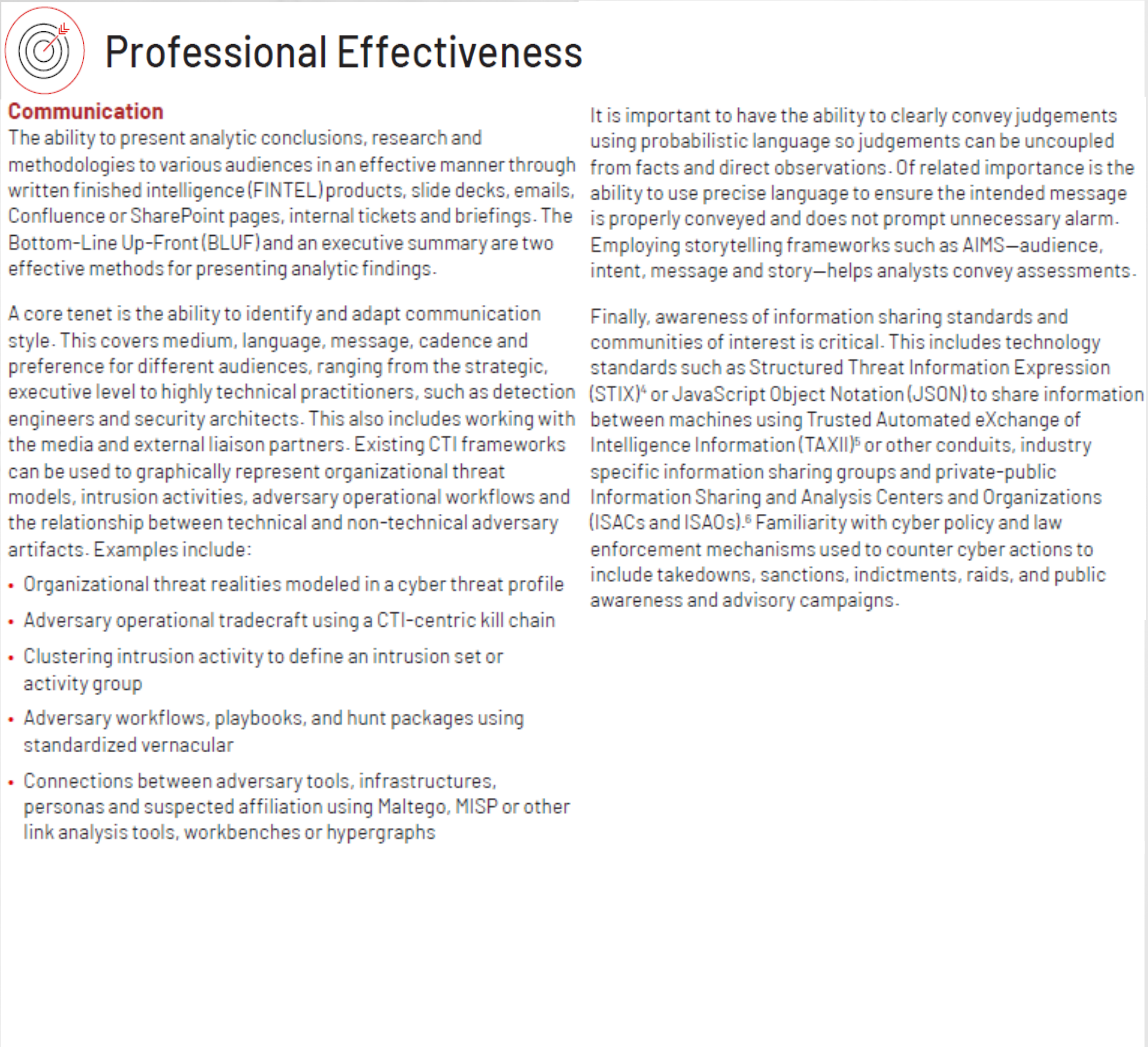
Research and Analysis

- Understand internal and external data sets and tools
- Understand the limitations of IOC types
- Identify unique fingerprints and patterns
- Mine, interpret, extract, store, and pivot on relevant content
- Generate intelligence on technical, cultural, or linguistical leads

Investigative Mindset

- Employ inquisition and familiarity with adversary operations, tradecraft, and forensic artifacts to determine logical next steps
- Devise novel solutions by applying out-of-the-box thinking

CTI Analyst Core Competencies



Professional Effectiveness

Communication

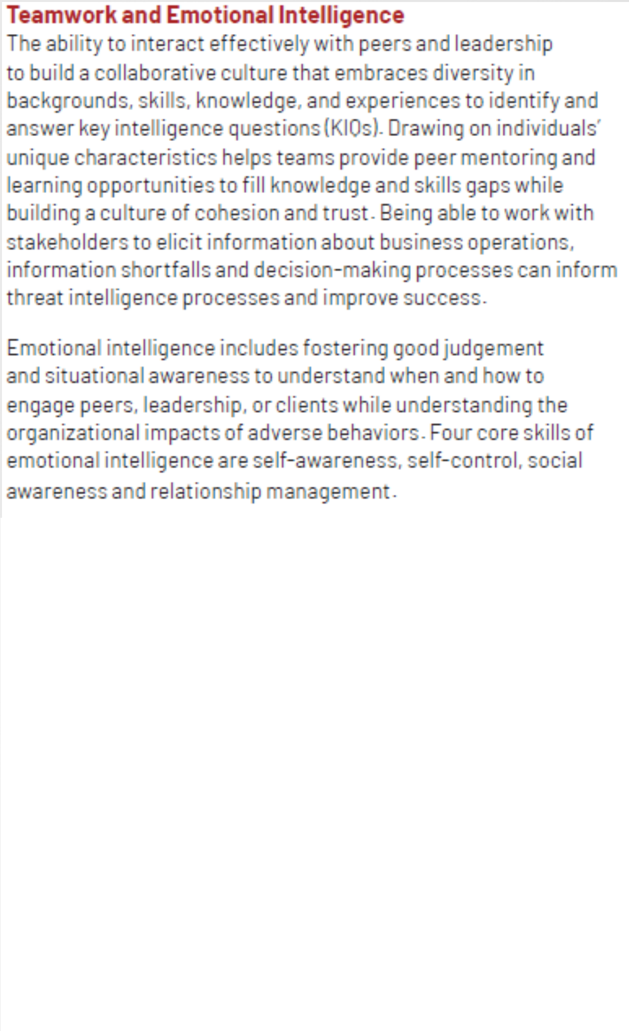
The ability to present analytic conclusions, research and methodologies to various audiences in an effective manner through written finished intelligence (FINTEL) products, slide decks, emails, Confluence or SharePoint pages, internal tickets and briefings. The Bottom-Line Up-Front (BLUF) and an executive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

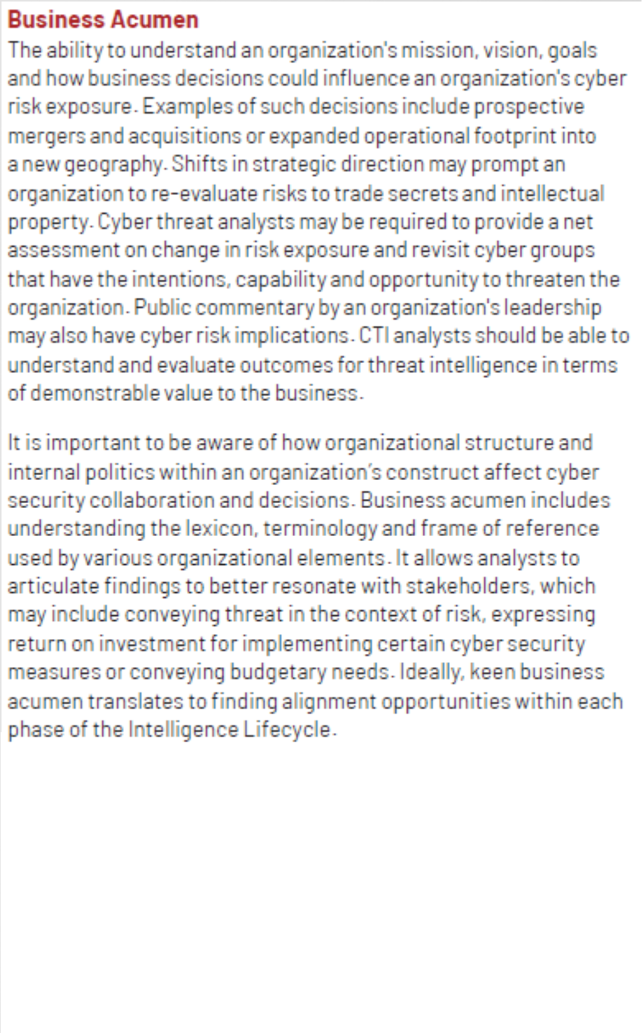
Finally, awareness of information sharing standards and communities of interest is critical. This includes technology standards such as Structured Threat Information Expression (STIX)[4] or JavaScript Object Notation (JSON) to share information between machines using Trusted Automated eXchange of Intelligence 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.

CTI Analyst Core Competencies

Professional Effectiveness

Communication

- Adapt presentation of analytic conclusions, research, and methodologies to audience type
- Leverage CTI and industry frameworks to graphically depict adversary workflows
- Understand how to leverage CTI data sharing communities of interest (ISACs/ISAO) and data storage and sharing standards (JSON/STIX and TAXII)

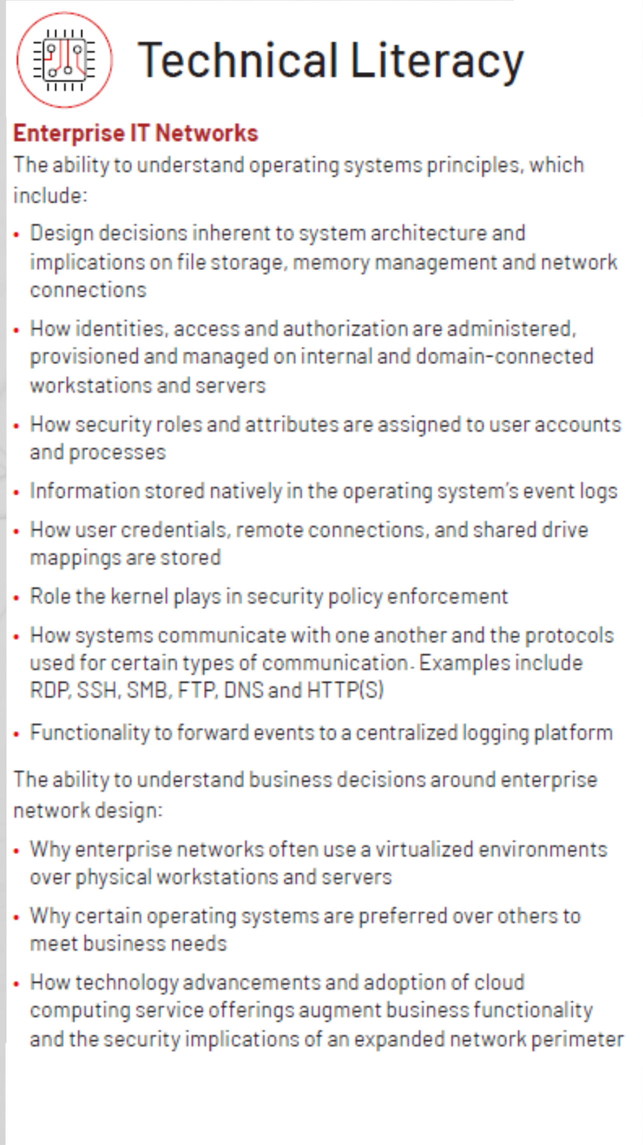
Teamwork and Emotional Intelligence

- Determine when and how to engage peers and leadership
- Provides opportunities and solutions
- Able to navigate tricky situations, diffusing conflicts as they arise
- Ability to motivate and cultivate a positive environment
- Awareness of how actions can be conveyed by others and calibrate responses accordingly

Business Acumen

- Forecast changes in risk exposure based on shifts in organizational mission, vision, goals, and public persona
- Understand industry specific processes and technologies ex) FinTech systems

CTI Analyst Core Competencies



Technical Literacy

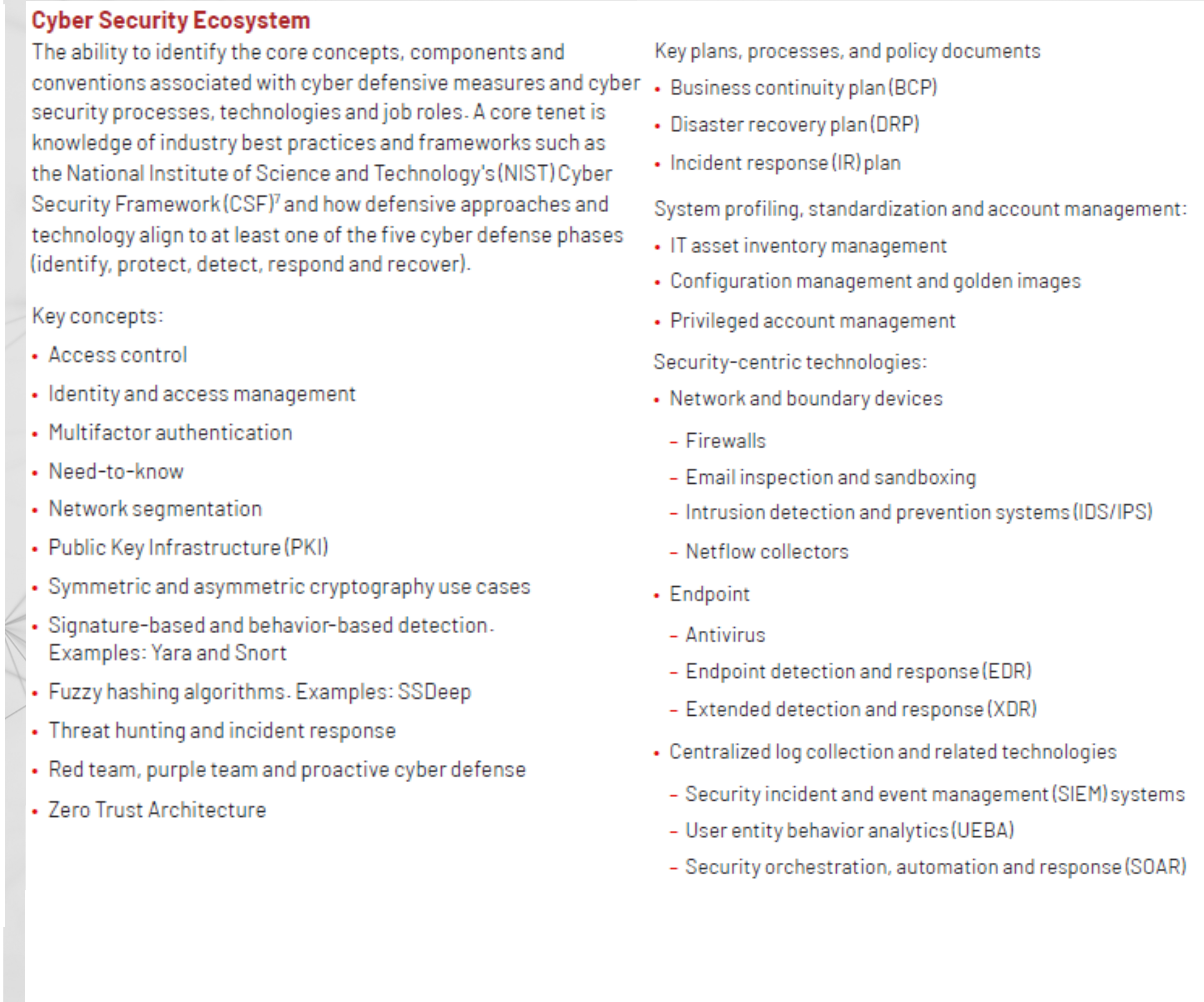
Enterprise IT Networks

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

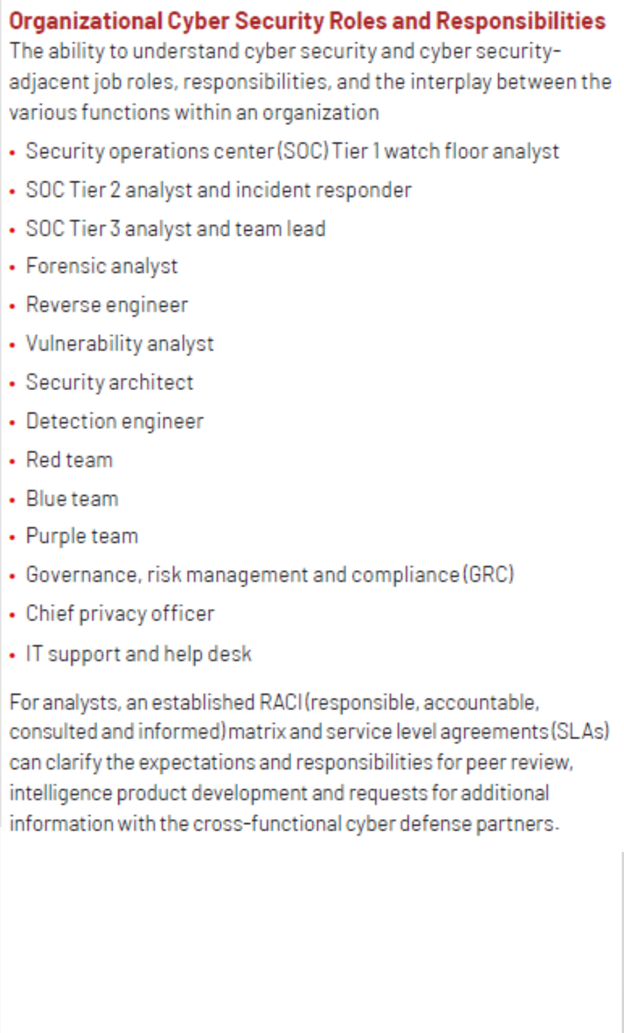
- Business continuity plan (BCP)
- Disaster recovery plan (DRP)
- Incident response (IR) plan

System profiling, standardization and account management:

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

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.

CTI Analyst Core Competencies

Technical Literacy

Enterprise IT Networks

- Active Directory, Kerberos, and the role of GPOs
- Identity and access management
- Security roles and attributes
- How systems operate and interact with one another
- Virtualized infrastructure
- On-prem, hybrid, and off-prem cloud computing solutions

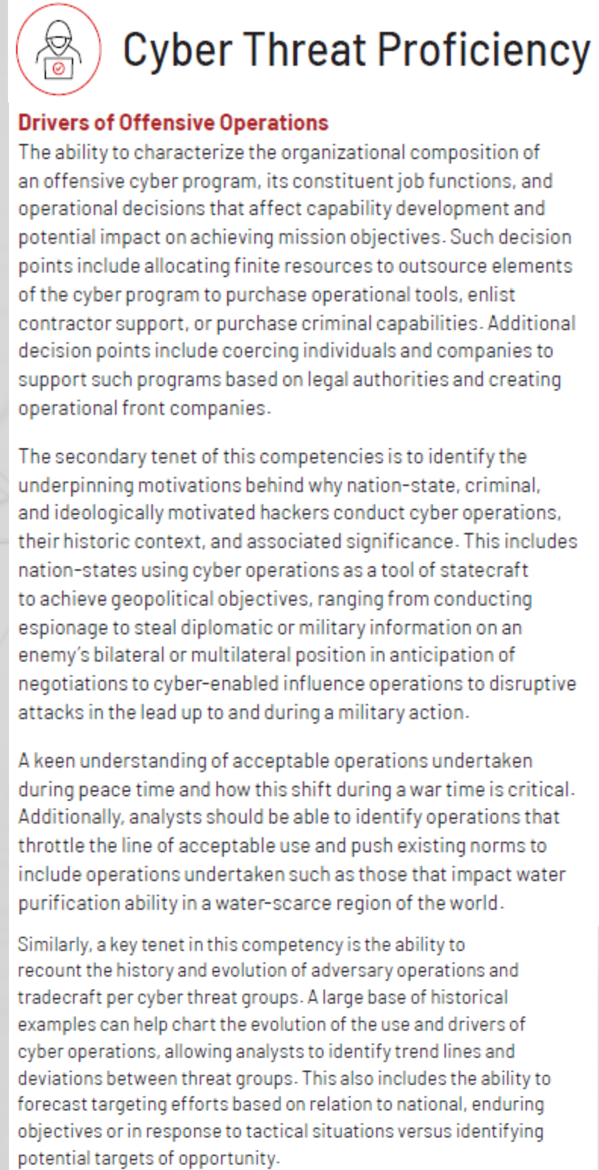
Cyber Security Ecosystem

- NIST Cybersecurity Framework (CSF) and its five phases
- NIST SP 800-53 cyber security controls
- Cyber security hygiene best practices

Cyber Security Roles and Responsibilities

- How each role supports risk exposure management
- Interplay between job roles to support collective defensive efforts
- *R*esponsible, *A*ccountable, *C*oordinated, and *I*nformed (RACI)
- Service level agreements (SLAs)

CTI Analyst Core Competencies



Cyber Threat Proficiency

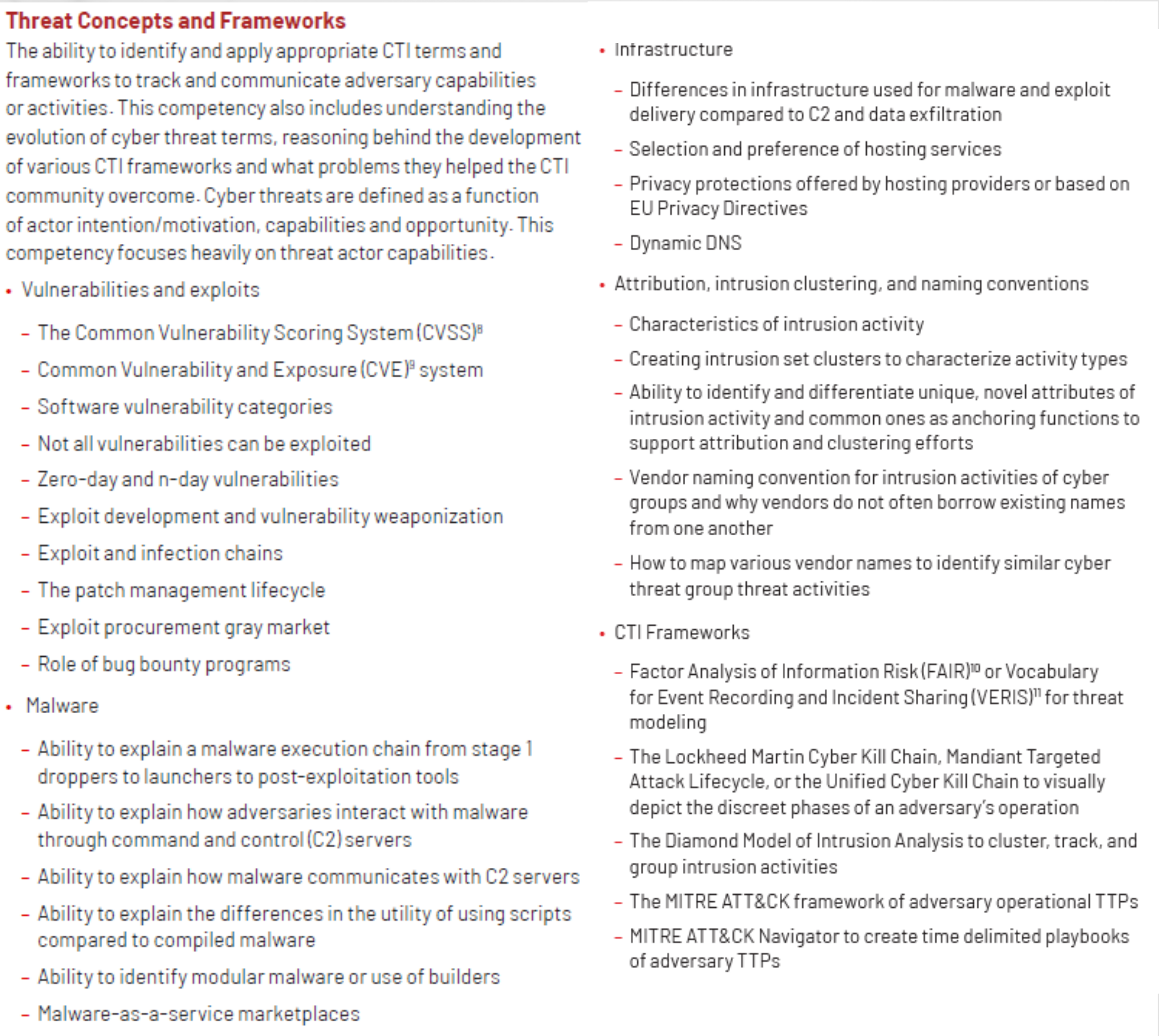
Drivers of Offensive Operations

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.

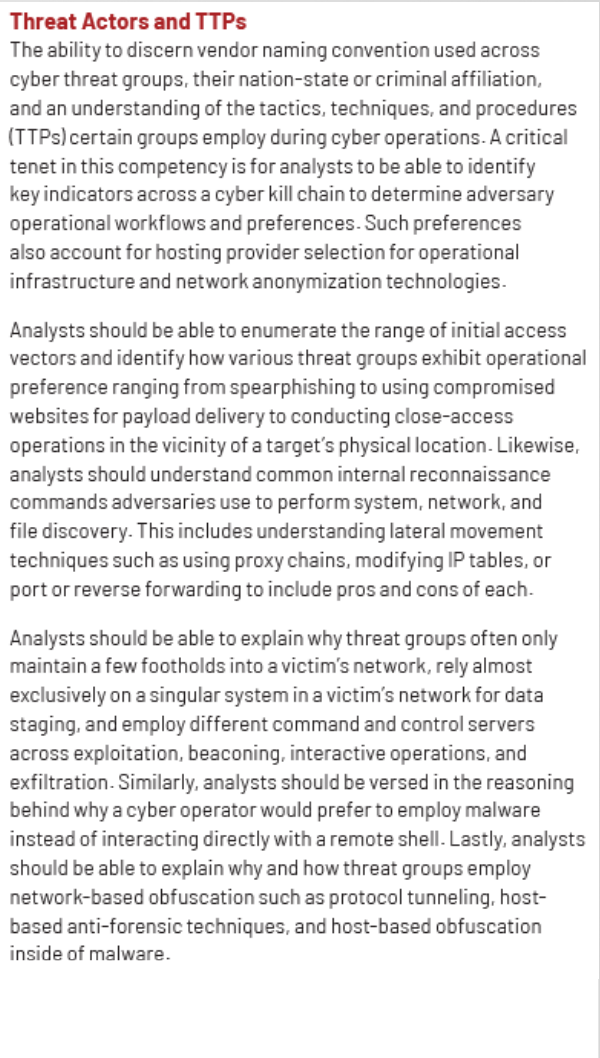
Similarly, a key tenet in this competency is the ability to recount the history and evolution of adversary operations and tradecraft per cyber threat groups. A large base of historical examples can help chart the evolution of the use and drivers of cyber operations, allowing analysts to identify trend 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
- 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.

CTI Analyst Core Competencies

Cyber Threat Proficiency

Drivers of Offensive Operations

- Identify the roles and responsibilities of individuals in an offensive cyber program
- Understand resource constraints and outsourcing considerations
- Understand actor motivations and differentiate between enduring vs. tactical requirements
- Pinpoint drivers that should shift targeting priorities or TTPs

Threat Concepts and Frameworks

- Vulnerabilities and Exploits
- Malware and interactive operations
- Adversary mid-point Infrastructure
- Attribution methodology, intrusion sets, and threat activity group nomenclature
- Key CTI frameworks and the problems they help the CTI community solve to include MITRE's ATT&CK, the various kill chain models, and the Diamond Model of Intrusion Analysis

Threat Actors and TTPs

- Loosely identify actor affiliation based on vendor naming convention
- Reasoning why vendors do not borrow each other's threat actor group names
- Characterize elements of adversary's operational tradecraft
- Explain how key concepts like remote access, persistence, lateral movement, staging, and data exfiltration

CTI Analyst Core Competencies

For nations, cyber is an asymmetric tool used as a form of soft power to augment existing tools of statecraft. A subset of these motivations exists for criminal elements.

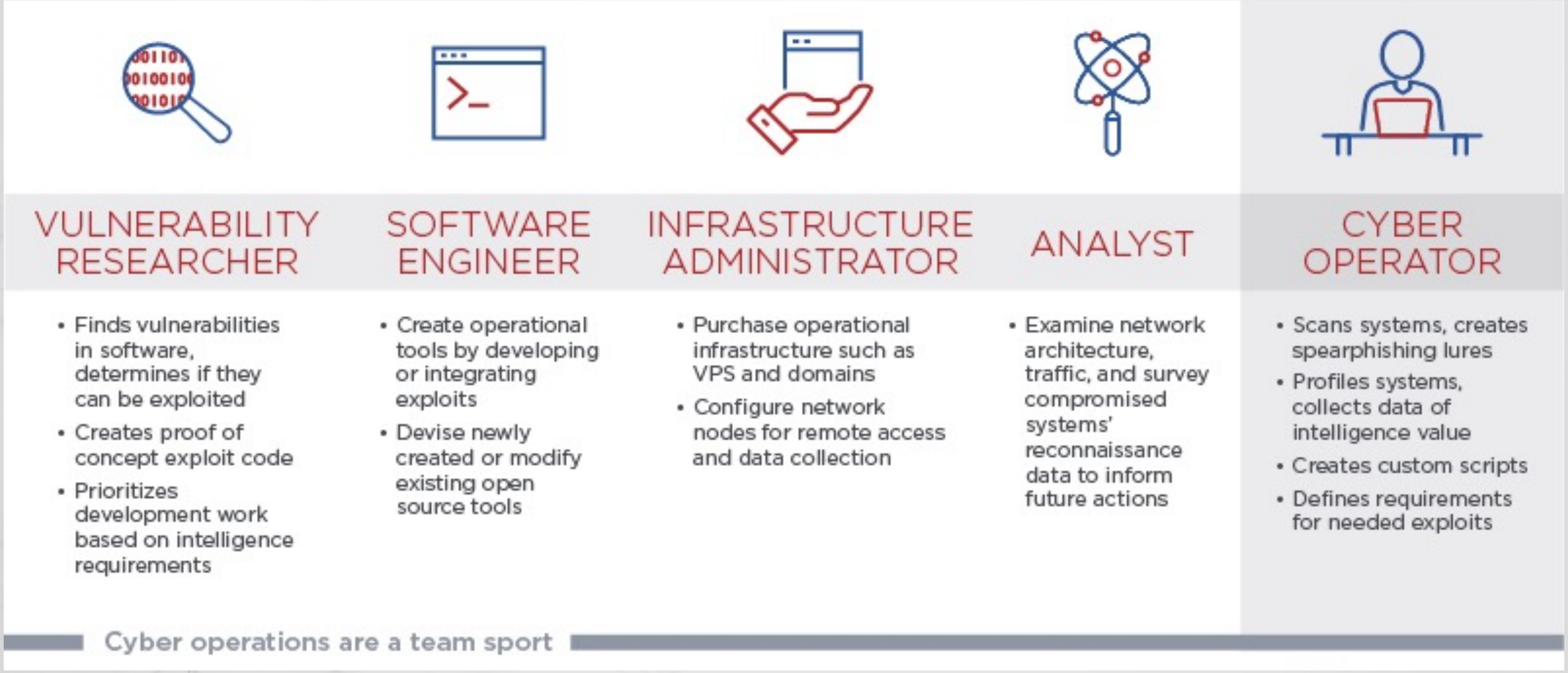
Espionage

- Political
    - Provide situational awareness of organizational decisions and plans
    - Inform course of action in bi- or multi-lateral negotiations
    - Identify potentially compromising information to use as a bartering chip
- Military
    - Understand capabilities, plans, decision calculus, and key stakeholders
- Economic
    - Bolster domestic competitiveness
    - Fund regime coffers

Attack

- Disrupt or degrade the availability of information systems and network access
- Destroy systems storing information
- Hide tracks
- Cause embarrassment
- Extortion or monetization
- Misdirection or false flag

CTI Analyst Core Competencies



VULNERABILITY RESEARCHER

- Finds vulnerabilities in software, determines if they can be exploited
- Creates proof of concept exploit code
- Prioritizes development work based on intelligence requirements

SOFTWARE ENGINEER

- Create operational tools by developing or integrating exploits
- Devise newly created or modify existing open source tools

INFRASTRUCTURE ADMINISTRATOR

- Purchase operational infrastructure such as VPS and domains
- Configure network nodes for remote access and data collection

ANALYST

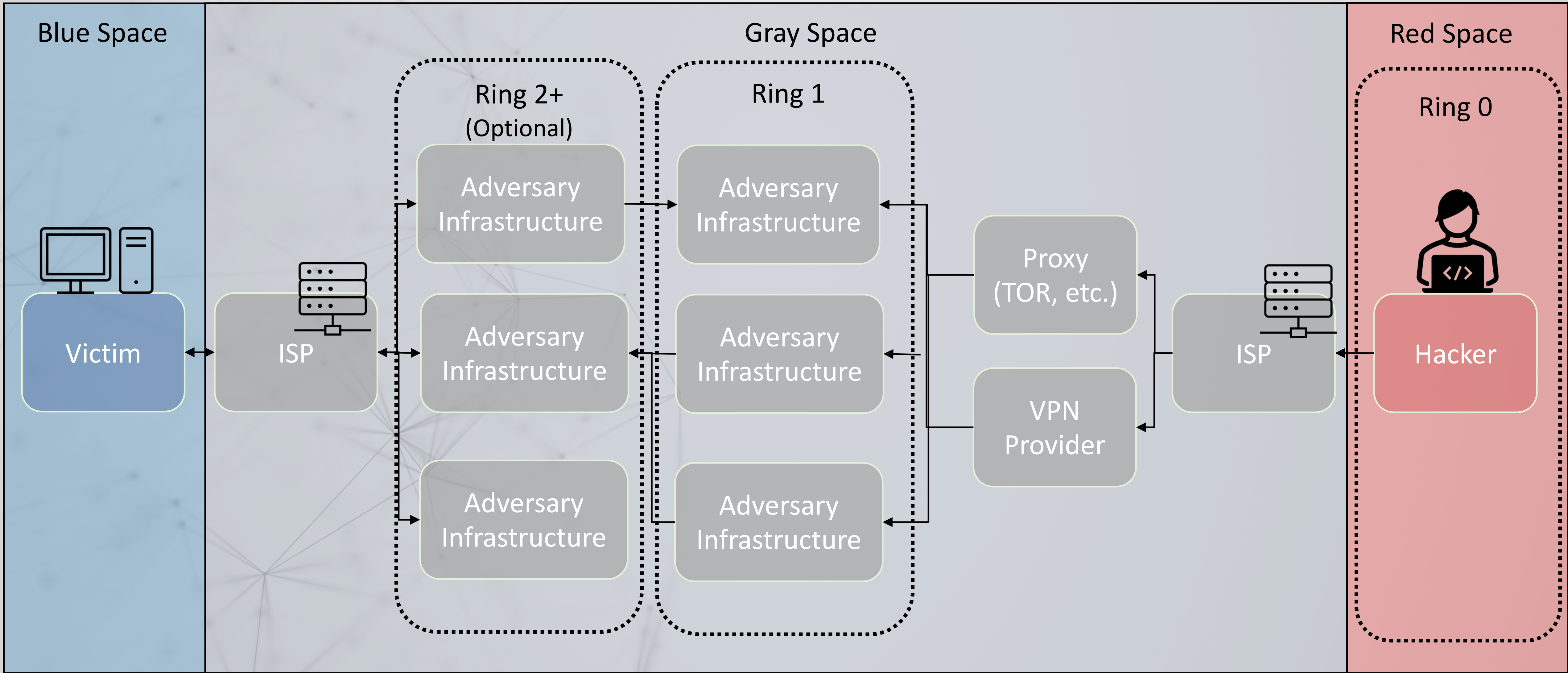
- Examine network architecture, traffic, and survey compromised systems' reconnaissance data to inform future actions

CYBER OPERATOR

- Scans systems, creates spearphishing lures
- Profiles systems, collects data of intelligence value
- Creates custom scripts
- Defines requirements for needed exploits

Cyber operations are a team sport

CTI Analyst Core Competencies



CTI Analyst Core Competencies

Framework Name	Public Release	Author(s)	Purpose
Malware Attribute Enumeration and Characterization	2009	Ivan Kirillov and Melissa Chase	Storing and sharing CTI in a machine-readable format
Vocabulary for Event Recording and Incident Sharing (VERIS)	2010	Verizon	Standardize the CTI lexicon
Mandiant's Targeted Attack Lifecycle	2010	Mandiant	Visually represent cyber intrusion activity
Lockheed Martin Cyber Kill Chain	2011	Eric Hutchins, Michael Clopper, and Rohan Amin	Visually represent cyber intrusion activity
OpenIOC	2011	Mandiant	Storing and sharing CTI in a machine-readable format
Cyber Observable eXpression (CybOx)	2012	MITRE	Storing and sharing CTI in a machine-readable format
Structured Threat Information eXpression (STIX)	2012	Sean Barnum	Storing CTI in a machine-readable format
Trusted Automated eXchange of Indicator Information (TAXII)	2012	Julie Connolly, Mark Davidson, Matt Richard, and Clement Skorupka	Sharing CTI in a machine-readable format
Diamond Model of Intrusion Analysis	2013	Sergio Caltagirone, Andrew Pendergast, and Christopher Betz	Visually represent cyber intrusion activity
Pyramid of Pain	2013	David Bianco	Categorize Indicators of Compromise (IoC) utility for adversary tracking
Malware Information Sharing Platform (MISP)	2013	Christophe Vandeplas, Andrzej Dereszowski, Alex Vandurme, and Andras Iklody	Storing and sharing CTI in a machine-readable format
MITRE Adversary Tactics, Techniques, & Common Knowledge Base (ATT&CK)	2015	Blake Strom, Andy Applebaum, Douglas Miller, Katie Nickels, Adam Pennington, and Cody Thomas	Standardize the CTI lexicon
ATT&CK Navigator	2018	MITRE	Visualizing Adversaries' TTP
OpenCTI	2019	French national cybersecurity agency (ANSSI), CERT-EU, and Luatix	Storing, organizing, visualizing, and sharing CTI
Unified Cyber Kill Chain	2021	Paul Pols	Comprehensive Examination of Adversary Workflows
Mandiant's CTI Analyst Core Competencies	2022	John Doyle	Identify knowledge, skills, and abilities required of CTI analysts

Parting Thoughts

- Unicorn analysts exist, but are rare
- No standard role designators lead to confusion
  - Threat Intelligence Analyst vs. Threat Researcher
  - Strategic vs. Context Analyst
  - Technical Analysts
  - Intelligence Engineer
- Unspoken expectations exist on both sides
- Be proactive as time permits
  - “Day in the life of” sessions are incredibly helpful
  - Lunch and learns/brown bags
  - Provide scoped RFIs and feedback
  - Establish service level agreements

Questions?

@_John_Doyle

Introducing the Mandiant Cyber Threat Intelligence (CTI) Analyst Core Competencies Framework Blog