CTI Analyst and Threat Actor Trait Mapping

CTI Pillar	CTI Competency	CTI Trait	Threat Actor Category	Threat Actor Parallel
Problem Solving	Critical Thinking	The ability to create outside-of-the-box solutions or frameworks when one does not exist.	Attack Development	Development of novel attack methods and zero-day exploits.
Problem Solving	Critical Thinking	Identify intelligence gaps and identify data sets, tools, or techniques to address the gaps.	Reconnaissance	Identifying security gaps and vulnerabilities in target systems.
Problem Solving	Research and Analysis	Mine, interpret, extract, store, and pivot on cyber threat data.	Data Collection	Gathering intelligence on targets and extracting valuable data.
Problem Solving	Research and Analysis	Discover infrastructure sharing similar characteristics using internet scanning data.	Infrastructure Analysis	Identifying connected systems and potential lateral movement paths.
Problem Solving	Research and Analysis	Analyze network traffic (pcap) and extract intelligence from it.	Network Reconnaissance	Analyzing target network traffic for vulnerabilities and data.
Problem Solving	Investigative Mindset	The ability to intuit the type or types of data found within data set fields or a file to include encoded text blobs.	Target Selection	Identifying valuable data and systems within target environment.
Problem Solving	Investigative Mindset	Determine what natural next steps and pivot points when supporting research or enriching known cyber threat data to help satisfy existing intelligence requirements.	Attack Chain Planning	Planning movement between systems and escalating access.
Technical Literacy	Enterprise IT Networks	Understand operating system architecture, file storage, memory management, and network connectivity.	Exploit Development	Understanding system internals for exploit development.
Technical Literacy	Enterprise IT Networks	Understand how identities, access, authorization, and auditing are performed on local and domain-connected systems.	Privilege Escalation	Understanding access controls for privilege escalation.
Technical Literacy	Enterprise IT Networks	Understand the protocols used for inter-system communications.	Network Exploitation	Understanding network protocols for C2 communication.
Technical Literacy	Cyber Security Ecosystem	Knowledge of why security controls are employed in an enterprise environment and its relationship with reducing risk exposure.	Defense Evasion	Understanding security measures to avoid detection.
Technical Literacy	Cyber Security Ecosystem	Understand the use cases and differences between signature-based detection and behavioral-based detection.	Defense Evasion	Understanding detection methods to avoid them.
Technical Literacy	Cyber Security Ecosystem	Familiarity with security incident and event management (SIEM) systems, log ingestion, and tuning requirements.	Defense Evasion	Understanding logging systems to avoid detection.
Cyber Threat Proficiency	Threat Concepts and Frameworks	Explain malware infection chains from droppers to launchers to post-exploitation remote access tools (RATs).	Attack Development	Creating malware deployment and execution strategies.
Cyber Threat Proficiency	Threat Concepts and Frameworks	Understand that adversaries are likely to use different infrastructure for exploit delivery, malware deployment, remote interactive commands, and data exfiltration.	Infrastructure Setup	Creating resilient attack infrastructure.
Cyber Threat Proficiency	Threat Actors and TTPs	Familiarity with lateral movement artifacts, protocols, and techniques.	Lateral Movement	Moving between systems in target environment.
Cyber Threat Proficiency	Threat Actors and TTPs	Familiarity with credential dumping and the use of pass-the-hash to move laterally on a victim's network.	Credential Theft	Extracting and utilizing stolen credentials.
Cyber Threat Proficiency	Threat Actors and TTPs	Familiarity with commonly used tunneling software and techniques to include establishing proxy chains, modifying IP tables, or port forwarding and the pros and cons of using each.	Command & Control	Establishing covert communication channels.

Cyber Threat Proficiency	Threat Concepts and Frameworks	Understand that exploits are often linked together in an exploit chain to provide a certain level of access to the attacker.	Exploit Development	Chaining vulnerabilities for system compromise.
Cyber Threat Proficiency	Drivers of Offensive Operations	Understand the resource constraints and decision making calculus for an enterprise nation-state cyber program to include contracting and procurement of cyber operations capabilities.	Operation Planning	Resource allocation and attack prioritization.

© 2025 Erica Peterson