Threat Actor Rules of Engagement Policy

**Last Updated:** [DATE] | **Status: Under review**

# 1.0 Introduction

Business needs will sometimes dictate the need to engage cyber threat actors online to ascertain insights that can be used to support organizational decisions. When engaging these actors, proper operational security measures must be followed to minimize any undue risk to the organization. All activities undertaken as part of intelligence collecting activities adhere to the stated policies of [COMPANY NAME] and do not break any local, state or federal laws.

# 1.1 Purpose

This document grants the cyber threat intelligence team with the authorities to engage adversaries online in a limited manner directed by general council guidance. This document also outlines the criteria for engagement, escalation threshold, and frequency in which authorities are reviewed and re-approved.

This document thus serves as an understanding between the cyber threat intelligence team, the privacy and legal department, and cyber security leadership about the appropriate channels, methodology, approvals and guardrails for direct-source intelligence collection activities. Please see policy document, [CTI Program Charter name and corresponding number] for additional understanding of the remit and purpose of the organization’s cyber threat intelligence team.

# 1.2 Common Use Cases

The CTI team is chartered with providing decision support to enterprise cybersecurity and risk functions. Common decision-making support requests include understanding claims of unauthorized access, stolen intellectual property, business communications, personally identifiable information (PII), customer data, or credentials belonging to [COMPANY NAME]. Direct-source intelligence gathering activities to support these use cases include the following:

* Passive observations to determine cyber threat actor credibility, validity of claims, or to gather information pertinent to an investigation or defined intelligence requirement.
* Direct engagement with cyber threat actors on a darkweb forum, marketplace, “onion” sites, chatrooms, or communications platforms.
* Acquisition of data suspected or confirmed to belong to [COMPANY NAME] from unauthorized sources.

If there is reasonable suspicion leaked data could present a risk or indicate an incident at [COMPANY NAME], intelligence staff is empowered to download available data samples accessible through passive activity (such as navigating to a TOR link or logging into a forum) for analysis. If this data contains excess sensitive information which is not relevant to assessing risk to [COMPANY NAME] it must be securely deleted immediately.

# 1.3 Research Guidance

Due to the potentially sensitive nature of this intelligence collection, [COMPANY NAME] requires research performed in support of investigations to be documented within [ticketing/knowledge management system]. At a minimum, the research findings should include reason for engagement, start date, end date, website/onion address, summary of activities undertaken, analytic assessment, and maintaining a record of relevant screen captures. Should analysts acquire sample data, this too, should be attached.

* All information about these activities including persona identifying information, online activities, missions and results are all considered *Confidential – Highly Restricted* data classifications.
* Conduct these activities from computer assets that are not network-connected to [company name] environment, using established department procedures and tools for privacy and anonymity. Specifically…
  + have a virtual machine environment established for triage and use the [SOFTWARE NAME] VPN client that [COMPANY NAME] has purchased when conducting threat research. Ensure this is turned on before connecting to forums, darkweb, or onion sites.
  + Build “personas” aka “sock puppet accounts” for intelligence activities specific for each social media, darkweb, market, chat application (e.g. Telegram, WhatsApp, TOX), etc. Document these personas, specific use cases, and where they have been used within an encrypted file shared with the CTI team to ensure deconfliction.
    - Do not create a sock puppet that impersonates any real person, current, or previous employee at [COMPANY NAME].
    - Never use a persona to contact existing employees.
    - Do not impersonate any representative of another company, business or any government official.
    - Do not threaten or harass any person, do not cause anybody to fear for the safety or wellbeing of another person, business, company or property.
    - Never encourage, direct, or advocate for illegal activity. Avoid conversations that could be interpreted as furthering criminal objectives of others.
    - Do not assist or advise on any illegal activities such as malware development, cyber-attack planning, phishing campaign development, target identification, vulnerability identification or exploit development.
    - Answer questions from threat actors or other intelligence sources with information that could identify yourself or [COMPANY NAME].
* Only use personas for their specific use case; sole use per site. A keychain manager can help with managing accounts and credentials.
* Do not log into any personal accounts when conducting research to prevent potential cross-pollination that would expose your true identity. Similarly, do not access work accounts on your research system.
* Ask only for or acquire data necessary to confirm ownership or to evaluate the validity of claims consistent with specific intelligence requirements. After transferring possession of data into a ticket, securely delete all copies of the data in your possession.
* Access to any forums or data should be carried out via the forums authorized means of access. Do not use stolen credentials or exploits to gather data from any server or system.
* General conversations about past activities, such as if a subject has previously stolen data, who may have bought data or know who possesses data, previous attacks, malware developed or exploits are allowed. Exercise caution when engaging in discussions about future activity, particularly when the details are clear a crime is being committed. Do not engage or participate in conversations about a specific target or intended victim.

# 1.4 Escalation Criteria

* Notify leadership immediately of any suspicion of physical or insider threat
* Establish incident response procedures if an employee is doxed during intelligence work - account appears to be burned.
* All direct-source information gathering ***will be passive*** and will not target any specific threat actor or group without prior approval from [AUTHORITY]. This approval will include a written ICP (Intelligence Collection Plan) with SIRs (Specific Intelligence Requirements) supporting the mission with clear, situation-specific do / don’t guidance.
* No direct request for proof, whole or partial datasets or other content outside of approved intelligence partners will be made unless prior approval from [AUTHORITY] is granted. Exercise caution when asking third-parties about specific data, to avoid any questions that could be interpreted as a request to attack an organization to get said data.
* Before purchasing data, assess to the extent possible that the U.S. Government has not imposed sanctions or prohibited economic transactions on the seller.
* No actor or campaign disruption activities will be conducted without approval from [AUTHORITY]
* Collaboration with law enforcement is guided and approved by [AUTHORITY]

# 1.5 Version Control and Approvals

Document last reviewed on \_\_\_\_\_[DATE]\_\_\_\_\_\_

Approval from Privacy and Legal \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

Approval from CISO \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

Acknowledged by CTI Manager \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

Acknowledged by [Employee] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_