Objective Threat Model (OTM)

The **Objective Threat Model (OTM)** prioritizes threat actors' objectives over the technical mechanisms of attack. Focusing on outcomes broadens understanding of how diverse threat mechanisms manifest. Unlike traditional models centered on technological vulnerabilities, OTM encompasses operational impacts, business risks, and non-technical threats.

Integrating psychological operations, business strategy, and information warfare, OTM is a versatile framework applicable across disciplines. Its flexible, context-aware design ensures relevance in dynamic and evolving threat landscapes.

Base Model

Threat	**Description**
Increased Overhead	● Costs, time, cognitive load, opportunity cost, and other burdens.
Degraded Capability	● Barriers or impediments to completing a desired action, including denial of service and communication blocks.
Manipulation	● Data harvesting, targeting, misinformation, or actions that trigger alterations in behavior or decision-making.
Reputation Attack	● Degradation of trust or perception between parties, including fabricated or leaked harmful information, spoofing, degraded reliability, and experience.
Vessel or Vehicle for Attack	● **Vessel**: Devices or systems that are accessed as containers for their natural contents (e.g., personal data, credentials, media) or co-opted to carry a harmful payload (e.g., malware). ● **Vehicle**: Devices or systems serving as launch points for attacks on resources, such as data exfiltration, privilege escalation, surveillance, or network attacks.
Longitudinal Risk	● Maintaining presence, propagating, or evolving over extended periods, leveraging interdependencies, residual data, or sustained impact to amplify risk. This includes cascading failures, latent data exposure, and threats that unfold through gradual escalation, time-based exploitation, or adaptive evolution in response to resistance.
Device Dependency	● Creating or exacerbating a reliance on a specific device, app, or ecosystem, reducing the user’s autonomy, decision-making capability, or ability to function independently.

Challenge Questions for Threat Detection

1. Does this increase my burden? (Threat: Increased Overhead)
2. Am I being held back or blocked? (Threat: Degraded Capability)
3. Am I being manipulated? (Threat: Manipulation)
4. Could this harm someone’s reputation? (Threat: Reputation Attack)
5. Does this present a vessel or vehicle for attack? (Threat: Vessel or Vehicle for Attack)
6. Am I subject to sustained risk? (Threat: Longitudinal Risk)
7. Am I losing autonomy? (Threat: Device Dependency)

JSON Representation of Threat Model

```
{
  "license": "CC0 1.0",
  "license_link": "https://creativecommons.org/publicdomain/zero/1.0/",
  "release_date": "2024-12-22",
  "ObjectiveThreatModel": {
    "overview": {
      "desc": "The Objective Threat Model (OTM) prioritizes threat actors' objectives over the technical mechanisms of attack. Focusing on outcomes broadens understanding of how diverse threat mechanisms manifest. Unlike traditional models centered on technological vulnerabilities, OTM encompasses operational impacts, business risks, and non-technical threats. Integrating psychological operations, business strategy, and information warfare, OTM is a versatile framework applicable across disciplines. Its flexible, context-aware design ensures relevance in dynamic and evolving threat landscapes."
    },
    "Threats": [
      {
        "type": "Increased Overhead",
        "desc": "Costs, time, cognitive load, opportunity cost, and other burdens.",
        "q": "Does this increase my burden?"
      },
      {
        "type": "Degraded Capability",
        "desc": "Barriers or impediments to completing a desired action, including denial of service and communication blocks.",
        "q": "Am I being held back or blocked?"
      },
      {
        "type": "Manipulation",
        "desc": "Data harvesting, targeting, misinformation, or actions that trigger alterations in behavior or decision-making.",
        "q": "Am I being manipulated?"
      },
      {
        "type": "Reputation Attack",
        "desc": "Degradation of trust or perception between parties, including fabricated or leaked harmful information, spoofing, degraded reliability, and experience.",
        "q": "Could this harm someone’s reputation?"
      },
      {
```

```
      "type": "Vessel or Vehicle for Attack",
      "desc": {
        "Vessel": "Devices or systems that are accessed as containers for their natural contents (e.g., personal data, credentials, media) or co-opted to carry a harmful payload (e.g., malware).",
        "Vehicle": "Devices or systems serving as launch points for attacks on resources, such as data exfiltration, privilege escalation, surveillance, or network attacks."
      },
      "q": "Does this present a vessel or vehicle for attack?"
    },
    {
      "type": "Longitudinal Risk",
      "desc": "Maintaining presence, propagating, or evolving over extended periods, leveraging interdependencies, residual data, or sustained impact to amplify risk. This includes cascading failures, latent data exposure, and threats that unfold through gradual escalation, time-based exploitation, or adaptive evolution in response to resistance.",
      "q": "Am I subject to sustained risk?"
    },
    {
      "type": "Device Dependency",
      "desc": "Creating or exacerbating a reliance on a specific device, app, or ecosystem, reducing the user’s autonomy, decision-making capability, or ability to function independently.",
      "q": "Am I losing autonomy?"
    }
  ]
 }
}
```

This JSON payload is estimated at 626 tokens for ChatGPT 4o using OpenAI Tokenizer API. Please date and name variants.

Sample Usage Prompts

Human-in-the-loop (HITL) is a critical control for any use of generative AI. The human driving the AI remains responsible for any actions taken. The following prompts are intended to illustrate how a generative AI prompt can leverage the JSON representation of a threat model:

- Based on this threat model, a threat response should be formed that is appropriate for a personal iPhone user at home.
- Based on this threat model, generate an exhaustive list of all common threats applicable to mobile devices.
- Contrast this threat model with traditional threat models. Map all traditional threats against this threat model. Identify potential gaps.
- Contrast this threat model with STRIDE and MITRE ATT&CK, consider approaches combining OTM.
- Based on this threat model, evaluate Verizon's latest Mobile Security Index coverage.
- Based on this threat model, formulate a threat response appropriate for a journalist at high risk for attack by nation-states and use a Google Pixel device running the latest Android operating system.
- Based on this threat model, formulate a threat response appropriate for a major company CFO with a business-owned and administered laptop and cellphone.
- Based on this threat model, design a security awareness program for small business owners relying on mobile devices and cloud-based services.
- Using this threat model, analyze the potential risks of implementing generative AI tools in a medium-sized enterprise, focusing on reputational damage and operational impacts.
- Apply this threat model to identify and prioritize mitigation strategies for a healthcare organization managing critical patient data in a hybrid cloud environment.