**MITRE ATT&CK, CISA, US-CERT validation and results**

**Code Implementation and Analysis**

To validate our ontological framework's effectiveness in supporting resilience through risk reduction, we implemented a Python-based intelligence integrator that analyzes threat data from multiple authoritative sources (MITRE ATT&CK, CISA, US-CERT). The code focuses explicitly on APT42 and related Iranian threat actors while monitoring for 5G infrastructure vulnerabilities and exploitation patterns.

This Python code defines a class called APT42IntelligenceIntegrator designed to gather and analyze threat intelligence data related to the activities of the Iranian state-sponsored APT42 threat actor group, particularly those targeting the 2024 U.S. presidential election and 5G infrastructure.

The class fetches data from various sources, including MITRE ATT&CK, CISA Known Exploited Vulnerabilities, CISA Alerts, US-CERT Current Activity, and Microsoft Security Guidance. It then analyzes this data for keywords related to APT42, disinformation campaigns, and 5G technologies. The code also assesses the risk level of identified threats based on predefined criteria and correlates patterns in the data to identify potential temporal trends and attack patterns. The results, including categorized findings and correlated patterns, are then printed to the console.

**Key Findings**

1. **Validation of Ontological Structure**

* Successfully categorized 82 distinct findings across the following: campaign targeting (18), 5G exploitation (51), and general activities (13)
* Demonstrated clear alignment with our classification system for threat actors, attack patterns, and targets
* Effectively mapped relationships between threat components, validating our ontological relationships

1. **Support for Resilience Approach**

* Identified high proportion of high-risk findings (64.6%), enabling prioritized defense strategies
* Mapped comprehensive attack patterns, particularly in infrastructure manipulation
* Revealed sophisticated technical capabilities requiring robust defensive measures
* Demonstrated effectiveness of risk-based categorization for threat assessment

1. **5G Infrastructure Integration**

* Identified both direct (4.9%) and indirect (8.5%) 5G-relevant threats
* Revealed sophisticated network manipulation capabilities
* Mapped specific attack patterns targeting network infrastructure
* Validated our focus on network slicing and edge computing vulnerabilities

This analysis demonstrates our ontology's practical value in:

* Supporting systematic threat classification
* Enabling risk-based decision making
* Facilitating comprehensive understanding of attack patterns
* Supporting resilience through effective risk identification and categorisation

The findings validate our approach to resilience through risk reduction by providing structured insight into threat actor capabilities, attack patterns, and infrastructure vulnerabilities, enabling more effective defensive strategies.

**BASED on:** *MITRE ATT&CK Python code and run results file*