Python Script for Transforming Domain Names from First Watch Malicious Domains Data Feed into STIX 2.1

Posted on March 21, 2025

WhoisXML API recently created a Python script to help users of First Watch Malicious Domains Data Feed, also known as “First Watch,” transform predictive domain intelligence into a machine-readable format—STIX 2.1—for automated data processing.

The script reads domain names from First Watch files, converts them to STIX 2.1 Indicator objects with domain-name observable types, and generates a TAXII 2.1-compatible STIX bundle. The output is downloadable as a JSON file in TAXII format.

For further information on our scripts or to submit a script idea that suits your requirements, please contact professional.services@whoisxmlapi.com.

How the Script Can Help First Watch Users

With the help of this script, First Watch users aiming to integrate threat intelligence into their security solutions and processes can experience:

- **Automated data processing:** The script reads domain names directly from a text or CSV file, making it easier to work with raw First Watch feed data. And since it generates a TAXII 2.1-compatible STIX bundle, it enables organizations to automate the ingestion and sharing of threat intelligence.

- **Better threat intelligence sharing:** The script converts the data feed into STIX 2.1 Indicator

objects, a widely used standard format for threat intelligence platforms (TIPs), SIEM platforms, SOAR systems, and other cybersecurity tools.

- **Flexible output format:** By default, the script generates a compact JSON file (ideal for automation) but users can also enable human-readable formatting with the **--pretty** flag for easier manual inspection.

Access the latest version of our script to easily convert First Watch domain lists to STIX 2.1 Indicator objects on GitHub.