Telos Red Widow™ Threat Feed

Telos' Advanced Cyber Analytics (ACA) practice includes Telos Red Widow™, our dynamic proprietary threat feed of global Internet Protocol (IP) addresses known to engage in potentially malicious activity, including mass scanning and generic opportunistic attacks.

Telos Red Widow allows security operation centers (SOC) the advantage of being able to reduce "noisy" IP security threat alerts, thereby increasing operational efficiency, the ability to potentially identify forthcoming mass exploitation events, and ultimately improve the focus of ongoing threat hunts.

Telos Global Sensor Network

A critical component of Telos ACA™ solutions is the Global Sensor Network (GSN). This proprietary network encompasses a worldwide footprint providing 24/7 intelligence on a wide array of attack surfaces. The GSN is a composition of propriety sensor nodes designed to capture cyber threat traffic traversing the Internet and command and control networks worldwide, providing insight into potential malicious activity, emerging threats, and bad actors attempting to infiltrate and/or compromise legitimate networks and infrastructure

Threat Feed Delivery

Telos Red Widow intelligence is seamlessly and conveniently delivered as an industry-standard Structured Threat Information eXpression/Trusted Automated eXchange of Intelligence Information (STIX/TAXII) based threat feed. STIX states the "what" of threat intelligence, while TAXII defines "how" that information is relayed.

STIX and TAXII are machine-readable and, therefore, easily automated. This allows for easy consumption into third-party security tools where it can be used to enrich and provide relevant information related to potential malicious network activity within environments.

Threat Feed Components

The Telos Red Widow Threat Feed provides the IP, metadata, and raw data elements to improve threat hunting and eliminate threat noise. The feed can be accessed on a pre-determined update cycle.

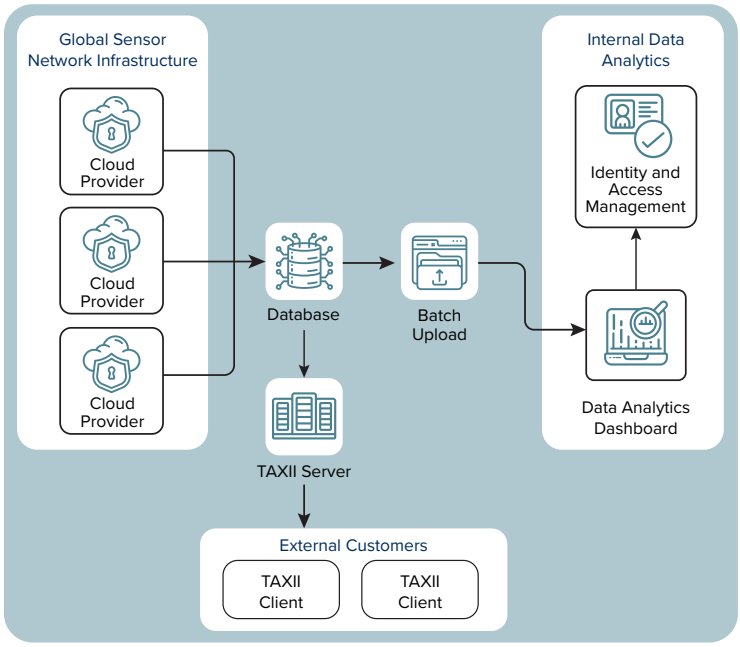

Figure 1: GSN 2.0 High-level Architecture

About Telos Advanced Cyber Analytics (ACA)

Telos' Advanced Cyber Analytics (ACA) practice offers proprietary and industry technologies with a global sensor network and extensive subject-matter expertise to create time-sensitive and actionable threat intelligence solutions for government and commercial enterprises. With Telos ACA, organizations are able to:

- Detect malicious activity sooner
- Assist in the attribution of events of concern
- Uncover and identify previously unknown attacks and new malicious behavior

The Telos Red Widow capability within the Telos ACA practice is ideal for organizations that need better threat intelligence data that is easily consumable into existing third-party security tools.

Telos® Solutions that **empower** and **protect** the enterprise.™

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com