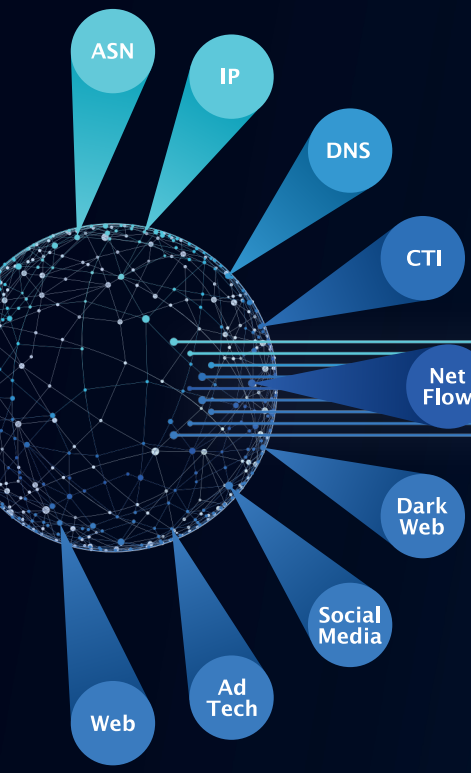
SHADOWVIEW

UNCOVER WHAT YOU DON'T SEE

In the age of information, security challenges equate to target opportunities for our adversaries. The sheer amount of publicly available information (PAI) can be overwhelming, but if extracted, correlated and analyzed correctly, it is a pivotal resource to minimize exposure and reduce risk. Inspired by our Red Team targeting process, ShadowView has evolved into an intelligent solution to perform tailored analysis across a broad spectrum of PAI data sources. As your digital footprint extends past the perimeter, ShadowView can serve as an extension of your existing security team, unmasking the shadow of the Internet.

Request for Information or Analysis

- Threat Hunting
- Malware Discovery
- Supply Chain
- Continuous Monitoring
- Cyber Targeting
- Asset Discovery
- Pattern of Life
- High Value Targets
- Intel Validation
- Criminal Investigation
- Missing Persons
- Risk Management
- Crisis Management
- Personnel Recovery
- Proof of Life
- Attack Surface Enrichment



Raw Aggregated Data

Flexible formatting options to ensure easy integration into your analysis engine and processes

RFI/RFA Analysis Report

Includes data enrichment and presentable content tailored for your specific needs

- Defensive Cyber Operations
- Offensive Cyber Operations
- Intel, Surveillance, Recon
- Law Enforcement
- Disaster Recovery
- Executive Protection

Learn more about our work at millgroupinc.com

MILLENNIUM CORPORATION

SHADOWVIEW

AGGREGATED TRACKING AS A SERVICE

Asset Discovery Case Study

Shortly after the SolarWinds compromise was made public, Millennium received an RFI to identify the potential exposed attack surface. Aggregating and correlating BGP, IP and DNS information, our analysts quickly found over 70 previously unidentified SolarWinds instances, many of which were not tracked assets by the customer's internal security team.

These instances were further confirmed through correlation of targeted network traffic analysis, providing the security team with a high confidence assessment of the potential attack exposure. Our analysts were able to produce a detailed, actionable report in less than two days.

2022 By The Numbers

- **6.4B** smart phone users
- **251M** apps downloaded every day
- **828M** tweets sent every day
- **2TB** DNS data collected daily
- **1700TB** of Internet data generated per minute

Attack Surface Enrichment Case Study

During a security assessment, our test team was not able to identify additional attack surface through traditional reconnaissance means. Turning to PAI, our analysts were able to start with attributed network blocks and through subsequent analysis were able to identify thousands of additional domains for consideration.

This additional attack surface was correlated through further enrichment data including vulnerability datasets and cyber threat intelligence. After only a few days of analysis, multiple attack points were identified, and the test team was able to gain initial access through a previously unknown vulnerable server. All attack surface analysis was performed passively on PAI datasets, requiring zero interaction with the assessed network.

MILLENNIUM CORPORATION™

HEADQUARTERS
1400 Crystal Drive
Suite 400
Arlington, VA 22202

HUNTSVILLE OFFICE
340 The Bridge Street
Suite 202
Huntsville, AL 35806

Jared Dible, Sr. Cyber Architect
PHONE 785.577.2433
E-MAIL jared.dible@millgroupinc.com

Ben Clark, Chief Technology Officer
PHONE 205.527.4112
E-MAIL ben.clark@millgroupinc.com