SILENT PUSH

INSIGHT

IMMEDIATE CLARITY INTO UNKNOWN INFRASTRUCTURE

Consolidate enrichment, analysis, and correlation into a single platform to eliminate manual pivots. Instantly understand what an observable is, how it is being used, and why it matters.

POWERED BY THE CONTEXT GRAPH

The foundational engine that maps global infrastructure relationships to enable preemptive cyber defense.

KEY CAPABILITIES

- **Accelerated Triage via Total View:** Consolidate 10+ data types, including P(A)DNS, WHOIS, and web content, into a single view to eliminate manual pivoting.
- **Granular Data Categorization:** Enrich assets with 100+ unique attributes and data tags for VPNs, proxies, and sinkholes to pinpoint high risk IPs.
- **Automated Risk Scoring:** Prioritize observables automatically based on technical and behavioral risk to reduce analyst workload.

ENHANCEMENT MODULE: TRAFFIC ORIGIN

Expose the true country-of-origin behind masked VPN, proxy, or residential traffic to identify high-risk remote sessions before they escalate into attacks.

PRIORITY USE CASES

- **Security Event Enrichment:** Verify risk levels by adding deep technical context to indicators and populating SIEM and SOAR workflows via API.
- **Infrastructure Hygiene:** Proactively identify forgotten servers and misconfigured records like Dangling DNS before they are exploited.
- **Rapid Risk Assessment:** Move beyond probability scores to deterministic certainty with binary True or False attribution. Establish a verified triage baseline without manual data reconstruction.

THE PREEMPTIVE ADVANTAGE

- **Reduced Triage Time:** Shorten investigation cycles by replacing manual data gathering with deterministic context in one place.
- **Tool Consolidation:** Lower licensing costs by replacing multiple standalone tools with a single interface.
- **Resource Optimization:** Ensure senior analysts focus on proactive mitigation rather than manual research and data reconstruction.

SILENT PUSH

NEUTRALIZE BEFORE COMPROMISE

Silent Push provides a Preemptive Cyber Defense platform that continuously discovers and tracks adversary infrastructure, enabling teams to detect and disrupt emerging threats before attacks launch.