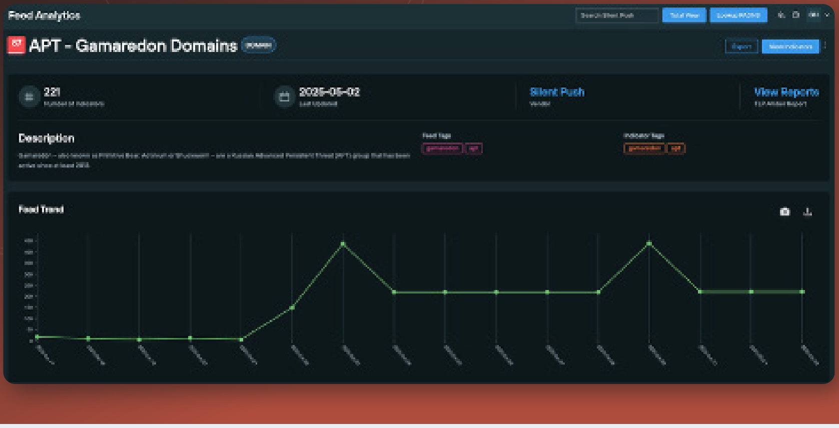
SILENT PUSH

DATA SHEET

# PRIORITY USE CASES FOR CYBERSECURITY TEAMS



## PREEMPTIVE CYBER DEFENSE

**Silent Push helps cybersecurity teams block threats early, by delivering attacker infrastructure intelligence at scale, with context and insight not available in any other CTI platform.**

By identifying adversary campaigns as they are being setup, Silent Push **minimizes risk, reduces cost,** and **improves efficiency** by replacing multiple CTI tools in one platform.

## REVEAL HIDDEN THREATS WITH IOFA™

Silent Push delivers **Indicators of Future Attack (IOFA)**™ - actionable domains and IP addresses that reveal where an attack will be launched from in the future, based on how an adversary manages their infrastructure.

- Attacker DNS automation
- Malicious hosting clusters
- Infrastructure changes over time
- Website content

## CISO

### MINIMIZE RISKS BEFORE THEY HIT

- Avoid costly cybersecurity incidents with better insight on who is targeting your organization, and from where.
- Enable faster, more informed CTI decision-making across all your teams.
- Reduce spend by consolidating multiple cybersecurity tools into one platform.

## CYBERSECURITY MANAGER

### IMPROVE INVESTIGATIONS WITH CTI DATA

- Ingest **IOFA**™ Feeds that help to reveal 100% of an attack landscape.
- Speed up triage by instantly enriching unknown indicators.
- Improve productivity and reduce the time it takes to discover domains and IPs for blocking.

## THREAT ANALYST

### CATCH THREATS EARLY, WITH REAL-TIME DNS

- Correlate billions of internet datapoints to quickly reveal patterns in adversary behavior.
- Access highly-detailed threat reports that guide you through complex APT investigations.
- Discover suspicious links between hosting providers to expose hidden domains and IPs.

## PROACTIVE THREAT HUNTING

Locate known and hidden threats by focusing on how adversaries manage and deploy malicious infrastructure across hosting clusters.

- Uncover suspect domains and IPs with unified DNS, scanning, certificate, and WHOIS data.
- Access hosting history, threat risk scores, and enriched **IOFA**™ Feed data to accelerate discovery.
- Feed precise, high-confidence alerts into your detection, investigation, and response workflows.

## BRAND IMPERSONATION DEFENSE

Avoid loss with the most effective and expansive anti-spoofing dataset available anywhere on the internet.

- Reveal fraudulent web portals, copycat content and hidden phishing infrastructure targeting your brand.
- Monitor newly registered domains using keywords linked to your organization's presence online.
- Correlate phishing kits to active and historic threat infrastructure, and specific APT activity.

## PASS CONTEXT-RICH INTELLIGENCE ACROSS YOUR SECURITY STACK

### SOC

IMPROVE TRIAGE WITH IOFA™

- Get immediate context on unknown domains and IPs in your alert queue.
- Eliminatte manual pivots, and automatically reveal hidden infrastructure.
- Reduce false positive indicators with enriched **IOFA**™ insights.

### IR

LIMIT YOUR EXPOSURE TO ONGOING ATTACKS

- Speed up investigations with high-confidence intelligence.
- Reduce the time it takes to contain a threat, once it's entered your network.
- Minimize damage by uncovering all the infrastructure involved in an attack.

### CTI

GAIN GREATER VISIBILITY TO PREEMPTIVELY AVOID LOSS

- Access DNS and web content intelligence not available through other vendors.
- Scan for APT activity across the public web and dark web.
- Ingest specialized **IOFA**™ Feeds that reveal known and hidden infrastructure.

## ABOUT US

Silent Push provides preemptive cyber defense exposing threat actor infrastructure as it's being set up. Our **Indicators Of Future Attack (IOFA)**™ act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

**Get started today.**

SILENT **PUSH**

PREEMPTIVE CYBER DEFENSE WITH
INDICATORS OF FUTURE ATTACK™

REQUEST A DEMO

| silentpush.com