



SILENT PUSH FOR CISOS

Preemptive Cyber Defense for the
security leaders answerable to the board.

WHAT SILENT PUSH DOES

Silent Push is a **preemptive cyber defense platform**. It continuously maps the domains, IPs, and hosting adversaries rely on. That mapping engine, the Context Graph, watches infrastructure while it is still being staged and generates **Indicators of Future Attack® (IOFA)** before a campaign launches. Your team gets early warning with real time to act, well ahead of any forensic report.

WHAT YOU TAKE BACK TO THE BOARD

01

Measurable risk reduction

Block pre-weaponized infrastructure and report threats prevented, not just alerts triaged.

02

A leaner stack

Consolidate redundant, noisy feeds into one source of high-confidence, block-grade indicators.

03

Early warning as a program metric

Lead time your team can act on, briefed with evidence.

WHO RELIES ON SILENT PUSH

Silent Push is trusted by **half of the Fortune 30, national governments, and the world's largest investment company, stock exchange, and retailer**. Preemptive data Silent Push generates has been acted on directly by Interpol and the US Treasury.

BOOK A WALKTHROUGH

Ask us what we can already see in your threat environment.
silentpush.com

YOUR BOARD IS ASKING ABOUT CYBER RISK

Your board measures security as operational, financial, and reputational risk. Tool counts and alert volumes do not answer what they are really asking, which is whether the organization is exposed right now.

The honest gap is that your stack was built to tell you what already happened.

Your SIEM fires once an attack is already in your logs. Threat feeds report indicators of compromise from breaches that hit someone else first. The weeks and months an adversary spends quietly building infrastructure stay invisible to every reactive tool you own.

"Your platform gives us a
super-unique perspective.
This is clearly the future."

— Big Four / Professional Services

FITS THE STACK YOU ALREADY RUN

IOFA feed directly into your existing **SIEM, SOAR, and firewall**, so it works without ripping out your stack or adding new workflows. Week one, your blocklists improve. By month three, your team is hunting full campaign clusters before a phishing email ever reaches an inbox.