SILENT PUSH INTERNAL SALES ENABLEMENT

Silent Push Personas

This document serves as the internal authority for persona-based sales engagements. It integrates detailed pain points from legacy documentation with the strategic positioning mandated by the 2026 Messaging Source Document (MSD).

BRAND AND CATEGORY COMPLIANCE

- **Market Category:** Preemptive Cyber Defense.
- **Core Tagline:** Neutralize Before Compromise.
- **Key Engine:** The Context Graph (mapping the "Internet's DNA").
- **Primary Output:** Indicators of Future Attack™ (IOFA™).

View full Messaging Source Document (MSD) here.

DETAILED PERSONA PROFILES

CISO / VP of Information Security

The Problem: Difficulty proving the ROI of security investments to the board. Leadership faces pressure to show measurable risk reduction while managing an average of 50 or more tools and expensive, noisy threat feeds that often duplicate data.

The Preemptive Shift: Silent Push provides earlier visibility into attacker activity occurring outside the enterprise, reducing reliance on reactive detection and post-incident response.

Relevant Modules:

- **Primary: Insight.** Provides foundational context and risk scoring to quantify organizational risk. It delivers the board level metrics (reduced risk, MTTD and MTTR improvement) required to justify security budgets.
- **Supportive: Defend.** Proves ROI by operationalizing data. It demonstrates how Silent Push trims the fat by pushing verified indicators into the existing stack, allowing for the consolidation of redundant feeds.

Silent Push Solutions:

- **Measurable Program Effectiveness:** Proactively block pre-weaponized infrastructure to report tangible outcomes like reduced incident volume.
- **Board-Ready Metrics:** Support real-time reporting on threats blocked and risk reduced.
- **Tool Consolidation:** Eliminate tool sprawl by combining active DNS, scanning, enrichment, and infrastructure mapping.

Messaging Example: Demonstrate measurable program effectiveness by proactively blocking known malicious infrastructure to enable your team to report clear board level metrics on threats prevented, risk reduced, and time saved.

SOC Manager

The Problem: The SOC is flooded with duplicative, low-confidence alerts. Analysts waste significant time triaging false positives and pivoting between multiple tools, slowing down investigations and preventing clear incident handoffs.

The Preemptive Shift: Identify malicious infrastructure as it is being created, allowing the team to anticipate campaigns instead of waiting for alerts from external tools.

Relevant Modules:

- **Primary: Defend.** The action engine. It allows the SOC Manager to automate the blocking of verified infrastructure level threats, directly solving alert fatigue.
- **Primary: Insight.** Total View serves as the primary tool for triage, providing geographic truth and first party data needed to verify indicators without pivoting.

Silent Push Solutions:

- **High-Fidelity Indicators:** Cut through alert noise with block-grade indicators to reduce analyst burnout.
- **Unified Enrichment:** Surface DNS, WHOIS, SSL, and scanning data in one click.
- **Automated Context:** Integrate enrichment directly into SIEM or SOAR pipelines to prioritize threats without manual involvement.

Messaging Example: Reduce investigation time and alert fatigue by automatically blocking verified infrastructure level threats to enable your team to focus on real incidents.

Incident Response (IR) Lead / Consultant

The Problem: IR teams often arrive after the damage is done. They struggle with infrastructure blindness where they cannot see the full scope of an attacker’s network, leading to incomplete remediation and repeat infections.

The Preemptive Shift: Shift from manual reconstruction of an attack to an infrastructure first view that reveals the adversary's entire staging environment.

Relevant Modules:

- **Primary: Reconnaissance.** Allows teams to map the adversary's entire staging environment and track infrastructure changes over time to ensure complete remediation.
- **Supportive: Insight.** During an active breach, IR needs instant threat clustering to identify the blast radius and see if other parts of the organization are being targeted by the same infrastructure.

Silent Push Solutions:

- **Infrastructure Mapping:** Use the Context Graph to find every IP and domain related to an initial indicator.
- **Historical Context:** Access years of DNS and WHOIS history to understand when an adversary first targeted the organization.
- **Deterministic Remediation:** Use verified infrastructure data to create comprehensive blocklists that prevent re-entry.

Messaging Example: Eradicate threats with confidence by mapping the adversary's entire external infrastructure, ensuring that your remediation efforts stop current and future access.

Threat Intelligence Lead / CTI Analyst

The Problem: Fragmented datasets prevent teams from generating deep insights into adversary infrastructure. Because DNS, scan, and WHOIS data live in separate silos, it is nearly impossible to cluster or fingerprint infrastructure at scale without significant cost and tool switching.

The Preemptive Shift: The platform continuously discovers and tracks the domains, IPs, and hosting providers attackers rely on to stage and execute operations.

Relevant Modules:

- **Primary: Reconnaissance.** The deep investigative workspace for behavioral fingerprinting and mapping malicious registration patterns before a payload is delivered.
- **Primary: Insight.** Provides the 70 to 100 plus attributes (certificates, JARM, etc.) that analysts need to build high fidelity profiles of threat actors.

Silent Push Solutions:

- **Infrastructure Fingerprinting:** Unify DNS, scanning, WHOIS, and SSL data for advanced clustering and pattern matching.
- **Shift Left Intelligence:** Identify behavioral patterns actors employ when setting up infrastructure to identify attack staging before operations go live.
- **Standardized Workflows:** Streamline how analysts enrich and verify indicators using a single interface or API.

Messaging Example: Accelerate adversary tracking and infrastructure clustering by working with context rich first-party data to fingerprint campaigns more accurately.

Security Architect

The Problem: Tool sprawl creates operational complexity and integration headaches. Lack of infrastructure-centric context makes it difficult to enforce detection at the edge or write effective firewall rules.

The Preemptive Shift: Adds external infrastructure visibility that complements internal controls and fits into existing operations without replacing core platforms.

Relevant Modules:

- **Primary: Defend.** Focuses on the plumbing. The 200 or more API endpoints ensure the data feeds directly into SIEM and SOAR pipelines.
- **Supportive: Insight.** Used to identify visibility gaps in the external attack surface. It provides the map that helps architects design a more robust, preemptive perimeter.

Silent Push Solutions:

- **API-First Architecture:** Ensures verified indicators push directly into core prevention and detection technologies.
- **Consolidated Enrichment:** Combine scanning, passive DNS, and enrichment in one platform to simplify the security stack.
- **External Perimeter Visibility:** Gain insight into attacker infrastructure created outside the perimeter, such as spoofed domains or exposed cloud assets.

Messaging Example: Reduce tool sprawl and operational complexity by consolidating DNS, scanning, WHOIS, and certificate enrichment workflows into a single tool that feeds your existing detection pipelines.

Brand Protection, Fraud & Digital Trust Teams

The Problem: A sophisticated "Superfake" economy where AI clones brand assets in minutes. Teams struggle with "Infrastructure Blindness," only discovering phishing portals or smishing campaigns after customers have already been compromised.

The Preemptive Shift: Moving from Reactive Takedowns to Preemptive Neutralization. By identifying lookalike domains and fraud kits during the registration and "aging" phase, teams can disrupt scams before they go live.

Relevant Modules:

- **Primary: Insight.** Provides the foundational "Geographic Truth" and automated forensic evidence (SSL, DNS history, and screenshots) required to prove malicious intent to registrars and hosts instantly.
- **Supportive: Defend.** Automatically feeds high-confidence brand-impersonation IOFAs™ into web gateways and firewalls to protect employees and customers from reaching malicious clones.

Silent Push Solutions:

- **Creation-Time Detection:** Identify spoofed domains and smishing infrastructure the second they are registered—often days before a phishing kit is even uploaded.
- **Origin Certainty:** Utilize Traffic Origin to unmask the true upstream source of sessions, identifying when "domestic" traffic is actually a fraudster or "laptop farm" hiding behind a residential proxy.
- **Ecosystem Monitoring:** Monitor the extended supply chain, including affiliates and resellers, for brand abuse or unauthorized asset use outside the immediate perimeter.

Messaging Example: Stop brand impersonation and customer fraud at the infrastructure level. Detect fake login portals at registration, not after an incident, and use Traffic Origin to unmask adversaries hiding behind local IP addresses.