Silent Push Battlecards 2026

This document serves as the internal authority for ideal customer profiles. 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™).

Remember: Silent Push is not a CTI platform; it is a Preemptive Cyber Defense (PCD) platform. While legacy CTI tells you who attacked you yesterday, PCD identifies the infrastructure adversaries are building today for use tomorrow. We don't just provide data for analysts to study; we deliver Indicators of Future Attack™ (IOFA™) that a SOC team can block before a campaign even launches.

View full Messaging Source Document (MSD) here.

Table of Contents

Censys

The Strategic Reframe: Censys is an **Asset Discovery** tool that catalogs your own internet-facing infrastructure (finding your unlocked doors). Silent Push is a **Preemptive Cyber Defense** platform that identifies the adversary while they are still in the staging phase (finding the person in your yard before they reach the door).

Capability	Silent Push	Censys
Operational Mission	**Neutralize Before Compromise:** Identifying staging infrastructure before it's weaponized.	**Asset Visibility:** Cataloging internet-facing assets to find misconfigurations.
Core Engine	**The Context Graph:** Mapping "Internet DNA" and management patterns.	**Internet Scanning:** Active IPv4/IPv6 scans to see what is currently live.
Key Signal	**IOFA™ (Indicators of Future Attack):** Verified pre-weaponized staging grounds.	**Raw Scan Data:** Datasets of IP/Port status requiring manual analysis.
Data Methodology	**PADNS:** Active force resolution to map infrastructure relationships.	**Passive Scanning:** Traditional scanning of known services and open ports.

Tactical notes (why we win):

Staging vs. Active: Censys sees what is active and "scannable". Silent Push identifies Adversary Infrastructure (domains, IPs, and hosting) weeks before they are weaponized.

Deterministic vs. Reactive: Censys provides raw telemetry that requires manual triage. Silent Push provides deterministic signals based on verified management patterns in The Context Graph.

Adversary Focus: Censys tells you what you have exposed. Silent Push tells you what the adversary is building to target you, even if they aren't using your brand name yet.

The "Kill Zone" (trap questions)

- "Your current tool shows you your open ports. But who is showing you the infrastructure being built specifically to target you next week?"
- "When a new domain is registered but has no content or server attached yet, how do you determine if it's part of an adversary cluster?"
- "How much time does your team spend manually correlating raw scan data into actionable threat intelligence?"

Recorded Future

The Strategic Reframe: Recorded Future acts as a retrospective encyclopedia of known threats, aggregating existing data to report on previous adversary activity. Silent Push is an early warning radar for Preemptive Cyber Defense that identifies the infrastructure adversaries are building today to use against you tomorrow.

Capability	Silent Push	Recorded Future
Operational Mission	**Neutralize Before Compromise:** Identify staging infrastructure before weaponization.	**Retrospective Intelligence:** Catalog known adversaries and global campaign trends.
Core Engine	**The Context Graph:** Mapping the "Internet's DNA" to expose hidden management patterns.	**Intelligence Aggregation:** Scrapes OSINT, dark web, and third-party partner feeds.
Key Signal	**IOFA™ (Indicators of Future Attack):** Verified, pre-weaponized adversary staging grounds.	**IOCs (Indicators of Compromise):** Reports on breaches and activity that have already occurred.
Data Methodology	**Deterministic Collection:** Proprietary data like **PADNS** for high-fidelity defense.	**Third-Party Heavy:** Heavy reliance on external partner data and open source collection.

Tactical notes (why we win):

Future vs. Past: Recorded Future relies on Indicators of Compromise (IOCs) from past events. Silent Push identifies Adversary Infrastructure during setup, allowing you to block threats weeks before an attack launches.

Action vs. Research: Recorded Future is built for strategic study. Silent Push is API-first, built for the SOC to automate enrichment and blocking directly in SIEM and SOAR workflows.

Deterministic vs. Probabilistic: Feeds often rely on inferred risk scores. Silent Push signals are deterministic, based on verified management patterns found in The Context Graph.

The "Kill Zone" (trap questions)

- "Recorded Future tells you who the actor is, but does it alert you when that actor registers a clean domain before it is used in an attack?"
- "How much of your analysts' time is spent reading strategic reports versus actually blocking pre-weaponized infrastructure?"
- "Does your current intel tell you who is building look-alike infrastructure to spoof your brand right now, or only after the phishing campaign starts?"

Mandiant

The Strategic Reframe: Mandiant acts as a central intelligence command, providing a retrospective encyclopedia of who attacked you and their tactics based on past incidents. Silent Push is an early warning radar for Preemptive Cyber Defense that identifies the infrastructure adversaries are building today to use against you tomorrow.

Capability	Silent Push	Mandiant

Operational Mission	**Neutralize Before Compromise:** Identify staging infrastructure before weaponization.	**Incident Response & Analysis:** Strategic reporting on post-compromise activity and actor playbooks.
Core Engine	**The Context Graph:** Mapping the internet's DNA to expose hidden management patterns.	**Intelligence Aggregation:** Mix of proprietary Google Cloud telemetry, partner data, and OSINT.
Key Signal	**IOFA™ (Indicators of Future Attack):** Verified, pre-weaponized adversary staging grounds.	**IOCs (Indicators of Compromise):** Short-lived tactical indicators and historical TTPs.
Data Methodology	**Deterministic Collection:** Proprietary data like **PADNS** for high-fidelity defense.	**Historical Telemetry:** Focuses on infrastructure post-attack or mid-campaign.
Integration	**API-First:** 200+ endpoints built for seamless SIEM and SOAR automation.	**Ecosystem Focused:** Primarily integrated within the Google Chronicle stack.

Tactical Notes (why we win)

Preemptive vs. Reactive: Mandiant reports on what already happened. Silent Push identifies Adversary Infrastructure in the setup phase to block threats before they launch.

Actionable vs. Strategic: Mandiant focuses on long-term risk and reporting. Silent Push provides deterministic signals for immediate, automated SOC action weeks before weaponization.

Upstream Visibility: While Mandiant tracks known C2 IPs, Silent Push moves upstream to uncover infrastructure relationships and management patterns that traditional tools miss.

The "Kill Zone" (trap questions)

- "Mandiant tells you who attacked you, but does your intel alert you when that adversary is building new, clean infrastructure to use against you next week?"
- "How much time is spent reading reports about past campaigns versus proactively blocking pre-weaponized infrastructure?"
- "When an adversary rotates IPs for a new campaign, how long does it take for your current feeds to update those indicators?"

DomainTools

The Strategic Reframe: The DomainTools Platform is a research and investigation tool used to pivot through historical records to map who owns a domain. Silent Push is a Preemptive Cyber Defense platform that identifies the infrastructure adversaries are building today, often before they are even registered or seen by traditional research platforms.

Capability	Silent Push	DomainTools
Operational Mission	**Neutralize Before Compromise:** Identify staging infrastructure before weaponization.	**Adversary Mapping:** Connect known indicators to map existing attacker footprints.

Core Engine	**The Context Graph:** Mapping "Internet DNA" and management patterns.	**Investigation UI:** A research workspace focused on pivoting through DNS and WHOIS data.
Key Signal	**IOFA™ (Indicators of Future Attack):** Deterministic signals of staging grounds.	**Risk Score:** Probabilistic scoring based on domain age and registration history.
Data Methodology	**Deterministic Collection:** Proprietary force resolution to find un-scannable clusters.	**Historical Aggregation:** Massive repository of global WHOIS and DNS records.
Detection Speed	**Pre-Weaponization:** Detects setup patterns before it hits your perimeter.	**Post-Registration:** Primarily relies on domains being registered or seen in traffic.

Tactical Notes (why we win)

Preemptive vs. Investigative: DomainTools is built for research after an alert. Silent Push is built for preemptive defense, identifying Adversary Infrastructure before it's weaponized.

Context Graph vs. Manual Pivoting: DomainTools requires manual pivoting to find connections, Silent Push uses The Context Graph to automatically cluster related infrastructure, reducing research time.

Deterministic Signals vs. Risk Scores: DomainTools provides a risk score based on probability. Silent Push provides deterministic IOFAs validated signals that the infrastructure is historically malicious or part of a known adversary staging ground.

The "Kill Zone" (trap questions)

- "DomainTools is great for looking up a domain you already know. But who is showing you the infrastructure being built to target you next week that has not been used yet?"
- "How much time do your analysts spend manually pivoting through records to find related domains instead of having those clusters automatically surfaced?"
- "Can your current tool detect a clean, newly registered domain that has no website content yet, but is part of an adversary setup pattern?"

Shodan

The Strategic Reframe: Shodan is a search engine for the Internet of Things (IoT), designed to help researchers find exposed devices and open ports on existing infrastructure. Silent Push is a Preemptive Cyber Defense platform that identifies the infrastructure adversaries are building today to use against you tomorrow, before those assets are even fully operational or scannable.

Capability	Silent Push	Shodan
Operational Mission	**Neutralize Before Compromise:** Identify staging infrastructure before weaponization.	**Asset Visibility:** Search and catalog publicly accessible devices and open services.

Core Engine	**The Context Graph:** Mapping "Internet DNA" and management patterns.	**Banner Crawling:** Scanning IPv4/IPv6 space to index service banners and metadata.
Key Signal	**IOFA™ (Indicators of Future Attack):** Deterministic signals of staging grounds.	**Technical Metadata:** Open ports, service versions, and vulnerability (CVE) correlations.
Data Methodology	**Deterministic Collection:** Proprietary force resolution to find hidden or un-scannable clusters.	**Active Scanning:** Regular probes of common ports to see what is currently listening.
Primary Use Case	**Preemptive Blocking:** Stopping attacks at the infrastructure setup phase.	**Vulnerability Research:** Auditing exposed assets and finding misconfigured IoT devices.

Tactical Notes (Why we win)

Staging vs. Exposure: Shodan tells you what is already exposed and scannable. Silent Push identifies Adversary Infrastructure while it is being built, allowing you to block threats weeks before they become active or appear in a traditional scanner.

Adversary Patterns vs. Device Queries: Shodan is great for finding a specific version of a router or a webcam. Silent Push uses The Context Graph to automatically cluster related infrastructure based on how an adversary manages their network, regardless of what device is on the IP.

Deterministic Action vs. Manual Triage: Shodan provides massive datasets of open ports that require manual analysis. Silent Push provides deterministic IOFAs, which are validated signals for immediate, automated SOC action to block emerging campaigns.

The "Kill Zone" (Trap questions)

- "When an adversary registers a domain but has not opened any ports or services yet, how do you detect that staging activity?"
- "How much time does your team spend manually correlating Shodan scan data into actionable blocks instead of having those adversary clusters surfaced automatically?"
- "Shodan shows you your open ports. But who is showing you the infrastructure being built specifically to target you next week that has not been used yet?"

Validin

The Strategic Reframe: Validin is a DNS intelligence platform designed for faster investigation and triage. It aggregates OSINT and historical DNS to help analysts connect the dots once a threat is already known. Silent Push is an early warning radar for Preemptive Cyber Defense that identifies the infrastructure adversaries are building today, allowing for automated blocking before those indicators are ever reported to OSINT.

Capability	Silent Push	Validin
Operational Mission	**Neutralize Before Compromise:** Identify staging infrastructure before weaponization.	**Threat Hunting & Research:** Pivot through DNS history and OSINT to investigate threats.
Core Engine	**The Context Graph:** Mapping "Internet DNA" to expose hidden management patterns.	**DNS Intelligence Platform:** A searchable database of DNS history and host responses.

Key Signal	**IOFA™ (Indicators of Future Attack):** Deterministic signals of staging grounds.	**Aggregated OSINT:** Sightings from hundreds of public blocklists and reputation feeds.
Data Methodology	**Deterministic Collection:** Proprietary force resolution to find hidden or un-scannable clusters.	**Historical Aggregation:** 4+ years of resolution history combined with active port scanning.
Primary Use Case	**Preemptive Blocking:** Stopping attacks at the infrastructure setup phase.	**Indicator Enrichment:** Triage and context for IPs and domains during an investigation.

Tactical Notes (Why we win)

Preemptive vs. Reactive Triage: Validin's "proactivity" is actually accelerated triage of reported threats. Silent Push identifies infrastructure in the setup phase, often weeks before it appears in the OSINT feeds that Validin aggregates.

Automation vs. Manual Research: Validin is built for manual pivoting by an analyst. Silent Push uses The Context Graph to automatically cluster related infrastructure, surfacing entire adversary ecosystems without manual effort.

Direct Defense vs. Enrichment: Validin helps you understand an alert. Silent Push provides deterministic IOFAs for immediate, automated SOC action to block threats before they touch your perimeter.

The "Kill Zone" (Trap questions)

- "Validin helps you research an IP you already found. Who is showing you the infrastructure being built to target you next week that has not been reported in OSINT yet?"
- "How much time is spent manually pivoting through DNS history instead of having related adversary clusters surfaced automatically?"
- "Does your tool provide deterministic signals for automated blocking, or does it require an analyst to manually validate every connection?"

Complimentary products

--- Coming soon