SILENT PUSH INTERNAL SALES ENABLEMENT

Silent Push Ideal Customer Profiles (ICP)

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.

DETAILED ICP PROFILES

Financial Services: Banking, FinTech, Fraud and Compliance

Business Impact: Credential theft and smishing result in immediate financial losses and increased customer churn. Passive response strategies allow for a "first-hour" surge of fraud where the majority of theft occurs before a site is taken down.

Operational Friction

- **SOC/IR:** Teams spend significant hours submitting takedown requests for domains that have already successfully harvested credentials, leading to a permanent "reactive" state.
- **CTI:** Analysts receive bulk threat data that lacks the infrastructure-level context needed to generate high-fidelity blocklists for the SOC.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Identification of smishing and fake banking infrastructure at the point of registration. This enables the SOC to block access before a single message is sent to customers.
- **CTI Support:** Delivery of Indicators of Future Attack™ (IOFA™) allows analysts to provide the SOC with validated data, reducing false positives.
- **Global Regulatory Alignment:**

- **EMEA:** Adherence to DORA (EU 2022/2554) regarding ICT risk and detection. Source: EUR-Lex
- **AMER:** Compliance with SEC Cybersecurity Disclosure rules requiring "timely" incident reporting and risk management. Source: SEC.gov
- **APJ:** Alignment with the Australian Privacy Act (APP) and similar regional frameworks regarding data breach prevention. Source: OAIC

Healthcare and Pharma: Ransomware and Patient Safety

Business Impact: Operational downtime in healthcare directly impacts patient care. Ransomware groups utilize distinct infrastructure patterns for staging; waiting for an endpoint alert means the network is already compromised.

Operational Friction

- SOC/IR: Teams lack visibility into the domain and IP health of clinical partners and vendors, which often serve as initial entry points for lateral movement.
- CTI: Analysts are frequently distracted by commodity malware, missing the subtle infrastructure cues that precede a targeted ransomware deployment.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Monitoring for spoofed patient and clinical trial portals at the domain registration level, preventing the initial credential harvest that leads to ransomware.
- **CTI Support:** Tracking the DNS and IP footprints associated with Ransomware-as-a-Service (RaaS) groups to provide Indicators of Future Attack™ (IOFA™).
- **Regulatory Context:**
  - **AMER:** HIPAA Security Rule requirements for proactive risk analysis. Source: HHS.gov
  - **EMEA:** GDPR Article 32 requirements for technical measures to ensure security. Source: GDPR-info.eu

---

Energy and Utilities: National Risk and OT Integrity

Business Impact: For Energy and Industrial Control Systems (ICS), availability is the primary metric. Nation-state actors build out infrastructure months in advance of an operation.

Operational Friction

- **SOC/IR:** Teams are forced into a reactive posture because traditional security focuses on file hashes, which are ineffective against custom, single-use infrastructure.
- **CTI:** Analysts lack the data to track how APT groups move across global ASNs and regions before they attempt to authenticate against VPNs.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Delivery of Indicators of Future Attack™ (IOFA™) that allow the SOC to harden the perimeter against specific nation-state infrastructure before an exploit is attempted.
- **CTI Support**: Mapping adversary staging areas across global ASNs to identify intent before the attack reaches the local network.
- **Regulatory Context:**
  - **AMER:** NERC CIP standards for cyber security of the bulk power system. Source: NERC
  - **APJ:** Security of Critical Infrastructure Act (SOCI) in Australia. Source: Home Affairs AU

Retail and E-Commerce: Brand Integrity and Account Takeover (ATO)

Business Impact: Seasonal fraud spikes result in massive volumes of Account Takeovers. The cost of manual evidence gathering and brand remediation often exceeds the direct fraud loss.

Operational Friction

- **SOC/IR:** Teams spend most of their time manually capturing evidence for takedowns rather than neutralizing the source of the campaign.
- **CTI:** Often misses brand-impersonation risks introduced by marketing affiliates and third-party vendors.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Automated provision of screenshots and metadata for spoofed domains, reducing the manual burden of takedown submissions and incident documentation.
- **CTI Support:** Identification of scam infrastructure targeting loyalty programs using Indicators of Future Attack™ (IOFA™).
- **Regulatory Context: Global -** PCI DSS 4.0 requirements regarding automated tools to detect and prevent web-based attacks. Source: PCI Security Standards

---

AMER: Department of Defense (DoD) and National Security

Business Impact: In a "Defend Forward" posture, waiting for a breach of the NIPRNet/SIPRNet is an operational failure. Nation-state reconnaissance and supply chain infiltration represent a constant risk to mission-critical uptime and personnel safety.

Operational Friction

- **SOC/IR:** Teams are overwhelmed by the scale of multi-layered IT/OT environments, often reacting to lateral movement rather than preventing the initial entry.

- **CTI:** Personnel struggle to provide deterministic evidence of adversary intent when state-sponsored actors use residential proxy "laptop farms" to appear as local traffic.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Use of Indicators of Future Attack™ (IOFA™) to identify and block C2 servers and phishing domains at the staging ground, before they touch defense networks.
- **Counter-Intelligence (Traffic Origin):** Unmask "Invisible Insiders" by identifying the true physical origin of traffic, bypassing fraudulent personas used to infiltrate defense projects.
- **Procurement Pathway:** Awardable status on the Tradewinds Solutions Marketplace (as of Dec 2024) provides a pre-vetted, post-competition pathway to bypass traditional acquisition delays. Source: Tradewinds Solutions Marketplace

---

AMER: Law Enforcement (LEO) and Federal Civilian (FCEB)

Business Impact: For LEO, success is measured by the disruption of criminal supply chains. For FCEB agencies (HHS, Treasury, VA), success is measured by the protection of citizen data and the integrity of public-facing portals.

Operational Friction

- **SOC/IR:** FCEB teams face constant spoofing of agency portals (e.g., fake IRS or FEMA sites) which leads to mass credential theft and the erosion of public trust.
- **Investigators (LEO):** Criminal "Infrastructure Laundering" via legitimate IPs makes traditional attribution nearly impossible without upstream visibility.

Preemptive Cyber Defense

- **SOC/IR Outcome (FCEB):** Preemptively flag and block spoofed domains mimicking federal services during critical periods, such as tax season or disaster response.
- **Upstream Attribution (LEO):** Use Traffic Origin data to see past "clean" residential proxies to the deterministic physical origin of a threat actor, providing the evidence required for warrants.
- **Regulatory Context:** Compliance with CISA Binding Operational Directives, specifically BOD 26-02 regarding edge device security and infrastructure visibility. Source: CISA.gov

---

EMEA: National Cybersecurity Authorities and CSIRTs

Business Impact: Under the NIS 2 Directive, national agencies are legally responsible for coordinated management of large-scale incidents. Success requires a "Common Operational Picture" across the entire national infrastructure.

Operational Friction

- **SOC/IR:** National-level CSIRTs struggle to coordinate cross-border takedowns when they lack deterministic data on where the adversary is actually hosting their infrastructure.

- **CTI:** The requirement for 24-hour "early warning" notifications is impossible to meet using reactive, signature-based intelligence feeds.

Preemptive Cyber Defense

- **SOC/IR Outcome:** National agencies use Indicators of Future Attack™ (IOFA™) to provide sectoral CSIRTs (Energy, Health, Finance) with the data needed to block infrastructure across the nation simultaneously.
- **Active Takedowns:** Provision of first-party DNS and scan data to provide the legal evidence needed for national-level domain seizures.
- **Regional Mandate:** Direct support for NIS 2 requirements regarding coordinated vulnerability disclosure and incident response. Source: EUR-Lex (EU 2022/2555)

APJ: National Security and Sovereign Resilience

Business Impact: APJ agencies face a high volume of regional APT activity (e.g., Lazarus, Volt Typhoon). Maintaining "Sovereign Resilience" requires the ability to verify the truth in data despite AI-driven misinformation and infrastructure migration.

Operational Friction

- **SOC/IR:** Regional teams lack "Region-Aware" data, often relying on global defaults that miss the rapid migration of infrastructure across local ASNs.
- **CTI:** Identifying the "Invisible Insider"—state-sponsored operatives using domestic residential proxies to appear as local residents—requires data that traditional feeds do not provide.

Preemptive Cyber Defense

- **SOC/IR Outcome:** Infrastructure fingerprinting to track the migration of state-sponsored nodes across regional ASNs, identifying C2 nodes as they are activated.
- **Supply Chain Sovereignty:** Mapping the external exposure of regional vendors and outsourced developers to prevent a "domino effect" compromise across the territory.
- **Regional Context:** Alignment with Australia's Security of Critical Infrastructure (SOCI) Act and Singapore's Cybersecurity Act. Source: Cyber Security Agency of Singapore

---

Regulatory Summary

Note that the following is not reflective of all regulatory requirements and mandates specific to a country or region, but a summary of several important ones.

Region	Primary Mandate	Key Requirement	Silent Push Operational Outcome

AMER	SEC Cybersecurity Disclosure	Timely disclosure of "material" incidents and risk management processes.	Preemptive Blocking: IOFA™ data allows the SOC to block staging infrastructure, preventing "material" breaches before they require disclosure.
AMER	CISA BOD 26-02	Enhanced visibility and security of edge devices and infrastructure.	Infrastructure Mapping: Provides a complete view of external exposure and identifies spoofed domains targeting federal edge services.
EMEA	DORA (EU 2022/2554)	ICT third-party risk management and high standards for detection.	Third-Party Monitoring: IR teams can monitor the infrastructure health of the entire supply chain to detect vendor-related risks.
EMEA	NIS 2 (EU 2022/2555)	24-hour "early warning" notifications and coordinated response.	Accelerated Warning: CTI teams identify adversary staging days in advance, providing the SOC with the "early warning" data required by law.
APJ	SOCI Act (Australia)	Protection of critical infrastructure assets and mandatory reporting.	Adversary Fingerprinting: Identify nation-state C2 nodes migrating across regional ASNs before they impact critical utilities.
Global	PCI DSS 4.0	Automated tools to detect and prevent web-based attacks/phishing.	Automated Evidence: Instant screenshots and metadata of spoofed portals allow for rapid, automated identification of phishing infrastructure.


SILENT PUSH