SILENT PUSH

DATA SHEET

BUILD PROACTIVE CYBER DEFENSE WITH SILENT PUSH SOAR AND SIEM INTEGRATIONS

Silent Push injects context-rich threat intelligence directly into your SOAR and SIEM platforms, using a suite of a native integrations optimized for large-scale cyber defense operations. Our proprietary DNS and web content datasets enrich internal alerts, enabling you to correlate **Indicators of Future Attack (IOFA)™** feeds with suspicious domains and IPs, and automate cybersecurity decisions to achieve preemptive threat discovery.

By integrating our datasets into your existing workflows, you'll achieve faster triage, earlier detection of attacker infrastructure, and accelerated response times. Silent Push helps your team shift from a reactive to a proactive defense posture by streamlining CTI workflows and automating responses, without the need for complex changes to your current security stack.

DNS AND WEB CONTENT ENRICHMENT

Silent Push applies 200+ enrichment categories to each indicator we scan, providing high-fidelity context from DNS and content-based datasets not available anywhere else.

Our data helps analysts locate hidden infrastructure involved in a campaign - not just publicly known IOCs. With coverage across DNS, WHOIS, certificate, and content scanning datasets, teams gain immediate context on unknown indicators in their alert queues.

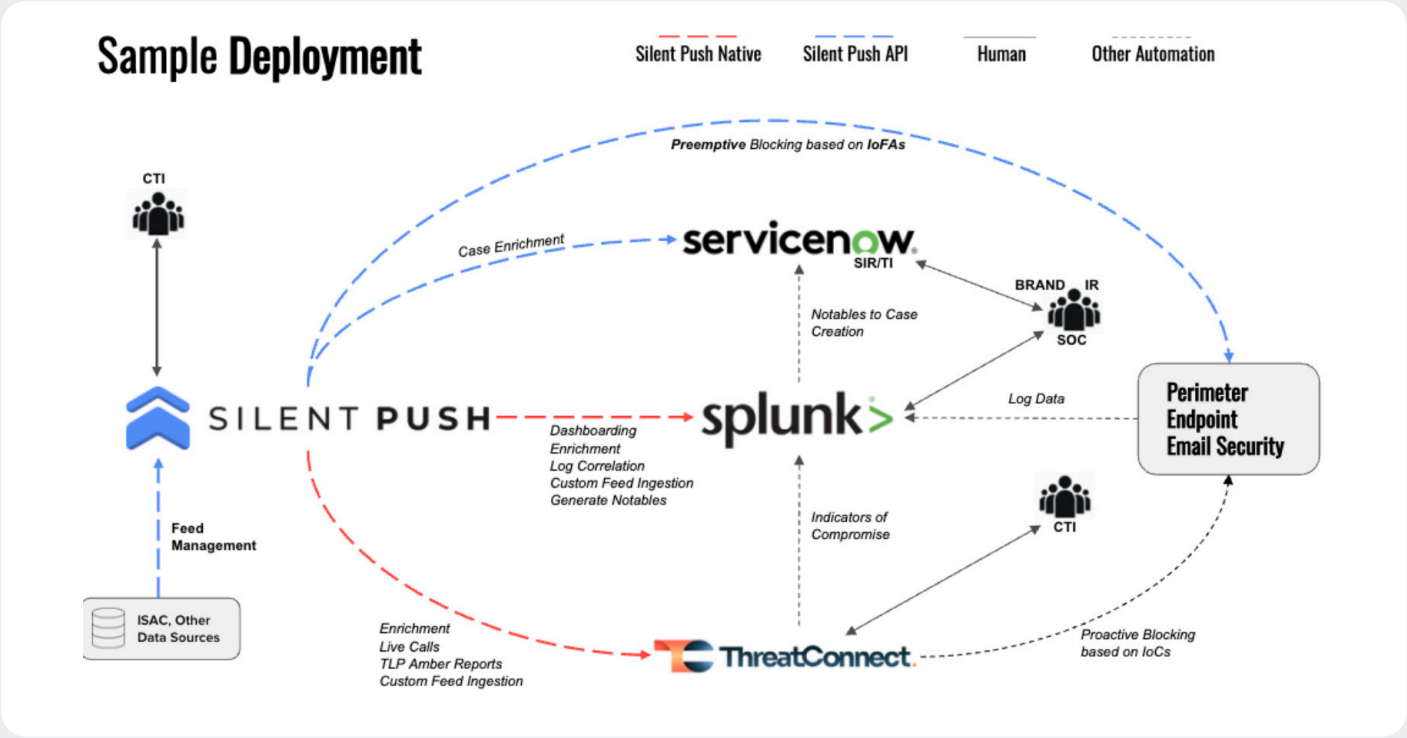
- Enrich domains, IPs, and ASNs with risk scores and reputation data.
- Visualize active infrastructure with live scans and screenshots.
- Apply context from **Indicators of Future Attack (IOFA)™** feeds.

AUTOMATE DECISION-MAKING

Our integrations allow teams to automate repetitive tasks and trigger actions based on indicator reputation and global DNS relationships, including malicious hosting clusters.

From auto-creating incidents and instant observable enrichments, Silent Push improves efficiency across your detection, triage, and response workflows.

- Initiate enrichment and correlation actions in SOAR and SIEM playbooks.
- Automatically trigger ticketing actions for high-risk indicators.
- Execute downstream workflow actions that remove manual intervention.



PREEMPTIVE DETECTION AND TRIAGE

Silent Push reduces triage investigation times, and discovers threats faster by providing instant context on unknown indicators in your alert queues. This enables security teams to identify and assess attacker infrastructure earlier, using **Indicators of Future Attack (IOFA)**™ and proprietary data types not found in traditional IOC feeds.

BETTER THREAT VISIBILITY

With over 200 enrichment categories applied to every scanned indicator, teams can connect the dots between billions of observable datapoints on the Internet, and locate hidden threat infrastructure linked to known malicious indicators. Live scanning, DNS pivoting, and risk scoring across domains, IPs, and ASNs helps analysts discover relevant context faster.

ELIMINATE MANUAL INTERVENTION

Give SOC and IR teams the time and space they need to focus on more critical tasks, by automating your threat detection and response workflows. Simultaneously save time and combat alert fatigue, by giving analysts context-rich intelligence that they can act upon immediately, without the need for endless pivots.

splunk>

SPLUNK SIEM

Our Splunk SIEM integration embeds Silent Push's threat intelligence alongside your information and event logging environment allowing security teams to correlate internal logs with preemptive threat insights, providing enriched context on unknown indicators, at scale.

EXAMPLE

An alert in Splunk SIEM flags unusual outbound traffic. Silent Push correlates the event with **Indicators of Future Attack (IOFA™)** Feeds, confirming the destination IP is a newly identified Command and Control (C2) server. This immediate context enables an analyst to isolate the network device, and prevent a malware attack from executing.

CORTEX XSOAR

By combining Silent Push data with XSOAR's playbook automation capabilities, security teams can transition from reactive IOC-based triage to proactive threat discovery, at scale.

EXAMPLE

An alert hits your SOC, it's passed through XSOAR to Silent Push, where the domain is enriched with DNS history, certificate associations, and similarity to known threat actor TTPs. After generating an enhanced risk profile based on the above information, the system can escalate, suppress, or initiate blocking – all without manual intervention.

OPENCTI

The Silent Push Internal Enrichment Connector integrates **IOFA™** data into OpenCTI, providing enhanced context on unknown indicators, and improving your teams' ability to visualize relationships between different clusters of threat activity within your Open CTI environment.

EXAMPLE

An analyst discovers a suspicious domain mentioned in an OpenCTI intelligence report. The connector adds Silent Push's **IOFA™** data, revealing the indicator's role in an emerging threat campaign. Your team gains instant context and can act on the threat proactively, directly within the OpenCTI platform, before an attack is launched.

SPLUNK SOAR

Our Splunkbase app for Splunk SOAR delivers threat intelligence and playbook automation within Splunk SecOps workflows. By embedding **IOFA™** data alongside Splunk datastreams, teams can move from manual investigation to proactive, TTP-driven responses.

EXAMPLE

Your SOC receives a phishing alert into your Splunk instance. A playbook takes the suspicious domain, enriches it via Silent Push, and calculates a risk score. If the domain is flagged as high risk, an automated response is triggered – such as initiating an action in a ticketing system, or isolating the asset via firewall integration.

SERVICENOW

The Silent Push ServiceNow integration connects incidents and observables inside ServiceNow's Security Operations suite with Silent Push datapoints, enabling teams to take fast, informed action on emerging threats before they turn into a breach.

1. Generate Tickets from an IOFA™ Feed

When Silent Push detects a newly registered domain mimicking your brand or infrastructure, a ServiceNow ticket is created that allows legal, brand protection, or threat intel teams to automatically initiate an investigation.

2. Enrich Existing Tickets with IOFA™ Context

If an indicator appears in Splunk that triggers a ServiceNow ticket, Silent Push is queried to retrieve DNS history, certificate data, hosting changes, and risk scoring to help assess its threat level.

3. Build Custom Enrichment Workflows

Directly leverage Silent Push APIs within your ServiceNow playbooks. For example, automatically capture a live screenshot of any domain included in a phishing report or correlate IPs with infrastructure clusters seen in IOFA™ datasets.

BOOK A DEMO

Our team will show you how easy it is to link your SOAR and SIEM platforms with the Silent Push API, and build faster, more efficient security workflows that remove manual intervention and give teams access to better insight on emerging threat infrastructure.

Contact us today to learn about how Silent Push can integrate with your security stack in a personalized demo.

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