SILENT PUSH

ANTICIPATING THE UNSEEN: Elevating Cyber Defense with Silent Push Preemptive Threat Intelligence

Author: Brad LaPorte
Gartner Veteran and Industry Expert

LIONFISH
TECH ADVISORS

CONTENTS

EXECUTIVE SUMMARY

The domain of Cyber Threat Intelligence (CTI) is experiencing a rapid surge in the quantity, sophistication, and frequency of cyber threats. Traditional security measures are failing against increasingly advanced and evolving threats.

Adversaries are deploying increasingly more complex tactics to circumvent standard protective barriers, prompting organizations to recognize an urgent need for a pivot towards more predictive defense mechanisms that can identify unknown threats prior to launch.

Compounding the situation is the rise of generative AI, a foundational concept growing in stature within the cyber arena. Automation provided by generative AI lowers the entry threshold for cybercriminals, enabling even those with minimal technical skills to execute wide-ranging attacks. The commoditization of offensive tooling is swelling the ranks of the cybercrime community and allowing adversaries to streamline their operations.

It is imperative for organizations to adopt **Preemptive Threat Intelligence (PTI)** - an approach to cyber defense and threat hunting that can identify emerging threats, allowing them to be neutralized before they become a problem. PTI is an innovative concept that is becoming a hot topic in cybersecurity circles and being delivered by a group of bleeding-edge organizations.

This report delves into PTI's methodology, its critical role in the evolving threat landscape, and how Silent Push—a U.S.-based threat intelligence vendor—delivers PTI through its platform.

INTRODUCTION

In an era marked by increasingly sophisticated cyber threats and considering the substantial financial repercussions of security breaches, the need for forward-thinking cyber defense strategies is self-evident. IBM's Cost of a Data Breach Report 2023 underscores this reality, with the average breach costing approximately USD $4.45 million.

Against this backdrop, the industry is developing mechanisms to identify unknown threats before they launch. PTI is one such mechanism. The term PTI was first coined in 2023 by numerous industry and analyst sources, often using similar terms such as 'Proactive Threat Intelligence,' or 'Predictive Threat Intelligence.' It's the opinion of the author that PTI will be in widespread use by the end of 2024.

This report examines PTI's emerging role in the modern cybersecurity arena, where traditional defenses based on Indicators of Compromise (IOCs) often fall short by only alerting organizations to what is already known as bad.

PTI, in contrast, aims to drastically change the equation and eliminate the traditional Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR), metrics by giving organizations the ability to block attacks before they are launched and prevent the financial operational and reputational consequences of cyber threats.

This report will explore the intricacies of PTI and its pivotal role in the current and future threat intelligence landscape before detailing the challenges organizations face and the benefits PTI provides. Lastly, we'll drill into Silent Push's PTI solution and what sets it apart in the marketplace.

MARKET LANDSCAPE

The current threat intelligence landscape is saturated with solutions that are increasingly falling behind the offensive capabilities of modern threat actors. These legacy systems are limited to identifying known threats, leaving organizations vulnerable to new, unseen attacks.

> *"The poor quality of threat intel makes organizations unwilling and unable to make decisions off their collected threat data. Threat intelligence is often incomplete, inaccurate, or outdated, and this makes it difficult for organizations to make informed security decisions."*
>
> ***— Dr. Anton Chuvakin, Google Cloud, August 31, 2023***

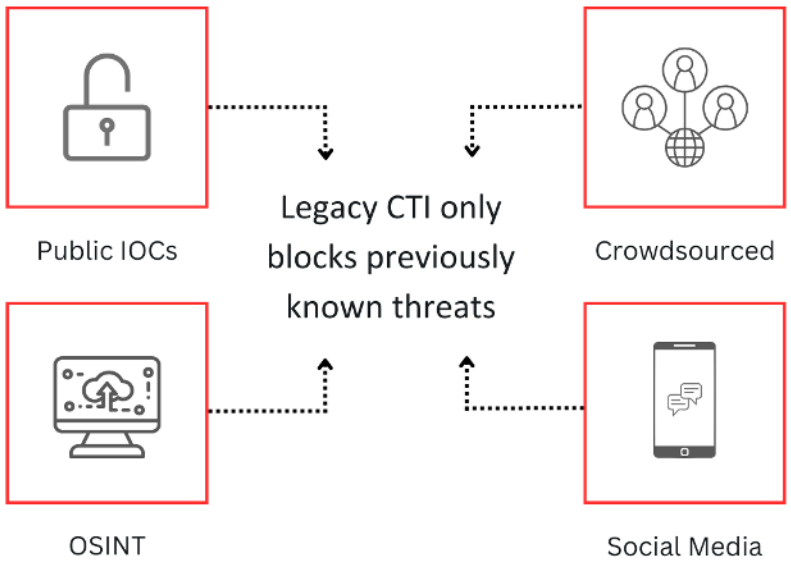

Figure 1: How Legacy Threat Intel assembles data

LEGACY CTI VS. PREEMPTIVE CTI

The term ‘legacy threat intelligence’ refers to a CTI methodology that relies on traditional Indicators of Compromise (IOC) - publicly available threat data obtained from OSINT sources, CTI vendors, post-breach security incidents, and published intelligence sources such as social media and blogs.

For teams tasked with both defending their organization’s public DNS presence and hunting for known and unknown threats, The disparate nature of legacy threat intelligence leads to numerous operational and technical difficulties, including:

- A distinct lack of meaningful aggregation.
- Complexity and overlap.
- Difficulty in creating relationships between data.
- Outdated, slow to search datasets.
- A reliance on what HAS happened.
- Too many false positives.
- Less actionable intelligence.

How Preemptive Threat Intelligence works (PTI)

By analyzing patterns and the underlying infrastructure that attackers utilize, PTI allows organizations to implement defense methodologies that track attacker infrastructure across the Internet - including nameservers, web content, registrar information, and hosting data - rather than relying on stale IOCs that limit intelligence gathering to a single point in time.

Establishing a pattern of adversary behavior is accomplished by enumerating the entire global IPv4 range—including domains, IP addresses, and DNS records—and using big data analytics to create predictive threat modeling, which gives security teams the ability to forecast and preempt adversary activity with remarkable accuracy.

One of the biggest advantages of PTI is that threats can be identified across the entire attack chain - including emerging attacks that have never been seen before

Data Independence

The above outcomes can only be achieved through a concept of **'data independence'** - a relatively new paradigm in CTI delivery where intelligence providers collect and own 100% of their data.

Owning the data allows for the creation of new attributes and relationships that allow patterns and changes over time to be quickly identified. The trustworthiness and actionability of PTI data is directly proportional to how complementary the data is towards itself and whether it's single-sourced.

Legacy CTI problems	Data Independent PTI solutions	Benefits
Multiple tools required, complexity, and overlap	Streamlined, self-reliant platforms	Better ROI, efficiency
OSINT data and sensor data are time-specific	Real-time detection, proactive response	Early threat prioritization, reduced discovery time
Data arrangement and threat type correlation is hard	Construct searchable threat-specific datasets	Resource efficiency, tailored insights
More data doesn't equal better security operations	Strong data relationships and focused workflows	Less false positives, actionable intelligence
Difficult data provenance, obscure aggregated data	Single-sourced, clear data promotes action	Trust in data, timely information
Decentralized, vague, and inflexible data	Agile first-party data for accurate threat counteraction	Meaningful insights, efficient resource use

Figure 2: Legacy CTI Comparison to PTI Solutions

Indicators of Future Attack (IOFA)

An IOFA is any piece of intelligence data (domain, IP, server, content hash, etc.) that tells a security practitioner where an attack is coming from, as opposed to an IOC, which is an indicator of where an attack has already been.

The concept of an IOFA is central to the ‘‘Preemptive’ in PTI. IOFAs give security teams visibility of attackers as they deploy their infrastructure across the Internet. Security teams can then leverage this knowledge to block emerging threats rather than defend against attacks as they occur.

Adversaries are human and, like all humans, have preferences and patterns of behavior e.g., using the same naming conventions, ASN hosts, nameservers, and attack patterns. An IOFA-led approach uses attacker TTPs against themselves, with SOC teams, threat hunters, and cyber defenders following the pattern of attack and deployment across the global IPv4 and darkweb space.

While IOCs are useful for identifying breaches that have already occurred, they fall short in a landscape where being reactive is synonymous with being too late. IOFAs, on the other hand, are the cybersecurity equivalent of a radar system that detects storms on the horizon long before they make landfall.

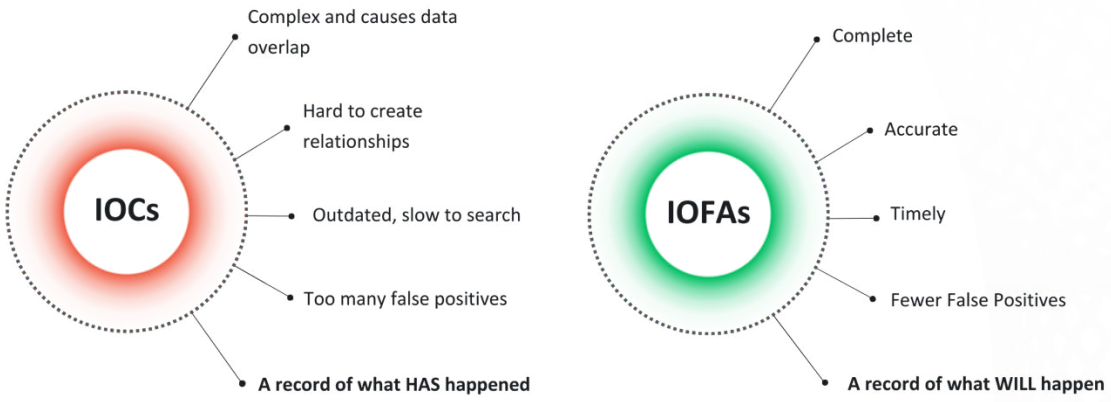

Figure 3: Overview of IOCs and IOFAs

Here are some of the key benefits of adopting an IOFA-led approach:

- **Proactive defense:** By acting on IOFAs, organizations can move from a reactive to a proactive defense posture, implementing protective measures before an attack occurs.
- **Resource optimization:** IOFA allows organizations to allocate security resources more efficiently, focusing efforts where the risk of attack is highest.
- **Resilience enhancement:** Organizations that adapt to IOFA-led security protocols can enhance their resilience against cyber threats, reducing the likelihood and potential impact of successful attacks.
- **Strategic planning:** IOFA informs strategic security planning, allowing for the development of long-term defenses against predicted future attack vectors.

THE SILENT PUSH PLATFORM

Silent Push entered the PTI market in 2023, in response to industry problems its founders experienced while working on CTI products at Mandiant - more specifically, IOCs were reactive and didn't alert security teams to emerging threats.

The Silent Push platform consists of a console and API that collects, aggregates, scores, and outputs PTI data and risk scores with a wholly data-independent scanning and collection engine.

Silent Push's innovative approach to threat data collection and delivery includes several key approaches:

- **Data Fusion:** Silent Push integrates data from a range of diverse sources to form a coherent picture of the global threat landscape, aggregating threat intelligence into a single, searchable, actionable framework.
- **Behavioral Analytics:** Silent Push utilizes advanced behavioral analytics to detect similarities in adversary behavior, including infrastructure deployment, attack vectors and naming conventions.
- **Infrastructure Traversals:** Silent Push gives security teams the ability to traverse attacker infrastructure, allowing for the identification and neutralization of associated threats before they become a problem.
- **Risk Scoring:** Silent Push outputs headline risk scores per domain and IP in a way that provides security teams with all the information required to make an informed decision on risk.
- **Machine Learning Models:** Silent Push's data models continuously learn from new data, refining predictions to become more accurate over time.

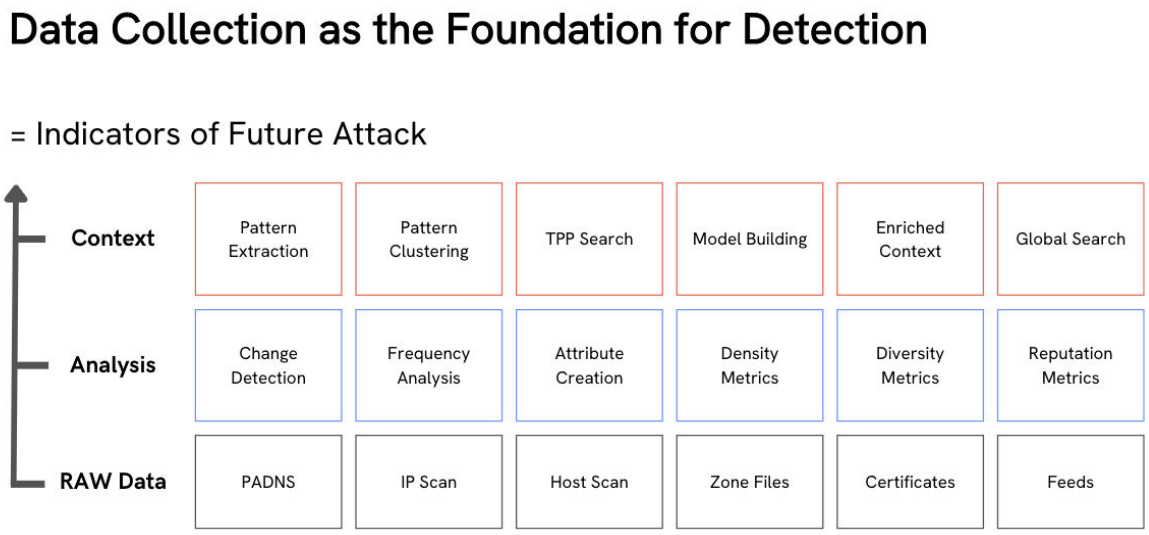

Figure 4: Data Collection as the Foundation for Detection

Differentiators

The first-party database that Silent Push uses to deliver threat intelligence solutions covers the entire IPv4 range and is purposefully structured to facilitate rapid searches within self-contained intelligence spaces, specific to each attack vector.

Silent Push's commitment to data independence allows teams to track attacker infrastructure across the Internet and create behavioral fingerprints of adversary activity that can be refined, modified, shared, and tracked from campaign to campaign.

Complete data ownership enhances the accuracy and relevance of intelligence datasets and ensures that outcomes are achieved across the full spectrum of CTI workflows and job roles.

This singular commitment to outcome-focused detection establishes Silent Push as a leader in the cyber threat detection and prevention space, offering a level of insight and control that is truly unique within the burgeoning industry.

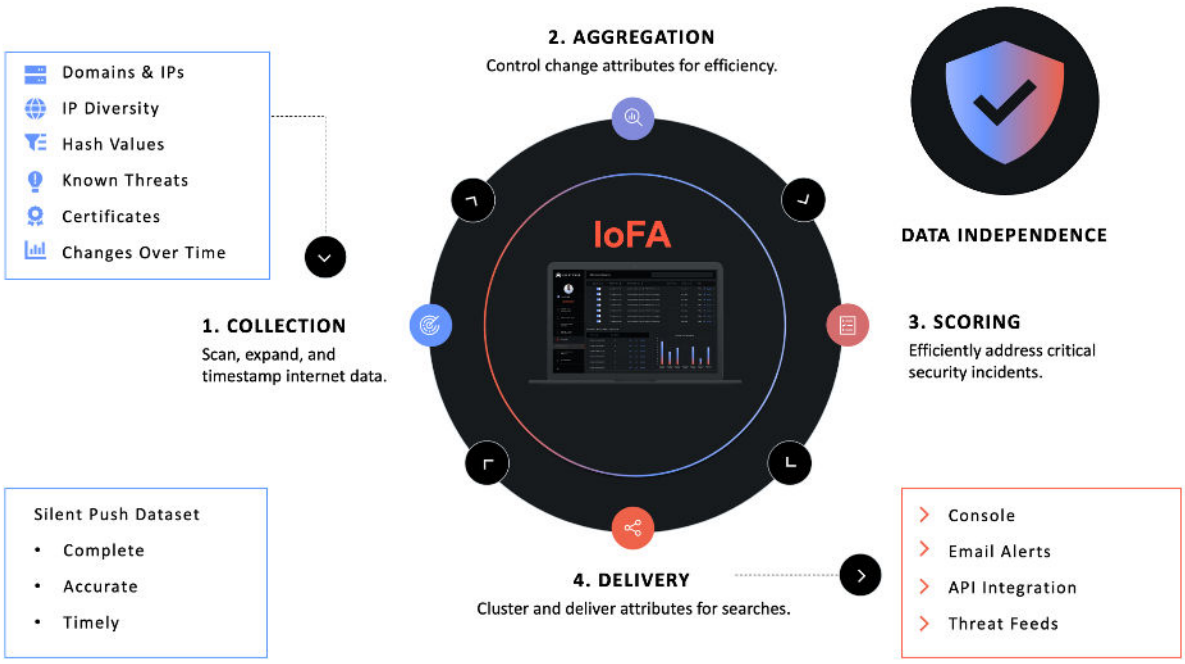

Figure 5: Silent Push Platform

The Silent Push Approach

- **Data Enrichment:** Silent Push adds context to each IP and domain it scans across 90+ categories, enriching observable data with a wealth of information.
- **Early Detection Feeds:** Silent Push provides Early Detection Feeds that monitor threat activity in a global early warning system. This includes real-time notification of changes within the global IPv4 space, tracking of Command and Control (C2) infrastructure, and Advanced Persistent Threat (APT) activity.
- **Reputation Scoring:** The platform evaluates risk with reputational scoring, which likely includes detailed insights into the credibility and history of domains, IPs, and URLs. This scoring system can aid in prioritizing threats based on their potential impact.
- **Integration of Multiple Data Sources:** Silent Push integrates various data points, such as passive DNS data, HTML content, and certificate values. The comprehensive integration of data sources may offer a more holistic view of potential cyber threats.

- **Predictive Approach:** The emphasis on predictive threat hunting and protection against impersonation campaigns before they are deployed indicates a forward-looking stance in cybersecurity defense.
- **Tailored solutions:** Silent Push caters to a wide range of industries with specific cybersecurity needs, which could mean that their platform is highly adaptable to different sectors and use cases.
- **Real-time monitoring:** With real-time notifications of changes in the global IPv4 space and monitoring of daily changes to an organization's public DNS presence, Silent Push provides timely updates that can be critical for rapid response to threats.
- **Community Edition:** Offering a Community Edition at no cost not only provides value to security researchers but also fosters a community around their platform, which can lead to shared knowledge and collective improvement in threat detection and response.

CONCLUSION

In the face of a rapidly evolving cyber threat landscape, the need for PTI delivering IOFA-focused intelligence has never been more urgent. Silent Push stands at the forefront of this market evolution, offering solutions that transform the way organizations defend against unknown and emerging threats.

As cyber adversaries continuously refine their tactics, the cybersecurity community must not only keep pace but also stay one step ahead. By harnessing the power of complete, accurate, and timely data, Silent Push allows organizations to anticipate and stop emerging and unknown cyber-attacks with unprecedented precision.

The future of cybersecurity is inherently bound to the innovation and adaptation of threat intelligence strategies. Silent Push is not just participating in this future; it is actively shaping it by pushing the boundaries of what is possible in cyber defense.

Preemptive threat intelligence delivering Indicators of Future Attack is essential in today's digital threat environment. Silent Push's leadership in the market is evident through their complete focus on evolving the current threat intelligence marketplace towards PTI and IOFA, exemplified by its motto **“We Know First.”**

ABOUT THE AUTHOR

Brad LaPorte is a cybersecurity industry expert and a former top-rated Gartner Research cybersecurity analyst. He was the lead analyst for Threat Intelligence at Gartner and was credited with creating five market categories during his tenure there, including Digital Risk Protection and Attack Surface Management. He has held senior positions in US Cyber Intelligence, Dell, and IBM, as well as in several startups. Brad has spent most of his career on the frontlines fighting cybercriminals and advising C-level executives and thought leaders on how to be as efficient and effective as possible. He is an advisor with Lionfish Tech Advisors, helping cybersecurity and tech companies grow their go-to-market strategies.

ABOUT LIONFISH TECH ADVISORS

Lionfish Tech Advisors offers advice to help businesses with their digital enterprise and IT initiatives. They work with enterprise and finance leaders, CIOs, CxOs, and technology organizations to give practical and strategic advice that can help modernize and transform their businesses.

Their advice is aimed at helping businesses understand and meet the changing demands of their customers. Lionfish Tech Advisors uses proven methodologies and industry best practices to help businesses overcome complex challenges and make decisive actions with confidence. Their analysts have decades of extensive experience working with a range of global and industry-leading clients.

Lionfish Tech Advisors takes an unbiased approach and connects with subscribers on a deep level.

Lionfish Tech Advisors Report: Anticipating the Unseen: Elevating Cyber Defense with Silent Push Preemptive Threat Intelligence is for buyers considering their purchasing options in a technology marketplace and is based on our analysis and opinion.