ThreatWatch for Continuous Threat Intelligence

ThreatWatch makes you hard to hurt.

Continuous threat intelligence that surfaces hostile signals while they are still signals. Read by analysts, not shipped as alerts, and measured in how early you knew.

EVERY FINDING READ BY AN ANALYST	COLLECTION INSTRUMENTED FOR YOU	INVESTIGATION HOURS INCLUDED	REPORTED AS A COMMAND BRIEF

Standing collection and analysis of hostile signals around a named person or organization: what is being said, by whom, and whether attention is turning into intent. Collection is scoped to you, your aliases and your household. Every finding is read by an analyst before it is sent, and what arrives states the finding, the confidence, and the recommended response.

If the deliverable were a feed you had to monitor yourself, you would have bought the wrong thing.

THE METHOD

MONITOR WHAT REMAINS

01 Discover	02 Reduce	03 Monitor	04 Investigate	05 Advise

ThreatWatch delivers stage 03 of the ObscureIQ method, with investigation hours included. The watch starts from the Exposure Discovery audit, which shows what is worth watching. Discovery and reduction are delivered through Obscurity DEP.

Monitor MONITOR WHAT REMAINS

ThreatWatch continuously monitors the information and activity that cannot be removed. It tracks meaningful changes in exposure, hostile online activity, public narratives, impersonation, threats, and other signals that may indicate growing risk. It is not designed to produce the most alerts. It is designed to surface the changes that matter.

CADENCE	REVIEW	DELIVERED AS
Continuous	100% analyst	Command Brief

Built to be read NOT TO ALERT

01 **An analyst clears every finding first.** Nothing reaches you that an analyst has not read.

02 **Collection is instrumented for you.** Built against your filings, your properties, your household, and the places your information actually circulates.

03 **We watch threat formation, not only triggers.** Escalation is caught while it is still talk, before it turns to logistics.

04 **Investigation is included, not upsold.** When something moves, the same team investigates it under a private investigator license.

WHAT IT WATCHES

SCOPED TO YOU, YOUR ALIASES, YOUR HOUSEHOLD

Social and alternative platforms

Accounts, mentions, and the communities where hostility toward you would form first.

Forums, paste sites, anonymous boards

The places identifying details surface before they move anywhere else.

Deep and dark web

Breach corpora and stealer data, read for your exposure rather than scanned for volume.

Names, aliases, addresses, phones

Exposure tracking on every identifier that resolves to you or your household.

Narrative and impersonation

The story before it carries your name: the grievance forming, the framing being tested, the fake account created.

Organizational footprint

The company, the board, the staff: the surfaces an adversary routes through to reach you.

COMPONENTS AND ADD-ONS

The watch and its instruments

CORE

ThreatWatch core

Continuous analyst-read monitoring

Scanning the digital oceans constantly for your personal data and for anything pointed at you. The standing coverage, delivered as monthly structured reporting plus immediate escalation when something warrants it.

COMPONENT

Named-actor watch

Standing watch on identified actors

Once an investigation names them, they stay under observation, and the record is kept in a form counsel and law enforcement can use.

COMPONENT

Event Monitoring

Raised posture around a moment

A public appearance, a filing, a launch, a verdict. Coverage concentrates around the date, the event name, the venue and location, and the people and organizations attached to it, then stands down after.

ADD-ON PROGRAM — IN BETA

The subscription already takes a first pass at the narratives forming near your name. NarrativeWatch is that work done properly, bought on top of the watch rather than inside it.

NarrativeWatch BETA

What is developing around you, and who is driving it

The base watch tells you a narrative is forming near your name. NarrativeWatch traces where it came from, who is shaping and amplifying it, and how it spreads, mutates and converges with the stories around it.

It also reads the narratives that do not name you yet: your industry, your affiliations, your interests, the forces shaping where you operate. Connected to your exposure, they show what is coming before it becomes personal, opportunities as well as threats. At that point the work is strategic as much as protective: advice about a position, before events force one.

Drivers	Who is driving it, and any sign of coordinated or inauthentic activity.
Trajectory	How it spreads and mutates, what it merges with, and where it goes next.
Adjacent ground	Stories in your industry and affiliations that have not reached you yet.
Position	What to say, what to leave alone, and when.

WHERE IT SITS — PART OF DIGITAL EXECUTIVE PROTECTION

BEFORE THE WATCH

Obscurity DEP

Where every engagement starts

The Exposure Discovery audit maps what can be found and shows what is worth watching. Exposure Reduction takes away what can be removed.

THIS PROGRAM

ThreatWatch

What cannot be removed

Continuous threat and narrative intelligence on what remains, read by analysts, with investigation hours included.

WHEN SOMETHING MOVES

Groundtruth

Who is behind it

Investigation and attribution under a private investigator license, to a standard counsel can file on.

Paired with Obscurity DEP, ThreatWatch is Integrated Protection: one named analyst across both.

HOW IT STARTS — THE FIRST SIXTY DAYS

PHASE 01

Instrument

Collection built against your identifiers, aliases, household, properties and filings, starting from the Exposure Discovery map rather than from zero.

PHASE 02

Baseline

The first weeks establish what ordinary attention to you looks like, so change is visible as change.

PHASE 03

The watch

Continuous collection, analyst review of every finding, monthly reporting, and immediate escalation. The watch holds until you stand it down.

THE DELIVERABLE

What reaches you is a judgment

Monthly structured reporting, and between reports, alerts only when an analyst decides you need one. Every finding states what changed, how confident we are, and what deserves consideration.

SPECIMEN · ANALYST ALERT

Classification	Escalation, assessed credible
Finding	Account activity shifted from commentary to logistics
Corroboration	Coordination confirmed across two platforms
Lead time	Client notified with time to act

Format of an analyst alert. Illustrative, not a client matter. Confidence is stated, not implied.

SPECIMEN · MONTHLY REPORT

Exposure	What changed on your surface: new records, resurfaced listings, removals confirmed.
Hostility	The read on attention pointed at you, and whether it moved.
Narrative	Stories forming near your name, and their specificity.
Actions	Requests and referrals made on your behalf, and what they returned.
Recommended	What deserves consideration next, with confidence stated.

Five questions, answered in order, every month. Between reports, silence means the analysts read everything and none of it warranted your attention.

PLATFORM COVERAGE

A SMALL SAMPLE OF OUR BROADER COVERAGE

MAINSTREAM SOCIAL	Facebook, X (Twitter), Instagram, Threads, LinkedIn, Reddit, TikTok
ALTERNATIVE PLATFORMS	Gab, Truth Social, Rumble, VKontakte, Bluesky, Mastodon
VIDEO AND STREAMING	YouTube, Twitch, Vimeo, Dailymotion
MESSAGING (OSINT-ACCESSIBLE)	Telegram, Discord
FORUMS AND ANONYMOUS BOARDS	4chan, 8kun, independent forums, chan boards
BLOGS AND NEWS	Global news sources, blogs, open web publications

Coverage varies based on source accessibility, platform conditions, and applicable legal and ethical constraints. All monitoring is limited to publicly accessible and OSINT-available sources.

ObscureIQ

Know when attention turns toward you.

obscureiq.com/contact 855.763.7273 info@obscureiq.com Signal on request

Conversations are private and off-the-record by default.