ONTIC

GUIDE

Turning Social, Fringe, and Dark Web Signals into Actionable Intelligence

Table of Contents

Introduction

Today's physical threats don't begin at the front gate — they're born and accelerated in the digital world. Online spaces have become breeding grounds for real-world violence, where ideological divides are deepening and fringe rhetoric spreads faster than ever. As these platforms grow more volatile, the early signals of danger often emerge long before an incident occurs.

Unfortunately, many corporate security teams are still stuck in a reactive model, forced to sift through massive volumes of online noise only after a threat surfaces. Executives, facilities, and employees frequently become the focal points of aggression online, but by the time the warning signs are recognized, it's often too late to prevent escalation.

To shift from reactive to proactive, corporate intelligence teams need more than manual monitoring or isolated alerts. It requires a Connected Intelligence approach: one that combines a clear understanding of threat signals, integrated data across social media, public records, and other key sources, and a coordinated response model that turns insight into action.

This guide will walk you through how to do exactly that — helping you stay ahead of fast-moving online threats, tie digital chatter to physical risk, and take decisive action before those threats materialize.

The Social Media Threat Continuum

Social media has dramatically reshaped the threat landscape. It has become not only a space for grievance expression but also a primary driver of radicalization and organization. As broadcast and print media lose dominance, social platforms have become the go-to source for news and narrative, many of which use algorithms to amplify messages.

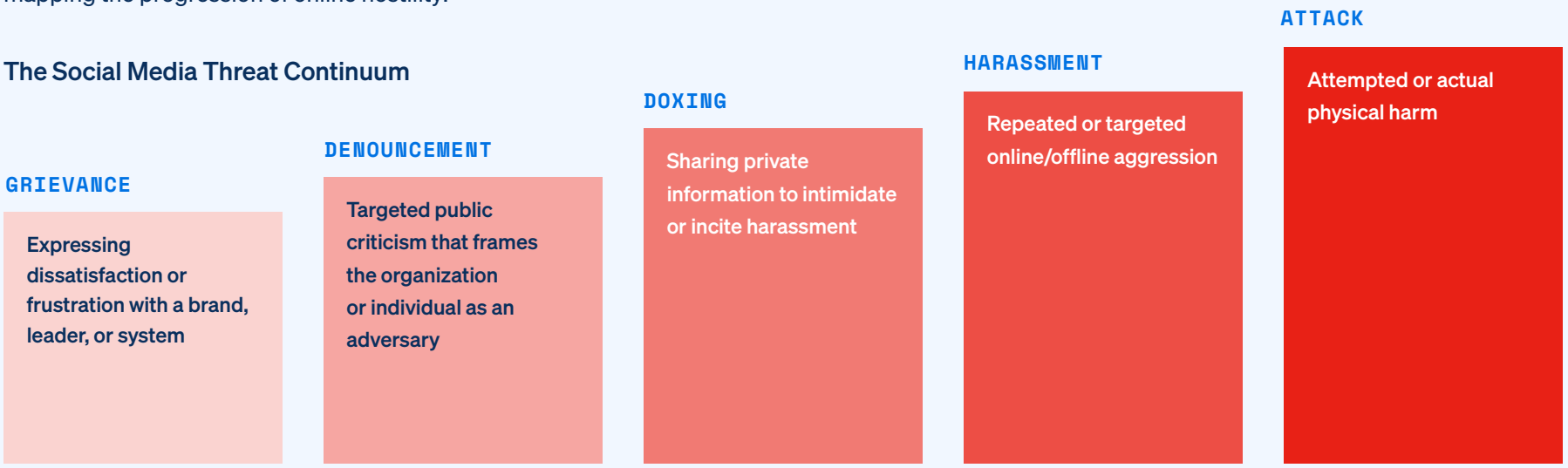
Extremist individuals and groups can now operate as their own media outlets, bypassing traditional gatekeepers and reaching massive audiences in real time. In many cases, encryption adds another layer of complexity, limiting the ability of law enforcement or corporate security teams to detect concerning conversations before they escalate.

Understanding how this environment fuels threat progression is essential. Much like with The Pathway to Violence, violent acts that originate on social media often follow a pattern of escalation. TorchStone Global's Social Media Threat Continuum provides a helpful lens for this analysis, mapping the progression of online hostility:

Keep in mind: The Social Media Threat Continuum is laid out in terms of increasing severity, but in reality, incidents don't always unfold in a straight line. Someone might jump from expressing a grievance straight into harassment or even violence, while others may never move beyond venting. And it's not always just one person driving action — different people with similar grievances might each take on different roles, like an influencer calling out a target, someone else doing the doxing, and another planning more direct action.

Because of this, it's more helpful to think of the continuum as a flexible guide rather than a strict step-by-step process. Even if behaviors don't follow a clear path, having a sense of the different stages can help you understand what's happening, spot signs of escalation, and respond more effectively.

The Social Media Threat Continuum



Source: TorchStone Global

Deepening your understanding of threat signals

Understanding how threats escalate on social media helps, but recognizing threatening behavior online still isn't always straightforward. Threats rarely appear as clear statements of intent — instead, they often start as offhand remarks, vague frustrations, or subtle cues that only become meaningful in a broader context. A threat actor might sound like just another angry customer at first, but with the right indicators, your team can catch early warning signs and step in before things escalate.

> Threats rarely appear as clear statements of intent — instead, they often start as offhand remarks, vague frustrations, or subtle cues that only become meaningful in a broader context.

Use the lists on the next page to identify the early warning signs that may otherwise blend into the digital noise, especially when a threat actor is still in the early stages of expressing grievance or shifting toward more targeted hostility. These indicators often appear subtle at first, but when contextualized with known threat actors or patterns, they can reveal actionable threats.

BOLO: Online indicators of risk

If you notice these, refer to your threat response standard operating procedure (see page 11) to determine the appropriate next steps.

Discontent and public displays of anger

- Broad industry hostility, like "The whole insurance system is corrupt and deserves to be burned down."
- Ambiguous or veiled threats, like “Someone’s going to pay for this soon.”
- Naming specific individuals or leadership, like “CEO John Smith is an awful person.”
- Personal anecdotes paired with outrage, like "After what they did to my claim, I won’t forget this."
- Pattern of repetitive complaints over time, like multiple posts over weeks indicating building frustration or obsession
- Appeals for group validation, like “Anyone else feel like [company] is getting away with something?”

Radicalization and ideological signals

- Use of extremist symbols or slogans
- Affiliation with known hate groups
- Praise for violent acts or individuals, like referencing prior attackers as heroes
- Justifications of violence as necessary or deserved
- Links to or reposts from known extremist channels
- Language that dehumanizes a target or group, like referring to company staff as “parasites,” “traitors,” or other inflammatory terms

Doxing and harassment behavior

- Sharing or requesting sensitive info, like “What’s CEO John Smith’s home address?”
- Publishing photos or screenshots tied to real-world locations
- Repeated tagging, messaging, or following of employees online
- Use of coded or veiled language to hint at offline action, like “They work at 123 Main St... just saying.”
- Attempts to incite others without direct calls to action, like “Wonder how long before someone steps up and handles this.”

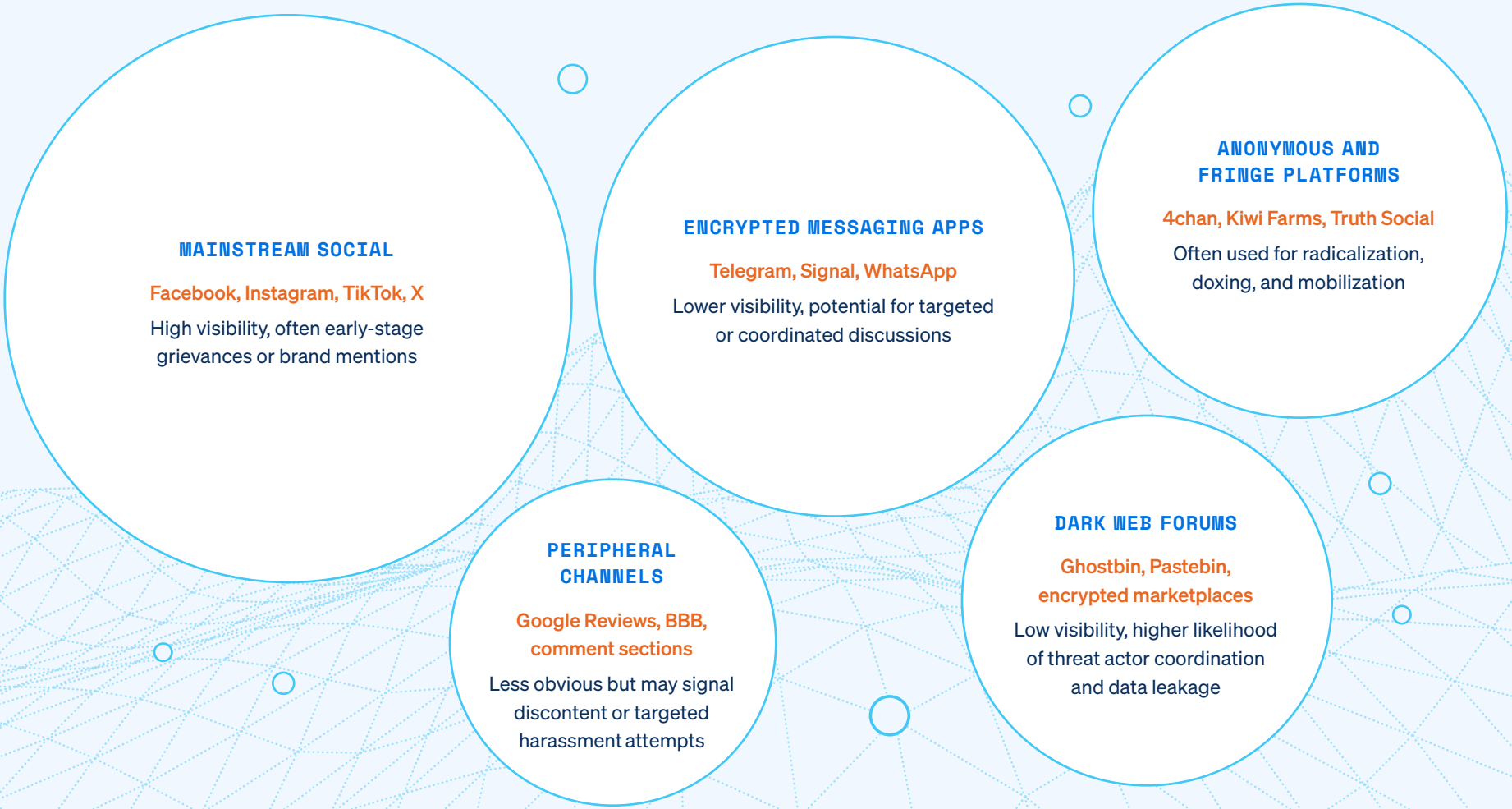
Direct threats and mobilization language

- Statements of intent, like “I’m going to handle this myself.”
- Tactical talk, like “The CEO is going to attend [event title] next week.”
- Calls to action, like “We should all show up to [event title] next week.”
- Sudden spike in urgency or frequency of posts (A burst of activity or tone shift often precedes real-world action.)
- Mentions of weapons or tactical preparation, like “It would be easy to get in through the side entrance.”

Mapping the digital landscape

Understanding how online threats escalate is only part of the equation. It's also important to know where to look. Threats can originate from a range of digital channels, each carrying different levels of visibility, credibility, and risk. By mapping the digital landscape, your team can align monitoring strategies with where threats are most likely to develop and escalate.

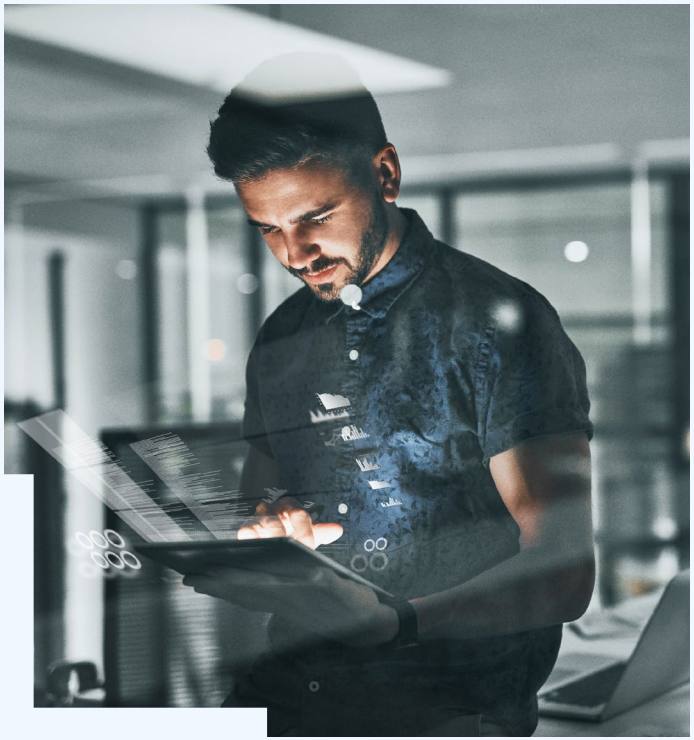
Establishing presence or visibility across this range of platforms enables your team to monitor holistically and respond more effectively, especially when behavior shifts across ecosystems. A centralized platform that consolidates monitoring across these diverse sources can significantly reduce the time and effort required to surface, evaluate, and act on critical signals — helping you focus less on chasing data and more on protecting people.



Building a smarter threat defense with continuous monitoring

Threats that originate on social media or other digital platforms can escalate rapidly — sometimes evolving from a single hostile post to a real-world incident within hours. Relying on periodic reviews or manual monitoring is no longer sufficient. You need continuous, around-the-clock monitoring to detect early indicators of threatening behavior and respond swiftly and intelligently.

However, establishing a monitoring program that truly delivers requires more than just setting up alerts. It demands a thoughtful strategy, high-quality data, and a streamlined process for surfacing the most relevant signals.



Core elements of a strong continuous monitoring program

1. **Clear objectives:** Start by defining what you're protecting — whether it's people, assets, data, or brand reputation. Then identify the language and other signals that could indicate a threat to those principals.
2. **Defined monitoring parameters:** Work closely with legal and compliance teams to determine which data sources and signals are appropriate and lawful to monitor. Common examples include public records of arrests, adverse media coverage, or access control violations.
3. **Strong OSINT topics:** Focused OSINT topics help filter out noise and surface the most relevant signals. Crafting effective topics starts with using well-structured Boolean searches, tailoring your queries by platform (what you monitor on X may differ from Truth Social), and localizing your intelligence efforts.

   For more guidance on building effective OSINT topics — and overcoming the fear of missing critical information — check out How to Beat Your Fear of Missing Key OSINT Information.
4. **Real-time, actionable alerts:** Ensure that alerts reach the right team members at the right moment. Design workflows that enable quick, informed decision-making and rapid response when threat indicators emerge.

Getting the full picture

Once a threat is identified, understanding its severity requires a complete picture of the individual or group behind it. What may appear to be a harmless online rant from a disgruntled customer could, in reality, come from someone with a history of violent behavior, prior interactions with your organization, or physical proximity to an executive location. Without this broader context, threats can be underestimated, delayed in response, or overlooked entirely.

Threat hydration is the process of gathering and connecting these critical data points to assess intent, capability, and urgency. When done effectively, it shifts your approach from reactive monitoring to proactive mitigation. Use the workflow at right to ensure a comprehensive and consistent threat hydration process that helps you act confidently and quickly.

Threat hydration checklist

01

FLAG AND LOG THE SIGNAL

- ☐ Capture the threat, post, or behavior across digital platforms
- ☐ Note the source, platform, and level of visibility

02

DETERMINE PROXIMITY AND PHYSICAL RISK

- ☐ Does the post include a specific person, location, or timeframe?
- ☐ Does it reflect movement along the Social Media Threat Continuum?

03

REVIEW HISTORICAL BEHAVIOR AND CONNECTIONS

- ☐ Examine prior posts and engagement history
- ☐ Identify any ideological patterns, grievances, or repeat targeting

04

VERIFY IDENTITY AND ONLINE FOOTPRINT

- ☐ Use OSINT tools to match usernames to real identities
- ☐ Conduct reverse image searches and cross-platform scans

05

DETERMINE PROXIMITY AND PHYSICAL RISK

- ☐ Check for location mentions, tagged places, or known addresses
- ☐ Leverage internal systems (like access logs or LPRs) to track movement

06

ASSIGN THREAT LEVEL AND RECOMMEND ACTION

- ☐ Use your SOP escalation tiers to determine next steps
- ☐ Document findings and circulate to relevant teams

Building trust across teams

Even when thoroughly researched with external data, a threat signal in isolation rarely tells the full story. To see the complete picture and respond with the right level of urgency, you need input from those who may hold critical context. HR may know of recent disciplinary actions. Legal may be aware of ongoing disputes. Marketing might have encountered the same individual through online brand channels. Without these perspectives, you risk overlooking important data points that can change the nature or severity of a threat.

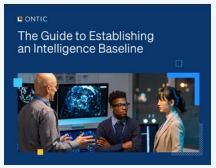
Effective threat intelligence hinges on collaboration. Working with internal teams (HR, Legal, Comms, IT) and external partners (law enforcement, security vendors) ensures your assessments are informed, your responses are aligned, and your actions are rooted in a 360-degree view of the risk landscape.

Real-world scenario

A former employee who was recently terminated begins posting vague threats on Facebook, saying, “They’re going to regret how they treated me.” HR recalls the individual was confrontational during their exit interview. Additional research reveals they also commented on a Reddit thread about insider access and tagged a coworker in a now-deleted Instagram post. With this context, the team elevates the threat, initiates monitoring protocols, and loops in legal and executive protection.

How to collaborate more effectively across functions:

- **Use shared incident intake workflows:** Create a centralized incident intake system where employees across departments can flag concerning behavior or digital interactions. Route submissions to the appropriate team based on content.
- **Designate internal liaisons:** Assign point people from HR, Legal, and IT to participate in threat review or debriefs. This helps streamline communication and reduces the risk of critical information getting stuck in silos.
- **Schedule recurring syncs:** Host monthly or quarterly threat intelligence briefings where key departments can review emerging risks, open cases, and process gaps.
- **Establish access-based permissions in shared platforms:** Use software that allows multiple teams to collaborate within the same platform while protecting sensitive information through role-based access controls. This ensures legal or HR-only data stays restricted, while still enabling security and investigations teams to see what’s relevant.
- **Educate beyond your team:** Provide brief threat awareness training to client-facing or frontline roles (like customer service, recruiting) so they know what to flag and how.



For more details on establishing baseline intelligence on a threat actor, read The Guide to Establishing an Intelligence Baseline.

Operationalizing escalation

Intelligence is only valuable if you know what to do with it. You can excel at gathering signals, investigating behaviors, and identifying credible threats — but without a structured plan for what happens next, even the best analysis can stall. When threats escalate, your team needs to be aligned on what to do next.

An effective response requires a clear, documented escalation structure. Standard operating procedures (SOPs) ensure everyone knows their role and response protocols at each stage of a threat.

Core SOP elements for responding to escalating threats

- Defined escalation thresholds (based on severity + confidence)
- Assigned roles and chain of command
- Integrated communication flow between Physical Security, Legal, HR, and Cyber or IT
- Action templates for security escalation and law enforcement coordination

Sample threat response framework

The threat response framework below provides an example of how your defined escalation thresholds might be structured, along with suggested high-level actions. Your specific response templates may include more detailed steps, depending on your existing protocols and the roles you've assigned within your team.

Level	Indicator	Action
1. Monitor	Vague grievances, industry complaints, no threat actor	Log and monitor for shifts or patterns
2. Investigate	Brand or staff named, veiled threats, doxing signals	Begin additional research, notify cross-functional security liaisons, check for prior alerts
3. Escalate	Known threat actor, physical reference, ideological support	Alert GSOC, coordinate internal stakeholders, prep response options
4. Respond	Direct threats, imminent risk, confirmed presence	Activate protection protocols, notify LE, restrict access

TIP: Customize these tiers to reflect your risk tolerance, industry context, and available resources.

Investing in the right technology platform

Even with strong workflows and clear escalation procedures, your threat intelligence program is only as effective as the systems it runs on. Many security teams already have access to the intelligence they need, but when that information is siloed across spreadsheets, email threads, internal systems, and disconnected third-party sources, it becomes nearly impossible to see the full picture and act quickly.

A Connected Intelligence platform brings together digital signals, physical data, and internal insights in one unified view. By eliminating the need to chase down context manually, your team can see the full picture of a threat faster. With this clarity, you can respond with confidence — addressing potential risks before they escalate and keeping people and operations safe.

Preparing for what's next

Online threats will only grow more complex — faster-moving, harder to trace, and increasingly sophisticated. Simply having access to intelligence isn't enough. The real advantage comes from knowing what signals matter, how to interpret them, and how to respond quickly.

Whether it's spotting vague threats on fringe platforms or activating real-time response protocols, the strength of a modern threat intelligence program lies in its ability to cut through the noise, focus on what's real, and take coordinated, decisive action.

Tie tech investments to business metrics

When advocating for a modern security platform, link security performance to the organization's broader priorities:

- **Cost savings:** Faster threat resolution minimizes productivity losses, reputational damage, and lawsuits — directly impacting the bottom line.
- **Risk reduction:** Proactive intelligence monitoring prevents incidents before they create risk to the business.
- **Resilience:** Faster threat response minimizes operational disruption and strengthens business continuity.
- **Operational efficiency:** Streamlined workflows reduce response time and free analysts to focus on high-priority threats.

Framing security upgrades as risk reduction and business enablers increases executive buy-in and long-term support.

For more guidance on demonstrating the ROI of security investments, download The Security ROI Cheat Sheet.

Stay ahead of the next threat with Ontic

Modern threats move fast. Your team needs to move faster.

With Ontic's Integrated Research and Risk Intelligence solutions, you can centralize risk signals, research threats more efficiently, and connect digital and physical activity before incidents escalate.

Here's how Ontic helps security teams go from signal to action:

Monitor smarter

Surface threat signals from across social, fringe, and dark web channels — all within one connected platform.

Research with speed

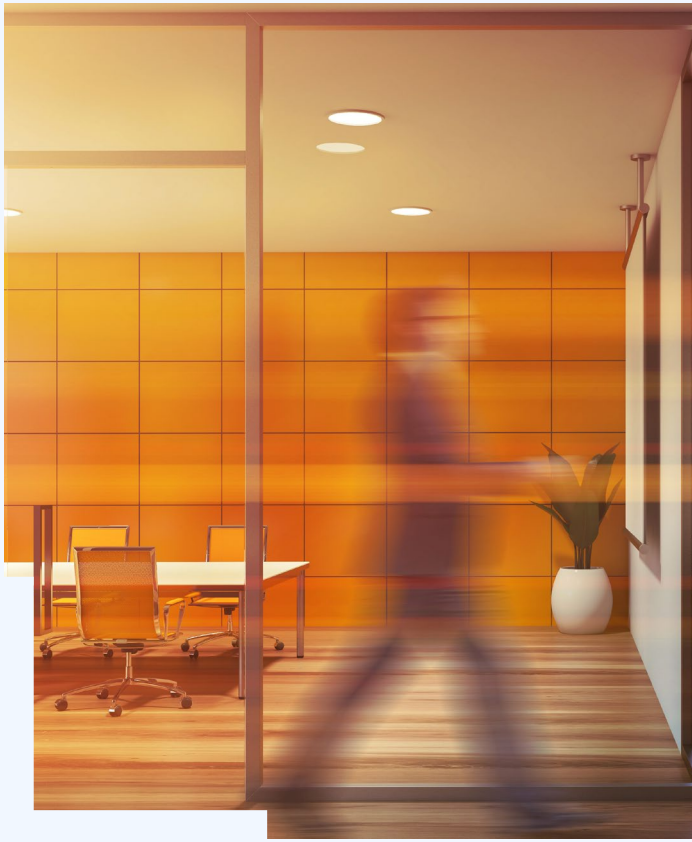
Combine OSINT, internal records, and investigative workflows in a single workspace.

Act confidently

Align cross-functional teams with permissioned access, audit trails, and embedded SOPs.

See the full picture

Access information on protected people and assets, threat actors, incidents, and vulnerabilities within a centralized database.



ONTIC

Ready to elevate your threat intelligence program?

Discover how Ontic can help your team protect what matters most.

Request Demo