ONTIC

GUIDE

How to Build a Modern Protective Intelligence Program

Table of Contents

Why protective intelligence matters

Great corporate security teams today go beyond response protocols and perimeter defense to identify and mitigate threats before they materialize. Protective intelligence (PI) is the strategic discipline that makes this possible.

At its core, PI is an investigative and analytical process used to proactively identify, assess, and mitigate threats to people, property, and brand reputation. It enables organizations to shift from reactive responses to a forward-looking security posture — one that supports business continuity, protects human capital, and builds resilience against emerging threats.

Rather than operating in a silo, protective intelligence is a critical capability within the broader corporate security department. It touches nearly every subprogram: from executive protection and event security to insider risk and workplace violence prevention. And when integrated properly, PI enables seamless collaboration across legal, HR, cybersecurity, business continuity, and global operations teams.

A mature protective intelligence program helps security leaders:

- **Understand** the types of threats the organization is exposed to
- **Assess** the risks those threats pose to the organization
- **Proactively identify** persons of interest (POIs) and concerning behaviors
- **Track and analyze** threats in real-time using technology and human intelligence
- **Communicate risk** effectively to stakeholders
- **Align** security investments with the threats that pose the highest risk

This guide outlines a step-by-step process for designing, launching, and optimizing a protective intelligence program, drawing from industry best practices and real-world operational templates.

The role of protective intelligence within corporate security

Depending on the organization's size and structure, PI may be a dedicated function or embedded within other teams. Either way, its value grows when treated as a strategic asset within security.

PI acts as a vital link across corporate security, ensuring threats are identified early and routed to the right stakeholders. When integrated effectively, it provides a centralized view of threat data — connecting digital signals, threat actor behavior, and situational context to enable faster, more informed decision-making.

Rather than working in isolation, PI intersects with executive protection, investigations, and GSOC teams, helping break down silos. This collaboration shifts security from reactive responses to a shared, proactive understanding of risks and escalation potential.

"Protective Intelligence isn't just about spotting threats; it connects the dots across global security. By turning isolated signals into a clear picture of risk, PI helps executive protection, investigations, and GSOC teams move from reacting to anticipating — making security a strategic advantage."

Fred Burton
Executive Director of Protective Intellingence
Ontic

PI in action

PI can support executive protection by providing pre-travel risk assessments that flag online sentiment or planned protests, allowing EP leaders to anticipate and prepare for threats. Similarly, PI might identify concerning employee behaviors before they escalate into workplace violence, enhancing overall safety.

Understanding PI's place within a corporate security team

A PI team's exact placement will vary depending on your organization's structure, size, and focus.

Here are the most common placements for PI teams within an enterprise security organizational chart:

Within corporate security

+ Advantages

Close collaboration with EP, investigations

✓ Considerations

Direct operational security impact

Within risk management or enterprise risk

+ Advantages

Enterprise-wide risk perspective

✓ Considerations

Strategic in nature

Standalone intelligence/ threat management unit

+ Advantages

Centralized focus, enterprise-wide coverage

✓ Considerations

Requires strong cross-department partnerships

Next, we'll explore what PI team structures look like across these three models, complete with sample charts to bring each scenario to life.

Within corporate security

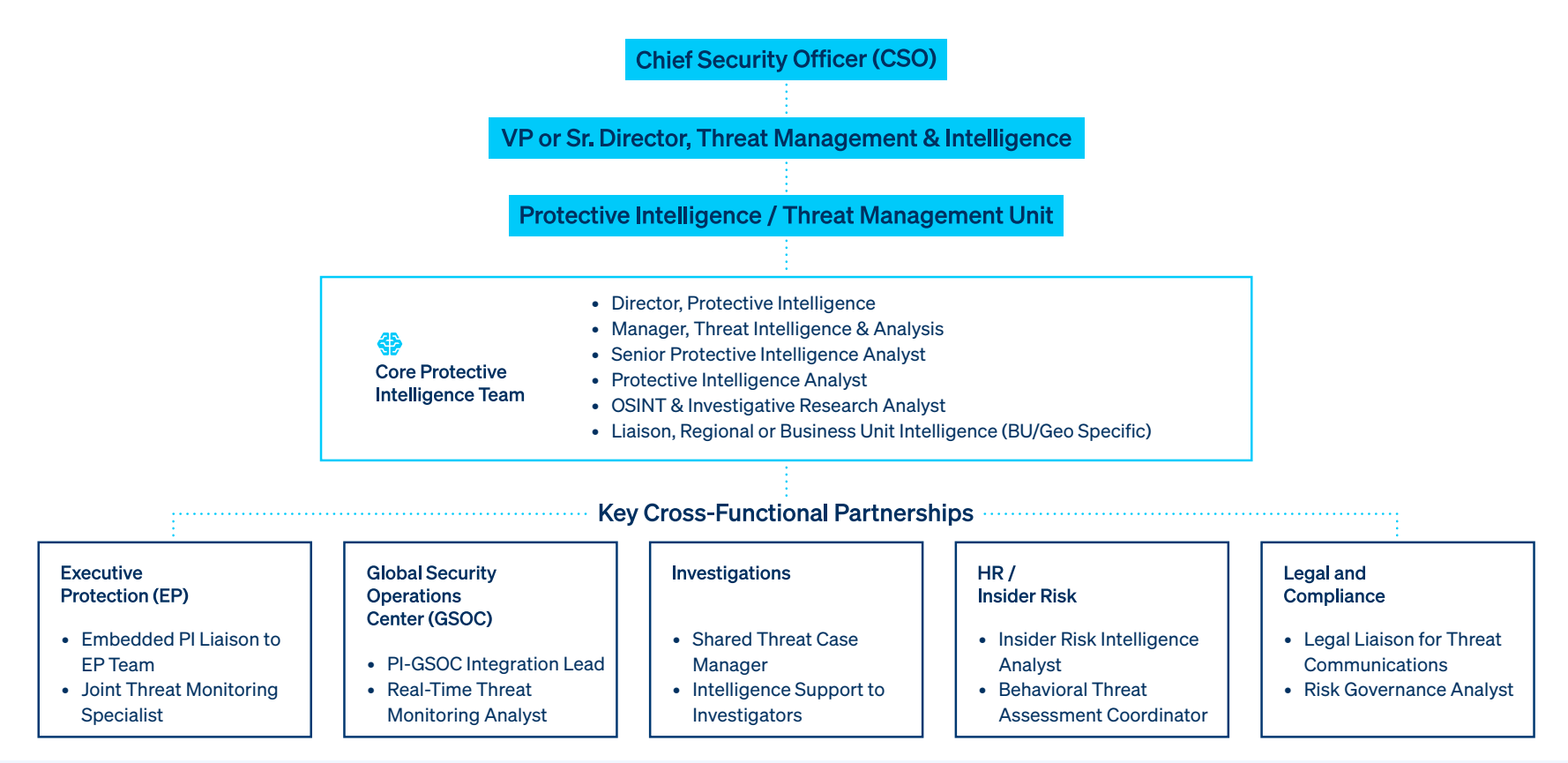
PI is often a subset within corporate security. In this structure, the PI team typically reports up to a Director of Corporate Security (or in some cases, a VP of Corporate Security), reflecting PI's role in providing strategic threat intelligence and risk analysis for the entire enterprise. This placement ensures close coordination with executive protection, workplace violence prevention, insider risk programs, and security operations.

Within risk management or enterprise risk

Some organizations place PI under a broader Enterprise Risk Management or Risk and Compliance function. In this model, PI is aligned closely with other risk disciplines (financial, cyber, compliance), focusing on identifying threats that could impact enterprise risk.

Standalone intelligence or threat management unit

In very large or security-mature enterprises, PI teams may exist as a dedicated intelligence or threat management unit that serves multiple business units. This unit often reports to Corporate Security leadership but has direct partnerships across departments (EP, investigations, GSOC, HR, legal). The team acts as a centralized hub for intelligence collection, analysis, and dissemination.



Before you begin: Questions for consideration

Scaling your program begins with a clear understanding of your baseline.
Use this checklist to assess which elements of your program are already in place.

1 Understand your foundation

Have we clearly identified our primary threats?	☐
Do we understand why these threats matter?	☐
Are there unaddressed vulnerabilities tied to those threats?	☐

2 Evaluate your intelligence detection channels

Do we have a system for detecting, managing, and assessing threats?	☐
Is our threat intelligence process real-time, automated, and always-on?	☐
Is there an accessible way for employees to report concerns?	☐

3 Revisit your processes

Are we tracking how much time is spent on threat detection?	☐
How is research on emerging events shared within our team and cross-functionally?	☐
Do investigations follow a defined workflow?	☐
Are alerting protocols clearly defined?	☐

4 Review your team structure

Do we have a dedicated team focused on threat detection?	☐
Does our team include both cyber and physical security expertise?	☐
How are other departments (HR, Legal, Compliance) involved in security decisions?	☐

Your answers offer a clear snapshot of where your program stands today. With these insights, you're ready to focus on the areas that matter most and move into the next stage of building a comprehensive protective intelligence program.

Establishing your protective intelligence processes

Many PI teams use the Intelligence Cycle as a repeatable framework for turning raw data into actionable insight. But it's just as useful when you're building your program from the ground up.

Below is a quick overview of how the six phases of the Intelligence Cycle can guide your program's development.

Intelligence Cycle phases:

01	**Requirements:** Define intelligence needs and assess threats/vulnerabilities
02	**Planning and Direction:** Align people, processes, and policies to mission goals
03	**Collection:** Gather relevant intelligence (digital, physical, and human)
04	**Processing and Exploitation:** Organize and prepare data for analysis
05	**Analysis and Production:** Evaluate threats and produce usable insights
06	**Dissemination:** Share findings securely and clearly with stakeholders

Read on for deeper guidance on each phase.

Define intelligence needs and assess threats/vulnerabilities

Before building a protective intelligence program, ask yourself, "*Why do we need this?*" Take a close look at what you're protecting and the risks tied to it. This means assessing the threats, vulnerabilities, and the digital footprint of the business and key principals through a formal threat assessment.

You'll want to answer these three questions with confidence:

- ✓ What threats are you facing?
- ✓ Why are the threats important to monitor and mitigate?
- ✓ What vulnerabilities associated with these threats are not being addressed?

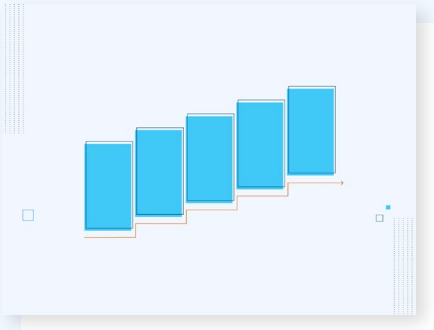
To guide your assessment, categorize threats into clear, actionable buckets — for example:

- Executive-directed threats
- Workplace violence
- Stalking and harassment
- Activist or protest activity
- Insider threats
- Theft or loss of property
- Travel-related risks
- Terrorism or geopolitical unrest

Prioritize each based on severity, likelihood, and proximity to your executives. This helps ensure your team focuses on the risks that matter most.

Next steps

- Assess your assets, threats, and potential risks
- Pinpoint weaknesses in your digital footprint and sensitive areas
- Align your intelligence goals with your broader risk strategy
- Categorize and prioritize threats to focus resources where they matter most



Read "*Understanding the Pathway to Violence*" to learn how to proactively identify behaviors associated with workplace violence, executive threats, and harassment — before they escalate.

Align people, processes, and policies to mission goals

The second core element of a protective intelligence program is how your team collects and manages threat information. This isn't just one system — it's a coordinated set of inputs and processes designed to surface risks early and support informed decision-making.

An effective collection strategy might include:

- **Monitoring open-source intelligence**, such as social media, news, and forums, for early indicators of threats
- **Reviewing public records** to uncover past behavior, legal issues, or affiliations tied to persons of concern
- **Leveraging verified intelligence databases** for timely, vetted threat information
- **Centralizing** how you store, track, and monitor individuals or groups who may pose a risk
- **Analyzing internal communications** or behavior patterns that may signal insider threats
- **Conducting threat assessments** on individuals to determine level of risk and appropriate response
- **Coordinating with law enforcement** and external intel partners to close gaps and validate findings

Together, these inputs form the foundation for a consistent and proactive threat picture — enabling your team to move from reactive to anticipatory.

At this point, it's also key to establish a process for briefing leadership regularly on emerging threats and potential impact to the business.

Next steps

- Collect and coordinate threat data from open sources, internal signals, and external partners
- Centralize and track intelligence to monitor potential risks consistently
- Determine how you'll keep leadership informed to support proactive, informed decisions

Gather relevant intelligence and make it accessible

It's one thing to collect intelligence, but it's of little use if it's not easily accessible and dynamically updated — in the form of a database.

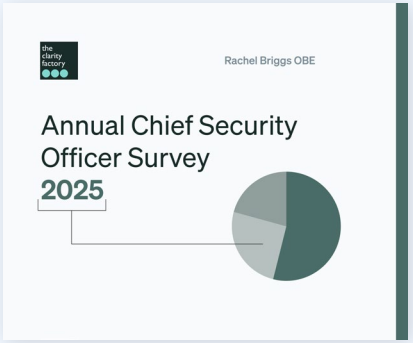
Regardless of the tools used for the threat database, several minimum standards are recommended to make practitioners the most effective:

- **Dynamic database**
  A database must stay dynamic, giving all relevant security team members immediate access to new information.
- **Seamless process for documentation**
  Data should be documented systematically for consistent and efficient tracking.
- **Automation**
  Automate simple tasks to save time and increase efficiency.
- **Security and privacy**
  Access to the database should be strictly controlled and limited to individuals on a need-to-know basis.

Let's not overlook the role of AI. According to The Clarity Factory Annual CSO Survey, 60% of CSOs report actively using AI to support intelligence gathering, threat assessment, and monitoring. AI is rapidly becoming the next frontier in intelligence work — automating routine collection and assessment tasks while freeing up your team to focus on what machines cannot replicate: applying human judgment and expertise to transform intelligence into decisive action.

Next steps

- Centralize intelligence in an accessible location
- Ensure your database is dynamic and documentation is consistent
- Automate low-level monitoring tasks when possible



Download the Report

Download the full report for more CSO insights.

Organize and prepare data for analysis

Once you've built a system for gathering and organizing your research, it's time to analyze. Threat analysis is the most challenging and high-stakes part of protective intelligence. While it leans heavily on intuition, science and the right tools can help you effectively assess potential threats and provide actionable recommendations to decision-makers.

Frameworks like WAVR-21 and the U.S. Secret Service's threat assessment model offer a structured starting point for evaluating threat actors. They help guide key questions: Is the individual progressing through the attack cycle? Do they have the intent and capability to cause harm? What does their past behavior reveal?

But today's threat landscape demands more than manual evaluation. Modern PI programs increasingly rely on technology that can auto-analyze large volumes of data, helping teams reduce noise, identify patterns, and prioritize threats faster.

However, while these tools are essential for scale, they're not perfect. Automation can surface critical signals, but human expertise is still required to interpret context, validate findings, and make sound decisions.

In short, it's important to leverage both structured frameworks and systems that simplify how complex information is organized, reviewed, and acted upon. The right balance of intuition, process, and technology turns raw data into actionable threat insights.

Next steps

- Apply structured frameworks to assess behavior, intent, and threat progression
- Use automation to scale, but always verify with human judgment
- Combine intuition, process, and tools to turn data into actionable insights

Evaluate threats and produce usable insights

This is where you define what you do with the intelligence you've collected. Start by establishing a clear case management process — the framework for handling incidents from investigation through continuous monitoring to resolution. Cases are typically triaged based on priority and addressed using the standard of care set by your leadership. This might include tasks like scheduling employee interviews or conducting external research on threat actors.

If you identify a threat to an executive that requires deeper investigation, use the checklist below as a guide. It provides a clear process to help you gather the insights needed to take the right actions and effectively mitigate the threat.


ONTIC

CHECKLIST

How to Run Thorough Investigations on Threats to Executives

Protecting corporate executives and high net-worth individuals at the office, at home, on-the-go, and online is a top priority for businesses. With the right tools and processes in place, executive protection and close protection teams have anytime, anywhere access to proactively monitor for potential physical threats. This allows them to streamline investigations, take swift action to protect principals, and gain insights to support ongoing protection activities.

Leverage this checklist to ensure you have a comprehensive corporate investigation process in place.

Pre-Incident

Establish comprehensive systems and processes

Ensure teams have the right tools in place to proactively monitor and hunt for threats to executives and establish processes to mitigate threats, take swift and intentional action, and create standardization in an investigation workflow.

Define individuals and locations for protection CEO, board members, executives, critical employees, high value customers or partners, families	☐
Define locations/boundaries for protection, if any handoff required Office buildings, parking lots, travel/private aircraft (FBOs), events, residence, estate, vacation homes, family office	☐
Consolidate connected systems data Vehicle, visitor management systems (VMS), access control, CRM, case management (past and current)	☐
Centralize research and monitoring tools Criminal and civil records, OSINT, social media, dark web, local news reports, localized crime data	☐
Review and update policies to support intervention; define response processes	☐
Define sources of concern Grievances (internal and external), lawsuits, sentiment analysis, business controversy, geo-political conditions, protection orders	☐
Set up notification flows based on threat type or area of responsibility Corporate security, HR, legal, third-party experts, estate protection teams, family office, local law enforcement	☐

Continued on next page

Download the Checklist

How to Run Thorough Investigations on Threats to Executives

However, not all intelligence warrants a formal case. Some insights may be shared as FYIs with stakeholders, or tied to immediate response protocols, communication plans, law enforcement coordination, and crisis management efforts. Regardless of whether intelligence escalates into a full investigation, you'll need well-defined processes for how it's handled and shared.

Success depends on using technology that continuously surfaces new information and enables ongoing threat reassessment. By integrating continuous monitoring into your case management workflow, you can automate time-consuming tasks — like social listening or receiving alerts on POI activity — freeing up time to focus on actionable threats.

Next steps

- Establish processes for investigating or immediately acting on new intelligence
- Monitor for patterns, escalation behaviors, and concerning trends
- Automating these workflows can save you time to focus on work that requires urgent human attention

Share findings securely and clearly with stakeholders

Effectively disseminating intelligence to the right stakeholders is just as important as collecting it. When briefing executives, clarity, relevance, and delivery style can make or break whether your insights drive action. How you share the information is almost as important as what you share.

Keep these best practices in mind:

- **Connect threats to business impact**
  Frame risks in terms of operational disruption, financial exposure, or reputational harm to make them meaningful to leadership.
- **Tailor your delivery**
  Match your briefing style to executive preferences — whether they want a high-level summary or detailed analysis, verbal updates or written briefs.
- **Make it actionable**
  Don't just present the threat — outline possible scenarios and recommended next steps to support timely, confident decisions.
- **Standardize with templates**
  Use consistent, well-designed templates to streamline communication, reduce confusion, and ensure key details aren't missed.

Don't forget to close the loop. Build in regular feedback channels to understand what's landing and what's not. If briefings aren't being read or alerts are ignored, adjust your approach. And always respect privacy: not all intelligence should be widely shared. For sensitive issues — like a private threat to a CEO — ensure access is limited to only those who need to know.

Next steps

- Tailor your delivery to executive preferences and tie threats to business impact
- Offer clear and actionable recommended next steps
- Regularly collect feedback to confirm your briefs are being received and understood

Metrics, tools, and demonstrating impact

With a PI program in place, it's time to show the impact of your work. Reporting plays a key role here. Start by defining your program's goals and identifying the data needed to track progress. Establish a baseline to spot anomalies and make informed, resource-smart decisions. Technology is essential for pinpointing risks quickly and effectively at scale.

Here's how you can highlight your program's success:

Key metrics

To understand the impact of your security program, it's crucial to track activity metrics that highlight your efforts and process effectiveness. Key metrics might include:

- **Risk distribution**
  Threats by executive, location, or business unit
- **Investigation timelines**
  Time taken to close cases or escalate concerns
- **POI volume**
  New profiles or incidents tracked over time
- **Efficiency gains**
  Time saved through automation or technology

While these metrics are valuable to your team, executives may see them as busywork, potentially framing your program as a cost center. To gain their support, focus on translating metrics into measurable business impact.

Demonstrating impact

Download the guide below for a quick-reference cheat sheet on demonstrating the ROI of your PI program.

Download the Guide

Additional PI program considerations

Reporting best practices

When reporting on your program to executive leadership, focus on clarity and relevance to your audience. You live and breathe protective intelligence, but your leadership doesn't. Avoid technical details and lengthy summaries. Instead, use concise visuals like charts and tables to highlight impact. And as noted earlier, always connect your numbers to business outcomes executives care about, such as cost avoidance or risk reduction.

Technology enablement

Great protective intelligence hinges on your ability to quickly gather and analyze data. Leverage solutions that connect intelligence gathering, research, and case management in one place — empowering you to respond faster and with greater confidence. Centralized threat actor management and automated alerting also help ensure you don't miss critical signals and make it easier to collaborate across departments. When your technology supports the full intelligence cycle — from collection to dissemination — you gain better visibility, reduce manual work, and scale your impact across the organization.

Final thoughts

A modern protective intelligence program is no longer a nice-to-have — it's essential for any organization serious about managing risk. By aligning security strategy with proactive intelligence and clear frameworks, your team can:

- ✓ Prevent rather than react to threats
- ✓ Communicate security value to leadership
- ✓ Empower collaboration across departments
- ✓ Strengthen trust with employees and stakeholders

The mission is simple: **make nothing happen** by acting before something does.

Centralized intelligence for a clearer threat picture

Ontic's Risk Intelligence solution enables protective intelligence teams to view complete data from trusted sources through a woven story of otherwise missing threat signals that expose your people, company, and reputation to unnecessary risks.

Ontic brings your intelligence together in one place with these powerful data sources, assessments, and workflow capabilities:

OSINT

Continuously monitor 10,000+ open sources (social media, blogs, dark web, fringe forums, and more.), using keyword-based topics tuned to your people, assets, or events.

Location-based intel

Track both global and local threats — from geopolitics, protests, natural disasters to local incidents — mapped to your facilities, teams, and assets.

Response workflow integration

Link threat signals to incidents, investigations, and case management. Coordinate across teams, assign tasks, and track outcomes within one platform.

Analyst-verified intelligence

Get deeper insight via trusted experts and sources; verify fast alerts to reduce false positives. Includes assessments, impact analyses, and recommendations so you can move forward with confidence.

Data layers and environmental context

Enrich signals with environmental and location data (weather, crime trends, etc.), to understand risks beyond simple events.

ONTIC

Request a demo to see Ontic in action

Schedule Now