ONTIC

# Protective Intelligence Toolkit

OPERATIONAL TEMPLATES FOR LAUNCHING YOUR PROGRAM

# The Evolution of Protective Intelligence and Why it Matters

Shifting your mindset to a more proactive approach to protection isn't an overnight process, but it shouldn't take a tragedy to change things. As a former agent I've witnessed that TRAGEDY HAS FORCED LOTS OF CHANGES, mostly driven by intelligence failures. Every decade since the 1960s has brought new challenges and critical shifts for our industry; however, adaptation and resilience have been our guiding strengths.

With these evolving trends, the industry has shifted from reactive to developing the discipline of protective intelligence. But what is it, exactly?

## PROTECTIVE INTELLIGENCE

An investigative and analytical process used by protectors to proactively identify, assess, and mitigate threats to protectees.

It's one thing to study it, and another to PUT IT INTO PRACTICE. Setting up a program that embodies this process looks different for each organization, as certain elements are more important than others. However, there are two key elements that are overarching — being aware of your unique threats and leveraging technology to manage them.

It is our hope that this collection of resources helps guide your program into a purpose-built, proactive stance — allowing teams to act on more than intuition.

Fred Burton

EXECUTIVE DIRECTOR<br>
ONTIC'S CENTER FOR PROTECTIVE INTELLIGENCE

# I. Before You Begin: Questions for Consideration

Each organization demands a program that caters to their specific needs. Here are four steps to understand existing opportunities for growth in building or refining a program.

## STEP 1 ESTABLISHING YOUR PROGRAM

When setting up a program, there are three foundational questions to address before taking any action to operationalize:

| | |
|---|---|
| 1 | **What is (are) the threat(s) you're facing?** |
| 2 | **Why is (are) the threat(s) important?** |
| 3 | **What vulnerabilities that are associated with these threats are not being addressed?** |

## STEP 2 DETECTING, MANAGING AND ASSESSING INTELLIGENCE

Once threat intelligence is established, it's important to know how information is being detected, managed and assessed. Given the expanding threat landscape, the ability to collect and connect the dots is critical, as is access to historical data and updates in real time. Evaluate your current process with these questions:

| | |
|---|---|
| 1 | **Do you have a means of threat detection, management and assessment?** |
| 2 | **Is your process automated, real time, and always-on?** |

## STEP 3 ENHANCING YOUR PROCESS

When thinking about how you are spending your time and what tasks you're prioritizing over others, here are some questions to consider.

| | |
|---|---|
| 1 | How much time do you spend on threat detection per week? |
| 2 | What is the minimum standard that each investigative case receives so teams can prioritize cases over others? |
| 3 | Do you have a corporate security team focused on threat detection? |
| 4 | How do you share information with those that need to know? |
| 5 | What are your alerting protocols? |

## STEP 4 EVALUATING TEAM STRUCTURE

It's essential to have a strong team at the helm of your program. Depending on the resources available at your organization, evaluating your security team's structure may lead you to consider the following.

| | |
|---|---|
| 1 | Are you involving other members of your organization (legal, HR, business continuity and risk and compliance) in your security decisions? |
| 2 | Do you have a team with experience in both cyber and physical security? |
| 3 | Do you have the means to gather research and analyze emerging events to share more broadly with relevant internal teams and leadership? |
| 4 | Do you have a fluid process to submit reports of suspicious or concerning behavior? |
| 5 | Do you have resources to support employees who are experiencing hardship, mental health stress, or workplace violence? |

I
Questions for Consideration

II
**Common Organizational Charts**

III
Job Descriptions

IV
Report Templates

# II. Structuring Your Team: Common Organizational Charts

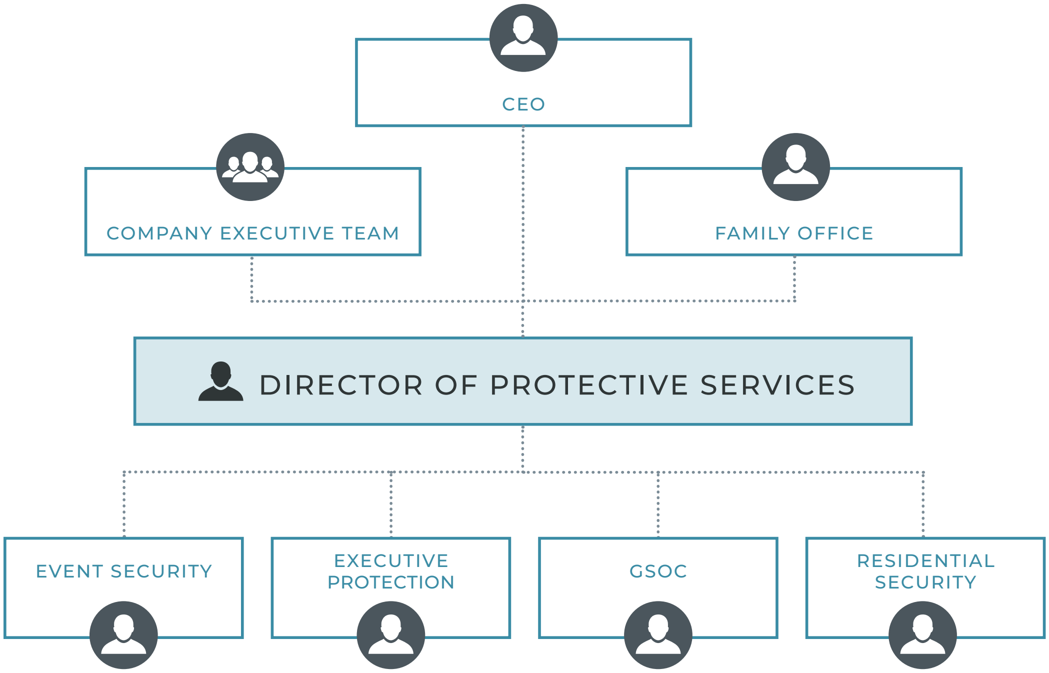
How a team is structured depends on the needs of the organization and the resources available. While a three-person team may work well for one company, another may benefit from a more robust structure that encompasses several different groups, or sub-programs, that ladder up to the security lead.

Below we describe common structures for both protective services teams and corporate security teams.

## PROTECTIVE SERVICES

A central theme in protective services is supporting multiple agendas. There is the core principal you are charged with protecting (the CEO, team owner, or high-profile individual), and then there is everything in their surrounding orbit — oftentimes involving family, philanthropy, and the executive team or advisory board. This orbit is constantly in motion, and the threat landscape changes depending on who is participating — and this all tends to happen faster than security teams would prefer.

Some principles require the resources of a broader team that funnel up through the security lead, providing intel around events, weather, and people in their vicinity.



## CORPORATE SECURITY

Investing time into planning how your corporate security team is structured allows for clearer lines of communication and greater day-to-day efficiency. It may make sense to organize your team regionally rather than have one centralized structure. For the sake of simplicity, our example below is representative of the latter.

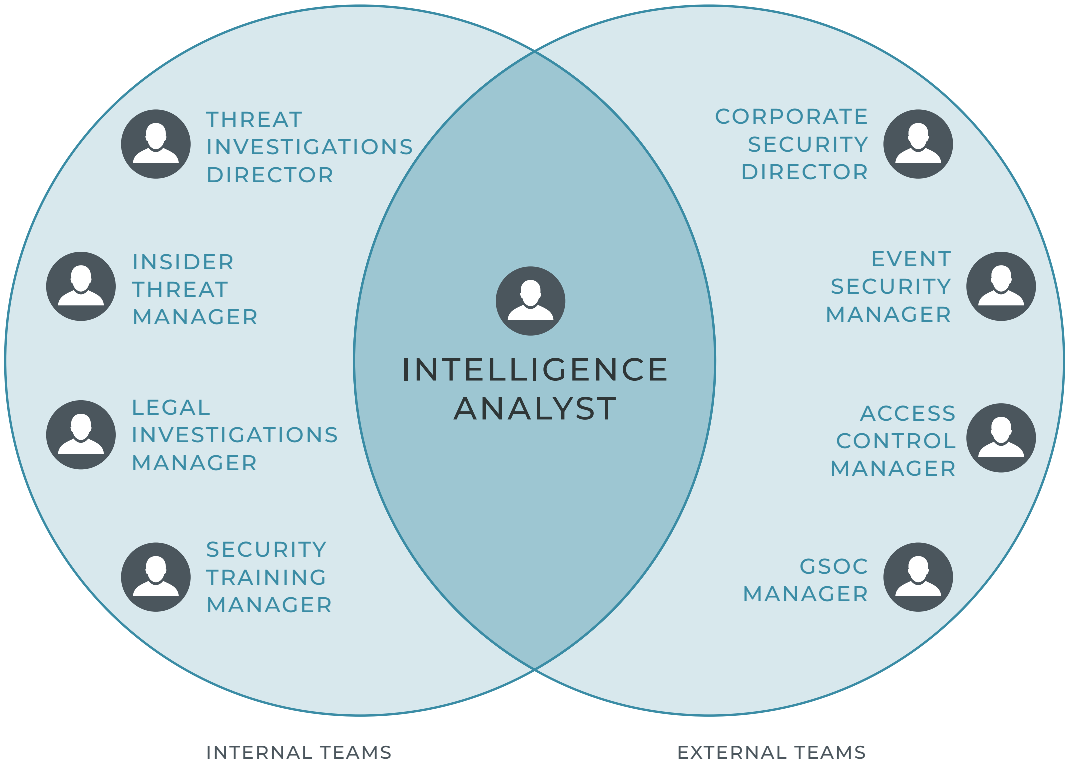
First, it's important that the head of security has not only visibility but a voice on the leadership team. It's critical they act as a unit with other key stakeholders in the organization, such as legal, human resources and business continuity.

Next, sub-programs under the head of security are often divided between internal and external threats. For instance, internal threats would cover workplace violence and insider threats, while external threats encompass facilities/access management, cameras, and events.

Below is a menu of functions typically seen in the industry:

### VICE PRESIDENT, GLOBAL SECURITY

(OVERSEES ALL TEAMS)



THREAT INVESTIGATIONS DIRECTOR

INSIDER THREAT MANAGER

LEGAL INVESTIGATIONS MANAGER

SECURITY TRAINING MANAGER

INTELLIGENCE ANALYST

CORPORATE SECURITY DIRECTOR

EVENT SECURITY MANAGER

ACCESS CONTROL MANAGER

GSOC MANAGER

INTERNAL TEAMS

EXTERNAL TEAMS

# III. Expanding Your Team: Job Descriptions

As you build out your security team, hiring the right people is crucial to SHAPING HUMAN CAPITAL within your organization. The following job descriptions will help you provide a framework for attracting talent for a variety of skill levels within your security structure, as well as address the growing need for risk management and compliance professionals — an example of how the threat landscape has pushed the limits of the traditional corporate security team.

## CHIEF SECURITY OFFICER

| | |
|---|---|
| ABOUT US | [Share relevant company information — mission, history, etc.] |
| ABOUT THE ROLE | • Responsible for the holistic security capabilities and activities of the company, providing strategic insight as a member of the Executive Leadership Team.<br>• Support the Leadership Team in the development and execution of the Global Security Strategy.<br>• Define, deliver and manage the security roadmap, including architecture, policies, processes, and strategy within the organizational context.<br>• Confirm the organization complies with relevant local, national and international regulatory procedures.<br>• Establish security and compliance goals, define security strategies, metrics and reporting mechanisms; and create maturity models and a roadmap for continual program improvements.<br>• Promote collaborative working across the organization and foster the environment to explore new ways of discharging security in ever-changing technological and threat environments.<br>• Provide proactive solutions that facilitate effective risk management while managing ongoing change to the organization’s security and risk posture.<br>• Research and deploy technology solutions and innovative security management techniques that ensure quality deliverables that meet organizational requirements.<br>• Coordinate incident response, management and recovery, including policies, plans, programs and exercises to establish baseline organizational responses.<br>• Partner with business stakeholders across the company to raise awareness of risk management concerns and deliver updates on the state of the security function. |
| QUALIFICATIONS | • Bachelor’s degree required and at least 15+ years related work experience, at least 5 years of experience in corporate security management is preferred.<br>• Previous government intelligence, national security, threat analysis, law enforcement or related government experience preferred.<br>• Proven proficiency in developing physical and digital security protocols and procedures.<br>• Solid communication and interpersonal skills.<br>• Exceptional managerial skills and the ability to lead a team.<br>• Ability to research and stay up to date with security trends, as well as changing government and state laws. |
| BENEFITS | [Add any benefits to the company or role, such as paid time off, insurance, training] |

## CORPORATE SECURITY MANAGER

| | |
|---|---|
| ABOUT US | [Share relevant company information — mission, history, etc.] |
| ABOUT THE ROLE | • Responsible for the administrative supervision of the security organization, providing protection for personnel and company property.<br>• Planning, scheduling, organizing and directing work, training personnel and recommending applicants for employment or corrective action.<br>• Teaches and enforces safety regulations and ensures security patrol priorities are followed based on company policy or client requirements.<br>• Analyzes loss control and accident reports. Prepares and maintains all required security manuals.<br>• Supervises (direct or via subordinate team leads) all proprietary or contracted security personnel.<br>• Serves as the primary contact for law enforcement agencies.<br>• Administers the operation of all security-related systems: access control, CCTV, digital video recording, photo badging, etc.<br>• Reviews utilization and maintenance of security equipment.<br>• Prepares and reviews periodic security reports to management, sharing key insights from software-based protective intelligence platforms.<br>• Recommends ways to improve security and or correct department function. |
| QUALIFICATIONS | • 5+ years of relevant work experience within a corporate security environment (public or private sector), with specific experience managing intelligence and travel security programs and initiatives.<br>• Strong interpersonal skills with the ability to facilitate meetings, resolve conflict, build consensus, establish rapport and collaborate effectively across departments and externally.<br>• Analytical and critical thinking skills with the ability to leverage data to influence decisions, identify risks and improvement opportunities, and distill complex issues into actionable plans.<br>• Effective verbal and written communication skills with the ability to create transparency and confidence and influence across all levels.<br>• Ability to adapt, prioritize and successfully manage multiple tasks or projects in response to ambiguous, changing or competing priorities.<br>• Ability to work autonomously and manage multiple projects simultaneously, maintaining appropriate prioritization and ensuring adherence to deadlines.<br>• Ability to apply discretion and sensitivity while working with confidential information. |
| BENEFITS | [Add any benefits to the company or role, such as paid time off, insurance, training] |

## GLOBAL RISK MANAGEMENT PRINCIPAL

| | |
|---|---|
| ABOUT US | [Share relevant company information — mission, history, etc.] |
| ABOUT THE ROLE | • Establishes, communicates and drives the investigative strategy for Global Security Operations.<br>• Serves as a subject matter expert on investigative strategy.<br>• Works with internal team to advise leadership and employees on legal matters, including security issues, contracting, international and global presence, intellectual property, employment matters, healthcare law, and national security issues.<br>• Supports the direction of operations, including enterprise risk management, global security services, facilities, and outreach and partnerships, which includes technology transfer to industry.<br>• Builds and leverages strong partnerships with stakeholders to enhance insights into investigations, compliance, and mitigation.<br>• Works with stakeholders to develop and enhance global investigative policy, training, and standards.<br>• Develops or recommends scalable and sustainable mechanisms supporting global investigations inclusive of technology advancements.<br>• Communicates data trends and proactively make recommendations on mitigation strategies at the senior leadership level.<br>• Develops business cases that receive the required approval, financial and technical resources, and the support of appropriate management to enact desired change. |
| QUALIFICATIONS | • 10+ years of experience developing global strategy and framework for investigations or security process enhancements across a diverse employee population.<br>• Experience in developing and analyzing metric-based reporting and leveraging protective intelligence software to drive business continuity, resilience and reputation.<br>• Experience with database querying and analysis.<br>• Experience managing for a federal, state or local law enforcement agency or the security function at a global company.<br>• Ability to influence others to apply skills and techniques to solve dynamic problems.<br>• Analytical leader experienced in performance-based, action and results-oriented management, strong project manager and effective problem-solver.<br>• Lean Six Sigma Certification preferred.<br>• CPP, PCI, CFI, or CFE certifications preferred. |
| BENEFITS | [Add any benefits to the company or role, such as paid time off, insurance, training] |

## SECURITY INTELLIGENCE ANALYST

| | |
|---|---|
| ABOUT US | [Share relevant company information — mission, history, etc.] |
| ABOUT THE ROLE | • Collect and analyze data from a variety of internal and external sources, including primary source intelligence, financial and business product data analytics.<br>• Prioritizing, validating, analyzing, and correlating information to identify existing and emerging threats to employees, facilities and operational continuity.<br>• Dark/deep web; brand protection, OSINT and competitive intelligence gathering capabilities.<br>• Support Security Intelligence program build out enterprise-wide.<br>• Conduct extensive due diligence investigations, and support enterprise risk management framework.<br>• Research and analyze emerging events to provide reports to share with relevant internal teams and leadership.<br>• Grow and maintain relationships with internal and external stakeholders to develop Security risk mitigating strategies.<br>• Align with policies and procedures to support the security program.<br>• Support development and delivery of security awareness activities. |
| QUALIFICATIONS | • Intelligence analytics experience, with at least 3+ years in corporate security<br>• Excellent verbal and written communication skills in English<br>• A positive attitude and attention to detail, integrity and professionalism.<br>• Proficiency in MS Office programs (Word, Excel, and PowerPoint, Office 365).<br>• Knowledge of due diligence platforms and protective intelligence platforms.<br>• Ability to work nights, weekends, and holidays as operational needs dictate and be able to travel domestically. Some international travel may also be required.<br>• CPP, PSP, CFE or equivalent certifications preferred.<br>• Proficiency in business intelligence data collection/analytics platforms (MySQL, Tableau, and QLIK) preferred. |
| BENEFITS | [Add any benefits to the company or role, such as paid time off, insurance, training] |

I
Questions for Consideration

II
Common Organizational Charts

III
Job Descriptions

IV
Report Templates

# IV. Knowing What’s Working: Reporting Templates

With a protective intelligence program in place, it’s time to think of how you will demonstrate the impact of your work.

This is where reporting comes into play. It’s important to assess your program’s goals and identify information needed to keep track of progress towards those goals. This starts with determining your baseline activity so you can proactively pick up on anomalies, and make data-driven decisions when allocating resources. The use of technology is a critical tool for knowing where to look to quickly identify potential risks to your organization, at scale.

Here are some examples of how to demonstrate the impact of your program:

| GOAL 1 | ASSESS DISTRIBUTION OF RISK SIGNALS ACROSS ASSETS |
|---|---|

**Impact:** Knowing how many people are talking about your principal or asset can help inform where to focus team resources.

| | |
|---|---|
| METRICS | **Average number* of social, OSINT and news mentions over a certain period of time per principal**<br>***Baseline:** If your asset or executive typically has around 100 social mentions per week, and one week over 400 mentions are documented, it may make sense to dig in and try to understand the reason behind this anomaly.* |
| | **Trends over time, noting increases or decreases from a baseline for a given timeframe** |

I
Questions for Consideration

II
Common Organizational Charts

III
Job Descriptions

IV
Report Templates

## GOAL 2 INCREASE EFFICIENCY OF INVESTIGATIVE PROCESS

**Impact:** Implementing a repeatable process of assessing risk and potential threats prevents missed signals and instills trust in the organization.

| | |
|---|---|
| METRICS | **Number of open or closed investigations over a certain period of time** |
| | **Time spent assembling and sharing investigative reports* (compared to previous, manual methods)**<br>***Baseline:** If you previously spent several hours assembling documentation around a case, and now leverage technology to automatically generate reports and share within the organization it's impactful to document that advantage.* |

## GOAL 3 TRACK NUMBER OF NEW INCIDENTS AND POIS

**Impact:** Having a method of collecting and managing POIs and incidents allows you to demonstrate the breadth of your threat portfolio and connect activity to evaluate the complete picture and stay on top of potential risk.

| | |
|---|---|
| METRICS | **Number of POI profiles* and incidents created over a certain period of time**<br>***Baseline:** Comparing the number of POIs and incidents created in one quarter, versus the same quarter from the previous year may indicate an increase or decrease in threat activity.* |
| | **Trends around updates to profile information, uncovering location intel, social media or OSINT activity, and more** |

Ontic's Protective Intelligence Platform enables enterprise security teams to see around corners and keep their businesses safe.

Learn More

## Let's make nothing happen together™

Named the top industry innovator in the Frost Radar™: Digital Intelligence Solutions, 2021, Ontic is the first protective intelligence software company to transform how Fortune 500 and emerging enterprises address physical threat management to protect employees, customers and assets. Ontic's SaaS-based platform collects and connects threat indicators to provide a comprehensive view of potential threats while surfacing critical knowledge so companies can assess and action more to maintain business continuity and reduce financial impact.

Ontic provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals through its Center for Protective Intelligence and Center of Excellence, the latter of which also offers program development and training services in behavioral threat assessment, threat management, and violence prevention for major corporations, educational institutions and government agencies.

For more information please visit ontic.co or follow us on Twitter @ontic_co

ONTIC®