ONTIC®

Whitepaper

The Definitive Guide to Establishing a Modern Protective Intelligence Program

Taking a thoughtful and logical approach to assessing risk is embedded in every successful security program. However, to do this effectively and consistently over time, there's a critical component — protective intelligence.

What makes up a protective intelligence program, exactly? This guide will describe the individual elements as it applies to the stages of the **Intelligence Cycle** and covers six core elements, listed below:

1 **REQUIREMENTS**
Risk Assessment and Planning

2 **PLANNING AND DIRECTION**
Intelligence Collection
- Physical Security Program
- Surveillance Detection Program
- Mail Screening Program
- Personnel Training Program
- Insider Threat Program
- Situational Awareness Program

3 **COLLECTION**
Database Curation

4 **PROCESSING AND EXPLOITATION**
Threat Analysis

5 **ANALYSIS AND PRODUCTION**
Case Management

6 **DISSEMINATION**
Case Management

Of course, every program will be different based on the unique context that it operates in, whether that's in a family office environment or in a Global Security Operations Center (GSOC) supporting international operations.

Requirements: Risk Assessment and Planning

> ***Why is a protective intelligence program needed and what protective security challenges will it help address?***

Before designing and implementing a protective intelligence program, we must first outline the "why".

As part of this, a comprehensive look at the assets being protected and the threats and vulnerabilities associated with them must be conducted. In most cases, this includes a thorough assessment of the digital footprint of the people or business entity being protected to identify what publicly available information can be exploited.

It's important to reverse engineer situations, and put yourself in the mind of the threat actor to imagine what vulnerabilities can be exploited for their own malicious gain.

Thomas Kopecky

Co-Founder and Chief Strategy Officer at Ontic

RISK ASSESSMENT IN ACTION

With a comprehensive risk assessment completed, the protective intelligence team is equipped to use their new insights to strategically plan and develop policies and procedures to support the needs of the program. Some of these planning activities might revolve around any of the following:

TRAINING

Train your team to know what action to take next when a threat is on the horizon.

BUDGET

What funding is available to maintain different aspects of the program on an ongoing basis?

PERSONNEL

What size and structure is optimal to support your program?

INVESTIGATIVE PROCESS

What is the minimum standard that each investigative case receives so teams can prioritize cases over others?

Planning and Direction: Intelligence Collection

The second major element of a protective intelligence program is the set of systems and processes in place to collect threat information. These can take many forms and can be mini-programs into themselves. For example, intelligence collection might be the combination of these sub-programs:

PHYSICAL SECURITY PROGRAM

A network of CCTV cameras, LPR (license plate reader) cameras, access control systems, intrusion detection sensors, and the human element of monitoring and maintaining these systems with complementary policies, procedures, and standards to keep assets safe.

SURVEILLANCE DETECTION PROGRAM

A systematic way of collecting information on potential surveillance activity, so that incidents can be analyzed over time and potential threat actors can be detected during the early stages of the attack cycle.

MAIL SCREENING PROGRAM

An established process for screening mail before it is admitted into sensitive areas or before it reaches the desk or home of key personnel. For instances where people are attempting to inappropriately contact key personnel, the development for a minimum standard for conducting investigative follow ups.

SECURITY TRAINING PROGRAM

The training of security and non-security personnel is critical. Security personnel might be trained in how to conduct field interviews with potential threat actors, while the average line employee might be taught what suspicious behavior looks like and how to report it.

INSIDER THREAT PROGRAM

Internal processes in place to limit the risk of an insider threat situation impacting the team / organization. Always think of the principle of least privilege — meaning, only give people access to what they need to execute their job and nothing more.

SITUATIONAL AWARENESS PROGRAM

A standardized approach to ensure that team members are aware of situations internal and external to the organization that may impact the safety and security of assets. This includes researching domestic and international news sources (i.e., social media chatter, police reports, transportation disruptions, social unrest, travel notices, and news mentions).

Collection: Database Curation

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, there are several minimum standards that are recommended to make practitioners the most effective:

DYNAMIC DATABASE

The database needs to be dynamic. When new information is added, it needs to be accessible by all security team members that need to know. No one looks their best referencing a two week old PDF BOLO report.

SEAMLESS PROCESS FOR DOCUMENTATION

Surveillance detection activities need to be documented in an easy, maintainable way. You can never detect the adversary if you are not looking for them in a highly systematic way.

COLLABORATION AND CASE MANAGEMENT

Task management needs to be a centerpiece. Managing a range of active threat cases or even one complex case can be daunting depending on the circumstances. There must be a simple way for assigning and managing tasks over time.

AUTOMATION

When simple tasks can be automated, automate them!

Processing and Exploitation: Threat Analysis

After all the necessary and available information has been collected, it's time to analyze.

The most difficult and high-stakes aspect of protective intelligence is the analysis of threats. It's more of an art than a science, but there is so much science that can support analysts in their goals to adequately assess potential threats and make appropriate security recommendations for their decision-makers.

Analysts need the right tools or processes in place that facilitate analyzing complex information. Oftentimes, organizing all of the information gathered into a form that is easy to digest is a significant challenge.

Once the information relating to the case has been gathered and processed, next, it's time to evaluate everything collected. There are many different ways to evaluate threats, especially those relating to potentially violent threat actors. There are threat assessment models such as WAVR-21, the Secret Service's model, and others. However, they all tend to have one common thread: assessing if the threat actor is involved in the attack cycle (and if so, to what degree), the capability of the threat actor to carry out an attack on their target, and past behavior of the threat actor.

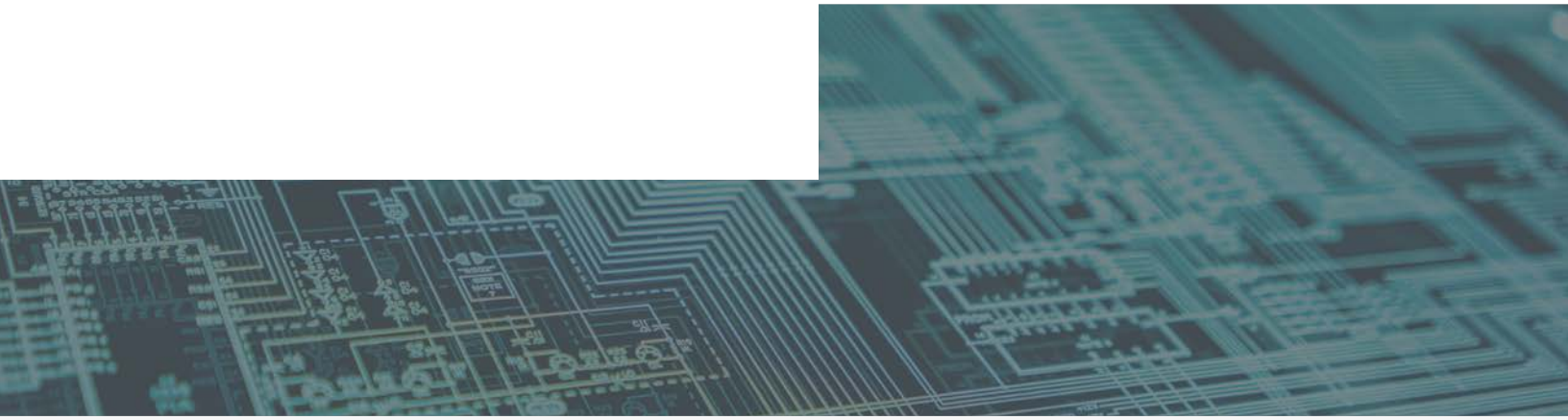
Analysis and Production: Case Management

Case management refers to how cases are handled by analysts throughout their lifecycle, from initial investigation, to continuous monitoring, to the closing of a case. It begins with triaging cases based on their criticality to the organization and then treating them with a designated standard of care prescribed by leadership.

The sequencing of this care takes on specific tasks and activities throughout any given month. This might include scheduling interviews with people involved or going to a court hearing to hear the results of a POI's court session.

The success of this process hinges on technology that curates new information and its inclusion in the analyst's re-assessment of the threat over time.

When analysts are able to incorporate continuous monitoring efforts into their case management process, they can automate many of the tasks that previously took significant time away from actioning threats. For example, streamlining social listening to surface POI activity or receiving alerts on a POI's new criminal records in their last known county can save an analyst a full day's worth of research over the course of a week.



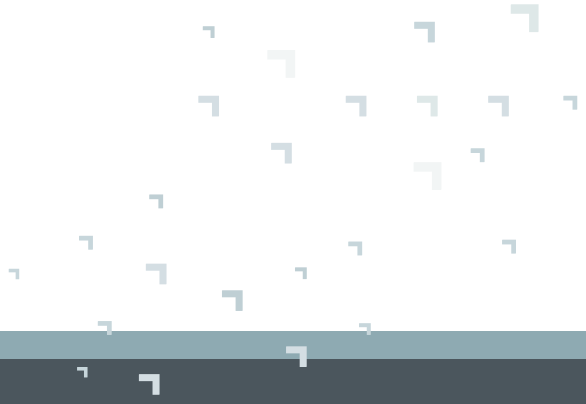
Dissemination: Sharing Information

The final element critical to protective intelligence programs is communication. Teams need a reliable, secure means for communicating their investigative findings and recommendations to team members.

It's also important to have a standard template that serves the needs of the particular program, so that all reports being sent to leaders or field agents have the necessary information for them to make appropriate decisions. In high stakes situations, making documentation and dissemination easy is an essential, but often overlooked part of the Intelligence Cycle.

Final Thoughts

While a protective intelligence program can take on many forms and incorporate multiple "sub-programs" depending on an organization's goals, there's something that stands true across all organizations — it is a foundational element to proactively mitigating risk and addressing threats before that can amount to a larger issue.



Let's make nothing happen together™

Ontic is the first protective intelligence software company to digitally transform how Fortune 500 and emerging enterprises proactively 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

ONTIC®