ONTIC

The Guide to Establishing an Intelligence Baseline

Table of Contents

Introduction

We know that organizations are fundamentally different and understand that very few have a standardized approach — one size does not fit all. Threats are highly contextual and are based on numerous factors, including industry type, company culture, geographic areas of operation, and both positive and negative media attention.

What's more, those of us in the corporate security and executive protection spaces are often confined to the operational constraints that our principals unknowingly establish for us. Security professionals must remain fluid and adaptable as the security landscape regularly evolves, often without any notice.

> Many security teams are expected to be out front and all-knowing, identifying threats before anyone else. They are then asked to force multiply (without force-multiplication in the security budget) and continue to do the heavy lifting when any issue arises.

Because of this, when conducting research and investigations, it's essential for security teams to have processes in place to better understand the data that informs their work.

We call this **establishing an intelligence baseline**.

Defining an Intelligence Baseline MVP

Defining a person of interest (POI) centric intelligence baseline can be a difficult task due to the nuance and ambiguity that each person and their specific circumstances provide.

To standardize the process, a best practice is to evaluate the POI's **intent** and **capabilities** as a baseline.

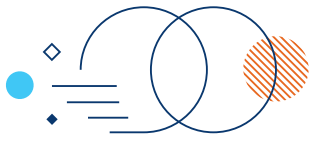
While somewhat self-explanatory, intent can be defined as: What is this person trying to accomplish? Is it bragging rights within a particular social circle? Is it virtual signaling online? Is it physical harm?

When we evaluate a POI's capabilities, the most significant factor is proximity to the target. Distance is the great equalizer when it comes to analyzing a threat, and if a POI is known to be in a different country or several driving days away, it can often be triaged as not an immediate threat.

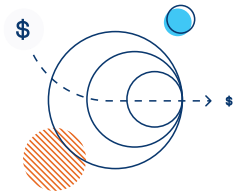
We could gather seemingly endless data points about a POI's intent and capabilities. But knowing that time and resources are finite, how do we establish a minimum standard for gathering or sharing information?

At Ontic, we know our clients need the right amount of data to make critical security decisions or deploy valuable resources.

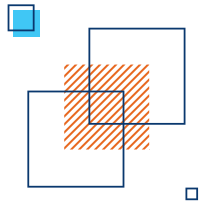
With this in mind, we saw three emerging opportunities:



Deliver data that informs intelligence quickly.



Gather data all in one place.



Provide cost-effective reporting.

Important security decisions don't always require an exhaustive investigative profile for every single person of interest (POI). Sometimes, you only need minimal investigative research to make an initial security decision. It's essential to remember that your investigation can be good enough in some situations. The technology industry labels this "good-enough outcome" a Minimum Viable Product (MVP).

Delivering an MVP means you're trading perfection for pretty darn good. The MVP is not the final version, rather, it's a prototype for you to understand and solve the user's basic needs to apply on the next version.

For example, let's consider a car. An MVP might be a box, four wheels, and an engine. This basic (very basic) build meets the driver's needs, works as designed, and is good enough to go from points A to B. The development team gathers more insights about the baseline product to build future improvements to the car – a windshield, seat belts, and comfortable seats.

Let's use the MVP process to compare the security domain. There needs to be a universally accepted MVP for detecting and evaluating threats. To address this blind spot, we propose introducing a workflow we've extensively tested to fill this gap.

Keep in mind that one size does not fit all; this isn't the definitive playbook for every team. Nor do we believe that investigations and threat assessment cases can always be reduced to one straightforward process. Gut instinct will always come into play.

This workflow does, however, provide a broadly applicable baseline framework. Returning to our MVP, security teams don't necessarily need an exhaustive due diligence investigation on every single POI that appears on their radar. They simply need a foundational level of understanding of the background of potential threat actors. This triage approach prevents the waste of significant human and financial resources.

Applying an MVP to Your POI Investigations

Most security teams work with limited resources (time, team size, budget, etc.). The workflow below is mindful of how to allocate time to investigative projects. Investigators should focus on each stage's outcome, as these outcomes define success. This means that what you use to achieve these outcomes will always change with the situation and the practitioner.

Though we value the entirety of the workflow in understanding your POI data, we specifically identify Stages 1-3 as the MVP of our investigative process. These initial three stages are foundational for a POI investigation, serve as a baseline, and should be executed for every POI.

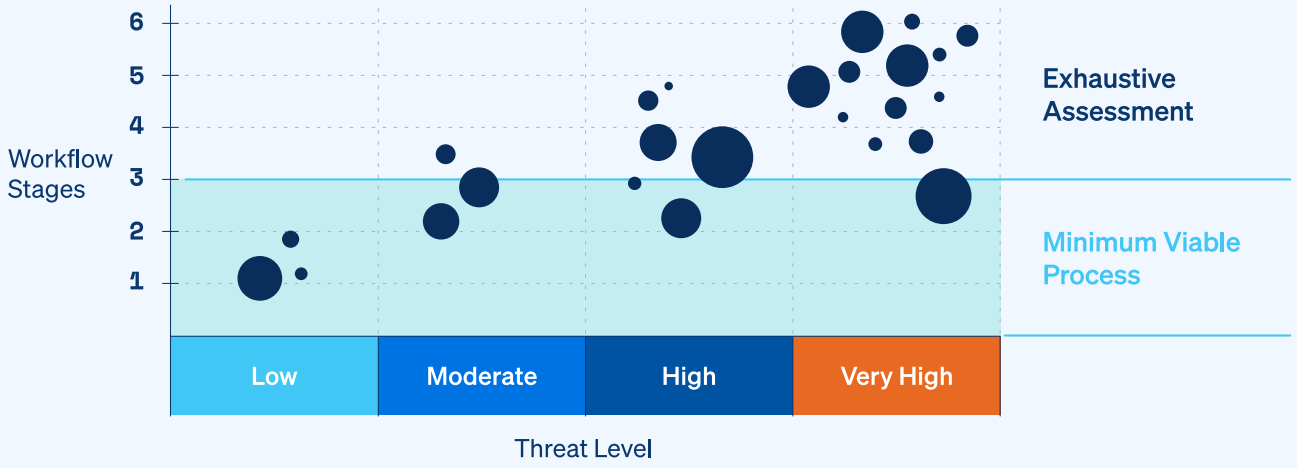
The first three stages are defined by:

01 Identity Resolution

02 Geo-Location Insights

03 Open-Source Analysis and Social Media Intelligence

As the threat level increases, we can always choose to conduct a deeper investigation and continue to stages 4-6 in this workflow. We believe defining these boundaries will maximize the use of finite team resources.



Investigative Workflow Stages

01 Identity Resolution

In this step, the analyst or investigator must confirm whom they are actually investigating. Who is the person behind the harassing email, touchpoint, or phone communications? Who owns the vehicle in that suspicious location near the principal's residence?

Once we resolve their identity, we need to know what our team and associates have already discovered about that person.

Ask yourself questions like:

Is there a baseline already existing on this POI, or is this one brand new to us?	☐
Do we have an initial understanding of the possible threat level based on the context of the interaction?	☐
How does a security team determine what information the business already possesses regarding a particular subject when they make an observation?	☐

→ **Example:** Does Human Resources consider this person a serious threat due to comments he or she made in an exit interview, or does Corporate Security know that this subject is part of a retail crime ring?

Moving forward, how do we quickly identify the person again when they resurface?	☐

→ To do this, we will need to learn about the person's additional identifiable attributes, including other personal identifiers: address, registered vehicles, social handles, phone number, physical attributes, employment, etc.

02 Geo-Location Insights

This step is all about location, location, location.

It's simple physics: The farther away a POI is from your principal or workplace, the less risk they pose for causing physical harm. We call this **threat context by geo proximity**. Of course, this rule has some exceptions, such as package bombs, chemicals mailed to a principal, IT vulnerabilities, etc. Essentially, is the POI on the other side of the country just making noise, or are they actively engaged in the attack cycle? Where is this person right now?

There are so many sources to review and steps an analyst or investigator can take to determine where a person is at any given time. Some are quick reference searches through social media or incarceration records, while other methods include human intelligence and pretext calls. Remember, doing these searches in a centralized database is more effective.

This step is one of the most critical because of its immediate impact on time and resources. If there's little physical distance between the POI, you may need to mobilize resources quickly. If the opposite is true, the team could relax while maintaining a vigilant posture. Determining the geo-location can help a backlogged team prioritize threatening communication from a POI amongst all other tasks. For example, suppose it's determined that a POI is a thousand miles away from the general area of the principal. In that case, the case can be momentarily deprioritized while other urgent responsibilities are attended to.

03 Open-Source Analysis and Social Media Intelligence

Undoubtedly, there's a deluge of information online that can be cultivated while assessing the threat of a POI. Key issues we typically look for are mode of living, mental state, access to weapons, past behavior, fascination with violence, and fixation / unhealthy pursuit of the principal or their family. For those instances where the POI practices digital privacy, it is often easy to research by proxy and investigate the online activity of those close to them, including friends and family. We also review deep web forums for information on the POI's potential affiliation with fringe groups, radical ideologies, and malicious protest activity.

Note: Having completed the initial phases of the MVP, we're progressing toward additional stages to delve deeper into the investigation due to specific indicators signaling an elevated threat. These indicators can vary significantly and might possess nuanced characteristics, which emphasizes the need for a comprehensive analysis rather than isolating single data points.

What prompts a more profound investigation? It could stem from a combination of factors such as physical proximity and concerning social media activity. Alternatively, it might solely revolve around physical proximity — for instance, if the POI resides along your executive's daily commute route or near their children's school. Irrespective of the precise scenario, it's a situation where your risk assessments suggest the necessity for further investigation to either enhance our understanding of the threat or take preventive measures.

04 Public Records Data

We can access public record repositories to formulate a deeper background story of a POI. These indexes provide exceptional access to case information, including criminal arrests, civil litigation, bankruptcies, liens, judgments, foreclosures, divorce, child custody, intellectual property, and trademark infringement claims. They're also a key indicator for recidivism, which is essential to have insight into as you conduct research.

During stages 5 and 6, we move on from preliminary data gathering to more accurately assessing risk, communicating our findings with those who need to know, and implementing security protocols for that case. At this point, investigators need to get their team leadership involved to review the facts of the case and then develop a plan consistent with the culture and mission of the organization.

05 Assess Risk Indicators, Trigger Events, and Formally Assign Threat Level

As analysts layer in all the information discovered in prior stages, they can make greater sense of the data points, identify potential trigger events, more formally assess risk, and prioritize other dates/events of importance for the threat actor (anniversary of termination, copycat workplace violence incidents, etc). With this connected intelligence at the fingertips of security professionals, they are empowered to make informed decisions about assigning a more accurate threat level to a case and move on to the next step.

TIP: Construct a timeline incorporating information to narrate the escalation journey with the POI. This timeline will assist stakeholders in grasping the progression of how the POI started on its current trajectory.

06 Develop and Implement Protection Strategies

There are many excellent resources about assessing potentially violent actors and developing case management strategies, such as those endorsed by the Association of Threat Assessment Professionals (ATAP Body of Knowledge).

After working with corporate clients, this is our philosophy:

Intelligence in a vacuum is useless, and inaction in light of it actually becomes a major liability.

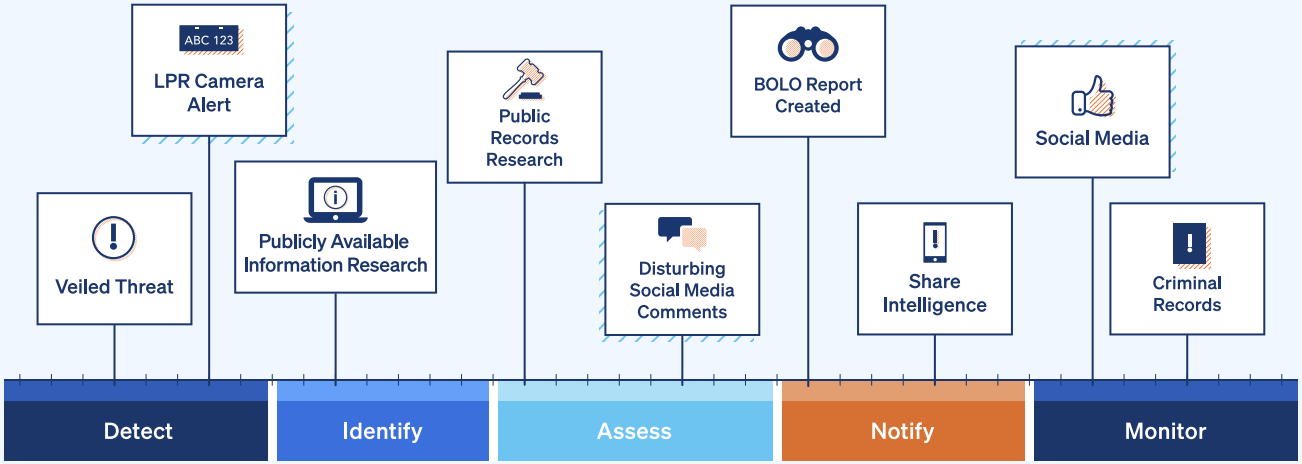
For example, if "Corporation A" knew a great deal about a POI who was harassing a workplace, making veiled threats, or displaying an unhealthy interest in C-Suite executives and then chose to do nothing with that information, what does that say about the company's duty of care?

When information is shared, it becomes actionable. Note: Sharing of information is not limited to this step of this workflow. It can and should happen throughout the process. We also find that after this much information is obtained and assessments are made, contracted professionals can be retained for guidance. For example, does this case get escalated? Does Law Enforcement become involved? Or does the corporation engage with the threat actor and their family to help the person get treatment from a trained mental health professional?

Connecting Data to Get a More Holistic View of Threats

With a holistic approach, you can now layer in all pertinent information to more accurately understand the evolution of a POI. You can even uncover potential trigger events in their life, such as the anniversary of termination, a death in the family, or perhaps a tense legal case involving a child custody battle. By surfacing this type of information, teams can better identify a trend or anomaly in behavior and more accurately assess threat levels.

As the timeline below illustrates, a security professional can see that all of the various data points – when visually connected – create a much bigger story. What could otherwise be cataloged by siloed teams as independent events now clearly demonstrates the evolution of a serious issue.



Putting It All Together

Establishing an intelligence baseline highlights the nuanced nature of threats within diverse organizational landscapes. Customized approaches are essential, and adapting to operational constraints remains challenging.

Balancing preemptive threat identification with resource optimization underscores the importance of defining a Minimum Viable Product (MVP) for intelligence gathering, prioritizing initial insights rather than exhaustive profiling at the onset, ensuring efficient resource utilization, and preventing unnecessary resource waste.

Our proposed investigative workflow outlines essential MVP stages for POI investigations that cover identity resolution, geolocation insights, and open-source analysis, which serve as crucial foundations. Further efforts delve deeper into public records, risk assessment, and protection strategies. Constructing timelines helps narrate the escalation story, aiding stakeholders' understanding of potential pathways.

All this enables the right time, resources, and reporting to be allocated within a confined security budget.