ONTIC®

Whitepaper

Level Up Your Threat Hunting Game

Creating Intelligence from Anomalies and Patterns - By Thomas Kopecky

WHAT THREATS MIGHT I BE MISSING BY FOCUSING TOO MUCH ON INDIVIDUAL DETAILS, RATHER THAN THE HOLISTIC PICTURE THAT THOSE DETAILS CREATE?

It seems that not too long ago, social media or emergency news alerts were the holy grail of early threat detection. While it's true that listening for threats in social media is effective and cannot be ignored, it is still only one type of data point among the many needed to adequately identify threats in an effective Global Security Operations Center (GSOC) or protective intelligence program.

With data surfacing at every angle at any time of the day, we are often asked where to start when developing a more proactive security model, including what tools to use. We are also asked how to "Threat Hunt," or as we often say, connect the dots. Equally as important, security leaders want to know how to instill a repeatable process.

In The Protector's Guide to Establishing an Intelligence Baseline, we outlined how to implement a minimum standard, and how to make it adaptable to the unique needs of your organization. In this whitepaper, we want to get more granular about some of the data types, or data intelligence, that we can tap into in order to be more effective in protecting assets.

The Protector's Guide to Establishing an Intelligence Baseline highlights the six workflow stages for effective protective intelligence.

"We need to be more granular about data intelligence to be more effective in protecting assets."

Thomas Kopecky
Co-Founder and
Chief Strategy Officer, Ontic

Looking at the holistic picture

This heightened level of granularity involves talking about characteristics and behaviors to analyze threats. When investigating and assessing threat actors, it's not always about what the threat actor says explicitly, it's also about how often they communicate and who their communications are directed at.

For instance, if a person expresses a fixation on your protectee and posts online commentary about them directly, this can be disheartening, but that alone does not provide full context. Perhaps this person routinely seeks out executives in the tech space in order to create controversy and rattle cages. Some threat actors actually get validation by knowing they hit their mark. Occasionally, the feedback a person of interest (POI) receives comes in the form of a legal threat or an admonishment by someone in a security organization.

When managing a threat assessment involving inappropriate pursuit, unhealthy fixations, and related behaviors, there are many trends to look for. It's critical to keep the full context in mind. Immediate examples include:

- Personalization of the communications
- The tone
- Escalating frustrations
- Indirect references to the principal
- Frequency of communications and commentary

When you observe any of these trends, it indicates that a POI is actively researching their target, signaling competency, and creating an urgency for the protectors to stay several steps ahead of any action this individual may take.

We also need to pay close attention to the frequency of communications or commentary, so that when these communications spike, create a pattern, or are synced with other important life milestones (anniversary of a termination, financial troubles, etc.), additional scrutiny is given to the investigation.

Moreover, if a person posts strange and inappropriate commentary, and then graduates to making direct physical approaches to the executive, we need to escalate our assessment. This indicates that the previous chatter has now evolved into action — which is an important step in the attack cycle.

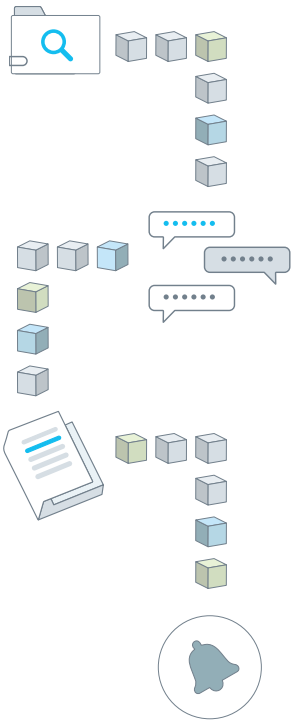
It's not any one action taken by the POI, but rather a series of behavioral steps that give us cause for concern and the information required for optimal decision-making.

What are your sources for data intelligence?

It's important to remember that our success is often limited by our creativity and skeptical curiosity. We have found that there is an abundance of easily available sources that can help surface pre-incident indicators of violence. Since we tend to have more sources of information than time to make sense of it all, we need to reconsider our methods to efficiently digest data from as many preferred sources as possible.

Below we cover a few sources that are readily available, as well as some that are less obvious which can help you uncover valuable information in your threat hunting efforts. Stretching beyond the traditional avenues for data will allow you to turn single events and observations from field operators into actionable intelligence.

Investigative Workflow



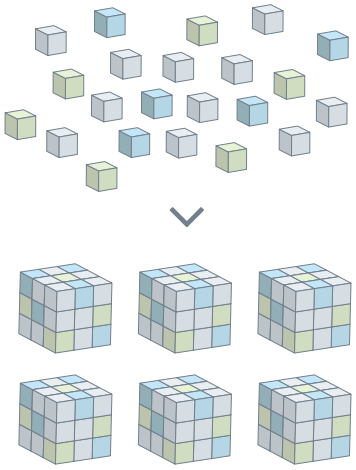
An indicator of threat escalation

Imagine if you were automatically notified when another team member, department, or associate organization is working on an investigation related to the same threat actor as you are. Then you receive a notification that the other team is running similar queries or investigative research, and even saving files with the same POI information.

Envision that you are assigned to the Corporate Security team, and someone in the Executive Protection group generates an internal Be on the Lookout (BOLO) report on a high-threat POI. It may be safe to assume that *something* occurred to kick off this notification since BOLOs are typically generated in response to an escalation or action carried out by a threat actor. Now both teams have consistent information and can determine the level of urgency for their collective plans.

Bridging intelligence gaps is key to operational success, and in our experience, getting teams talking and sharing more intel is a huge benefit for everyone operating under the same security umbrella. The technology exists to make this part of your daily routine, and combining it with the elements we outline next can make it invaluable for staying ahead of threats.

Routine Communications

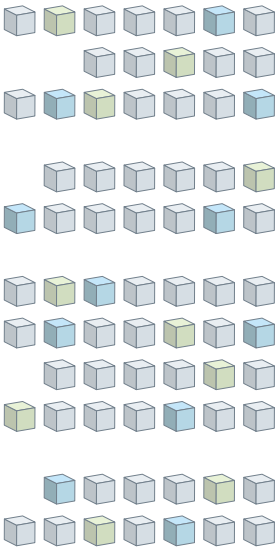


Ditch the sticky notes

A large part of successfully protecting people and assets is ensuring that your team does not lose track of information that may someday become key to uncovering a threat issue. Practitioners typically build internal ad hoc processes that function adequately at a smaller scale; however, there is rarely a central source of truth or a consistent, convenient process to store and share case notes when new intelligence is accumulated. Using a unified platform to store your baseline intelligence allows you to easily measure trends and identify patterns in behavior from a threat actor.

Properly saving key data points related to field observations, images, threatening communications, and team notes can make the difference between detecting and disrupting a threat, or letting one slip. It doesn't take an expert to tell you that even the smallest mistake can lead to irreparable damage.

Your Internal Library of Threat Data

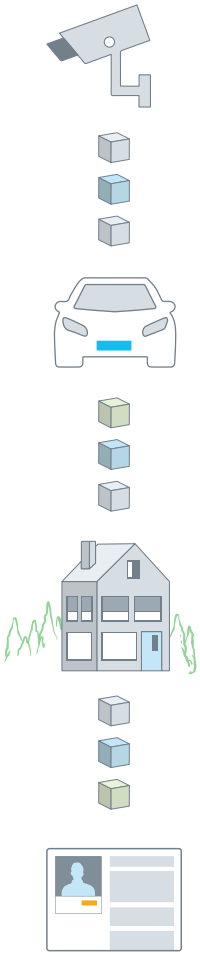


Real time access to the facts

Every security program has access to information that can help them guide how they use security resources and efficiently address threats. In one program, this might be something done with pen and paper, only pertaining to threats that impact that individual team. Then in other more mature programs, this likely includes a detailed database of threat information that spans multiple business units, such as: human resources, executive protection, global security, and more.

The point is this: today, you already have vast amounts of information to help proactively address threats. However, this information is only as valuable as it is available and accurate. Security teams need the ability to retrieve data quickly on past incidents to identify behaviors and patterns. Sorting through data manually and requesting access to cross departmental systems while a potential threat is active is one way to ensure lost productivity. Leveraging a database of information that's on 24/7 with real-time alerts lowers the likelihood that significant changes in information will slip through the cracks, and will increase a security team's ability to take proactive action.

IoT Devices and Hardware



Getting a comprehensive view of integrated systems activity

When in the office, employee badge readers, visitor management / access control systems, and CCTV networks provide a wealth of knowledge to the security practitioner. Surfaced and analyzed in one platform, this information becomes intelligence that practitioners rely on day in and day out. With a proactive security program and process in place, we can better detect and manage the attempted visits of a POI, and broadly communicate those to teams that need to know. Insider threat management programs can benefit from being alerted to “out of norm” access to facilities, or even attempted access by unauthorized persons.

Now more than ever, we are seeing a great deal of success with the use of license plate reader (LPR) cameras at client-owned facilities. Imagine pushing out your security perimeter even further by relying on discrete, low profile LPR cameras that not only alert to “hot listed” vehicles associated with known POIs, but also report anomalous and volumetric activity by others.

LPR cameras in action

A POI drives by two of your principal locations on the same day — one of which is a corporate facility, while the other is the CEO’s residence. With a proper LPR camera integration, you can now be alerted to this activity immediately. As a security practitioner, we don't even need to know what else that person did to be legitimately concerned. We can deduce that they not only remain fixated on the protectee, but have also crossed into a dangerous phase of the attack cycle — pre-operational surveillance and planning.

The Attack Cycle

It's about perspective

Think about this for a minute. We don't always have to know the content of the communication, or the specific details of the incident or action that took place. Simply knowing that such a data point exists can tell us that something urgent is happening.

If we can get even more creative, or level up our threat hunting and track the frequency of behaviors and trends, including spikes and dormancies, we can catch more and miss fewer signals.

Patterns of data points become pre-incident indicators. For example, if a threat actor has a known steady cadence of communication, and that stream suddenly becomes quiet, what does that tell us? Inversely, if a POI redlines their activity level, how does that impact our assessment of the threat?

When it comes to actively hunting for threats, it's easy to be overwhelmed with noise. Therefore, we recommend looking at the situations from another perspective:

What threats might I be missing by focusing too much on individual details, rather than the holistic picture that those details create?

Shifting from the “old way of doing things”

When we take a macro view of our program that is reliant on information sharing across departments, as well as anomalies detected by smart systems integrated into our security toolbox, we're able to arrive at insights that were previously unavailable to us.

As the approach to protecting assets across all industries evolves to incorporate a more holistic view, we expect that organizations will significantly increase their ability to protect their assets. Moving away from old habits of fixating on specific details rather than the complete story will allow us to glean new insights. And with the process of threat hunting growing more complex, this shift in approach can make all the difference in separating noise from an immediate threat.

At Ontic, we believe that businesses like yours can be safer by serving intelligence to those who protect. Visit the Center of Protective Intelligence to learn more.

Learn More

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 also provides strategic consulting, multidimensional services, education and thought leadership for safety and security professionals at major corporations via its Center for Protective Intelligence.

To learn more about Ontic's Protective Intelligence Platform, contact us at info@ontic.co

ONTIC®