ONTIC®

Whitepaper

Continuous Monitoring in the Intelligence Cycle

Embracing an always-on security approach - By Thomas Kopecky

Now more than ever, we have heard about continuous monitoring taking place in virtually every segment of security. It has been adopted in Corporate Security, Supply Chain Management, and Executive Protection, as well as Vendor Management and Insider Threat programs. The practice of continuous monitoring is relied upon by many to detect and assess threats. This isn't because of intuition or chance — experience has demonstrated that it works.

What is continuous monitoring?

Continuous monitoring is the "always-on" engine of the security intelligence gathering workflow that does exactly what it says. You take a set of "knowns" (such as PII, online behavior, or recent litigation), and then utilize various tools to monitor 24/7 for changes, or potential indicators of threats. Alert rules are set so when something of importance either occurs or changes, you and your team are notified immediately so that proper action can be taken to assess the new information and consider it in decision making.

Why is continuous monitoring needed?

The datasets available are as unique as the objectives of the various security teams using them. While many of the groups referenced above work in silos across the organization, they share an overlapping goal — *to keep people and assets safe.* Human brain power and grit can only process so much before burnout, as the mountain of data to monitor is far too great.

Rather than requiring teams to passively learn or manually search for new information, continuous monitoring allows teams to be proactive. Risks and potential threats are uncovered earlier — often as soon as the risky behavior occurs. With continuous monitoring, a scalable plan requires the right technology for it to work.

> *
>
> *The ability to be proactive — identifying factors that indicate an escalation of threat or risk — is not a one-time task. Rather, it is an always-on approach that enables detection of even the slightest deviations from a baseline.*

Putting continuous monitoring into practice: Four corporate security scenarios

Given my experience working in the security intelligence world, I'll share several scenarios that typically benefit from the use of continuous monitoring.

1. Insider Threat

Across all organizations, there are teams of employees working on sensitive projects. They have access to business financial accounts, intellectual property, and other confidential business information. It's critical for these employees to be aware of financial difficulties, new arrests, and even adverse news that might precede similar situations. It's critical to be able to proactively identify events in an individual's life that might influence malicious behavior toward your organization.

A 2020 report from the Association of Certified Fraud Examiners showed that internal threats detected through active monitoring resulted in the lowest median dollar loss per event out of all possible detection sources. *Nearly all internal fraud cases tend to start off the same way — where the employee perceives that their actions are justified, then (incrementally) their fraud grows increasingly bold over time.*

2. Brand and Reputation Protection

It's no surprise that continuous monitoring to protect a brand's reputation is a prudent practice, as these threats can evolve into threats to people and property. It often takes a crisis or inflection point to help organizations see the value in monitoring for threats to the brand via online media, and continuous monitoring allows teams to stay ahead of adverse news headlines.

Protecting Employee Safety and Brand in a Retail Environment

A customer goes into a Fortune 500 retail store to purchase an item, and the sales associate refuses to serve them because they were not wearing a mask — a requirement for all customers. This situation resulted in the customer going to social and news media to start a crusade against the individual sales associate (with the company name associated), which included doxing.

A follow-up investigation revealed that the customer had an extensive history of civil litigation and a criminal history.

In this case, being proactive with monitoring threats to a brand directly translated into an immediate assessment of a threat and enhanced protective measures for an employee's safety.

3. Executive Protection

For executive protection teams managing a series of active threat cases, continuous monitoring is critical. The biggest gap we've found is that colleagues in the industry tend to be less aware of solutions relating to arrest and incarceration data and public records.

Thinking Beyond a Single Point in Time

A person of interest tried to make contact with your principal because he wanted to solve a business dispute. Next, you conducted an investigation and assessment of that individual, at that single point in time.

But how do you know if additional threat indicators, such as those relating to arrests, become available in the future?

You might conduct criminal record searches at the county court level every 30 or 60 days to see if anything changes, but this would be a time consuming and costly process.

On the other hand, you might use arrest and incarceration data providers to get alerts for person of interest (POI) activity.

Given the length of time between initial arrest and final adjudication, arrest alerts often surface 6-12 months prior to the record appearing in a reoccurring background check. *This type of data can inform us about activities that are indicative of potential violent behavior, as well as the physical location of the POI.* For example, are they in proximity to the principal or their family?

4. Contractor and Vendor Management

For teams large and small, vendor management can be a monumental task. Consider how many vendors a team at a static location may interact with on a daily basis. Next, consider vendor management for an enterprise that is built upon contracted service providers. For them, it is crucial for reducing liability and preventing service interruption. *When every vendor and contractor is an extension of the company, continuous monitoring becomes even more important for far-reaching, global brands.*

The Value of Real-Time Notifications

Throughout 2020, we observed a significant ramp-up of continuous monitoring in Last Mile Driver and Delivery Programs. With the proper program in place, an enterprise can effectively manage a wide array of issues involving conflicts of interest, violations of the company's internal policies, and safety for the end customers.

Imagine being updated in real time when a contracting company:

- Declares bankruptcy
- Loses authority to operate in a given state
- Is indicted on federal fraud charges
- Has a driver arrested for a DUI, or other criminal activity

This technology for contractor and vendor management is in its infancy, but we predict that in the near future it will be the backbone for corporate security programs to protect their customers and their reputations.

Planning your continuous monitoring program

When we look at these four scenarios, we can start to see a pattern of what is required. Here are three steps to take when developing your continuous monitoring program.

Of course, these recommendations are not an authoritative framework, and they should be customized based on the creativity and culture of your security team.

Steps for Program Development

1 Define objectives

At the most basic level we are trying to protect assets, but there are a range of highly specific pre-incident indicators of threats that different teams use depending on their focus areas.

2 Determine what data points can be monitored

This is where every business needs to rely on the advice of counsel and stakeholders in order to work within the boundaries of what is consistent with the organization's risk appetite. Consider what is legal, compliant, and acceptable, as well as what solutions will be used to monitor the necessary information.

3 Configure alerts and workflow

It's important that the right information goes to the right person at the right time. When teams aren't notified in a timely manner, minutes (and even seconds) can result in unfortunate circumstances.

Time-Sensitive Data Points

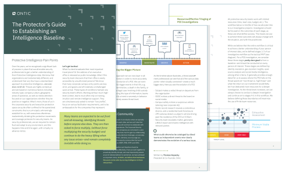
Two common examples of data points that need to be continuously monitored:

- CONFIDENTIAL BUSINESS INFORMATION SHARED
- UNAUTHORIZED ACCESS TO SENSITIVE AREAS

Continuous monitoring **is** protective intelligence

In a majority of instances, you can simply replace “continuous monitoring” with “protective intelligence” and you end up speaking the same language. Sure, certain nuances may not pair up perfectly, but the concept, workflow, and communication structures are nearly identical.

Continuous monitoring is a critical part of the protective intelligence workflow that supports early identification of factors that indicate escalations of threats to our assets. *When we enhance our program to rely more on smart systems integrated into our security infrastructure, we're able to arrive at insights almost in real time.* As this approach evolves, we expect that organizations will significantly increase their ability to more effectively protect their assets.



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

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

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.

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

ONTIC®