ONTIC

GUIDE

How to Take Your Investigations Program From Good to Great

Table of Contents

A New Level of Excellence

It's no longer enough for your corporate security investigations process to be good — it must be great. Most teams already have a solid investigative process, but evolving challenges in the security landscape require a new level of excellence.

If you play a role in corporate investigations, you understand the importance of thoroughness, accuracy, and speed in your work. You probably also feel the traditional methods and practices that once worked well now leave you falling behind threat activity and prone to vulnerabilities.

This guide is designed to help you elevate your investigative processes from good to best-in-class, ensuring you can quickly and effectively address the complexities of today's corporate security investigation challenges.

We'll explore strategies like modernizing your incident intake process, centralizing workflows to enhance collaboration, and getting actionable with the metrics you track. By elevating your processes, you not only improve the outcomes of your program but also position your team as an essential player in the overall operations of your enterprise.

Assessing Your Investigation Process

By nature, investigative work is unpredictable and multifaceted. It can be tempting to dismiss difficulties that arise as inherent to the complexity of the job — but it's crucial to identify and understand the specific challenges that may be hindering your progress. By pinpointing these issues, you can implement more effective strategies and improve the overall efficiency of your investigations.

Here are four red flags to look for in your investigative process:

Each member of your team follows their own process

If your metrics reveal that crucial investigative steps are being skipped, it may signal a workflow breakdown. For instance, some analysts might not thoroughly gather background information or research OSINT. Alternatively, your team may not consistently triage new information to assess the need for further investigation.

Onboarding new team members is challenging

Does the work required to onboard a new analyst outweigh the benefits of growing your team? This could signal that you lack clear workflow and documentation guidelines. This requires you to put in more time and effort training new analysts, which leads to longer onboarding periods and stunted scalability.

You're unable to step back and see the full picture

If you feel like you're constantly working to piece together disconnected data related to any given case, this typically signals a problem. It means you're using disparate systems that prevent holistic visibility. An inability to see the full picture can become an even deeper problem as the threat landscape evolves — for example, are you able to adapt your intelligence-gathering process as alternative social media platforms have emerged?

You're reactive more often than you're proactive

Do you find yourself reacting to incidents more often than proactively preventing them? Do you feel like you're always so behind that you can't analyze your metrics and adjust your processes accordingly? An inability to proirize elevating your program is a clear sign that your current approach may need adjustment.

If any of these red flags sound familiar, it may be time to adjust your processes. Doing so can improve the outcomes of your investigative work and position your team for long-term growth and scalability.

7 Steps for Taking Investigations From Good to Great

Even good investigative processes are vulnerable to blind spots today. No matter how hard your team works or how diligent your investigators are, your team likely still lacks the full picture for most investigations — especially if the red flags above feel familiar. You might also feel overwhelmed by threat signals or struggle to execute investigations quickly enough to keep pace with the speed of business.

Take these seven steps to elevate your investigative process from good to great.

01 Create a Connected Path for Incident Intake

02 Set Clear Incident Triage Rules

03 Define Standard Policies and Procedures

04 Remove Team Silos and Facilitate Collaboration

05 Integrate With Research Sources and Other Critical Systems

06 Improve Adoption of Your Case Management Solution

07 Establish Actionable Reporting Processes

Create a Connected Path for Incident Intake

★★★

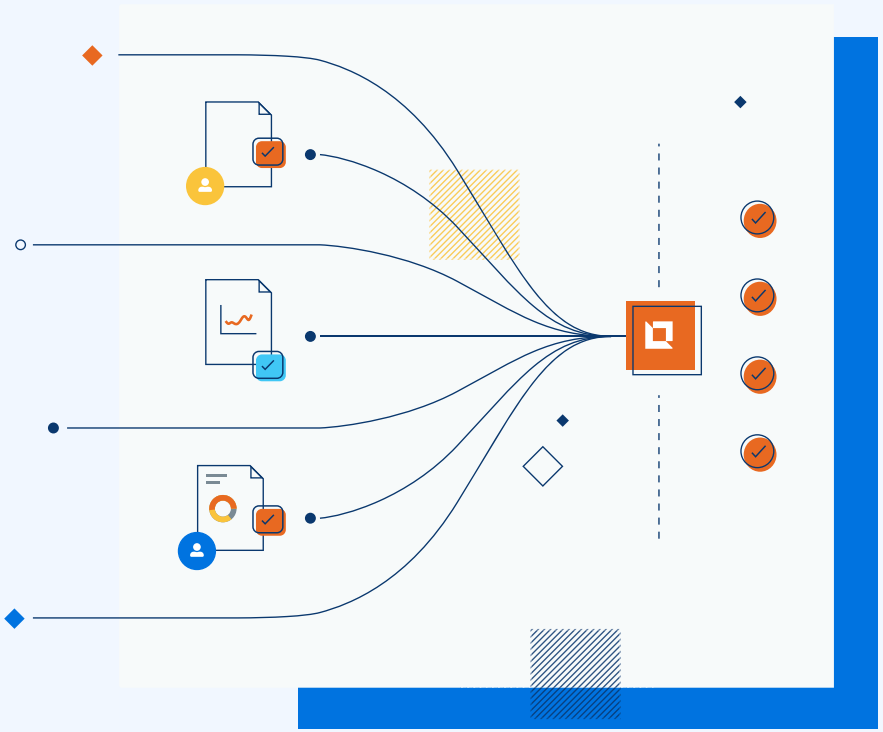
GOOD

You use basic intake forms created in Google or a generic form builder

★★★★★

GREAT

You use custom intake forms that connect with your central investigations system



A good incident intake process today typically involves standardized forms for stakeholders across the organization to log incidents. You might use templates in Google Docs, Google Forms, or a more advanced tool to build custom forms like AirTable.

Using digital forms for intake is an improvement over email or paper forms. Still, if these forms are disconnected from your case management workflow, they can hinder your investigative process by wasting time through manual data entry, increasing the risk of human error, and causing a lack of coordination as incident submissions might not be visible to everyone on your team.

Security teams with best-in-class incident intake processes fully integrate incident forms with their case management system. With a direct integration, you can create 1:1 mapping from the intake form to your investigation workflow — saving time, reducing error, and empowering your team to act fast.

Client Spotlight

meijer

Using custom incident reporting forms helped supermarket chain Meijer manage an increasing case volume across more than 400 locations, distribution centers, and offices.

Before modernizing their incident intake forms, the team relied on templated documents to log incidents. While this was manageable at first, over time, the team found they were missing critical context across incidents, and the information they did have felt disconnected and unorganized.

After moving to custom incident intake forms that included required fields and specific answer values, the team eliminated the need to contact store leaders to collect specific information. Meijer can now better manage increasing case volumes, and the field team can easily report incidents, ultimately closing awareness gaps.

Read the Full Story

Set Clear Incident Triage Rules

★★★

GOOD

You have protocols in place for investigating and monitoring anything and everything

★★★★★

GREAT

You prioritize what's most important with clear triage rules system

Good investigators want to be aware of anything that might become a threat. You likely have a protocol that requires thoroughly researching and examining any incident submitted — even if it's something relatively minor, like an open door. This is important because it ensures that your team has eyes on everything that might pose a risk to your organization.

However, human beings can only process so much information at once. With so many incidents to investigate and, in some cases, thousands of persons of interest to monitor at a time, you need a more efficient way to triage and prioritize incidents. Without clear triage rules, you risk:

- Missing threats due to signal overload
- Spending too much time on the wrong incidents
- Losing sight of current investigations when new, priority incidents happen

What does this look like in practice? Start with a flowchart that outlines who is responsible for reviewing incident intake (maybe all new incidents are routed to your GSOC) and determine the subsequent steps. Depending on the type of incident, you might address it without creating an investigation or automatically create an investigation requiring additional research. You might also define when a cross-functional group must meet to brief on the situation and decide the next steps together.

Great investigative teams take this even further by leveraging case management solutions that allow you to set up automation and alerts that trigger the next steps and streamline work. By leveraging technology to reduce manual work, you can focus your immediate attention on more pressing incidents without losing momentum on existing cases.

There are no right or wrong rules for great incident triage. What matters is clearly defining and communicating a process that helps you prioritize the most severe and urgent threats.

Tip From the Field

One Ontic client leverages incidents as a dispatch tool. The team set up automation to create and assign tasks based on the type of incident created. Now, tasks are automatically assigned, and the work can be done immediately. This eliminates manual administrative work at the onset of the incident, and urgent work can be completed much sooner.

Define Standard Policies and Procedures

★★★

GOOD

You have loosely defined processes for investigation workflows and documentation

★★★★★

GREAT

You have standard policies and procedures that guide end-to-end case management

Most corporate investigation teams follow loose workflows and documentation rules. While these guidelines can help you stay on track while giving your team some flexibility, a lack of standardization often leads to inconsistencies. Team members follow their own rules and use their preferred tools (like Jira or Asana) over time, leading to silos, missed threats, and a lack of centralized visibility.

To take your workflows from good to great, create a standard operating procedure (SOP). Start by defining your policy (what are you going to do?) and your procedures (how are you going to do it?). This serves as a step-by-step guide to conducting investigations, enabling more thorough research, better link analysis between incidents and cases, and accurate data collection for security metrics.

Standard policies also make scaling your team easier. With clear rules for workflows and data collection, new investigators can learn quickly and contribute sooner.

Tip From the Field

One Ontic client sets requirements for how much time should be spent on each step of an investigation to guide the team in their work. By completing all of the work within Ontic, it's easy for the team to tell if steps took longer than anticipated (they even set up alerts for when steps take too long). This degree of visibility keeps the large, multi-location team accountable for following through on tasks and completing workflows as planned.

Remove Team Silos and Facilitate Collaboration

★★★
GOOD
You involve the necessary teams across the organization to inform cases where needed

★★★★★
GREAT
You proactively facilitate ongoing cross-functional collaboration

Even if you have a process in place for bringing the right teams (like legal, HR, or cyber) into your investigative process, without ongoing collaboration, your relationship with non-security teams will always be reactive, and you'll only ever have an incomplete picture of the threat at hand. Great investigations require more than just a snapshot in time.

Centralized documentation leads to fewer blind spots and faster case resolution, separating great processes from good ones.

Breaking down silos starts with building both relationships and processes. This involves regular briefings with corporate security, HR, legal, and cybersecurity leaders to keep everyone informed about ongoing investigations and proactively solicit support. It's also important to use these meetings to check in on daily activities, like expected performance plans or terminations, to cross-functionally coordinate mitigation efforts.

While in-person connection and relationship-building will always be crucial, the best corporate investigative teams also remove technology silos by leveraging centralized case management systems that everyone can access and contribute to. Centralized documentation leads to fewer blind spots and faster case resolution, separating great processes from good ones.

Tip From the Field

Disengaged employees are more likely to put a company at risk. But avoiding these potential threats is tough when you lack seamless collaboration with HR. That's why one Ontic client integrated Ontic with their HR system, Workday.

With this integration, they could set up notifications for when an employee is marked as disengaged (maybe they put in a two-week notice or were placed on a performance improvement plan). By removing this silo, the team has a better idea of employees who might be disengaged and now proactively monitor for any threatening behavior.

Integrate With Research Sources and Other Critical Systems

★★★

GOOD

You're leveraging a case management platform that requires manually adding research findings to investigations

★★★★★

GREAT

You leverage a case management solution that fully integrates with a range of research tools and other relevant systems

Many corporate security teams use off-the-shelf case management platforms built specifically to facilitate investigative work. If this sounds familiar, you probably also have access to some integrations with data sources that automatically bring research into the cases you're managing in the platform.

The problem is that many simple case management solutions — even those with some integrations into research sources — lack the full integration capabilities that bring that data directly into the part of the platform where you're managing incidents, investigations, or entity profiles. You must still manually add information (like social media activity, public court records, etc.) to your case documentation. Platforms like these are nothing more than a small step up from pieced-together systems of generic tools.

You need comprehensive data to elevate your processes to best-in-class, which means your investigations platform needs to connect with a breadth of data sources, including OSINT, the dark web, social media, and public records data. With a full range of integrations into research sources, you can accelerate the process of creating the fullest possible picture of an investigation.

Additional Integrations to Consider

Great investigative teams leverage solutions that integrate with a range of critical systems that can help aid investigations, including:

- HR systems
- Access control systems
- Visitor management systems
- Customer relationship management systems
- Form submission tools (like AirTable)
- Workflow tools (like Slack)

Client Spotlight

One Fortune 100 consumer packaged goods company used Ontic's integrated research capabilities to dramatically reduce time spent on investigative research. Before improving their integration capabilities, the team would spend 8+ hours assembling information for an investigation (with a heavy reliance on Google search). With Ontic's integrated research tools, the team can create a comprehensive profile for persons of interest in just 30 minutes.

Read the Full Story

Improve Adoption of Your Case Management Solution

★★★

GOOD

You have a purpose-built case management solution in place, but your team doesn't use it consistently

★★★★★

GREAT

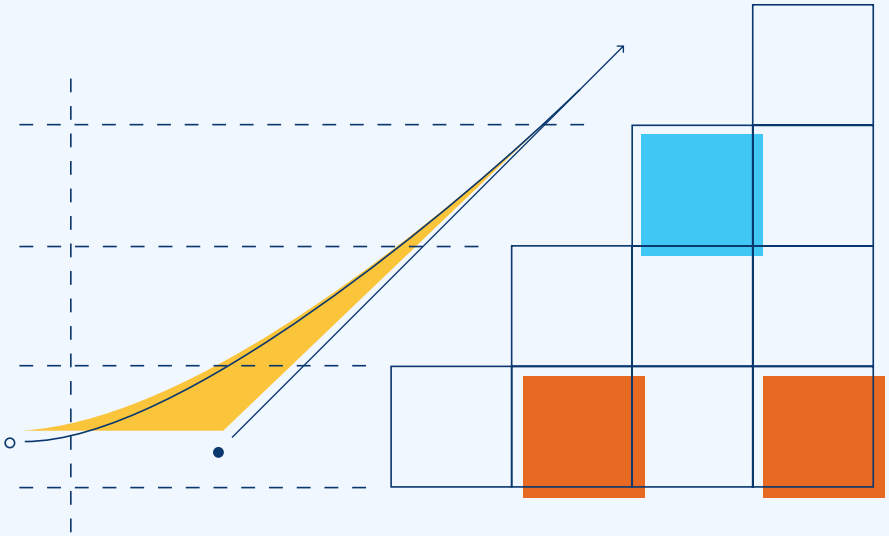
Everyone contributing to investigative work — within and outside of your team — has bought into the value of your case management solution

Great investigative teams don't stop after implementing a purpose-built case management system; they work to ensure consistent and ongoing use across the organization. Without cross-functional buy-in, the tool becomes as ineffective as disparate or home-grown systems, leading to the same blind spots you faced before adopting it.

As noted earlier, good corporate investigation teams use purpose-built case management solutions. However, many teams struggle to get everyone involved in investigative work to use the system. To elevate your process, you must ensure consistent cross-functional use.

Achieving this requires more than just a mandate. Start by uncovering why people aren't using the system. They might lack confidence in their skills, resist change due to the complexity of their current workflows, or fail to see the solution's value.

Once you identify the reasons, implement a tailored plan of action. This likely starts with better training (either internally-led training or vendor programs like Ontic Academy) or leveraging your vendor's implementation team to migrate existing data and workflows into the system. Improving adoption might also require a deeper explanation of why the solution was implemented and the long-term value it will provide.



Gap Analysis Model

If you need to improve the adoption of your case management system, you can use the **Gap Analysis Model** to create a plan:

Define your ideal use case Outline exactly how your organization should use the system to maximize efficiency, referencing the policies and procedures you created in Step 3 of this guide.	☐
Benchmark your current use case Interview and shadow your team members and cross-functional stakeholders to understand their current system usage. Aim to get a first-hand look at the pain points preventing them from reaching the ideal state.	☐
Analyze gap data Compare the ideal state with the current state, looking for patterns and similarities across users.	☐
Create a cadence of accountability Determine several hypotheses about why the system isn't being adopted, verify those hypotheses with your users, and develop an action plan for closing the gap.	☐

Establish Actionable Reporting Processes

★★★

GOOD

You track a wide range of metrics and regularly report on progress

★★★★★

GREAT

You set goals and track leading metrics that help you illustrate your progress toward those goals

If you're like most leading corporate security teams today, you probably track a range of metrics like incident volume and case resolution rate. You might even have a purpose-built tool that helps you manage this data and monitor it over time.

While it's good to have a baseline understanding of your key metrics, like speed to resolve cases, this data is not useful unless you plan to act on it. Why are you tracking this metric? What is your goal? What are you planning to do to achieve that goal? You want to avoid tracking metrics just to track metrics.

Best-in-class investigative teams first determine what metrics they care about most (this will differ based on your organization's priorities). They also know what "great" looks like and exactly what it will take to achieve "great." The best teams do this with ongoing dashboards that show real-time data and are integrated with the team's day-to-day work.

Not only does tracking the right metrics and setting actionable goals help you improve your program's overall effectiveness, but it's also a great way to gain influence in your organization. When you can show real progress and what you're doing to achieve your goals, getting the support you need to elevate and invest in your work is easier.

Client Spotlight

UNFI

Metrics and reporting can also help prove the value of your work. United Natural Foods, Inc. demonstrated progress against metrics to show recovery savings of $4.5M in 2023, which helped them make the case for gaining additional funding for their security program.

> "We had a four-person corporate security and asset protection team responsible for tracking an increase in workplace violence, fraud, and theft-related incidents at more than 50 of our distribution centers and multiple corporate office locations. Using Ontic for our research, investigation, and case management needs has saved us millions in recovery and cost avoidance and has helped our team grow to 16 because we can consistently show how our work mitigates concerns before events occur."

— Steve Slyter, Sr. Director of Corporate Security and Asset Protection at United Natural Foods, Inc.

Read the Full Story

4 Disciplines of Execution

Consider the **4 Disciplines of Execution** when setting your goals and planning the metrics you'll track to show progress to:

Focus on the wildly important Narrow down your goals — and the necessary metrics to track progress — to what matters most to your organization.	☐
Act on the lead measures Identify and act on your leading indicators (metrics that can help predict future progress).	☐
Keep a compelling scoreboard Visualize your metrics in a dashboard or scorecard that clearly shows progress toward your goals.	☐
Create a cadence of accountability Regularly discuss progress and failures with your team and course-correct when necessary.	☐

The Outcomes of Elevated Investigative Processes

Making these changes can be hard in an enterprise organization, but even small improvements over time can lead to significant benefits down the line, including:

Enhanced safety

By centralizing research related to an investigation, you can better assess threats and make cohesive and informed decisions, reducing the impact of incidents and keeping your people and assets safer.

Cost savings

Integrating and streamlining various security tools into a centralized platform eliminates redundant tools and, thus, costs. Enhanced investigative capabilities lead to quicker incident resolution and mitigation, decreasing the overall impact and associated costs (like a loss of property, reduction of productivity, or lawsuits).

Time savings

Automating repetitive tasks and processes reduces manual workload — particularly for ongoing case management — freeing up time for your team to focus on incidents that require immediate attention. By centralizing your investigative work, you can also speed up the time it takes to resolve cases and reduce coordination time between disparate systems.

Elevated perception of security

Demonstrated success and efficiency with clear goals and reporting can help you secure buy-in and budget allocation from leadership — ultimately fostering a culture of security awareness and commitment throughout the organization.

Ontic: The End-to-End Investigations Solution Designed for Today

Ontic's Incidents, Investigations, and Case Management solution helps remove silos, create and manage threat visibility, and move at the speed of business. It gives your team the capabilities needed to take your investigative processes from good to great, including:

Flexible configuration

Customize workflows to suit your industry, location, compliance requirements, and other specific needs.

Centralized workflows

Utilize centralized workflows and in-platform chat for collaboration across departments and teams.

Connected incident intake

Create custom intake forms with required fields to streamline the information gathering process for investigations.

Continuous case monitoring

Monitor for new information and set alerts even after cases close, enabling trend analysis, pattern recognition, and tracking of costs and recovery.

Metrics and reporting

Generate reports with standard and custom metrics, share them securely, and automate recurring updates.

Integrations with other tools

Connect to real-time and historical public records, internal systems, external systems, and active threat actor databases.

ONTIC

Request a demo to see Ontic in action

Schedule Now