ONTIC

An Inside Look at a Corporate Investigation

If you're not a security professional, you likely don't see what really happens behind the scenes of a corporate security investigation. The steps below offer a simplified look at how a case is handled effectively — helping you understand just how much goes into getting it right.

7 phases of a typical corporate security investigation

1. Set the foundation before a case emerges

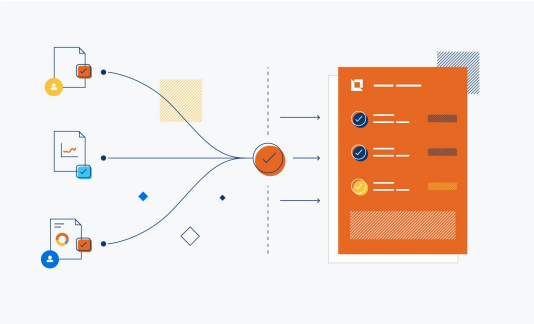
- **Define what needs protection:** People (employees, executives, customers), assets (facilities, equipment, inventory), and information.
- **Centralize and integrate data sources:** From access control and HR systems to CRM, surveillance feeds, cyber alerts, and more.
- **Clarify roles and responsibilities:** Determine who can access, create, or close reports; set clear notification protocols by incident type.
- **Update policies and workflows:** Make sure documentation, privacy, and escalation policies reflect how your business operates (remote vs. in-office, multi-site, etc.).

Potential slowdown

Without a centralized system for threat actor details and case information, security teams are left with spreadsheets, emails, and siloed systems, making it hard for the right stakeholders to access the information, slowing investigations, and increasing the risk of missed threats.

2. Detect and monitor early signals

- **Automate monitoring for anomalies:** Use connected systems to detect physical access anomalies, social media threats, policy violations, and unusual behavior.
- **Define triage workflows:** Assess whether each concern meets the threshold for formal investigation, and assign urgency levels.



Potential slowdown

Using manual, pieced-together systems to monitor and prioritize signals increases the risk of missed warning signs, delayed response, and focusing on the wrong threats due to an incomplete understanding of the full threat landscape.

3. Launch the investigation

- **Initiate workflows and assign a lead:** Use a centralized platform to begin the process, document activity, and notify stakeholders (HR, Legal, etc.).
- **Identify the person(s) of interest:** Use internal records, surveillance, and behavior analysis to determine who may be involved.
- **Gather foundational facts:** Document the "who, what, when, and where" — ensuring all relevant context is captured.

4. Collect, interview, and analyze

- **Conduct structured interviews:** Talk to employees, managers, and other witnesses who may have knowledge of the incident.
- **Investigate historical and external data:** When appropriate, look into prior incidents, third-party intelligence, and community sources.
- **Interview the subject of concern:** This may be handled by HR, Legal, or Security, depending on severity and context.
- **Analyze patterns and related incidents:** Use past investigations and behavioral trends to identify risks or links.
- **Continuously monitor threat actors:** Even if you've resolved a situation involving a potential threat actor, it's essential to keep monitoring their behavior to proactively identify any signs of escalation.

Potential slowdown

Getting a complete view of a case — and maintaining ongoing threat actor monitoring — is nearly impossible when research and workflows are disconnected. This often leads to time-consuming manual searches across multiple sources, overlooked critical details, and delayed responses that increase risk.

5. Assess threat level and mitigation options

- **Use a formal risk or threat framework:** Determine if there is a pathway to harm or material impact.
- **Document and act on findings:** Implement security, HR, or operational strategies to contain or mitigate risk.
- **Notify internal leaders and stakeholders:** Expand communications based on severity, including media relations, legal, or external partners as needed.

Potential slowdown

When case documentation is spread across siloed systems, getting the right information to the right people is challenging. This slows response and makes it harder to contain risk. A centralized system with controlled access helps ensure clarity, speed, and coordination.

6. Close the case (with the right caveats)

- **Document everything:** Ensure every step is centrally recorded and accessible to those with appropriate permissions.
- **Set closure conditions:** Whether mitigated, unresolved, or referred externally, make sure closure reflects current knowledge — and plan to reassess if new data emerges.

7. Learn, evaluate, and improve

- **Track investigation metrics:** Analyze resolution rates, incident types, timelines, and team performance.
- **Conduct after-action reviews:** Capture lessons learned and update protocols accordingly.
- **Preserve institutional knowledge:** Build dashboards and documentation practices that scale and adapt to emerging threats.

Potential slowdown

Without a system to track metrics and preserve case information, historical data gets buried in siloed systems and spreadsheets, making it hard for security teams to learn, improve, and scale over time.

ONTIC

Doesn’t cybersecurity have a tool to manage this?

Corporate investigations are too complex to manage with generic cybersecurity tools or project management platforms. A purpose-built investigation solution brings together intelligence, threat actor data, and critical case information in one centralized location, so nothing falls through the cracks.

Explicitly designed for investigative workflows, modern security platforms help teams connect the dots faster, maintain clear audit trails, and act decisively. Unlike pieced-together or homegrown solutions, the right tools eliminate silos and inefficiencies while ensuring that only the appropriate stakeholders have access to key data. This gives you a clear, unified view of threats — and the peace of mind that case information is properly controlled.

Who benefits from better investigations?

Human Resources

Receives support in addressing employee issues early, preventing them from escalating into productivity losses or, in the worst cases, violence.

Legal

Benefits from clear documentation, defensible processes, and early risk detection.

Finance

Avoids potential legal settlements, operational disruption, and reputational damage.

Executive Leadership

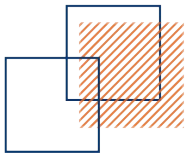
Gains confidence in achieving business goals by resolving incidents that threaten financial losses or growth.

ONTIC

Ontic unifies research and investigations for stronger corporate case management

Ontic is the only solution purpose-built to meet the complex needs of today's corporate investigations teams. By integrating research and investigations in one platform, Ontic gives security teams a complete picture — so they can close cases faster, respond more effectively, and better protect the organization.

With Ontic, security teams can leverage:

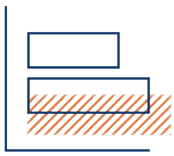


Integrations with other tools

- Real-time and historical public records research
- Connections to internal and external systems
- Active threat actor database

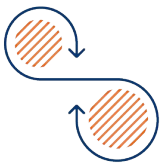
Connected incident intake

- Incident triage and tracking from any source
- Customized setup to match business processes
- Automated incident to investigation transition



Centralized workflows

- Automated activity timelines and analyst notes
- Secure storage of documents, details, and associations
- Task assignment, notifications, and chat



Continuous case monitoring

- Automatic scanning and alerts for new data
- Trend analysis and pattern recognition
- Cost and recovery tracking

See Ontic in action