How to Run Effective Insider Threat Investigations

Protecting employees, assets, and intellectual property against the negligent, accidental, and malicious actions of insiders is a priority for organizations. With the right tools and processes in place, insider threat teams can work to support continuous monitoring, recognize potential threat indicators, take proactive action, streamline investigations, and gain insights to support insider threat programs.

Leverage the following checklist to ensure you have a comprehensive investigative process in place.

Pre-Incident

Establish systems and processes

Ensure teams have the right tools in place to proactively screen and monitor for insider threat risk and establish processes to mitigate risks, reduce response times, and create standardization in an investigation workflow across the team.

Conduct a risk assessment to define critical assets for protection Sensitive or protected data, intellectual property (IP), credentials, corporate devices, systems, secure facilities, high value individuals	☐
Map information sources and resources Individual teams sources, disparate information streams, intelligence capabilities	☐
Consolidate connected systems data Vehicle, visitor management systems (VMS), access control, CRM, case management (past and current), legacy systems (past and current), legacy systems	☐
Centralize research and monitoring tools Criminal and civil records, OSINT, social media, dark web, local news reports, localized crime data	☐
Review and update insider threat programs and policies Pre-employment background checks, continuous review cycles, post-termination monitoring, define trigger points, establish escalation paths, and establish privacy controls	☐
Define tripwires Grievances (internal and external), lawsuits, terminations, policy violations, disengaged employees, reported disruptive or concerning behavior, unusual visitor requests, unusual physical or digital access requests, negative online commentary	☐
Set up notification flows based on threat type or urgency level Corporate security, HR, legal, third-party experts, PR, local law enforcement	☐

Continued on next page

Establish reporting protocols If not through the Insider Threat Working Group, how are issues documented, reported, and (if necessary) briefed to decision makers?	☐
Select conditions for report status or closure and length of storage Inactive, referred to police, threat mitigated, unresolved (most report closures will be 'soft' based on the information at the time of closure)	☐

Monitor and identify potential concerns

By establishing situational awareness based on systems and tools, teams can monitor data sources for pre-incident indicators and/or behaviors of concern.

Continuously monitor connected systems for sources of threatening or concerning behavior Localized crime trends, activist group activity, executive name searches, social media activity, updates to historical cases that trigger a pattern alert	☐
Monitor unusual alerts from connected systems License plate recognition, access controls, visitor management check-ins	☐
Review alerts from adjacent systems Intrusion detection, endpoint protection, cyber threat intelligence, fraud detection	☐
Identify potential threat indicators Grievances (internal, external), insider threat awareness feedback programs, connected system alerts, reports (HR, supervisors), casing/surveillance, law enforcement reports	☐
Identify point of contact (POC) outside of your organization Local, state, and federal law enforcement, associations, or partner organizations	☐
If a potential threat is identified, trigger escalation and mitigation plans, including notifying and standing up the Insider Threat Working Group	☐

TIP: Information stemming from an insider threat investigation should be made available only to the Insider Risk Working Group. As a critical risk function, it's a key task for this group to decide actions and communicate activity to the appropriate places in an organization.

Threat Intake and Investigation

Capture and prioritize the threat

With the aid of the established protocols, processes, and systems, risk based teams can quickly capture the concerns, enabling notification to appropriate stakeholders for further inquiry/investigation, as needed.

Capture the basic details What is the concern, how was it identified, who is the person of interest (POI), when and where did it occur	☐
Set incident priority based on threat level or incident severity	☐
Coordinate appropriate response actions with stakeholders and partners, both internally and externally; record response, if any	☐
Conduct damage assessment and, as appropriate, engage internal or third-party experts IT, engineers, Threat Managers	☐

Continued on next page

Take immediate containment actions in consideration of physical, informational, or digital risk	☐
Assign lead investigator and/or analyst and initiate investigation workflow	☐

Action investigation steps

Leveraging a consolidated platform for documentation, investigation, and collaboration, teams can accelerate detailed investigations to scope, document, and resolve the incident.

Collect relevant information from individuals to understand the concern, the timeline in which it occurred, who was impacted and what parts of the business were disrupted, if any Interview the person who reported the incident, manager/co-workers of the POI	☐
Collect supporting information to identify a POI, examine their history, establish a timeline of the incident Prior performance history, criminal history, civil judgments (if authorized and legal), social media, dark web, local and third-party surveillance footage (e.g. building security), email, text or audio information, access controls, surveillance, travel patterns	☐
Interview the POI Conducted by either HR, legal, security, police	☐
Analyze previously documented incidents, investigations or crime data to determine if there are any connections or related concerns	☐
Expand notifications as appropriate to internal and external stakeholders Building security, media relations	☐
Log follow up requirements and communications Each dispatch, assignment, activity, piece of evidence, or communication between individuals, across functions, or with external third parties	☐
Take any appropriate management actions based on security, HR, and risk management input to contain or mitigate the threat	☐
Take necessary legal and administration actions Work with legal and/or police for trespass warnings and protection orders; limit network activity, lockdown information flows	☐
Re-evaluate incident priority based on threat level or incident severity	☐
Update findings and report to the organization's Insider Threat Working Group What has been uncovered, immediate threats, potential risks; seek guidance, as appropriate	☐
Regularly review and update case disposition status (Open, Closed, Ongoing)	☐

Post-Investigation

Analyze data, metrics and trends

Teams with robust metrics and dashboards can analyze threat trends and data to inform preparation and response activities, preserve knowledge, and evolve investigation best practices.

Track investigation data across a wide variety of variables Case disposition status, case resolution rate, threat type, personnel, location	☐
Build custom reports against any collected data field or emerging threat signal to gain investigation insights	☐
Define document retention period to ensure you're legally compliant and to guard against re-emergence of issues	☐
Conduct an after action review What happened, what was learned, what can be done to improve	☐
Set up evaluation dates Trigger a threat review on significant dates (e.g. termination anniversary)	☐