ONTIC

CHECKLIST

Investigating Workplace Threats at Manufacturing Companies

Manufacturing companies may face a range of external and insider threats, including threats of workplace violence, sabotage of production lines, and theft of proprietary information. This checklist is designed to help security teams at manufacturers establish program components, processes, and tools to systematically investigate, mitigate, and track these threats to enhance the security of their employees, facilities, and operations.

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

Set Up In Advance

Establish program components, processes, and tools to support threat investigations

Ensure teams have the right systems in place to proactively monitor for behaviors of concern and establish processes to identify concerns, gather relevant information, assess the concern, mitigate risks, manage/intervene the person of concern, and create standardization in an investigation workflow across the team.

Define who/what needs protection Executives, employees, facilities, critical assets (proprietary schematics, intellectual property), other assets	□
Consolidate data from various systems Vehicle, visitor management systems (VMS), access control, CRM, case management (past and current)	□
Centralize research and monitoring tools Criminal, civil records, OSINT, social media, dark web, local news reports, localized crime data	□
Create and authorize a multi-disciplinary Threat Management Team Representatives from Security, HR, Legal Counsel, IT Security, EAP, or other mental health professional	□
Establish mechanisms for reporting threats and other concerning behavior Anonymous tip lines (by text, webpage, phone, app), identified points of contact in security, HR, EAP, etc.	□
Define triage processes to screen and prioritize reports of threats and other concerning behavior Determine the threshold for initiating a threat investigation or referring incidents to other departments	□
Set up notification flows based on incident type or urgency Corporate security, HR, legal, third-party experts, PR, police, or EHS	□

TIP: Sensitive data should be limited to those who have a true need-to-know, like executive protection and insider threats teams, unless certain at-risk conditions are met.

Continued on next page

Clarify who has the authority to read, write, share, or close a report	□
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)	□
Update policy/procedures for emergency situations	□
Provide training to all stakeholders about how and where to report concerns	□

Identify and monitor threats and other 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.

In the case of an imminent threat, follow internal policy and scripted dialogue for contacting police, then notify appropriate stakeholders.

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, HR reports	□
Review alerts from adjacent systems Intrusion detection, endpoint protection, cyber threat intelligence, fraud detection	□
Review other sources for behaviors of concern Grievances (internal, external), direct employee or guard observation, connected system alerts, reports (HR, supervisors, co-workers), reports of casing/surveillance, observed tailgating, outside sources (family, police)	□
Screen incident reports and alerts to determine if there is a need for further investigation	□

Intake and Investigation

Identify the person of interest (POI)

With the aid of the established systems and processes, teams can quickly capture and identify the person behind the threat, whether they're an insider or external threat actor.

Capture the basic who, what, when, and where details What is the concern, how was it identified, who is the victim/target/complainant, who is the POI, along with the when and where, if known	□
Screen the concern and determine if it meets the team threshold for investigation	□
Assign lead investigator and initiate investigation workflow	□

Continued on next page

Gather information about the reported concern and make an assessment

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

Collect supporting information to examine the POI's behavioral history, current concerning behavior, and any other information that could be beneficial for the team to know and understand 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	□
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, the potential victim(s)/target(s), manager of the victim and/or POI, or co-workers/others who may have information	□
Collect supporting information from external sources Law enforcement, mental health, community stakeholders	□
Analyze previously documented incidents, investigations, or crime data to determine if there are any connections or related concerns	□
Document all information gathered in a central platform	□
Involve the Threat Management Team to make the assessment – based on the information gathered and known at this time, does the person of concern pose a threat to themselves, others, or both? Utilize the Ontic Threat Assessment & Management workflow, WAVR-21 workflow, or other behavioral threat assessment processes to determine if the POI is on a pathway to violence, sabotage, or otherwise poses a threat	□
If your team uses a priority level to help classify threat level, assign priority level based on threat assessment	□

Built into the Ontic Platform, the Ontic Threat Assessment & Management workflow and WAVR-21 workflow help teams organize and analyze the information gathered to determine if someone is on a path to harm. These workflows add fidelity to your inquiry by showing that each concern is treated equally.

Intervene to manage the threat and reassess regularly

Implement any appropriate intervention strategies to reduce the threat posed, based on input from Threat Management Team and/or security, HR, mental health, and/or risk management professionals Explore intervention/management strategies available internally and externally	□
Notify leadership team and others as needed Building security, victims/targets, media relations, internal communications, any parties who need to know	□
Document management strategies implemented	□
Regularly monitor POI's behavior and reassess, and update priority level and management strategies as needed	□

When a case closes, always caveat it as "based on the information available at this time." Should new information become available, the team should reopen or continue the investigation.

Continued on next page

Post-Investigation

Analyze data, metrics, and trends

Teams with robust metrics and dashboards can analyze 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, incident 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. event anniversary)	□

Proactively evaluate behavior signals and investigate incidents to manage workplace threats at manufacturing companies

Ontic's Incidents, Investigations and Case Management solution is purpose built within an end-to-end threat management solution for early capture of concerning behavior signals, pre-incident indicatirs, and alerts from many sources to help security teams mitigate the risk of violence.

Learn More