ONTIC

CHECKLIST

How to Run Thorough Investigations on Threats to Executives

Protecting corporate executives and high net-worth individuals at the office, at home, on-the-go, and online is a top priority for businesses. With the right tools and processes in place, executive protection and close protection teams have anytime, anywhere access to proactively monitor for potential physical threats. This allows them to streamline investigations, take swift action to protect principals, and gain insights to support ongoing protection activities.

Leverage this checklist to ensure you have a comprehensive corporate investigation process in place.

Pre-Incident

Establish comprehensive systems and processes

Ensure teams have the right tools in place to proactively monitor and hunt for threats to executives and establish processes to mitigate threats, take swift and intentional action, and create standardization in an investigation workflow.

Define individuals and locations for protection CEO, board members, executives, critical employees, high value customers or partners, families	□
Define locations/boundaries for protection, if any handoff required Office buildings, parking lots, travel/private aircraft (FBOs), events, residence, estate, vacation homes, family office	□
Consolidate connected systems data Vehicle, visitor management systems (VMS), access control, CRM, case management (past and current)	□
Centralize research and monitoring tools Criminal and civil records, OSINT, social media, dark web, local news reports, localized crime data	□
Review and update policies to support intervention; define response processes	□
Define sources of concern Grievances (internal and external), lawsuits, sentiment analysis, business controversy, geo-political conditions, protection orders	□
Set up notification flows based on threat type or area of responsibility Corporate security, HR, legal, third-party experts, estate protection teams, family office, local law enforcement	□

Continued on next page

Clarify who has authority to read, write, share or close a report Executive protection details should be limited to those who have a true need-to-know, unless certain at-risk conditions are met	□
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 threats

By establishing a complete view of all known threats and continuous monitoring for unknown threats, teams can monitor data from multiple sources for early warnings before a threat escalates.

Monitor unusual alerts from connected systems License plate recognition, access controls, visitor management check-ins, observation cameras, social media for adverse intelligence	□
Continuously monitor for sources of threatening or concerning behavior Localized crime trends, custom searches (terminated employees, name searches, activist groups), a principal's online vulnerabilities, updates to other or historical cases that trigger a pattern alert	□
Monitor alerts from adjacent systems Intrusion detection, endpoint protection, cyber threat intelligence, fraud detection	□
Identify potential threat indicators/conduct pre-operational surveillance Grievances (internal, external), active persons of interest (POI) monitoring, connected system alerts, casing/surveillance, residential disturbances	□
Connect/coordinate with local police about any identified trends or concerns to ensure a coordinated action plan if an incident occurs	□
If a physical or cyber threat is identified, action mitigation strategies Escalate to corporate security/behavioral threat assessment management (BTAM), issue be on the lookout (BOLO), increase surveillance, notify front-line security and front-of-house staff, notify leadership team, notify external protection teams	□

Threat Intake and Investigation

Capture and assess the threat level

With the aid of the established systems and processes, teams can quickly capture the concerns and easily notify appropriate stakeholders for further inquiry/investigation, as needed.

Capture the basic who, what, when, and where details What is the concern, how was it identified, who could be impacted, is there a person of interest (POI), when and where did it occur	□
Coordinate with local police or FBI (if deemed appropriate); record response, if any Police incident number, intelligence learned	□
Assign lead investigator and/or analyst and initiate investigation workflow	□

Continued on next page

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

Conduct a threat assessment (as needed) to gauge the credibility of the threat and the likelihood of potential violence, if not urgent SIGMA and/or WAVR-21, threat assessment	□

Action investigation steps

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

Collect relevant information from individuals to understand the concern and identify a threat actor/POI Investigate known vehicular information, circulate photographs or video footage of the POI	□
If the POI is not identified, determine if the principal should be interviewed or observed for additional intelligence	□
If the POI is identified, collect and examine supporting evidence about the POI and their history Prior performance history, criminal history, civil judgments (if authorized and legal), access to weapons, mental health history, known associates, social media actions (pace and tempo), and email, text or audio information	□
Interview the POI or assess whether on-going surveillance is warranted (conducted by security or local LEO)	□
Analyze previously documented incidents, investigations, or local crime data to determine if there are any connections or related concerns	□
Issue a more detailed BOLO and log what actions should be taken if the POI is observed (who should be notified)	□
Log follow up requirements and communications Each dispatch, assignment, activity, piece of information, or communication between individuals, across functions, or with external third parties	□
Take any appropriate management actions based on principal, protection team, and estate team input to contain or mitigate the threat or increase countersurveillance	□
Work with legal and police for trespass warnings and protection orders	□
Set incident priority based on threat level or incident severity	□
Regularly review and update case disposition status (Open, Closed, Ongoing)	□

Post-Investigation

Analyze and report on data, metrics, and trends

Teams with robust metrics, high-quality reporting capabilities, and customized dashboards can analyze critical threat trends and data to inform preparation and response activities, preserve knowledge, and evolve the executive protection strategy.

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 on what happened, what was learned, what can be done to improve	□
Set up evaluation dates and trigger a threat review on significant dates (e.g. violent event anniversary)	□

Proactively detect, evaluate, and investigate threats against executives

Ontic's Incidents, Investigations and Case Management solution is the only software integrated with an end-to-end threat management platform to capture pre-incident indicators and alerts from any source to help security teams act on high-risk signals before they turn into targeted attacks.

Learn More