ONTIC®

Tipsheet

What Security Teams Miss by Only Relying on Social Media

BROUGHT TO YOU BY THE CENTER FOR PROTECTIVE INTELLIGENCE

In today's rapidly evolving and expanding threat landscape, the volume of data corporate security teams are dealing with has become unmanageable. There is more distraction, data, and disinformation, and knowing what to rely on can be challenging. While social media is a helpful tool during the investigative process, it is limiting when security teams depend on this information alone.

Here's some guidance on when to use social media, limitations to be aware of, and tips for how to leverage diverse data sources to generate more reliable insights.

How should corporate security teams factor social media into the larger investigation workflow?

TIP 01 SOCIAL MEDIA'S ROLE IN INVESTIGATIONS

- ✓ Quickly identifies possible threats and surfaces anomalies that need to be further investigated
- ✓ The tip of the iceberg that gives investigators hints for where to look next
- ✓ A small piece of the overall investigative process, lacks the ability to confidently resolve the identity behind the threat and gain deeper insights

What limits inherently exist that make social media hard for investigators to leverage?

TIP 02 ROADBLOCKS

- ✓ Terms of service — Ensure you are not violating terms of service with social media platforms
- ✓ Internal company rules and regulations — Be aware of company-specific rules for using public social media profiles in investigations
- ✓ Patchwork approach — Analysis is time-consuming when using an assortment of free / less reliable tools, often overlapping in purpose
- ✓ Anonymity / deception — Be prepared for the inability to tie activity to a confirmed identity

What Security Teams Miss by Only Relying on Social Media

Where should physical security teams look to source better pre-incident indicators of violence and determine the criticality of threats?

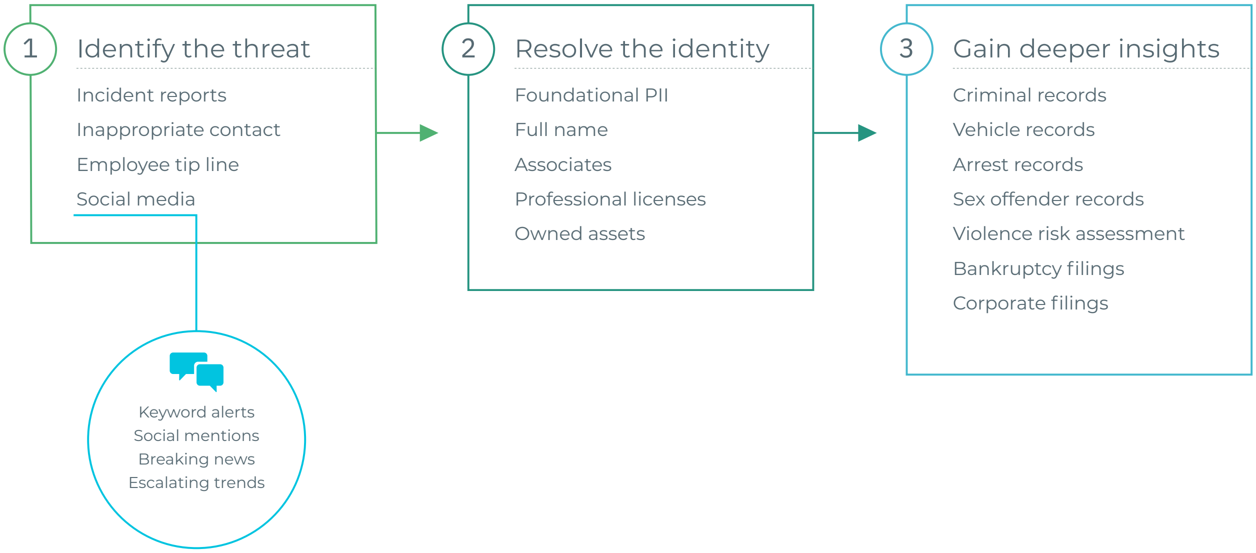
TIP 03 RESOURCES FOR INFORMED DECISIONS

✓ The most verifiable pre-incident indicators of violence tend to be found outside of social media (e.g. life events, criminal history, financial history)

✓ In a recent survey of investigators, the tools identified as being most useful for assessing threats were:

1. Credentialed databases (such as TLO, Lexis, etc.)
2. Social media tools
3. Criminal court record repositories
4. Vehicle data repositories
5. Dark web

Three Phases of the Investigative Workflow



1 Identify the threat

Incident reports
Inappropriate contact
Employee tip line
Social media

Keyword alerts
Social mentions
Breaking news
Escalating trends

2 Resolve the identity

Foundational PII
Full name
Associates
Professional licenses
Owned assets

3 Gain deeper insights

Criminal records
Vehicle records
Arrest records
Sex offender records
Violence risk assessment
Bankruptcy filings
Corporate filings

Use these tips as a guide to assess how you are leveraging social media and other diverse data sources in your investigative process, and reach out to the Center for Protective Intelligence for support from our team of corporate security experts.