Digital Threat Assessment One Day Training

Digital Threat Assessment training will give attendees a stronger understanding of the current social media world, provide tools to proactively identify student safety concerns, and provide strategies for dealing with the new digital playground. After attending the training, the student will have a thorough understanding of:

1. Current social media platforms
    - look at the reality of current school digital baselines across communities
    - current trends of youth behavior online and the risks with this use
    - how to find a person across multiple social media apps and sites
    - use open source tools to assist in data collection (Twitter and Instagram analytic tools)
    - how to obtain user information from social media in response to school safety
2. The data collection process
    - training to see past the noise and overwhelming amount of social media content and focus on relevant findings
    - how to accurately keep specific media notes on what you find and how you find it
    - screen capturing and documenting open source social media to preserve for school data collection/evidentiary requirements for police
3. Establishing a social media baseline for your school, community and individual of interest
    - location specific social media searches (GPS coordinate searching) monitoring the digital heartbeat of your community
    - use geolocational searching to identify potential school safety concerns and student mental health concerns
    - boolean keyword search operators
    - facebook data baselines
4. Tools for emergency management—social media data collection in critical time periods
    - where to start looking to find as much relevant content as possible before it disappears-for example a bomb threat, school lockdown and/or grad events preparation
    - working with law enforcement in contacting social media companies to obtain critical exigent circumstances information
    - assessing validity and veracity of online and social data
    - timely responses to online threat-related behaviors and anonymous threats using anonymous apps and proxy servers
5. Procedural recommendations for law enforcement and senior school administration in their use of social media
    - use of personal account vs. professional accounts
    - current case law and school policy surrounding social media
    - best practice information in harvesting social media content

Attendees should bring their personal laptops with access to the internet. Bring a fully charged laptop, MacBook, Microsoft Surface or Google Chromebook in order to get the most out of the hands-on portion of the training. Tablets are not compatible with some aspects of the training and searching capabilities are restricted with iPads. Your computer will need unrestricted Wi-Fi access – please test connectivity to a public network (Starbucks) before attending. Pro Tip: Bring a wireless mouse.