Closing the Digital Gap in Threat Assessment

SAFER SCHOOLS TOGETHER

DA District Administration®

Introduction: The Missing Link in Threat Assessment

Threat assessment/school safety teams play a critical role in identifying and addressing behaviors that may place students or school communities at risk. Traditionally, these teams rely on strategies such as interviews, academic records, counselor input, locker searches, and conversations with peers or parents to understand a situation. While these approaches remain essential, they no longer capture the full picture for an accurate threat assessment.

Research from the National Threat Assessment Center (NTAC) indicates that 85% of threat assessment teams are missing significant data during assessments, largely because only 15% consistently analyze students' publicly available social media presence.

This gap persists even though the digital world has become a primary space where students express thoughts, emotions, grievances, and warning signs. Because much of this activity occurs on personal devices and platforms outside school networks, traditional monitoring tools often miss concerning behaviors that could provide important context during an assessment.

Digital Threat Assessment and Management® approaches are designed to close this gap by helping teams systematically collect publicly available open source information, analyze digital behaviors, and integrate those insights into broader threat assessment processes.

In this white paper, we explore how Digital Threat Assessment® can strengthen early intervention, how publicly available open source online activity can reveal warning signs, and how schools can incorporate digital insights into existing threat assessment practices to better protect students and school communities.

Understanding Digital Leakage in the School Community

One of the most important concepts in Digital Threat Assessment® is **digital leakage**. Digital leakage refers to **concerning behaviors, thoughts, or intentions that individuals share publicly online**, either intentionally or unintentionally. These indicators may appear in posts, images, comments, usernames, hashtags, or interactions with others. Because social media is designed for sharing thoughts, feelings, and experiences, it often becomes a space where warning signs emerge before they are expressed elsewhere.

Digital leakage can include a wide range of concerning behaviors that appear on publicly available open source social media accounts outside school networks, including but not limited to:

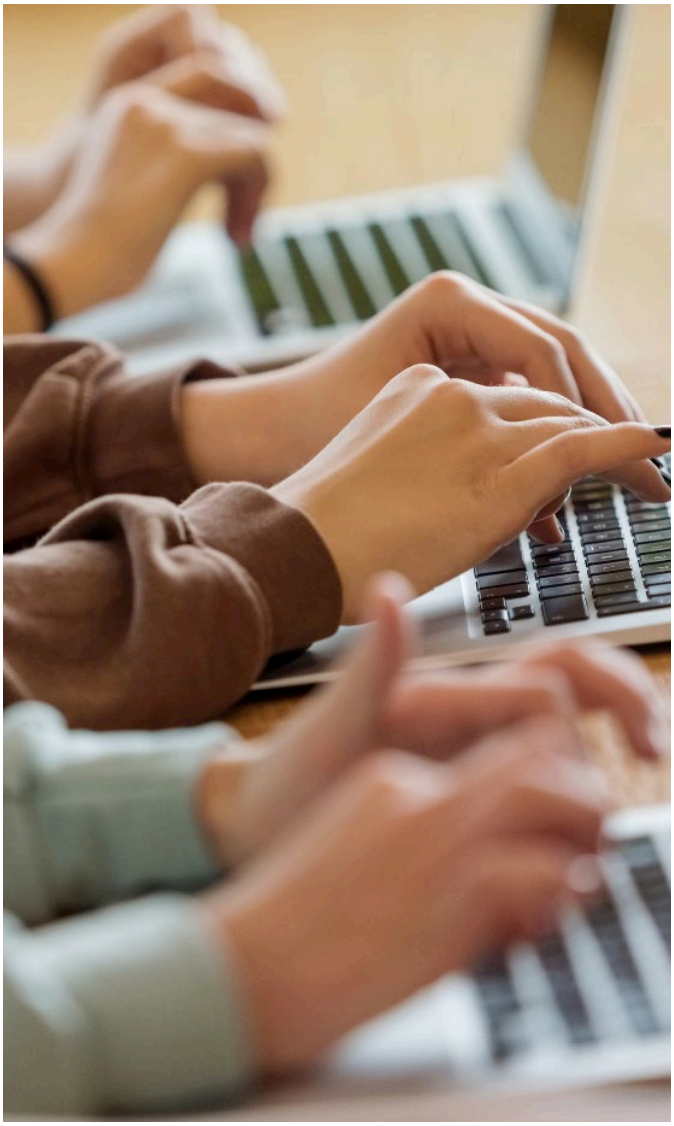
- Weapons and Firearms
- Threat-related Behavior
- Anonymous Threats
- Physical Violence
- Gang-related Activity
- Self-harm Indicators

These concerning behaviors often occur on personal devices rather than school systems and so therefore traditional school-based monitoring tools cannot detect them. However, when threat assessment/school safety teams analyze publicly available open source digital activity, they can identify these concerns and a potential shift in the student's behavioral baseline providing the opportunity to intervene before a situation escalates.

The Pathway to Violence and Prevention

According to best practices referenced by the National Threat Assessment Center (NTAC), individuals typically move through a series of stages rather than acting suddenly. This progression may begin with a perceived grievance, injustice, or other risk enhancer. From there, individuals may develop ideation, begin planning or preparing, and eventually move toward a potential act of violence. Threat assessment models often describe this progression as the pathway to violence.

Throughout this process, many individuals share their intentions online by expressing thoughts, frustrations, and/or cries for help on social media. This type of sharing provides valuable opportunities for early detection and intervention of emerging grievances or signs of distress long before an incident occurs.



Importantly, these pathways are not limited to violence. Similar behavioral patterns may emerge in situations involving:

- Cyberbullying
- Sextortion
- Radicalization
- Suicidal Ideation
- Substance Use
- Mental Health Concerns
- Hate/Racism
- School Community Concerns

These behaviors frequently manifest online and digital information becomes a critical component in identifying early warning signs and shaping effective interventions. In many cases, digital evidence can help teams move from uncertainty to actionable insight.

Why Schools Struggle to Incorporate Digital Leakage

Despite widespread recognition that digital data matters, many threat assessment/school safety teams struggle to incorporate it effectively, in part, because of **a lack of clear processes and tools**.

Many teams know that social media analysis should be included in assessments, but they face questions such as:

- Where should we start searching?
- How do we locate accounts when we don't have usernames?
- How do we verify whether content is authentic?
- How do we determine if digital behavior is concerning?
- What should we do with the information once we find it?

Without structured workflows, collecting and interpreting digital evidence can become time-consuming and inconsistent. This lack of standardized processes prevents many teams from building digital analysis into their regular threat assessment practices.

A Systematic Approach to Digital Threat Assessment®

To address these challenges, threat assessment professionals have developed structured methods for collecting and analyzing publicly available open source digital information. These approaches rely on **open-source intelligence (OSINT)** techniques, which involve gathering information that individuals have made publicly accessible online.

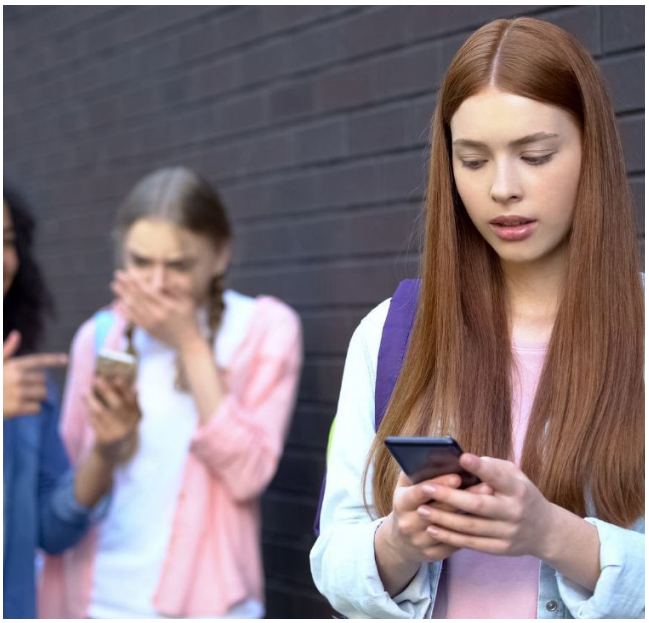
Through systematic analysis of social media accounts, images, and online interactions, teams can develop a **digital behavioral baseline** for individuals of concern. This baseline helps teams understand patterns of behavior, including but not limited to:

- Shifts in emotional state
- Social relationships
- Risk enhancers
- Protective factors

Each piece of digital data can be evaluated through the six social developmental domains, including:

- Individual factors
- **Family** environment
- **Peer** relationships
- **School** context
- **Community** influences
- **Digital** activity

By mapping concerning behaviors across these domains, teams can develop a more informed understanding of the situation and determine appropriate interventions.



From Digital Data to Intervention

Digital data is only valuable if it leads to meaningful action. Once concerning behaviors are identified, threat assessment/school safety teams must determine how to respond. In many cases, digital information can inform **risk-reduction strategies and intervention plans**.

Digital data often provides insight into factors that may increase risk or indicate distress. For example, posts or images may suggest access to weapons or firearms. Individuals tagged in posts or conversations can reveal a collaboration of peer(s) involved in the concerning behavior. Other content may highlight emotional distress, including references to anxiety, depression, substance use, or thoughts of self-harm. In some cases, students may also engage with harmful online communities or “meme pages” that amplify conflict or harassment. Each of these digital signals helps threat assessment/school safety teams better understand the broader context surrounding a case.

Once digital data is collected and analyzed, threat assessment/school safety teams can use the information to guide intervention strategies. This may include next steps such as:

- engaging school counselors or mental health professionals
- conducting suicide risk assessments
- working with families to address underlying concerns

In cases where access to weapons are identified, law enforcement may be involved to remove access to those means. Teams may also implement structured digital safety plans and monitor behavioral changes over time to determine whether risk levels are increasing or decreasing.

Early intervention is the primary goal. By identifying risk indicators sooner, schools can respond before situations escalate.

Building Capacity Within Threat Assessment Teams

Many districts rely on external experts or consultants when complex digital investigations arise. While this expertise remains valuable, schools increasingly need the capacity to conduct digital assessments internally.

Building that capacity requires tools that help teams:

- Locate publicly available open source social media accounts
- Organize digital data
- Evaluate concerning behavioral indicators
- Collaborate across multidisciplinary teams
- Document findings within structured case management processes
- Understanding what to do with this information once it is documented.

When teams can conduct digital analysis consistently, they reduce reliance on ad hoc investigations and ensure that important evidence is not overlooked.

Integrating Digital Data Into Case Management

A comprehensive Digital Threat Assessment® process includes several key steps that multidisciplinary teams should follow.

Case Creation and Documentation

Begin by documenting the situation, identifying individuals involved, and establishing an initial level of concern.

Subject Identification

Identify the primary subject of concern (SOC) and any secondary individuals connected to the case.

Digital Evidence Collection

Using structured workflows, locate publicly available open source accounts and collect relevant posts, images, and interactions.

Data Analysis

Each digital artifact can be analyzed to identify potential risk enhancers or protective factors across multiple life domains.

Collaboration and Intervention Planning

Collaborate together to develop safety plans and recommended interventions based on the available data.

Reporting and Case Integration

Digital findings can be compiled into reports and integrated into broader Behavioral Threat Assessment® systems.

This process ensures that digital insights become part of a structured decision-making framework rather than isolated observations.

The Emerging Role of AI in Digital Threat Analysis

Analyzing digital behavior requires interpreting complex indicators, including coded language, hashtags, emojis, and references to online subcultures. These indicators can carry important meaning but may be difficult for teams to interpret quickly.

Emerging AI tools are designed to support digital threat analysis by helping teams interpret complex online indicators. These systems are trained on thousands of examples previously analyzed by threat analysts, allowing them to recognize patterns that may indicate risk.

For example, AI can help identify concerning trends within images or posts, interpret coded emojis or hashtags, and explain references to online subcultures associated with harmful behaviors such as self-harm or eating disorders. The goal is not to replace professional judgment, but to provide rapid contextual insight so safety teams can understand potential risks more quickly.

Rather than replacing human judgment, these tools aim to support threat assessment professionals by accelerating analysis and providing contextual insight.

The goal is to allow teams to reach informed decisions faster while maintaining professional oversight.

3 Leadership Strategies to Strengthen Digital Threat Assessment®

School and district leaders face increasing responsibility for ensuring safe learning environments while supporting student well-being. Strengthening Digital Threat Assessment® capabilities requires a strategic approach focused on three priorities.

1. Recognize the Digital Dimension of Student Behavior

Leaders must acknowledge that a significant portion of student communication and behavioral expression now occurs online. Threat assessment practices should reflect this reality.

2. Provide Teams With Structured Tools and Training

Threat assessment teams need clear workflows, resources, and tools to collect and interpret digital evidence effectively.

3. Support Early Intervention and Collaboration

Digital insights should be used to inform multidisciplinary responses involving educators, counselors, families, and, when necessary, law enforcement.

When these priorities are addressed, schools can move from reactive responses to proactive prevention.

From Insight to Action: A Purpose-Built Solution

As schools work to strengthen their threat assessment practices, one challenge remains consistent: knowing that digital information is critical, but lacking the tools, structure, and time to collect and analyze it effectively.

The gap is not awareness. It is capacity.

District leadership is asking threat assessment/school safety teams to make high-stakes decisions, often without access to the full picture of a student's behavior. While digital activity offers critical insight into warning signs, risk factors, and cries for help, many teams still lack a consistent, systematic way to gather and interpret that information.

The Digital Threat Assessment and Management (DTAM™) platform by Safer Schools Together was developed to address this need directly.

Built on more than a decade of case management experience and Digital Threat Assessment® training, DTAM® provides a secure, cloud-based solution that enables teams to collect publicly available digital evidence, analyze behavior within a structured framework, and collaborate in real time. The platform incorporates guided workflows, open-source intelligence tools, and evidence-based methodologies that help teams move from uncertainty to informed action.

Importantly, DTAM® is designed to enhance professional judgment, not replace it. By organizing digital evidence, identifying patterns, and supporting intervention planning, it allows multidisciplinary teams to focus on what matters most: early identification, meaningful intervention, and student safety.

In doing so, DTAM® helps schools close the digital gap in threat assessment, transforming fragmented information into clear, actionable insight and empowering teams to intervene earlier, collaborate more effectively, and reduce risk before situations escalate.

To learn more, watch our webinar.

Watch On-Demand

This white paper is based upon the webinar "Spotting Online Cries for Help: Early Intervention Strategies That Keep Students Safe" with Colton Easton Director of Project Development at Safer Schools Together.

Colton has presented to thousands of organizations, including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), numerous other law enforcement agencies, and both K-12 school districts and higher education campuses.

The Ed Talk and this white paper were produced by District Administration and sponsored by Safer Schools Together.

About Safer Schools Together

Safer Schools Together (SST) is committed to ending school violence by encouraging school districts to create positive, safe, and caring learning environments for every student, staff, and parent. With comprehensive prevention and intervention strategies, SST provides School Safety and Threat Assessment Teams with the tools needed to build capacity and sustainability. SST's services are designed to ensure students, staff, schools, and communities have access to a safe, caring, and inclusive learning environment, both online and offline. https://saferschoolstogether.com

About District Administration

District Administration (DA) print and digital media serve the top K12 leaders for districts across the U.S. with strategic information on how to most effectively manage their school systems. DA helps administrators make informed decisions about best practices and research-based approaches designed to help them improve teacher quality and increase student achievement across their districts. DA brings journalistic excellence with in-depth reporting and analysis, as well as success stories that can be shared among peers from district to district.