ONTIC SUMMIT 2026

Navigating the Rise in Targeted Violence: How Intel Teams Can Adapt

This session examined the accelerating rise of targeted violence and the emergence of "assassination culture" in a digitally amplified threat landscape. Speakers highlighted how online forums, AI, and compressed attack cycles are reshaping risk. The discussion emphasized the growing importance of protective intelligence, sentiment analysis, and cross-functional collaboration. Panelists also stressed the need to distinguish credible threats from noise, adapt to residential targeting trends, and strengthen executive awareness through data-driven, proactive security strategies

Speakers

Fred Burton
Executive Director, Protective Intelligence
Ontic

Susan Goggin
Senior Director, Physical Security
Coinbase

TJ Klomp
Chief Physical Security Officer
Amazon

Scott Stewart
SVP, Protective Intelligence
TorchStone Global

Key Themes and Topics

Convergence of Threat Drivers

Modern threats are shaped by overlapping forces including political polarization, global conflict, ideological extremism, and online radicalization. This convergence increases unpredictability and scale, requiring security teams to monitor multiple drivers simultaneously and reassess traditional threat models that no longer operate in isolation.

Time Compression in Attack Cycles

The shift from weeks or months of planning to hours or days has significantly reduced response windows. Digital tools and AI accelerate reconnaissance and mobilization, forcing organizations to adopt faster detection, decision-making, and response capabilities to remain effective.

Influence of Online Sentiment and "Assassination Culture"

Public sentiment, online narratives, and influencer amplification now play a direct role in inspiring violence. Echo chambers and social validation normalize harmful behavior, making sentiment analysis and monitoring of digital communities essential to identifying escalation toward real-world threats..

Continued on next page

Key Themes and Topics

Blurring of Signal and Noise

The overwhelming volume of data creates challenges in distinguishing credible threats from irrelevant information. Security teams must contextualize intelligence, align it with business risk, and deliver precise insights to maintain credibility and ensure executive engagement.

Expansion of the Attack Surface to Residences and Families

Threat actors increasingly target executives at home, where visibility and emotional impact are higher. Family members, personal data exposure, and lifestyle patterns introduce additional vulnerabilities. Organizations should prioritize educating families on these risks, reinforcing a more holistic and proactive approach to executive protection.

Actionable Takeaways

Build or Formalize a Protective Intelligence Program

Establish a dedicated protective intelligence capability that integrates threat monitoring, analysis, and operational response. Without this foundation, organizations remain reactive. A structured program enables early detection, proactive mitigation, and informed decision-making aligned with executive risk exposure.

Integrate Sentiment Analysis Across Functions

Develop a coordinated approach to monitoring public sentiment by linking security, communications, and social media teams. This integration ensures early identification of reputational risks and emerging threats, allowing faster escalation and more informed protective decisions.

Leverage AI While Maintaining Human Validation

Adopt AI tools to automate data collection, pattern detection, and prioritization of risks. Pair these capabilities with experienced analysts who validate findings, provide context, and guide operational responses to avoid reliance on unverified or misleading information.

Prioritize Residential Security and Family Awareness

Expand protection strategies beyond corporate environments to include executive residences and family members. Conduct vulnerability assessments, promote digital privacy hygiene, and educate households on threat indicators to reduce exposure in increasingly targeted personal environments.

Continued on next page

Actionable Takeaways

Strengthen Intelligence-to-Business Translation

Ensure all intelligence outputs clearly explain relevance to business risk. Focus on the “so what” by linking threats to operational, reputational, or personal impacts. This approach improves executive buy-in and positions security as a strategic partner rather than a reporting function.

Build and Maintain External Intelligence Networks

Invest in relationships with peer organizations and law enforcement to validate information quickly and share insights. Strong networks enable faster verification of emerging threats and improve the organization’s ability to respond effectively in a rapidly evolving environment.

Notable Quote

“The time compression issue is real. What used to take months is now a matter of hours. The traditional attack cycle… has collapsed… and we don’t have as much time."

- **Scott Stewart**
SVP, Protective Intelligence
TorchStone Global

Final Message

Corporate security leaders must shift from reactive protection to intelligence-led prevention. The pace, scale, and nature of threats demand faster decisions, stronger collaboration, and deeper integration with business strategy. Organizations that operationalize protective intelligence and adapt to this evolving landscape will be best positioned to safeguard people, assets, and reputation.