Dataminr®

Ask the Expert:

Leveraging Real-Time Intelligence for Executive Security

The landscape of executive security has dramatically evolved in recent years, with corporate leaders facing increasingly complex and diverse threats. The tragic killing of UnitedHealthcare CEO Brian Thompson has served as a catalyst for organizations to reevaluate and strengthen their executive protection measures. This incident highlighted the importance of comprehensive security approaches that address physical threats and broader challenges posed by today's socio-political climate.

Executive protection has become a boardroom-level priority, especially for companies operating in industries with heightened public scrutiny. The risks extend beyond traditional security concerns, as personal information about executives, their families, and their activities is increasingly accessible online. Likewise, the line between corporations and politics has blurred significantly, with business leaders often taking public stances on sensitive issues, potentially exposing them to various forms of targeting.

Below, Hugh Farquhar, VP of Product for Corporate Security at Dataminr, shares his insights on modern executive protection. With over a decade of experience in corporate security and crisis management at Citigroup, including roles as Head of Global Intelligence & Analysis for EMEA and Head of Major Events & Crisis Logistics, which focused on executive protection plans for executive offsites and corporate events, Farquhar brings deep expertise in protecting corporate leaders and assets in today's complex threat landscape.

Hugh Farquhar
VP of Product, Dataminr

How has the landscape of executive security evolved, and what new challenges are security teams now facing?

Executive protection has become a major concern, particularly for companies in industries with heightened public scrutiny. Unlike government officials, where protection is often mandated, corporations must carefully evaluate their security needs and approach.

The challenges are multidimensional. Personal information about executives and their families is increasingly accessible online, and risks often extend beyond the executives themselves. Family members, especially children active on social media, can unknowingly expose private details about an executive's whereabouts or associations. Additionally, as corporate leaders increasingly engage with political and social issues, they face new threats from individuals and groups who disagree with their positions or company policies

We're seeing increased targeting of executives both online and in the physical world. How can security teams effectively detect and respond to threats across these different domains?

Effective executive protection starts with a holistic risk and vulnerability assessment to understand specific types of threats. Security teams must detect early indications of potential risks and negative public perception to their industry, company, and individual executives.

A critical challenge is the sheer volume of public data that needs to be processed. For perspective, social media platforms alone generate massive amounts of content. X (formerly Twitter) produces hundreds of millions of public posts every day. Security teams need sophisticated tools that can analyze multiple data sources, including social media and the deep and dark web, while maintaining awareness of executive locations and travel plans.

The key is implementing a comprehensive system that includes wide-ranging public data sources, domain awareness capabilities, geovisualization tools for specific risk context and location awareness, and sophisticated AI that goes beyond simple keyword tracking. However, gathering data is just the start. Teams must also develop effective response protocols and maintain strong relationships with law enforcement agencies.

What role does artificial intelligence play in modern executive protection, particularly when analyzing vast amounts of public data for potential threats?

AI has become indispensable in modern executive protection due to the overwhelming volume of data that needs to be processed. To give this some context, processing just 1% of the daily global text-based digital content Dataminr ingests would require 30,000 human analysts working around the clock. However, organizations need to be discerning about AI capabilities, as many solutions marketed as AI are simply using basic rules-based logic or Boolean searches.

The most effective AI systems for executive protection must be able to process multiple languages and various content types, including text, audio, video, and imagery. This is critical because threatening content often combines elements such as benign text with threatening images. Additionally, AI models need to be specifically trained to recognize executive names and company identifiers, such as logos, while filtering out content that does not indicate a safety risk to a protectee.

How can organizations effectively coordinate between executive protection teams, corporate security, and crisis management to ensure comprehensive security coverage?

Successful executive protection requires seamless coordination between threat monitoring teams, on-ground protection personnel, and crisis management units. The key is implementing a centralized digital risk management platform that enables real-time information sharing and collaboration.

This platform should allow teams to collate threats and local alerts in real time, assign and track response tasks, share critical documents like schedules and evacuation routes, and generate situation reports instantly. The system must also be fully mobile so that field teams can receive and respond to alerts immediately while maintaining a connection with headquarters and intelligence units.

Looking ahead, what emerging trends or threats should organizations be preparing for regarding executive security?

While specific threats vary by industry and company, organizations need to pay particular attention to security around high-profile business events such as industry conferences, annual shareholder meetings, and board of directors' meetings. These events present unique challenges and vulnerabilities.

Major industry conferences are implementing enhanced security measures, including increased law enforcement presence and more stringent access controls. Shareholder meetings require special attention as they create greater risk exposure for executives and other high-profile individuals. Board meetings present additional complexities when they include high-profile directors who may bring their own security considerations and threat profiles.

The key is understanding that each type of event presents distinct security challenges. Organizations must develop specific protocols for different scenarios while maintaining the flexibility to adapt to emerging threats and changing security landscapes.