Solution Innovation Case Study:
Enhancing Situational Risk Understanding with an Always-On Approach to Collecting Critical Intelligence and Conducting Threat Analysis

The SEC's Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of possible options in the marketplace. Proven Solution Innovation Practice Case Studies help evaluate performance claims and differentiate solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates a Fortune 200 electric company's innovative capabilities to protect one of its plant locations using the Ontic Protective Intelligence Platform.

Risk Issues and Mitigation Opportunities:
- The corporate security team lacked sufficient situational risk awareness and understanding tools needed to effectively monitor the area around each facility location.
- Large amounts of unorganized, unactionable social media data made it difficult to proactively identify negative complaints and isolate threat-related content.
- Person of Interest (POI) data was stored in a static spreadsheet, limiting the team's ability to action the data.
- The volume and severity of customer complaints against the company had grown to a point where it was easy for more potentially threatening complaints to slip through the cracks.
- There was a lack of visibility process to prioritize more severe complaints.
- Increased threatening protest activity created the need for more nimble data analysis to alert stakeholders of this trend.
- Keeping the facility location(s) discrete was needed to keep employees, the property, and other assets protected and safe, as well as maintaining a positive neighborhood sentiment.

Solution Requirements:
- Utilize a database to evaluate and manage POIs as well as archive and store past threat data.
- Obtain a holistic view of historical and real-time threats from human observations and data from public records, social media, location detection, threat assessments and integrations with internal systems to better identify pre-incident indicators, assess risk, and mitigate potential threats.
- Proactively monitor activity on various social channels with real-time signals and gain the ability to set up filters to monitor posts specific to each plant location for increased threat visibility and risk management.
- Allow for integration with other physical security software and data providers.
- Comply with SOC 2, GDPR and other ethical governance.
- Have a dedicated Client Success team for easy implementation and onboarding, hands-on training, and ongoing support to help execute security strategy through technology.

Delivered:

- With Ontic's Real-Time Threat Detection solution, the security team could more easily monitor social media and other OSINT feeds on a continuous basis to help identify potential threats or concerning behavior by persons of interest.
- Easily collaborate with connected workflows: The security lead was able to forward the posts of concern and action plan to the social media team within minutes, mitigating the threat while also demonstrating the security team's value.
- Demonstrated broader impact with metrics: Report metrics were easily available on signal volume, by topic, and by trends over time. The team could see holistic numbers around social chatter, with the ability to dig into specific areas to investigate further.
- Timely alerts for new threat entities (person/places/things) signals: Constant monitoring of entities– especially with Ontic's License Plate Recognition and Location Sighting capabilities to enable proximity alerts for plant, administrative, and corporate locations.
- A platform with POI capabilities: research tools to continuously collect and store data on POIs in one central system.
- Ontic's entity dashboards help segment out entities and share cross-functionally as agreed upon.

Outcome and Benefits of Service Including ROI:

- Increased visibility of potential threats and the ability to quickly assess and rank their severity through a holistic picture of their threat landscape and ongoing monitoring.
- Ontic's operational threat analysis process enabled significant improvement to the company's time to resolution for potential threats and reported incidents
- More actionable signals and a fuller picture of their threat landscape allows for easier prioritization of threats that pose a greater risk.
- Analyst labor was re-deployed to also analyze other risk areas that were previously underserved.
- Improve leadership's confidence in Security risk mitigation efforts from 5/10 to 9/10

"Now with a holistic view of our threat landscape, we have the ability to run down every single identified threat. We can categorize and prioritize all our threats to better determine which ones are important and which ones are not. Having this platform allows us to make better use of our time and focus on what is critical." - Director of Security at Fortune 200 Company

SIP Case Study Authentication Process
This process was overseen by a Council Faculty member with 20+ years of experience in developing and leading people and asset protection programs as trusted security advisor for global, multinational organizations. Client end-user authenticated May 2022**.**

Note: *The Security Executive Council's Solution Innovation case study represent a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

Solution Innovation Case Study:
Enhancing Situational Risk Understanding with an Always-On Approach to Collecting Critical Intelligence and Conducting Threat Analysis

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/about/solution_innovations.html