

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 how a Fortune 50 technology company used the Ontic Protective Intelligence Platform to unify all critical historical and real-time data to gain a faster, clearer, and more holistic view of situational risk and physical threats to the company. This proactive approach to managing threats not only improved risk understanding and drove more timely threat detection, but it also helped mitigate liability for the business while improving confidence for keeping employees, executives, facilities, and assets safer.

Risk Issues and Mitigation Opportunities:

- Data to detect, analyze and mitigate potential risks and threats resided in multiple disparate publicly available resources and tools as well as company-proprietary records and communications (mail, letters, calls).
- Person of Interest (POI) data was stored in a static spreadsheet, limiting the team's ability to collaborate.
- Large amounts of unorganized, unactionable social media data made it difficult to identify negative commentary and isolate threat-related content.
- Static "Be on the Lookout" (BOLO) reports were created manually and sent via email to the appropriate team members.
- Alerts and notifications to stakeholders in the field were overwhelming and disconnected from POI data.
- Inability to collect and report on metrics to discern insights about how the current threat landscape impacted the company and informed resource decisions.

Solution Requirements:

- Utilize a database to evaluate and manage POIs and threat makers 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.
- More effectively manage incidents and investigations, conduct research using investigative tools, monitor real-time feeds and get alerts, and conduct assessments in a single SaaS-based platform.
- Allow for integration with fixed license plate reader (LPR) cameras and other physical security software and data providers.
- Serve an always-on, virtual GSOC, allowing team members to connect and collaborate from anywhere, on any device.

Solution Innovation Case Study: Continually Improving Situational Risk Understanding Through Proactive Physical Threat Management

- Use intuitive automation with customized rules and if/then workflows for automated alerts and to drive predetermined outcomes.
- Get comprehensive reporting and metrics that are easily configurable and shareable with required stakeholders from different functions across the organization.
- Include rigorous privacy and governance capabilities with the ability to configure and manage workspace and user access with appropriate permissions.
- Comply with SOC 2, GDPR and other ethical governance.
- Dedicated Client Success team for easy implementation and onboarding, hands-on training, and ongoing support to help execute security strategy through technology.

Delivered:

- Intuitive, user-friendly platform to store and manage threats, resulting in clearer situational risk awareness and improved understanding across the business.
- Ability to identify, investigate, assess, and manage threats, while informing users of potential risk with improved situational context, such as a fixed camera LPR integration.
- Capacity to easily watch multiple open-source channels in real time.
- Measurable performance with flexible, dynamic, and customizable metrics dashboards and reporting capabilities.
- Daily, weekly, quarterly, and annual reporting capabilities with high-value, actionable, situational risk mitigation understanding.

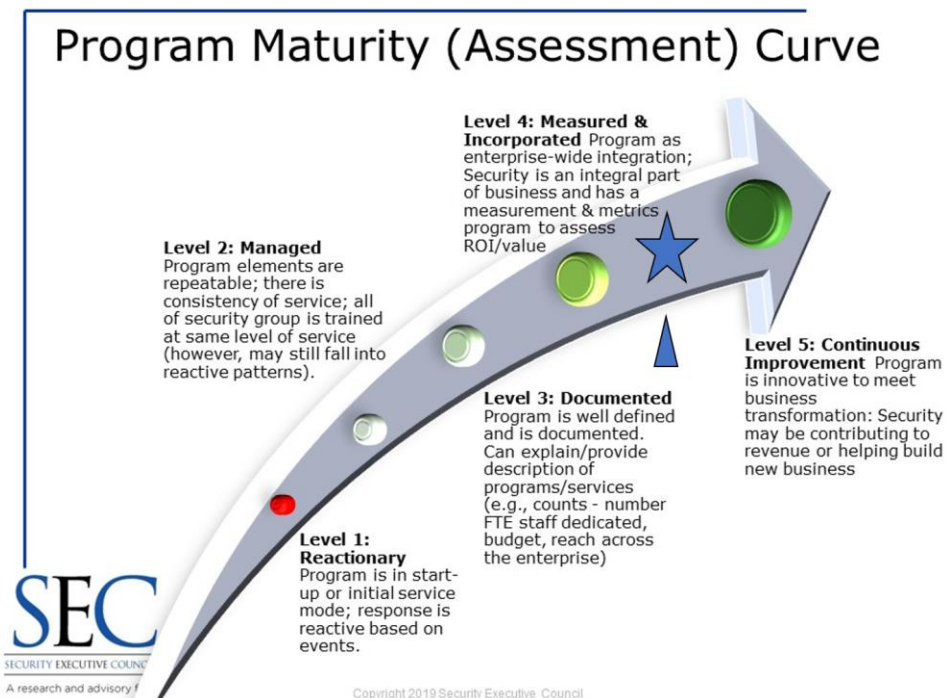


Figure 1: SEC Program Maturity Curve

Outcome and Benefits of Service Including ROI:

- Allowed operational maturity perception advance from documented, to measured and incorporated, setting the stage for continuous improvement. See Figure 1: SEC Program Maturity Curve above.
- Boosted confidence rating of protective service team from 4.5 to 8.5 by optimizing finite service resources.
- Contributed analytic capability for dynamically determining top 5 threats.
- Operational in two weeks, providing accelerated speed-to-value through fast implementation and effective training.
- Displaced manual processes and gained the ability to efficiently store and manage data while using proprietary workflows and always-on external data integrations to facilitate critical intelligence collection and conduct effective analysis.
- Facilitated smarter collaboration with critical stakeholders throughout the enterprise, enabling dispersed global teams to easily share the critical real-time and historical intelligence needed to better identify pre-incident indicators, assess risk, and mitigate potential threats.
- Enabled the Protective Intelligence team to more efficiently and effectively serve as the nerve center for global monitoring, triaging threats, determining threat level and escalating to the right person in the right office.
- Allowed for easy monitoring of changes to threat levels of entities over time.
- Seamlessly isolated threat intelligence from general social media chatter.
- Enabled a uniformed process for managing and monitoring threats, ensuring compliance and a proper audit trails of all activities.
- Incorporated the mobile app into workflow for quick, on-the-go incident management by field operators, including real-time notification to analysts when incidents are logged, enabling proper triage and action.
- Leveraged dashboards for visibility across all incident cases, allowing insight into where incidents stem, and who the targets are.
- Improved reporting capabilities of operational measures and metrics for both practitioners and managers including number of entities, distribution of threat level, reason for inclusion, state distribution, number of entities on BOLO status, number of entities associated to target, and entity update trend.
- Augmented ability to provide customized monthly reports to leadership including high level categories and detailed data points such as motive category and motive, target, relationship to target, property involved, and case reporter.
- Incorporated fixed camera feeds for continuous watching of vehicles at key locations, giving the ability to view vehicle sightings in real-time, and display previously sighting trends for anomaly detection.
- Automated real-time alerts for suspicious vehicle sightings based on client's chosen criteria and set monitor list for team to review based on rule triggers.
- Notified management when new incidents or entities created for necessary visibility and threat assessment workflow.

**Solution Innovation Case Study:
Continually Improving Situational Risk Understanding Through Proactive
Physical Threat Management**

“Ontic has transformed how we protect our people and company value and has become a critical part of our protective intelligence security program by giving our team the ability to proactively and continually manage threats in a single platform. Ontic helps me be a half step ahead and gives me confidence in knowing our team has the right technology and strategies in place to mitigate risk and avoid crises while ensuring that we are following processes along the way. The speed at which Ontic innovates, while asking for and considering client feedback, is the best we have seen in the industry.” – Senior Director, Protective Services, Fortune 50 Technology 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 on January 13, 2021.

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.

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