SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:

Real-Time Open Source and Dark Web Risk Intelligence Gathering to Protect People, Assets, Information, and Brand

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved as a means for practitioners to choose a trustworthy risk mitigation provider with confidence when there is a myriad of options in the marketplace. Proven Solution Innovation Practice Case Studies help to evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

The following case study is a demonstration of a global Pharmaceutical Company utilizing the LifeRaft solution as part of its strategy to protect its brand and proprietary information. This Solution Innovation Case Study offers a proven process approach for mitigating risk(s) online that could result in injury or impairment of people, assets, critical processes, products and/or brand reputation. This proof point examines representative risk issues, mitigations and result outcomes as validated by the Security Executive Council and the end-user.

Risk Issues and Mitigation Opportunities:

1. Proactively obtain information posted on open source and dark web sites to mitigate risks that may compromise, embarrass or threaten key personnel, stakeholders, assets, critical processes, proprietary information, or brand reputation.
2. Provide alerts of actual or implied hazards to people, product, reputation or revenue as a result of proprietary information fabrication, leaks, spills or illegally or improperly posted subject matter on open source and dark web sites.

Solution Requirements:

- Obtain risk intelligence related to critical personnel, process, products and proprietary information and the company's reported internal data leak from several open source channels including social media, blogs, forums, and the dark web
- Obtain risk intelligence related to sensitive information in real-time alerts to designated company stakeholders when open source posts meet high-risk criteria (such as sensitive information or threats to company executives/employees)
- Ability to compile information on a wide spectrum of open/dark source posts using minimal search criteria
- Easy to use with simple-to-understand training sessions
- Dedicated, and easily accessible training support which fit the needs and culture of the business
- SaaS Based platform with several user log-ins
- Easily customized reporting capabilities

Delivered:

- ✓ Intuitive user-friendly interface resulting in clear situational risk awareness
- ✓ Ability to monitor several open source and dark web channels in real time
- ✓ A highly trained, customer success support team
- ✓ Daily, weekly, quarterly, annual reporting capabilities with high-value, actionable, situational risk mitigation understanding

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Real-Time Open Source and Dark Web Risk Intelligence Gathering to Protect People, Assets, Information, and Brand

Outcome and Benefits of Service Including ROI:

- Identified a data breach of internal code on a social channel which, if not found, would have resulted in significant brand impairment.
- Company-wide internet source situational risk understanding confidence rating went from a 3 to a 7.
- Social media situational risk incidents went from 1-2 monthly to an average of 45 monthly, resulting in increased leadership value perception of the Security brand.
- Enabled added GSOC capability to monitor for proactive risk monitoring of supply chain.
- Enhanced investigative team can now more effectively query stolen and counterfeit product appearing on deep & dark web
- Improved reporting functionality allows information to be more quickly shared amongst Security & management
- Delivers superior results faster with managed risk outcomes; rather than sourcing manually, saving time, personnel costs and related financial resources.
- End user testimonial - "*If my team had to still do this manually, I would never be able to secure this depth and breadth of actionable intelligence. I am confident that we are getting to 90% of the internet's risk areas, which currently satisfies the company's risk appetite*"

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations. Client end-user authenticated March 2019.

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.*

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	**Liferaft YES/NO**	Company A YES/NO	Company B YES/NO	Company C YES/NO
Aggregation of social data	**Yes**	Yes	Yes	No
Monitoring & alerting of keywords	**Yes**	Yes	Yes	Yes
Global event monitoring map	**Yes**	No	No	Yes
Tracking & alerting of social accounts	**Yes**	Yes	Yes	No
Link analysis of social accounts/communities	**Yes**	Yes	No	No
Topic based queries	**Yes**	Yes	No	Yes
Location based queries	**Yes**	Yes	Yes	Yes
Deep Web searching and filtering (including Telegram)	**Yes**	No	No	No
Deep Web tracking (including Telegram)	**Yes**	No	No	No
Dark Web tracking, searching and filtering	**Yes**	Yes	Yes	No
Dark Web tracking	**Yes**	Yes	No	No
Relevance scoring and filtering	**Yes**	No	No	No
Reporting capabilities	**Yes**	Yes	No	No

Exporting to PDF	**Yes**	No	Yes	No
Exporting to CSV	**Yes**	Yes	No	No
Content categorization	**Yes**	No	No	No
Alerts via SMS	**Yes**	No	No	Yes
Alerts via email	**Yes**	No	Yes	Yes
Dashboard view of aggregated content	**Yes**	No	No	No
Content visualization: maps	**Yes**	Yes	Yes	Yes
Content visualization: word clouds	**Yes**	No	No	No

Security Process Optimization Data

Client Available Capability	Pre - Prior Year	Phase One - Year(s)
Automated location monitoring	**NO**	**YES**
Global mention monitoring	**NO**	**YES**
Real-time alerting for open source data	**NO**	**YES**
Ability to monitor and track the deep web	**NO**	**YES**
Ability to monitor and track the dark web	**NO**	**YES**
7-day social media post look back and capture	**NO**	**YES**
Identify data leaks on social media and deep & dark web	**NO**	**YES**
Detect threats to executives made online	**NO**	**YES**
Identify online distribution of stolen goods automatically, rather than searching manually	**NO**	**YES**