Solution Innovation Case Study:
Strengthening Security: Stress Testing Physical and Operational Security to Better Protect a Global Enterprise

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

This case study demonstrates Pine Risk Management's innovative capabilities to test, validate, and improve a security program through regular exercises, tests, and training.

Pine Risk Management (PRM) was brought in to stress-test and improve this company's Security Operations Center (SOC). The client had four goals:

1. Test, assess, and validate current security capabilities. Figure out a state-of-the-state and gather data on performance: you cannot manage what you don't measure.
2. Uncover vulnerabilities and gaps. What isn't working and how can it be improved?
3. Increase security awareness, engagement, and security through the act of testing. PRM set out to gamify the tests, so the general workforce is more engaged and eager to succeed.
4. Establish an ongoing quality improvement program, the client established monthly tests to gather longitudinal data and invest in their security program's success for the long run.

Many security companies sell physical penetration tests, physical intrusion tests, or red teaming. Pine Risk Management is the only company focused solely on physical red teaming.

Risk Issues and Mitigation Opportunities:

Challenges and opportunities included:

- **Leadership Insight:** Leadership wanted clear, specific, and compelling business use scenarios to understand the capabilities of the team they were funding and depending on.
- **Vendor Accountability**: Provide insight into whether vendor solutions worked until they faced real-world scenarios or discovered a bug by luck during an audit or regular use.
- **Managing by Measuring**: Increase data about the success of security programs.
- **Certifications:** Measure how difficult it was, or not, for an adversary to physically access office areas, server rooms, data halls, and other secure locations.
- **Low Security Employee Engagement:** SOC employees were disengaged and distracted without challenges, rewards for success, or opportunities to prove their capabilities.
- **Lack of Practice:** SOC operators' first experiences in high-stress situations were frequently real scenarios where mistakes could cause significant physical, financial, or reputational harm. On the job, realistic scenarios with operators both in the field and the SOC identified gaps.

- **Unknown Unknowns:** On a regular basis and often at the worst moments, the SOC would discover that something had gone wrong, and it was a scenario that had not previously been thought of or prepared for. The need to uncover hidden gaps and vulnerabilities quickly became apparent.
- **Regular proactive testing**: Security measures and teams could be tested more frequently, ideally regularly, to identify and address uncovered vulnerabilities.
- **Creation, revision, or development of Incident Response Plans**: Tested and proven response plans that reflect the true process of the response teams ensure quick and effective action during security incidents.
- **Effective Use of Technology**: Test the effectiveness of the SOC's current technology, as well as its configuration, implementation, and use.
- **Increased Collaboration across Teams/Reduction of Silos**: Assess collaboration and open lines of communication between relevant teams.

Solution Requirements:

The client required a solution that bridged the gap between their open culture and their need to safeguard highly sensitive trade secrets and prototypes, without creating additional risk or affecting the employee experience. Specifically:

- **Trusted Measurements:** Independent assessments of the security program, with high-level scorecards for leadership, and detailed findings for the teams responsible for managing and improving the program to action.
- **Ongoing Assessments:** A long-term partnership involving monthly tests, which integrate with training, risk management, and operational readiness programs.
- **Improve Leadership Confidence**: The ability to confidently answer key questions for leadership, stakeholders, regulators, insurance underwriters, and employees regarding components of the client's physical and operational security program.
- **No Additional Risk:** The solution had to measure and mitigate risk without adding to it. Testing must not cause alarm, have unexpected costs, or create additional liability.
- **Culturally Sensitive**: Testing scenarios and outcomes had to match company culture without causing undue stress or offense.
- **Realistic:** Assessment scenarios need to be realistic to be compelling.
- **Compelling:** Tests needed to deliver compelling results, including videos and media, to brief leadership on the security program's status and to enhance security awareness training for employees.
- **Test Diversity:** To include broad physical and operational security components.

Delivered:

The client sought longitudinal data about their performance. Although they originally requested a full-scale assessment, PRM suggested lower-cost monthly assessments to meet their needs. For each exercise, the clients received five deliverables:

1) **Risk Register**: A list of findings and their potential root causes, along with brief descriptions of the most cost-effective methods to mitigate the risk.
2) **Written Report**: A report that includes a summary scorecard, along with details of each scenario, test, finding, and potential mitigation actions. All reports include commendable elements that showcase security controls that were validated by testing.
3) **Presentation**: A presentation to security leadership of each finding, including video, diagrams, and detailed explanations of all critical findings.
4) **Body-Cam Footage**: Where relevant, hidden button-cam footage from operators will be provided to add useful context and details to security teams.
5) **CCTV Footage**: Where allowable, CCTV footage is pulled and provided for each test to be used for training and remediation purposes.

Each monthly test included:

- Test 1: Control Improvement Simulation
- Test 2 - Asset & Threat Based Simulation
- Test 3 - Leadership Request
- Test 4: Threat-Based Exercises

Outcome and Benefits of Service:

Each exercise had 12-20 findings.

- Increase in proactive reporting at sites aware of monthly testing.
- Decrease in successful breaches at the company's most secure locations.
- Compelling media to leadership, demonstrating previously successful breach attempts being detected and thwarted.
- Briefings to the client's insurance underwriters with data collected as independent assessors, helping reduce casualty, liability, and cyber insurance premiums.
- Numerous technology vendors were asked to return to remediate configuration and implementation issues that did not meet their statements of work, significantly improving security at no additional cost.

- Where security was validated as effective, the client could remove or pause unnecessary, costly measures, or replace them with more effective and cheaper alternatives. For example, the client removed anti-tailgating technology that was only 18% effective, eliminated badge-readers from those doors, and prioritized intrusion alarms on infrequently used doors at no cost.

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 25+ years of experience in developing and leading people and asset protection programs as a trusted security advisor for global, multinational organizations. **This was validated by the Security Executive Council and the client end-user September 2024.**

Note: *The Security Executive Council's Solution Innovation case study represents 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	**Pine Risk Management YES/NO**	**Company A YES/NO**	**Company B YES/NO**	**Company C YES/NO**
Company is Focused on Physical Red Teaming	**YES**	**NO**	**NO**	**NO**
Trusted International Footprint of Red Team Operations	**YES**	**NO**	**YES**	**NO**
Monthly Improvement Testing	**YES**	**NO**	**YES**	**YES**
Global Physical Penetration Testing Experience	**YES**	**NO**	**NO**	**NO**
Publishes Open-Source Articles on Red Teaming	**YES**	**YES**	**NO**	**NO**
Trains and Develops In-House Red Teams for Major Corporations and Government Entities	**YES**	**NO**	**NO**	**YES**
Experience Leading In-House Red Teams at Fortune 500 Corporations	**YES**	**NO**	**NO**	**NO**
Extensive Knowledge of Laws, Rules, and Regulations around Physical Security Exercises	**YES**	**NO**	**NO**	**NO**

Threat-Model Based Red Team Assessments	YES	YES	NO	YES
Extensive Private Sector Experience	YES	YES	NO	NO
Physical Security Expertise	YES	NO	UNSURE	YES
Understanding of Red Teaming Mindset	YES	YES	YES	UNSURE
Expertise in Physical Security Domain	YES	NO	UNSURE	YES
Focus only on Physical Security	YES	NO	YES	YES
In-House Team of Experts in Physical, Technological, and Human-based Security Measures	YES	NO	NO	NO
Experience Testing Non-Traditional Areas of Security Programs	YES	NO	UNSURE	NO

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/solutions/vendor-innovations