SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Hyper-growth Tech Company Uses a Data-driven Security Platform to Gain Long-term Savings of $28 Million

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 HiveWatch's innovative capabilities to deliver more streamlined, cost-efficient, and scalable security operations management for a global logistics company.

Risk Issues and Mitigation Opportunities:

- Siloed security operations created barriers for operators and analysts to glean the information they needed to provide informed responses to incidents and events.
- The high cost of security officers (SOs) and field resources prompted the company to look at ways to make operators and SOs more efficient across the company's locations.
- Communication challenges between the global security operations center (GSOC) and SOs/field resources at various global facilities and across multiple SO providers created gaps in information sharing. Resources were being dispatched without full context of what was happening. Efficacy of communications from the GSOC to the field was a challenge with no real metrics to report on against SLAs.
- Analog standard operating procedures (SOPs) increased response times and complexity of training operators.
- False alarms from multiple sensors were creating more than a 98% false alarm rate, causing operators to miss critical events or significantly delay their detection.
- The company did not have a way to track and store data related to security incidents, such as tailgating, false alarms, or time to resolve incidents.
- With operators spending most of their shifts responding to primarily false alarms, the amount of time spent led to a minimally effective, high-cost, and purely reactive security program.
- The company needed visibility into its security operations and functionality that would allow operators to have the information needed when they needed it. This included the need to integrate systems that were not natively integrated already, which was causing increased response times and workflow inefficiencies.

Solution Requirements:

- The company's presence in major cities, manufacturing facilities and offices meant a distributed workforce handling sensitive, proprietary information across multiple locations.

- Coupled with a sizable number of physical assets, its GSOC was tasked with managing alerts, incident response, and coordination with field (SO) resources and needed a way to achieve a more proactive response.
- Security leadership also needed data to help them understand the effectiveness of their GSOC operations and security program, as well as its overall return on investment (ROI) for the business. The company needed to understand SO program performance and the data around where and how many resources were needed across the multiple locations.
- The level of growth this company was experiencing meant that being able to find programmatic efficiencies was essential to being able to do more with existing resources.
- Disparate security systems with multiple applications to manage made it difficult for GSOC operators to quickly identify and triage incoming events and validate that those events were legitimate. Data from access control systems, video surveillance, and analytics needed to be collected and disseminated in an organized, easy-to-understand way.
- The company's GSOC was plagued with incoming false alarms from misconfigured sensors, noisy sensors, and offline cameras.
- The company had physical assets based across a wide geographic area that were not facilities. As a logistics company, when they had an incident in the field, it was difficult to integrate field operations with the security infrastructure they had in place at fixed assets like corporate offices and facilities.
- Operator turnover was high, creating the need to have a way to quickly onboard and train new employees as needed and get them up to speed efficiently on how the GSOC operates. Additionally, there was a need to help with retention by increasing job satisfaction and retention for operators.

Delivered:

- Security leadership at the company tested the HiveWatch® GSOC Operating System (OS) for 6 months across two GSOCs. One used the platform and one did not.
- The benefit of implementing the HiveWatch® GSOC OS was validated by data, such as time to acknowledge the alarm. The data from the platform was used to understand the company's third-party SO spend, operator efficiencies, device health, and more allowed security leadership to make meaningful operational decisions that saved money and resources.
- The data highlighted locations with the most alarms as well as where having a SO/field resource present would deliver the greatest benefit to proactively address incidents. Conversely, in addition to the false alarm reduction provided by the software, noise was identified from sensors that were configured improperly or broken and corrected to contribute to significant reduction of these alarms.
- Working with HiveWatch, the company wanted to see where their assets were and could route the correct staff to the location, giving them a quick way to navigate to the scene. With the

scalability of the platform, HiveWatch was able to deliver this level of visibility for operators that encompassed their needs and layered data-driven insights to determine patterns and potential improvements that could be made to the company's operations.

- The ability to embed customized SOPs based on incident type was a big benefit of implementing the HiveWatch platform in the customer's GSOC. As a result, training new employees and operators was more streamlined, with reduced time to navigate physical notebooks and the ability to provide an efficient workflow for operators.

Outcome and Benefits of Service Including ROI:

- Time to resolve alarms went from 15 minutes to less than 1 minute: Prior to leveraging HiveWatch, there was a 15-minute average time to resolve an incident, from acknowledgement to closure. This means that the moment the alarm was sent to operators and evaluated for whether it was a false alarm or an actual event, it took 15 minutes or more for operators to resolve the issue. After HiveWatch, that number was less than 1 minute.
- Root cause of false alarms found on 30% of false alarms in the first 60 days of deployment: Using the platform, the customer was able to have their systems team address the root cause of 30% of their false alarms within the first 60 days.
- Addressing false alarms freed up 57% of operators' time: Prior to implementing HiveWatch, the customer had so many incoming alarms, they determined the organization would need six times the number of operators they currently had per day to respond to every alarm as they scaled the business.
- The 3 key benefits noted above delivered a 3-year savings of $28 million (including the investment in the HiveWatch software). This $28 million dollar savings from implementing the HiveWatch® GSOC OS was primarily derived from the optimization and/or reduction of resources needed to respond effectively to alarms, the reduction in the number of field resources and GSOC operators to monitor multiple locations, and the increased efficiency seen related to training, onboarding, and implementation of new operators and analysts. HiveWatch was able to find areas where the business could save resources and time, and backed it up with data to prove it.

End User Testimonial – "GSOC Operator engagement increased after we implemented HiveWatch. They enjoyed their daily work much more. The implementation was very straightforward."

Watch a short video about HiveWatch here.

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	Hivewatch YES/NO	Company A YES/NO	Company B YES/NO	Company C YES/NO	Company D YES/NO
Tailgate detection	Yes	Yes	Yes	No	No
Security program and performance data analytics and reporting, including time to acknowledge and time to resolve	Yes	Unknown	No	Unknown	No
Incident reporting, case management, and incident management	Yes	No	No	Yes	Yes
Noise and false alarm reduction	Yes	Yes	Yes	No	Unknown
Guard Mobile App/dispatch and two-way communication	Yes	No	No	No	Yes
Embedded Standard Operating Procedures (SOPs) to guide incident response	Yes	No	No	No	Yes
Manual incident creation from platform and via mobile app from the field	Yes	No	Unknown	No	No
E911, or emergency services communication directly from the platform, routed by location	Yes	No	No	No	No

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 June 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.*

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