Case Study: Global Fuel Corporation Threat Management and Compliance

Companies in the energy sector provide critical services that must be available and monitored 24 hours per day. They must not only respond to existing events as quickly as possible but also address issues proactively by identifying potential risks and problems before they happen. To accomplish this, companies must have comprehensive and effective solutions for monitoring, identifying, prioritizing, and escalating potential or existing security issues in order to respond to them as quickly and efficiently as possible.

The Client

Our client is a leading energy corporation focused on global logistics of fuel products and services. They provide both cyber security and physical security as part of these logistics and as such must have solid plans for monitoring and responding to potential security incidents in order to respond to them as quickly as possible. Their industry is also subject to compliance with various regulations, including GDPR and SOX.

The Challenge

The client was searching for a more strategic approach to corporate security. They needed security event monitoring and incident management, including threat analysis, event monitoring, and notifications.

The Solution

We perform monitor alerts and policy exceptions generated by our Security Operations Center (SOC), which are then analyzed to determine if the event is a security incident, in which case we and the client initiate the mutually defined incident response plan to classify, prioritize, and escalate the security incident accordingly. We perform incident handling capabilities such as:

- Executing predefined incident playbooks for incident handling of events
- Adjusting alert prioritization based on criticality and risk-based response profiles identified in the customer portal
- Escalating security incidents to an authorized security contact or designated services contact
- Assisting the security teams with performing root cause and impact analysis
- Providing remediation/countermeasure recommendations
- Performing advanced threat hunting to identify root cause and impact analysis
- Performing remediation or deployment protection techniques in accordance with defined incident response processes
- Managing and tracking ticket progress to resolution and closure
- Documenting experiences to improve policies and response plans
- Updating incident response and communications plans to reflect any process changes and perform updates to existing policies and procedures

The Results

The client's alignment with the SOC enabled the corporate security department to become more strategic and effective in their operations:

- Technological complexities were reduced by consolidating numerous portals, alerts, notifications, and points of investigation, which reduced the overhead of managing the security technology stack.
- Personnel shortages were mitigated by converting their security operations into a 24/7/365 solution with the SOC.
- Costs were decreased by eliminating licensing for products that were no longer needed.
- Security posture was matured across multiple regulations, including GDPR and SOX.
- MTTD and MTTR were decreased, including incidents from both host detection analytics and network detection analytics.

Case Study: Government Organization Strategic Planning Facilitation

We facilitate strategic planning sessions in order to help companies improve their communication and response plans. We review and analyze existing plans, gather information from various sources throughout the organization about the existing plans and how they can be improved, and present the results of the analysis to the company along with recommendations of how to improve their plans and implement them strategically.

The Client

Our client is a government organization dealing with regional communications. They wanted to develop a strategic plan to provide more proactive communications in response to incidents affecting their region.

The Challenge

The client needed assistance to develop a new "bottom up" strategic plan to reduce the sense of "reactive" responses.

The Solution

We empowered the client to develop a 3-5 year strategic plan for regional staff using our facilitation toolkit for the three phases before, during, and after the facilitation.

- In the pre-planning phase, we reviewed and analyzed the client's strategic planning content as well as best practices with respect to communications strategic plans. We reviewed and analyzed existing survey results, consulting reports, guidance documents, and other assets identifying gaps between current and future strategic direction, including the current draft business/operating model for the organization.

- We supplemented document reviews by interviewing leadership stakeholders from each of the five separate organizational functions represented by the client, actively engaging stakeholders from all key parts of the organization to ensure full context.
- We designed an activity-based approach to source strengths, weaknesses, and opportunities directly from staff, management, and leadership and conducted an event to gather information from stakeholders.
- We used pre-meeting research and extensive planning to ensure the conceptual and logical framework was ready to guide stakeholders through the actual facilitation.
- We prepared checklists, conducted a walkthrough, and performed multiple checks to ensure an extremely high level of quality control for the event execution, ensuring nothing would distract from the core event activities.
- During the event, we led and ensured forward progress through the structured meeting agenda, guiding participants through criteria-based analytical exercises to understand problems and establish goals, objectives, and related strategies for accomplishment.
- After the event, we used detailed documentation to produce a report that empowered the organization to improve its own capacity within its organizational context.

The Results

This successful strategic planning facilitation demonstrated the three-phase approach using specific knowledge, tools, and approaches that also supported effective exercise facilitation.

- We used a rigorous, analytical facilitation methodology to ensure that the outcomes provided the client with high-quality, carefully documented information and analysis to support lasting change.
- The final product was a 6-goal strategy, with aligned objectives and implementation strategies that would be effective for guiding and coordinating the efforts of the communications division at the regional office.