

Maximize Retail Security with SOC Innovation

Industry: Retail

Size & Revenue: 500+ employees | \$350 m (approx.)



Business Problem

The client sought to enhance their SOC by clarifying the scope of services, standardizing risk assessment and prioritization, and defining roles and responsibilities. They aimed to establish a clear strategic vision and identify the necessary people, processes, and technology to create a more effective SOC.

How Intertec Helped

- **Strategic Development:** Intertec developed a comprehensive Cyber Security Operations strategy, outlining a clear vision, mission, goals, and objectives for the SOC.
- **Role Definition:** Specific SOC roles and responsibilities were clearly defined, ensuring that every team member understood their duties and how they contributed to overall security.
- **Tailored SIEM Use Cases:** Intertec developed SIEM use cases tailored to address the specific risks applicable to the retailer, ensuring targeted threat detection and response.
- **Prioritized Security Controls:** Cybersecurity controls were recommended and prioritized to mitigate identified risks, enhancing the organization's overall security posture.
- **Best Practice Frameworks:** Designed and implemented an operational framework for the SOC, adhering to international standards and best practices to ensure robust security operations.

Business Outcomes Delivered

Through this comprehensive approach, Intertec successfully implemented a Global Security Operations Center that not only met the retailer's immediate needs but also positioned them for future growth and security challenges.

- Enhanced management oversight, allowing for more informed cybersecurity budgeting and decision-making.
- SOC services are now fully aligned with the current business requirements and are flexible enough to cater to future needs.
- The organization now has clear accountability for cybersecurity, with well-defined roles and responsibilities.
- Strategic roadmap: A strategy-aligned roadmap guides the SOC organization in achieving its goals, ensuring long-term success.
- Justified SOC costs: The value of the SOC services to the business is now realized, with costs fully justified by the enhanced security capabilities.
- Continuous improvement: SOC processes are statistically measured and continually improved, ensuring that the SOC evolves to meet new challenges.