Security Tools Rationalization Assessment

Evaluate the coverage and effectiveness of your existing security tools - accounting for capabilities, threat landscape, and risk tolerance.

The status of an organization's security program, and the tools and applications it uses, is the product of past decisions and business context. This previous context must be re-validated to ensure it is consistent with present corporate objectives and desired risk tolerances. EVOTEK's Tools Rationalization Assessment (TRA) works in collaboration with client stakeholders to inventory existing security services, applications, and tools to evaluate their efficacy. The assessment determines whether current security tools are adequately addressing the organization's security and risk objectives.

Business Challenge

The risk-based approach from EVOTEK to assessing cybersecurity tools for efficacy and business alignment provides a roadmap for clients to understand where their programs are performing well, where there are areas for improvement, and specific guidance on how to achieve a future desired state. The TRA provides a broad evaluation of the organization's cybersecurity program against the material business applications to understand what strategic adjustments can be made to close gaps and mature the cybersecurity program. Recommendations for maturity may be relevant across business functions such as security operations, vulnerability management, cloud security, and governance and compliance programs.

A Proven Solution

Our TRA evaluates client cybersecurity tools against best practice, known adversarial behaviors, and client operating environments including IT infrastructure and assets, tool implementation, staffing levels and knowledge, and operating procedures. The assessment offers a mix of technical and business-focused insights into security tools and their implementation to offer context and perspective to both security and executive leadership as well as to security, infrastructure, and operations leads. The strategic roadmap provides key recommendations to address material risks and weaknesses, supporting the maturity of client cybersecurity programs aligned to business objectives.

Solving Challenges

EVOTEK engaged with a client that wanted to ensure their cybersecurity spending was aligned to the broader context of organizational priorities and objectives and ensure that there were both no gaps in coverage or redundant tools. By discovering services, applications, and tools used for cybersecurity across the business, EVOTEK was able to reveal interdependent and overlapping security tool functions, leading to a decrease in security tooling expenditures. Additionally, our process identified key risks in visibility and alerting and vulnerability management. Our team was able to make relevant and timely recommendations aligned to a roadmap to mature client security operations based on current tool contract status, licensing, and renewal dates.