ARCTIQ

# Security Operations Assessment

Prepare your operations team to defend against cyber-attacks, assess maturity, and chart a strategic evolution toward next-generation defense.

The Security Operations Center (SOC) has an unprecedented challenge: to defend against advanced threats on a day-to-day basis while also proactively designing for the next generation of automation and artificial intelligence. Regular operations leave minimal time for projects and incremental improvements let alone the generational leaps in capabilities needed to address the rapidly changing cyber landscape.

Arctiq's Security Operations Assessment (SOA) provides a rigorous, data-driven evaluation of your cyber operations capabilities. We deliver unparalleled clarity into your people, processes, and technology, transforming these insights into strategic analysis and an actionable roadmap.

## Resiliency by Design

Arctiq took a resiliency-centric approach as the foundational theme for evaluating and building a highly capable, mature, and functionally implemented SOC. We utilize a long-term perspective approach to distinguish from incremental improvements and quick fixes compared to addressing systemic challenges and implementing generational leaps and advanced practices.

Our background and experience in security architecture, solution design, managed services, and infrastructure give us the best approach to understanding and building advanced security operations with you. Secondly, we have aligned our approach to NIST CSF , NIST 800-53 Rev. 5 , CMMI , and FIRST to base our approach off industry leading and recognized frameworks for security programs and operations. The assessment includes:

- Comprehensive documentation, resource, technology, and process review to understand your SOC's current posture and capabilities to detect, respond, and mitigate cyber threats.
- Tailored workshops to ensure we assess and evaluate our six key domains of SOC operations effectively.
- In-depth analysis of the SOC's capabilities to execute across management, communications, incident response, cyber threat intelligence, security technology, and metrics.
- An advanced evaluation of the SOC's resources and competencies contrasted against a skills evaluation to determine gaps from a vertically integrated viewpoint that exposes key constraints on people, process, or technology.
- Clearly outlined and detailed measures of maturity and capability implementation levels designed to pinpoint where SOC operations resiliency is at risk of material weakness.

## Key Outcomes:

- Open discussion and collaborative workshops to discover and discuss current day operations, current state architecture, and future state desired capabilities for the SOC.
- In-depth and detailed reporting that incorporates a balanced approach to what Arctiq has observed and analyzed vs. the real-world constraints the SOC operates within.
- Our reporting is actionable, and reality-based with a focus on helping you achieve long-term success. We've incorporated maturity and implementation capabilities to ensure a balanced and contextual approach to gap analysis.
- Functional and usable resource competency and skills matrices that enable our customers to spotlight existing resource capabilities and plan for future desired state staffing models.
- A strategic roadmap based on desired state architecture that designs a path based on initial gap remediation, then builds long term resiliency and growth next-generation cyber security capabilities.

Partnering with Arctiq to mature your SOC operations enables your team to strengthen its defenses, stay ahead of adversaries, and build resiliency that adapts to modern attacks.

Contact Arctiq today for a complimentary consultation.

**Book a Consultation**