capability

Cybersecurity

steampunk®

# Working in Steampunk's Cybersecurity Practice

## Protecting our Client's Data and Systems

For more than sixteen years, we have protected our clients' data and systems. We continue to take pride in the expertise we provide in this area, and as we pivot to our new company vision, as Steampunk, we are doubling down on providing leading cybersecurity capabilities for our clients. Our corporate experience is rooted in governance, risk and compliance, and we have expanded beyond that to provide cybersecurity services to our clients in a wide variety of areas:

+ Cybersecurity Engineering
+ Insider Threat
+ Penetration Testing
+ GRC Modernization
+ SOC/DSOC Monitoring and Management
+ Continuous Monitoring
+ Continuous Authority to Operate

**By blending advanced technology capabilities such as cloud & data engineering, advanced analytics, artificial intelligence, DevSecOps, and automation - Steampunk delivers modern, transformative cybersecurity solutions. Our approach prioritizes customer experience, ensuring that we address key challenges while fostering user adoption through modern change management practices. All of this is facilitated through our innovative Design Intelligence delivery framework, which integrates CX, integrated technology competencies, and proven delivery methods.**

## GRC Modernization

A comprehensive and coordinated Governance, Risk, and Compliance (GRC) program sets the tone for a wellfunctioning cybersecurity capability. We help our customers mature their GRC program to align with commercial and government best practices and emerging trends or we help to establish a GRC program should one not exist already. We help organizations understand roles and responsibilities related to cybersecurity and craft processes for developing the right organization structure and processes to support GRC. We create or refine a structured approach to cybersecurity and risk management across IT system teams, business/mission teams, and security teams

## Continuous Authority to Operate

cATO is a modern, dynamic approach to maintaining the security and compliance of government IT systems by shifting from periodic, point-in-time assessments to ongoing, automated monitoring and risk management. Unlike traditional ATO processes, which can be slow and only provide a snapshot of security posture, cATO leverages automation, continuous monitoring, and DevSecOps practices to ensure that security controls are assessed and maintained in real time as systems evolve and new code is deployed. This enables agencies to rapidly deliver new capabilities while maintaining a robust security posture and compliance with regulatory requirements.

## Penetration Testing

Successful penetration test can provide an organization with invaluable information about the vulnerabilities at the system, infrastructure, and personnel. We identify system and network vulnerabilities as an ethical hacking organization in order to prevent actual malicious actors from compromising an organization. Often, we find our clients deploying pen testing services to test and strengthen the veracity of the other cybersecurity services running at an organization.

## SOC Management and Monitoring

The SOC is the brain of a cybersecurity organization. It sits squarely in the center of all the security operations, monitoring, and response activities and is responsible for protecting the organization and their people, data and systems. Our cybersecurity experts bring monitoring & response, prevention & detection, incident management, and overarching SOC management experience that we apply to the complete SOC lifecycle. In many organizations, the SOC is ultimately responsible for all operational aspects of cybersecurity. All of the people, processes and technology involved in securing an organization and its assets are in the purview of the SOC, and our teams are experienced and ready to lead your organization's SOC management.