capability

DevSecOps

steampunk®

Working in Steampunk's DevSecOps Practice

The Brightest Minds, Bold Solutions, Mission-Focused Outcomes

We work at the intersection of software engineering, IT operations and cybersecurity to design, implement, test, secure and deploy large-scale systems reliably, efficiently, and at-scale. Our DevSecOps team is dedicated to innovating with technology in new ways and using this technology to help meet this mission of our customers.

Steampunk believes people are at the core of everything we do. We value the development of our employee's careers and build our teams to enable continuous learning, not just in one skill but cross-domains. Our teams value diversity of people and ideas to build the best solutions and are comprised of individuals with a variety of skill sets including:

+ Software Engineering
+ Test Automation
+ Site Reliability Engineering
+ Cloud Infrastructure Engineering
+ DevOps Pipeline Engineering
+ Integration Engineering

As part of the Steampunk DevSecOps Practice, you'll work alongside motivated technologists and get the opportunity to solve complex challenges using cutting edge technologies. You should be passionate about software solutions, automation, operational excellence, and infrastructure. Your technology toolkit is wide, but there is probably one area you specialize in. You can efficiently tackle problems through code, hardware, networking, or storage within complex systems.

Leverage open-source and enterprise technologies in addition to the Steampunk Foundry to deliver best-of-breed software solutions using Continuous Integration and Continuous Delivery.

Create state-of-the-art automation capabilities to support delivery by leveraging automation in testing, security, infrastructure, networking, configuration management and deployment.

Our DevSecOps Practice Delivery Capabilities:

+ DevSecOps Maturity Assessment
+ Full Stack Software Development
+ Organizational Transformation and Coaching
+ Managed DevSecOps Services
+ CI/CD Pipeline Engineering
+ Infrastructure Automation
+ Test Automation
+ IT Operations
+ Application Security

capability

Data Exploitation

steampunk®

Working in Steampunk's Data Exploitation Practice

The Best Data Scientists, Complex Problems, User-Focused Outcomes

We are a team of talented data practitioners working together to solve real-world, complex data challenges. We keep our customers at the center and are guided by Steampunk's principles of Design Intelligence® and DevSecOps. Our Data Exploitation team solves problems in areas ranging from data strategy, to data engineering, to advanced machine learning.

Steampunk believes that people are at the core of everything we do. We value the development of our employees' careers and build our teams to enable continuous learning – not just in one skill but cross-domains. Our teams value diversity of people and ideas to build the best possible solutions and are comprised of individuals with a variety of skill sets including:

+ Data Architecture
+ Data Engineering
+ ETL Development
+ Data Visualization
+ Predictive Modeling
+ Machine Learning and Artificial Intelligence

As part of the Steampunk Data Exploitation Practice, you will work with a group of talented, passionate, and highly specialized data practitioners, who persistently strive to craft state-of-the-art solutions. As a prospective data punk, you are self-starter looking to hone and grow your skill set and possess data exploitation knowledge that you can bring to bear on day one. Whether you are a data engineer or a machine learning specialist, you understand the field of data exploitation and you are able to write elegant, optimized code. You love working in teams and cherish the opportunity for peer review and constructive ideation, networking, or storage within complex systems.

Architect data models, engineer data pipelines, develop features, train, test, and validate machine learning models, to create high-end ML and AI solutions to client mission challenges.

Implement state-of-the art MLOps pipelines to create, deploy, monitor, and continuously train machine learning systems. Reinvent data science practices through collaboration, automation, and best-of-breed tools.

Our Data Exploitation Practice Delivery Capabilities:

+ Data Strategy, Architecture, and Governance
+ Data Platforms
+ Data Integration
+ Automation
+ Visualization
+ Data science
  - Artificial Intelligence
  - Machine Learning
  - Deep Learning
  - MLOps

capability
Salesforce

steampunk®

Working in Steampunk's Salesforce Practice

Accountable, Competent, Forward Leaning, and Transparent

We represent disruption in the federal government space with a commitment to do things differently. Because of this people WANT to be a part of what we have going on. Leveraging Design Intelligence®, we partner with the Design & Strategy Practice on every engagement so we can begin to build almost immediately, allowing our clients to see, feel, and touch the solution as early as possible.

Salesforce talent is hard to find and highly sought after. We are building our practice differently, in a way that is sustainable, and in a manner that will continue to attract exceptional teammates into the practice. We focus on investing back into our resources by providing them the challenge and means to grow in their technical expertise and as leaders.

Our practice is comprised of all levels of business/functional analysts, application developers and application architects, technical architects, project/program managers, and Directors of customer engagement, but we are one team, focused on the success of everyone.

We are looking for difference makers; people who want the chance to develop unique Salesforce solutions to our government partners mission critical needs.

Helping our clients harness the power of their increasing investment and desire for low code or no code platforms.

More rapid development and deployment of solutions, as well as lower cost and more reliable ongoing operations.

Our Salesforce Practice Delivery Capabilities:

+ Security and Application Architecture
+ Object Modeling and Scalability
+ Service Cloud
+ Community Cloud
+ Digital Engagement
+ Customer Portals
+ Customer Engagement and Project Delivery
+ Integrations
+ Lightning Web Components
+ Salesforce DX and CICD

capability

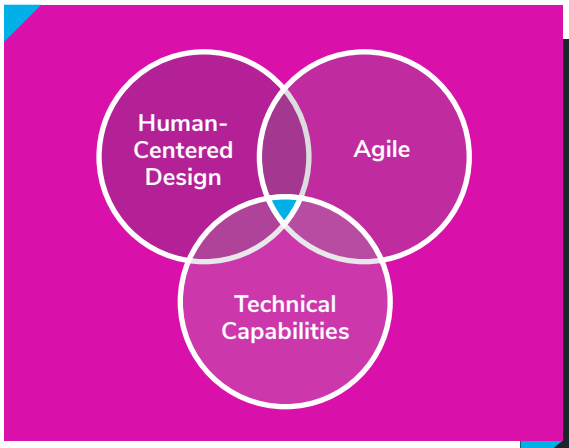
Design & Strategy

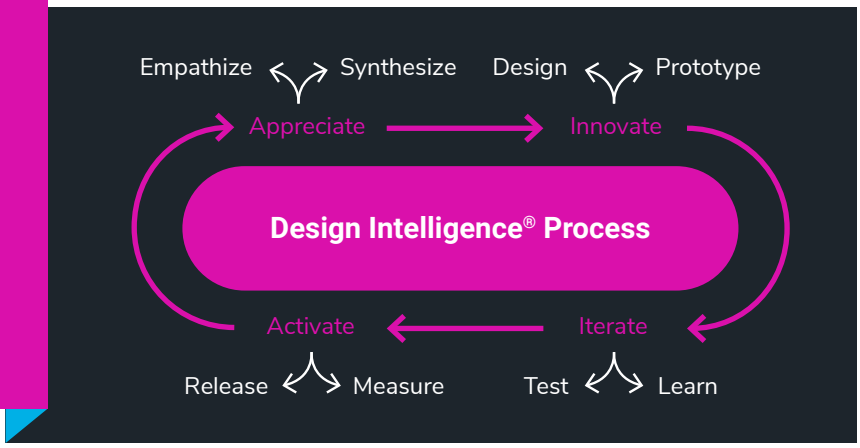
steampunk®

Working in Steampunk's Design & Strategy Practice

Design. Disrupt. Repeat.

Steampunk's Design & Strategy practice is integrated within our delivery teams and capability offerings to develop human-centered solutions through our Design Intelligence® process. DI is the nexus of how we define, create, and deliver products and services—grounded in the understanding of the people who use them.





We operate across the organization, in tandem with the other Steampunk practices, to support customer portfolios within government sectors. "People at the Core" is Steampunk's number one value. We promote the development of our employees' careers and build our teams to enable continuous learning – not just in one skill but cross-domains. Our teams believe that diverse perspectives build the best possible solutions.

The Design & Strategy team is a blend of Service and UX designers who untangle wicked problems through divergent and convergent thinking—uncovering pain points and opportunities and making sure stakeholders' needs are met within a proposed solution. They take challenges from "don't know, could be" to "do know, should be".

Our Design & Strategy Practice Delivery Capabilities:

+ Workshop Facilitation
+ Service Design
+ Design Research
+ Design Strategy
+ Project Management
+ User Experience Design
+ User Interface Design
+ Content Strategist
+ Information Architecture
+ Visual Design
+ Interaction Design
+ Data Visualization
+ Communication Design
+ Change Enablement

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
+ Incident Response
+ SOC/DSOC Monitoring and Management

Governance: The overall management approach, strategy, and policies for an organization's cybersecurity practice. Risk Management: The process for identifying, analyzing, and responding to cybersecurity risks. Compliance: The procedures, guidance, best practices, and checks that define organizational cybersecurity practices and ensure they are properly implemented.

Governance, Risk and Compliance

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

Incident Response

Cyberattacks or data breaches can be catastrophic to an organization's infrastructure, reputation, budget, and perhaps most importantly – the safety and security of American citizens. Organizations must now ensure they are set up with thorough network monitoring and incident response (IR) capabilities to ensure they have the strongest protections against malicious actors. We help our customers protect their networks, data, and reputation from security breaches and attacks by implementing an end-to-end incident response program.

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.