



CYBER WARFARE

SECURE THE ASSETS
NEUTRALIZE THE THREATS

Cyber attacks are dominating the headlines. Today's cyber threats are compromising infrastructure, technology, and data operations leaving our military and governments vulnerable. Cybersecurity threats represent one of the most serious national security challenges.

Technica[™]

DEFENSIVE CYBER INTEGRATION SERVICES

Technica was founded on engineering methodologies and best practices by engineers passionate about researching new technologies that tackle tough challenges. Cybersecurity serves as the backbone of our company.

Today, the integration and consulting services of Technica Next-Generation Defensive Cyber Services are at the forefront of AI/ML-infused cyber solutions. As more organizations expand and modernize their environments, the attack surface grows and makes it more challenging to defend against advanced threats. Handling these and other persistent digital-age cyber challenges requires shifting from a traditional, reactive, maintain-the-perimeter approach to a modern, proactive, dynamic-defense model. We created these service offerings to rethink defensive cyber and enable the detection and discovery of new threats in a secure and timely manner.

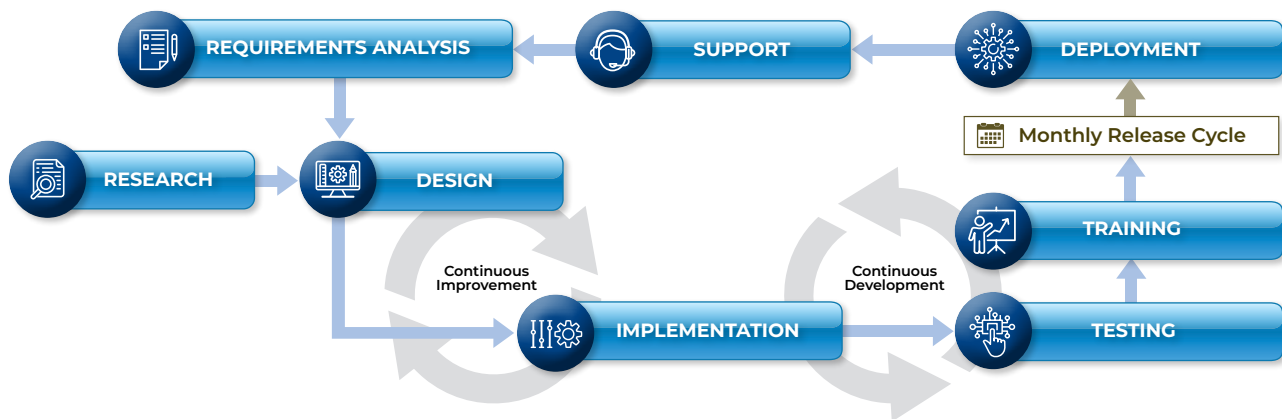
RECONFIGURABLE SOFTWARE FOR CYBER MISSIONS

Technica's Defensive Cyber Integration Services operate with a modular mindset that allows customers to adapt their cyberinfrastructure to specific needs. We improve defensive cyber operations by fusing disparate data sources and tools to accelerate threat detection and response. No single cybersecurity tool can do everything, no matter how well it works. Organizations need to employ various tools to play a distinct role in a broader, integrated security solution. Customers can add and remove functionality by installing cyber tools, easily configuring them based on unique mission requirements. This process eliminates the walls of traditional application architecture, allowing for varying functionality combinations in a single, seamless environment and easy-to-use dashboard.



DEFENDING THE **NATION'S CRITICAL NETWORKS AND SYSTEMS** THROUGH THE USE OF ADVANCED SOLUTIONS THAT **IMPROVE THE SPEED AND EFFECTIVENESS OF CYBER MISSIONS.**

TAKING FULL ADVANTAGE OF TECHNICA'S CONTINUOUS SYSTEMS ENGINEERING AND DEVELOPMENT



REQUIREMENTS ANALYSIS: The mission requirements for defensive cyber are constantly changing as the cyber-attack battlefield changes. Our team includes cyber threat hunt SMEs to support the customer and analysts to break down the use cases in question to the toolset, hardware, and storage requirements for any given mission.

RESEARCH: We maintain a robust innovation and research practice supported by subject matter experts. We house this capability in our state-of-the-art Cyber Innovation Lab where disruptive innovations create new value systems by focusing on nascent and novel technologies. Sustaining innovations are incremental. For example, a new AI algorithm that spots network traffic anomalies better than hard-coded, signature-based rules engines could be a disruptive innovation.

DESIGN: Our design component is closely tied to both the research and implementation services, taking the requirements analyzed by the SMEs and appropriately applying the available innovations that can be realistically implemented securely. Technica takes a holistic approach to design that supports the overall mission.

IMPLEMENTATION: We take control of the development process, implementing a SAFE Agile DevSecOps Continuous

Improvement/Continuous Development pipeline to ensure the consistent creation of secure code. Technica development includes peer review, unit performance, and end-to-end functionality testing.

TESTING: Technica operates testing ranges that meet defense and intelligence requirements to allow developers to battle-test solutions before they go live. This ability allows for the quick creation and execution of new solutions that seamlessly fit inside the overall architecture.

TRAINING: Our team provides comprehensive classroom, online, and video training. We customize each session to the customer, location, and classification level.

DEPLOYMENT: We support the cyber analyst by providing automated deployment of the available tools in the configuration needed for the specific mission – mission ready.

SUPPORT: Technica's holistic implementation of IT Service Management leverages ServiceNow modules that promote shared learning, faster resolution, and product improvement. In addition, our service desk has training in installing the kits, and this hands-on knowledge is a crucial enabler for problem resolution.

ON THE CUTTING EDGE OF R&D

Within Cyber Innovation, research and development is core to our mission. The senior scientists and engineers in our advanced Cyber Innovation Lab solve complex problems in applied data science, artificial intelligence, machine learning optimization, and edge computing.

The key areas of research include:

- Explainable AI for Cyber Hunt
- Natural Language Processing for Log Analysis
- Improved Graph Based Visualizations for Cyber Hunt Analysis
- Improved Intrusion Detection for ICS and SCADA Attacks

Technica[™]

WE LISTEN. WE APPLY. WE SOLVE.

Technica™

Technica Corporation, founded in 1991, provides high-end system engineering services to Defense, Intelligence, Law Enforcement, and Federal civilian agencies. Technica brings knowledge, solutions, and secure process management to environments of diverse functions for its customers' rapidly changing and urgent requirements. With groundbreaking R&D, Technica's senior scientists and engineers are always finding new, innovative ways to solve complex problems and overcome today's Cyber Warfare challenges by leveraging deep experience in Systems Architecture & Integration, DevSecOps, IT Service Management, AIOps, Machine Learning, and Artificial Intelligence.

