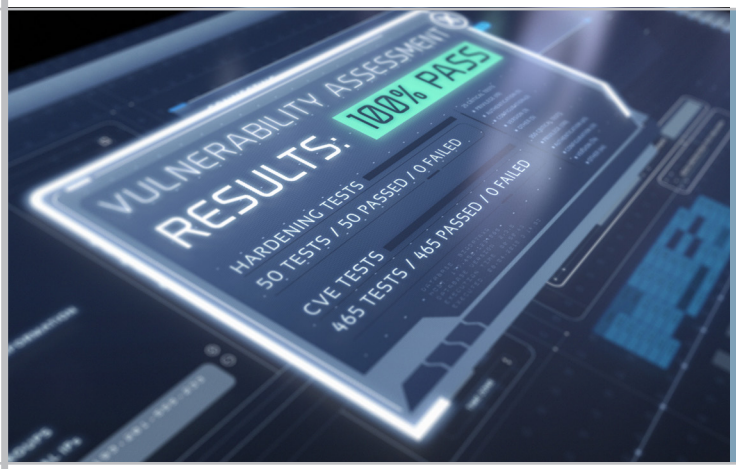
Raytheon

Raytheon CODE Center

A Leading-edge, World-class Cyber Range



The Raytheon Cyber Operations, Development and Evaluation (CODE) Center is a state-of-the-art cyber range available for internal customer work to test and ensure the resiliency of existing and future mission-critical systems against cyberattacks.

Benefits

- Access to state-of-the-art facility and industry-leading cyber experts and to effectively test for, mitigate and harden against vulnerabilities
- Use of proprietary tools to assess DoD and other U.S. government systems, networks and platforms based on real-life attack scenarios
- Conduct force-on-force cyber exercises and training in simulated environment
- Use innovative engineering environment and technologies to safely and affordably test and integrate cyber technologies
- Better manage geopolitical risks and military operations with well-tested DoD team and systems

Raytheon CODE Center
CYBER OPERATIONS
DEVELOPMENT & EVALUATION

The battlefield that the U.S. Department of Defense (DoD) faces today relies heavily on cybersecurity, electronic warfare and air and missile defense to eliminate threats and gain strategic advantage. Having resilient in-service systems is key to maintaining our military edge and keeping our service members safe.

The Raytheon (CODE) Center is a state-of-the-art cyber range used to test and ensure the resiliency of existing and future mission-critical systems against cyberattacks.

Realistic and Robust Tests and Evaluations

Raytheon built this 30,000 square-foot live-fire cyber range to test the resilience of systems against cyber attacks. The CODE Center is used to test networks, systems and platforms by exposing them to realistic nation-state cyber-threats in a secure facility with the latest tools, techniques and malware. Our cutting-edge vulnerability testing and mitigation approaches leverage Raytheon's significant $3.6 billion cyber investments in acquisitions, research and development with the best cyber experts in the industry.

We bring Raytheon's decades-long experience and domain expertise in protecting our own systems, our products and our customers. This experience has given us the unique capability to cultivate the CODE Center's cyber talent, technologies and processes that deliver field-proven and mission-reliable cyber solutions.

Innovative, Versatile Cyber Environment

To set up realistic tests, Raytheon's cyber range operators can create an accurate replica of a system. The CODE Center can emulate a variety of sizes and types of networked environments and cyber-physical systems, including air traffic control, power grids, water supplies, missiles, radars, or security and network operations centers.

With Raytheon's range automation software, operators can rapidly set up, tear down and sanitize a massive test range in hours or days, instead of months. Environments can be created to assess the destructive effects of attacks by nation states or sophisticated cyber criminals.

CODE Center Capabilities

- Vulnerability assessments of architecture, software and networks
- Hardware security assessment using reverse engineering, firmware code analysis and other tools
- Radio frequency and wireless vulnerability and radiated emissions testing
- Penetration testing and evaluation
- Mitigation planning and consulting

With the industry's best vulnerability assessment and mitigation tools within reach, the CODE Center can help the DoD prepare for the "Internet of Things".

Red Versus Blue Team Exercises and Skills Maintenance

For any type of DoD or U.S. government mission, investing in skills maintenance cyber professionals is critical to effective defense. The CODE Center's force-on-force "blue/red" team rooms, simulation tools and the massive data center enable customers to simulate real-world cyber challenges in a protected environment. In these simulated environments, an aggressor red team is pitted against a defending blue team that provides critical infrastructure protection. Blue team members hone their skills as they defend systems against these mock attacks.

Tests involve rapidly evolving cyberthreats and are designed to be conducted at multiple levels of security. Re-running exercises reinforces training and enables knowledge transfer for new cyber operations personnel.

Raytheon's Global Cyber Innovation Network

The CODE Center is part of Raytheon's network of cyber innovation and demonstration centers around the world. Raytheon's cyber centers assist customers in assessing technologies and finding integrated solutions for their most challenging operational cybersecurity needs. Each of the centers that comprise Raytheon's Global Cyber Innovation Network is uniquely focused on different areas of this critical mission space:

- Global Cyber Solutions Center (GCSC): A state-of-the-art environment that enables rapid assembly and assessment of technologies in addressing customers' operational cyber requirements. Built to be a modular, versatile Security operations center, the GCSC can simulate real-world events for training purposes. Based in Dulles, Virginia, close to Washington, D.C., it's geared toward international government and commercial customers.
- Raytheon Vulnerability Research Ranges: Industry-leading vulnerability research experts in Raytheon's various Vulnerability Research Ranges are capable of conducting hundreds of millions of tests a week.

CODE Center lobby and reception area

Classroom Training

- Cyber executive session: Raytheon executives receive a review of available cyber resources within the company.
- Cyber professional: technical practitioners including tools/techniques used by attackers/defenders; builds on reverse engineering fundamentals, attack techniques and human dimensions to design sophisticated attack/defense scenarios; culminates in a four-day, realistic capstone exercise.
- Cyberforce superiority belts: exportable classes covering penetration testing methodology; an overview of the methods/mindset of a cyber attacker.

Working With the CODE Center

The following indefinite-delivery, indefinite-quantity (IDIQ) vehicles provide an avenue for customer needs to be easily contracted with the CODE Center. Additional contract information and opportunities are available at : www.raytheon.com/ourcompany/idiq

- GSA Schedule 70
- ATSP4: Advanced Technology Support Program IV
- CIO-SP3: CIO Solutions and Partners 3
- OASIS: One Acquisition Solution for Integrated Services
- SSC PAC: Space and Naval Warfare Systems Center Pacific cybersecurity support

For further information contact:

Intelligence, Information and Services
22260 Pacific Boulevard
Dulles, Virginia
20166 USA
code_center@raytheon.com

www.raytheoncyber.com

Raytheon