
# Cyber Assessment Services

## Beyond the Checkbox

Millennium's Cyber Assessment Services leverage our threat-based assessments to the Department of Defense (DoD), providing holistic risk analysis of enterprise and standalone environments.

Millennium risk assessments go beyond compliance analysis and policy validation, focusing on testing **'the way things are' as opposed to 'the way things should be.'** Combining grounded study, with a creative out-of-the-box thought process, our threat actors have identified vulnerabilities in systems, networks, and human processes that, when combined, represent critical system and mission failures. Vulnerabilities are often overlooked by other teams focusing on technical aspects of tools and process without investigating the greatest weaknesses in systems, the people that use and configure them.

Millennium assessment services are backed by real-world threat intelligence, and represent capabilities of threat actors, including nation states, insider threats, terrorist/hate groups, and others ranging in sophistication and technique. Combined with our capability development services, we can portray the abilities of nearly any team of any size or sophistication.

## The Millennium MILSPEC Approach

Millennium has provided specialized technical expertise to the Department of Defense (DoD) Red Team community for over 9 years. From enterprise networks, to accounting platforms, one-of-a-kind military networks, and aircraft and network connected weapons systems, we have completed hundreds of security assessments on complex and widely distributed tactical and enterprise networks, systems, and applications.

## How We Can Help

Millennium provides Cyber Assessment Services to corporate and government customers. Using threat-intelligence backed tools and methodologies, we identify true risks present in our customers' environments. Millennium has decades of experience performing offensive cyber campaigns against corporate, government, and hardened military networks and weapons systems.

## Cybersecurity Services Provided

- Red Team Services
- Insider Threat Risk Analysis
- Penetration Testing
- Vulnerability Assessments
- Network Architecture Reviews
- Wireless Security Assessments
- Web Application Assessments
- Social Engineering Campaigns
- Physical Security Assessments
- Secure Code Reviews
- Tailored Software Development
- Technical Research and Development
- Offensive Cyber Training

## Who is Millennium

Millennium Corporation is a strategic management, cybersecurity and IT consulting firm and committed partner to the Government– driven by results and people focused. We have a dedicated team of security consultants trained by the Department of Defense (DoD) including testers, assessors, trainers and instructors, hackers, administrators, and technical Subject Matter Experts (SMEs).

## How to Acquire Services

Millennium Cyber Assessment Services are purposely designed to make it easy for customers to engage us on a long term, short term or even ad hoc basis. Our goal is always to maximize the quality of services and minimize costs and burden to our customers.

Our access to a broad portfolio of contract vehicles and partners sets the standard for excellence – spanning the lifecycle of professional services, including:

- ARDEC LRED
- GSA IT 70
- JPEO CBD OPETS
- Seaport-e 8(a)
- SSC PAC CSRETI
- B2S2
- GSA 00CORP PSS
- NAVAIR Cyber Warfare Detachment (CWD)
- USPS OIG Penetration Testing Service

## Staff Certifications

- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Offensive Security Certified Expert (OSCE)
- GIAC Penetration Tester (GPEN)
- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- CISSP –Information Systems Security Management Professional (ISSMP)
- Cisco Certified Network Associate (CCNA)
- Red Hat Certified System Administrator (RHCSA)
- Microsoft Certified Professional (MCP)

## Case Study

**Customer's Challenge:**
Over the past 7 years, Red Team operators have become high-demand, low-density assets. To bridge this gap DOT&E refined and expanded the use of long-duration Red Teaming, termed the Persistent Cyber Opposing Force (PCO). PCO is far better at emulating advanced, persistent nation-state cyber threats, while more efficiently utilizing scarce Red Team resources.

**Millennium's Response:**
Millennium Red Team members have been instrumental in the execution of PCO activities which have identified, and rapidly addressed, serious vulnerabilities. Millennium has been able to continuously provide an extremely high level of expertise by only hiring the best in the industry. Our DoD Red Team customer said it best: "Red Teaming is extremely complex and rapidly changing, and Millennium has routinely exceeded the government's expectations. If we did not have the support of Millennium, government systems would be put in jeopardy of not being able to defend against foreign or domestic cyber invaders. Millennium has shown a great, if not unique, ability to find the right people at the right time. Millennium management has demonstrated they know brilliant cyber operators."

## Millennium Contacts


Ben Clark
*Director, Cybersecurity & IT*
256-876-2062
ben.clark@millgroupinc.com

Keith Cromack
*VP Business Development*
703-447-6711
keith.cromack@millgroupinc.com


MILLENNIUM CORPORATION