



# Cybersecurity on a mission

FROM AI TO ZERO TRUST, WE'RE SECURING WHAT'S MOST IMPORTANT






# OUR CAPABILITIES

Cybersecurity is more complex—and more important—than ever before, especially for government agencies and large enterprises. Leidos is a trusted cybersecurity provider, operating on the cyber front lines with 4,000+ cybersecurity certifications across the corporation and home to cyber’s top minds, invaluable expertise, and proven processes.

Leveraging our technical core capabilities, Leidos specializes in providing critical services, systems, and solutions, and leading nation-scale IT transformation programs that integrate breakthrough technologies as a force multiplier to enable and drive customer objectives via:

- **Optimized tools**
- **Enhanced situational awareness**
- **Informed decision analysis support**
- **Mission-focused innovation**


From transition to fully digitized government services, secure hybrid cloud, business process optimization, and the full spectrum of cybersecurity capabilities, our ability to deliver transformative digital solutions for customers is unmatched. Leidos is ranked #1 on *Washington Technology’s* Top 100 and we’re committed to investing in capabilities designed to help national security organizations and agencies outpace adversaries and protect citizen, assets, and information:




DIGITAL  
MODERNIZATION



CYBER  
OPERATIONS



MISSION  
SOFTWARE SYSTEMS



INTEGRATED  
SYSTEMS



MISSION  
OPERATIONS

# EVOLVING TECHNOLOGY TO OUTPACE ADVERSARIES

Information technology and security threats evolve and change rapidly, and the cyber threat from nation state actors continues to grow. These threats put pressure on agencies to upgrade and modernize their technology to ensure systems and networks are more reliable, efficient, and secure while reducing costs.

When it comes to securing data, applications, and networks, many government agencies are reliant on legacy systems that are vulnerable to malicious attacks. Investing in innovative, resilient solutions enables agencies to respond to sophisticated threat actors, adversaries, and environments that require security, precision, speed, and scale.

Leidos takes a proactive approach to cybersecurity. We focus on maximizing resources and ensuring the cyber resiliency of the mission using a threat-based methodology, leveraging knowledge and intelligence. Our cyber experts go beyond fundamental cyber hygiene and information assurance, bringing to bear our proven Defensive Cyber Operations tactics, techniques and procedures (TTP), and implementing advanced cyber analytics to anticipate and prevent cyber threats, including Advanced Persistent Threats (APT) and insider threats.

Leidos has the depth and breadth to support advanced cyber missions, both on the defensive and offensive sides. We defend the most targeted networks in the world and help our customers use cyberspace as an advantage. Lessons learned from our full-spectrum cyber operations are fed back into our other technical competency areas, so cybersecurity is embedded in Leidos software development, systems engineering, and solution architectures.

# Cyber 101

- **Cyber Physical Systems**—assets that interact with the physical world, which are either protected (DCO) or exploited (OCO) using cyber actions to perform a mission.
- **Defensive Cyber Operations (DCO)**—operations to preserve the ability to use friendly cyberspace capabilities and protect data, networks, platforms, and systems.
- **Offensive Cyber Operations (OCO)**—operations to collect intelligence or project power by the application of force in or through cyberspace.
- **Security Operation Center (SOC)**—centralized function within an enterprise employing people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

# How does Leidos define cyber as a capability?

For most government agencies, ‘cyber’ refers to cybersecurity efforts that protect systems and resident data through security-focused engineering, defensive activities, risk management, and regulatory compliance. Given the proper authorities, cyber capabilities also include work that supports the U.S. government’s offensive cyber missions.

**Leidos offers Full-Spectrum Cyber, a term coined by the Department of Defense (DOD), to include both defensive and offensive cyber operations.**

We support DOD and Intelligence Community customers across the entirety of their cyber missions, and at large enterprise scale. Our Full-Spectrum Cyber capabilities expand beyond defense and intelligence communities—Leidos also supports the broader government and commercial sectors, from enterprise cyber and network defense, to cyber defense of military platforms and Industrial Control Systems (ICS). Our capabilities span the entire cyber lifecycle, from providing network architecture design to operational, hands-on-keyboard analysts and cyber training and exercise support.



# TRANSFORMING IT AND CYBERSECURITY

Leidos is a recognized leader in cybersecurity across the federal government, bringing more than 30 years of experience defending global cyber interests and delivering advanced capabilities honed from protecting some of the world’s most valuable assets. Our solutions and services ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture.

We use intelligent automation and AI/ML-driven analytics, combined with our experience in detecting and mitigating complex security breaches and threat actors, to deliver cyber solutions that protect and defend the nation’s largest and most attacked mission-critical networks.

# DEVELOPING CYBER LEADERS WITH UNMATCHED EXPERTISE

The cybersecurity industry faces a unique challenge magnified during the past decade—an acute shortage of qualified personnel. As a powerhouse provider of IT solutions and services, Leidos is uncompromisingly committed to addressing the systemic cyber talent challenges across the cybersecurity landscape.

We’ve collaborated with cybersecurity experts across multiple industries to identify the skill sets and roles that Leidos—and our government customers—requires to support vital cybersecurity mission efforts. Our program maps to the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) and in 2020, we officially launched our CyberEDGE training academy. The program has exponentially grown the skills and experience of individuals looking to enter the cyber and IT realm into cybersecurity experts. To date, 100% of graduates have remained with Leidos and support active government programs.

# Impactful transformations

## WE'RE ON THE CYBER FRONT LINES



Using our cybersecurity maturity model, Leidos has led transformations for federal government Security Operations Centers (SOCs) and more than 20 geographically dispersed Fortune 500® commercial SOC's.



Our analysts operate 5 of the largest federal SOC's with continuous support—every hour of every day.



For a U.S. Government Agency, we successfully implemented our cyber method within six months to quantify and track all advanced persistent threat activity.

**\$1B**  
CYBERSECURITY  
ANNUAL REVENUE

**1,800+**  
EXPERTS IN  
CYBERSECURITY AND  
NETWORK DEFENSE

**30+**  
YEARS OF  
EXPERIENCE

**#1**  
US DOD AND  
INTEL COMMUNITY  
PARTNER

**#1**  
IT PROVIDER FOR  
US GOVERNMENT FOR  
22 YEARS

**15,000+**  
CYBERSECURITY PROS  
TRAINED

**1,000+**  
CERTIFIED SECURITY  
PRODUCTS VIA CC  
AND FIPS 204-2 TESTING LAB

**21**  
CYBERSECURITY  
PATENTS

## A RECOGNIZED CYBERSECURITY LEADER

Leidos is a Fortune 500® information technology, engineering, and science solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, civil, and health markets. The company's 40,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately \$12.30 billion for the fiscal year ended January 1, 2021. For more information, visit [www.Leidos.com](http://www.Leidos.com)



[leidos.com/cyber](https://leidos.com/cyber)

©2021 Leidos. All rights reserved. The information in this document is proprietary to Leidos. It may not be used, reproduced, disclosed, or exported without the written approval of Leidos. 21-leidos-0716-23111. Leidos Creative:20-284880

