DEFENSIVE CYBER PRACTICE

Unlocking advanced proactive protection to support secure and resilient environments

Delivering advanced, innovative, continuously improving cybersecurity solutions, technologies and practices to mission-driven organizations

OUR APPROACH

Leidos offers adaptive, scalable and secure defensive cyber solutions, combining proven tactics, techniques and procedures and industry best practices with advanced technology. Leidos optimizes previously untapped features of existing customer tools to rapidly improve security postures and increase value of previous investments. The practice delivers offerings in the form of blueprints, comprehensive content that represent proven existing solutions as well as prototype, proof of concepts, and minimum viable products which speed time to value and offer customers demonstrable proof to support proposals and other transaction authorities.

EMPOWERING YOUR MISSION

Leidos defends customer organizations with cutting-edge defensive security operations that leverage advanced data science and machine learning. Expertise and rapid deployment capabilities provide secure solutions that mitigate risk, enhance resilience, and ease operational burdens. Leidos offers advanced protection and peace of mind in an increasingly complex and aggressive threat landscape.

KEY CAPABILITIES	CUSTOMER BENEFITS
Security operations center transformation	To gain real-time threat detection and rapid incident response, Leidos consistently applies best practices, shared tactics, techniques and procedures, along with automation and optimized technology configurations, to enhance performance, efficiency, and protection of critical assets.
Cyber analytics and data science	The right data to the right system at the right time, unlocking actionable insights that seek to reduce data management costs, improve outcomes and speed actions across the entire cyber lifecycle.
Cyber workforce development and training	Integrated multimodal learning systems teach, test, reinforce and prepare staff for real-world, complex scenarios from single staff member to full-team simulations.
Risk management framework	Automation, inheritance, and templatization, when combined with continuous monitoring, speed time to value, maintaining continuous ATO status, and mitigating risk for resilent operations.
Enterprise security engineering	Cybersecurity and enterprise IT are both complex and complicated. Enterprise security engineering makes existing enterprises more secure with every change and secure by design makes it easier for all new capabilities to start and stay that way.

Through a defense customer, Leidos cybersecurity and operational services team effectively blocks an average of 231 million intrusion attempts, 26 million threat detections and 3.5 million spam messages each month.

With enterprise security engineering for a key defense organization, Leidos delivered cyber capabilities for secure 24/7/365 operation and sustainment, an 11x increase in cyber analytics and increased security awareness of connected assets by more than 20%.

CLOUD AND DATA CENTER / INFORMATION ADVANTAGE / APPLICATION MODERNIZATION / DEFENSIVE CYBER / NETWORKS / ENTERPRISE DIGITAL EXPERIENCE

FOR MORE INFORMATION
leidos.com/capabilities/digital-modernization | leidos.com/contact

leidos.com