

CYBERSECURITY

Solutions for an Increasingly Contested Environment



For programs of national importance, a robust, risk management-focused cybersecurity approach is essential to achieve objective protections for federal programs, particularly those considered National Security Systems (NSS).



The Space Dynamics Laboratory's (SDL) blue team/red team approach to cybersecurity provides resilient solutions that are effective in cyberspace and compliant with industry standards and Government regulations.

SDL provides research and development services across the cyber spectrum with an emphasis on complete system cyber resilience. Services range from hardening legacy systems to developing new systems that incorporate the latest in cyber technology.

SDL'S CYBER ENGINEERING PROCESS

SDL's experience with systems security engineering includes successful development and execution of strategies and solutions for attack surface mapping, network awareness, penetration testing, intrusion detection/prevention, network analysis, and cyber exercise execution.

SDL incorporates key industry and DoD cybersecurity best practices throughout the development cycle to increase the system resilience and prevent or mitigate cybersecurity attacks.

SDL embeds key cybersecurity processes into the standard Systems Development V-model, beginning with the requirements analysis phase and ending with Authorization to Operate (ATO) and system delivery.

FEATURES

- Risk management framework (RMF)-compliant, secure architecture design
- System threat & vulnerability assessments
- Red team evaluation & penetration testing

