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).

SDL's cybersecurity solutions enable Joint All-Domain Command and Control (JADC2).

The Space Dynamics Laboratory's (SDL) systems engineering 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.

CYBER ENGINEERING PROCESS

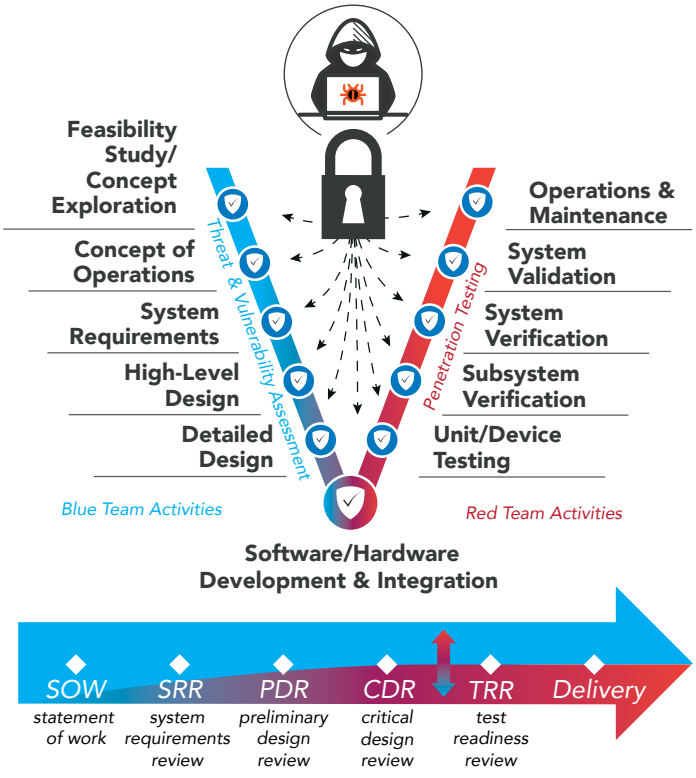
SDL's experience with systems security engineering includes successful development and execution of strategies and solutions for threat modeling, attack surface mapping, network awareness, penetration testing, intrusion detection/prevention, network analysis, and cyber exercise execution.

SDL incorporates key industry and DoD cybersecurity best practices throughout the development cycle to increase 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 on-prem & cloud architecture design
- Network analysis & intrusion detection/prevention
- Systems engineering approach, including threat modeling, secure architectures & vulnerability assessments
- Expertise in securing cyber-physical & operational technology systems



UTAH STATE UNIVERSITY
SPACE DYNAMICS LABORATORY®

416 East Innovation Avenue | North Logan, Utah 84341 | info@sdl.usu.edu | www.sdl.usu.edu

SDL/19-2045 Rev. E