We help harden platforms and control systems against cyber threats without the need for costly and risky redesigns.

CYBER HARDENING
Platform Protection to Neutralize Cyber Attacks

As cyber threats from nation-states, terrorist organizations, and other adversaries grow, the Department of Defense (DoD) and other federal agencies are working to protect both new and legacy systems from attack.

CYBER FROM THE PLATFORM PERSPECTIVE

While leaders have begun to look at inter- and intra-networking to provide total cyber security, certain systems have traditionally been considered "non-critical." For example, while cyber security implementation for shipboard operational networks is much better than it was 10 years ago, there is not yet a holistic approach to platform-level cyber security that also takes machinery control systems into account. Hackers can infiltrate these systems as a way to access other mission-essential systems and launch a cyber attack.

To address these vulnerabilities, leaders must consider the entire platform and how it communicates. From there, they need to invest in cyber hardening solutions that work with current systems to reduce the threat surface at the platform level.

CLOSING THE GAP ON CYBER THREATS

At Huntington Ingalls Industries (HII), we help close the gap by embedding cyber hardening across a variety of platforms and control systems that others leave unprotected— even if they're already deployed. We apply artificial intelligence (Ai) and custom-built products to help you implement, operate, and maintain cyber hardening tools without the need for costly and risky redesigns.

With solutions to assess, prevent, and mitigate attacks, our off-the-shelf, drop-in tools give you a fast, affordable way to neutralize current platform threats, while using deep and machine learning to build cyber hardening into the systems of the future. That's because our engineers have pioneered a new approach to hardening using an appliance layer on a deployed network without requiring changes to existing defensive tools or the underlying control system.

Through full-lifecycle support, we help you protect platform integrity and system uptime with the only complete, compliant cyber hardening suite for military platforms and control systems on the market.

HII'S CYBER HARDENING SOLUTIONS

Few things change as quickly as modern technology. That's why we apply our vendor-agnostic approach and agile security engineering methodology to every project and program, saving you time and money while delivering industry-leading cyber hardening solutions that are tailored for maximum effectiveness and able to evolve even as the threats and military platforms change.

CYBER THREAT ASSESSMENT

Using scalable, web-based tools, we gather and analyze your custom or situational inputs to assess specific cyber security risks. Then we recommend a plan to mitigate them.

CYBER HARDENING

Our experts come armed with hardening solutions for immediate deployment as well as the skills to provide security engineering or system modules for lifecycle integration.

DETECTION & MITIGATION

We provide active protection for your equipment and networks, by ensuring cyber attacks are prevented before a targeted system can be compromised or damaged.

SHIPBOARD CYBER REVIEW

We recently performed a top-to-bottom analysis of U.S. Navy shipboard networks, systems, and external interfaces to provide a baseline for lifecycle cyber engineering. This analysis collected data from all available sources on the "as built" configuration of networks and systems— from network topologies to all communication systems.

Based on this first-of-its-kind architecture package, we determined potential vulnerabilities, mitigations, and opportunities for cyber hardening as well as a starting point for lifecycle cyber security management at the platform level.

HARDENING AIRCRAFT CONTROLS

Our cyber hardening experts are working with the Air Force Research Laboratory (AFRL) at Wright-Patterson Air Force Base to develop a passive, hardware-based solution that leverages the inherent device physics of the 1553 bus to improve air-frame-level resiliency to cyber attack.

As part of this effort, we developed a number of hardware-based cyber defense techniques to ensure our system's survivability and reliability in the face of cyber attack, including a System-on-a-Chip-based solution to identify, contain, and recover from attacks on the aircraft 1553 command bus.

CONTACT:
John Eubank
Vice President
Cyber & Electronic Warfare
john.eubank@hii-tsd.com
443.717.2100

Our team is ready to support your mission with secure, RMF-compliant solutions to protect America's critical assets. To learn more about our complete package of cyber hardening solutions, or to get connected with one of our experts, visit us online at tsd.huntingtoningalls.com.

Huntington Ingalls Industries

Hard Stuff Done Right ™

tsd.huntingtoningalls.com