Cyber Range

A Virtual Environment

KBR's cyber range is a virtual environment used for testing, vulnerability assessments, training, and development of cyberwarfare technology and defensive countermeasures. The range has the ability to create IT and OT virtual environments that mimic real-world enterprise networks and industrial production backbones. It provides tools and a training environment that assist with strengthening the security, performance, and protection of Information (Internet of Things) and Operational Technologies (Industrial Internet of Things) used globally. Because the cyber range is a controlled environment and virtual, it can simulate working conditions and performance results can be replicated to reduce failures and mistakes.

Cybersecurity

KBR offers customized, efficient and effective solutions to assess, remediate, manage and assure.

EXPERTISE

- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Vulnerability and Mitigation Assessments
- Computer Network Defense
- Risk Management Framework (RMF)
- Software development
- Security Operations Centers (SOC) design, installation and sustainment
- Vulnerability assessment and evaluation
- Independent Verification and Validation (IV&V)
- Cyber policy development, interpretation, execution and training

KBR ADVANTAGES

- Heritage of critical infrastructure protection
- Proven experience leading cyber efforts that involve multiple U.S. Department of Defense service branches
- Able to develop and customize cyber tools based on customer need
- Recognized expertise in critical infrastructure protection
- Mature assessment processes
- Certified, trained workforce
- Proven expertise in DIACAP to RMF transition with a RMF Guidebook
- Certified by U.S. Department of Homeland Security for Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act
- Navy-qualified validators
- Ethical hackers