Cyber Range

Secure Virtual Environments

KBR's cyber range is a virtual environment used for testing, vulnerability assessments, training and development of cyber warfare technology, and defensive countermeasures. The range can create Information Technology (IT) and Operational Technology (OT) virtual environments that mimic real-world enterprise networks and industrial production backbones. The range leverages virtualized and real-world assets to develop a realistic testing and training environment for the discovery of cyber vulnerabilities and the "art-of-the-possible" cyber attacks, as well as "kill chain" development. The cyber range provides tools and a training environment that assists with strengthening the security, performance and protection of IoT (Internet of Things) and IIoT (Industrial Internet of Things) used globally. Because the cyber range is a virtual controlled environment, it can simulate working conditions and performance results can be replicated to reduce failures and mistakes, as well as the development of future tactics, techniques and procedures for cyber operators.

AREAS OF EXPERTISE

Within the cybersecurity domain, KBR technology and IT professionals are developing the necessary tools to combat the ongoing evolution of cyber attacks on our Nation's critical infrastructure. KBR offers customized, efficient and effective solutions to assess, remediate and manage the discovery and mitigation of cyber vulnerabilities. Areas of expertise include:

- **Industrial Control Systems (ICS):** Protection of critical infrastructure control systems
- **Supervisory Control and Data Acquisition (SCADA):** Discovery of hidden cyber vulnerabilities within OT domains
- **Vulnerability and Mitigation Assessments:** Independent discovery of cyber vulnerabilities and how to mitigate them within the domain
- **Computer Network Defense:** Holistic approach to protect data for unauthorized access
- **Risk Management Framework (RMF):** Cyber tools, techniques and procedures to manage authorization to operate (ATO) process and expedite receiving accreditation to operate
- **Security Operations Centers (SOC):** Design, installation and sustainment of technologies and operations of Security Operations Centers

Cyber Range

PROVEN PERFORMANCE

Technology changes rapidly, as do adversary tactics, which require defenders to continually improve their craft to detect, deter and defeat system and network intrusions. KBR's cyber range brings advanced network environment simulations to customers who need to perform real-world cyber testing without impact on mission-critical systems. With our extensive scientific and programming expertise, KBR experts are engineering the next wave of hardware and software security solutions for government and private agencies, helping them secure information and systems from destructive cyber threats. KBR's certified, trained workforce has proven experience leading cyber efforts that involve multiple U.S. Department of Defense (DoD) service branches and the Intelligence Community (IC):

- Ability to develop and customize cyber tools based on customer needs
- Demonstrated history of leveraging Subject Matter Experts (SME) experienced in effectively enacting a risk-based approach to complete and support all steps of the Risk Management Framework (RMF)
- Recognized expertise in critical infrastructure protection
- Mature assessment processes
- Improved RMF practices through automation enhances efficiency and consistency, and provides significant cost savings to end users
- Use of Navy-qualified validators and ethical hackers
- A cost-effective "Cyber Range as a Service" model
- Ability to leverage KBR's cyber range community of interest to support customers

WHY KBR?

Utilizing digital battlefields through virtualization and cloud computing, KBR simulates large-scale and complex networks, conducts scientific cyber testing, and uses collected data to create security tools that meet functional and performance requirements — all before deployment. By enabling real-world testing within controlled conditions, KBR cyber warriors can learn more about current threats and use those experiences to inform future solutions for real-life scenarios. KBR collectively bundles its expertise and offers "Cyber Range as a Service" in addition to customized, on-premise cyber ranges tailored to the client's need.

NEXT STEPS

Contact us to learn more about KBR's cyber range capabilities at kbr.com/contact-us.

ABOUT US

We deliver science, technology and engineering solutions to governments and companies around the world. KBR employs approximately 28,000 people performing diverse, complex and mission critical roles in 34 countries.

KBR is proud to work with its customers across the globe to provide technology, value-added services, and long-term operations and maintenance services to ensure consistent delivery with predictable results. At KBR, We are the Team Behind the Mission[SM].

kbr.com