City Block

For more information, visit:
caci.com/cyber

To contact us, email:
cyber@caci.com

Cyber simulations and training for operational technology

Modern industrial control systems (ICS) and operational technology (OT) systems are connected to IT networks and the internet, making them vulnerable to cyberattacks, natural disasters, and other hazards. Public utilities, manufacturing plants, military bases, and other local and national critical infrastructure require trained defenders to protect against these dangers.

CACI's City Block offers software-based, cyber-physical modeling and simulation environments tailored for cybersecurity professionals, network administrators, and ICS/OT engineers to conduct testing, training, and research. By integrating ICS/OT and IT networks within a scalable 3D or virtual reality (VR) platform, City Block provides realistic, cost-effective alternatives to physical testing. This solution enhances system resilience and operational continuity by allowing teams to simulate, prevent, and recover from potential attacks.

CACI

Cost-effective testing of OT/IT networks

IT networks are significantly different from ICS/OT networks and call for a different approach to training for ICS/OT cyber defense and network operations. City Block presents security testers and trainees with a completely software-based cyber-physical interface that increases their understanding of ICS/OT systems and their interconnectivity with traditional IT networks.

City Block provides a cost-effective representation of an ICS/OT environment that can be connected to IT networks for testing, training, exercises, and mission rehearsals. City Block can host audiences around the world, thanks to its software-based cyber-physical interface. City Block allows the customer to model specific hardware, software, and physical environments, making it particularly useful for customers with specific ICS/OT needs. With City Block, users develop a deeper understanding of ICS/OT infrastructures and their vulnerabilities, as well as the interdependence between cyber and physical systems.

Use cases

Testing: Test software patches and upgrades in a safe environment; test efficacy of control system isolation; test control system-specific intrusion detection and prevention systems; and test the safety of network scanning tools

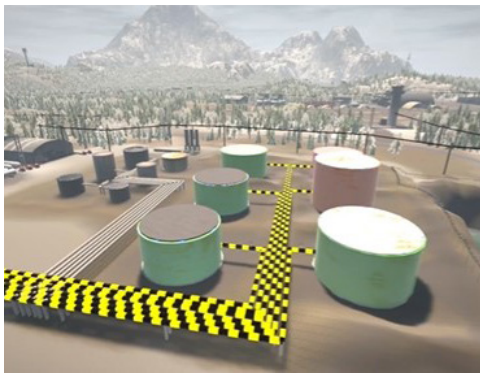
Training: Train system operators how to operate, patch, back up, and restore control systems and how to respond to suspected intrusion; train offensive and defensive cyber operators on ICS/OT networks, tools, and equipment

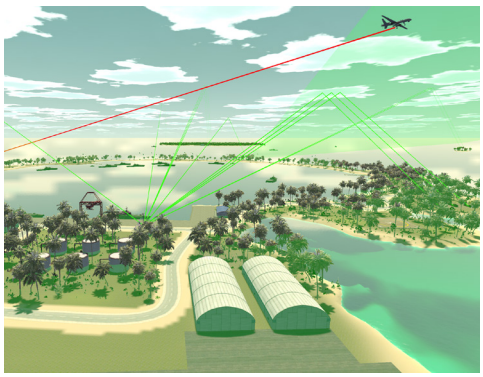
Network modeling and simulation: Provide virtualized systems and network environments to conduct cybersecurity vulnerability assessments against critical infrastructure; model OT and ICS network environments; model current and future enterprise network environments

Supply chain risk management: Test systems against known vulnerabilities and conduct penetration testing with a standardized process; assess control systems prior to fielding; conduct security activities against foreign-made chips, system components, and code

Red Team support: Provide high-fidelity visual environments to support information warfare events and provide mission rehearsal environments

Exercise support: Support operational planning for DoW and Department of Homeland Security exercises





caci.com

CACI