Red Balloon Security

RED BALLOON SECURITY
CASE STUDY: DARPA RADICS PROGRAM
SECTOR: US GOVERNMENT
AGENCY: DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)
PROGRAM: RAPID ATTACK DETECTION, ISOLATION AND CHARACTERIZATION (RADICS)

RED BALLOON SECURITY ENABLES CYBERATTACK DETECTION AND RECOVERY CAPABILITIES FOR THE ELECTRICAL GRID.

RESULTS:

- ENHANCED SITUATIONAL AWARENESS, ALLOWING OPERATORS TO UNDERSTAND THE STATE OF A GRID'S EMBEDDED DEVICES BEFORE, DURING AND AFTER A CYBERATTACK.
- IMPROVED ABILITY TO IDENTIFY GRID CYBERATTACKS AND COUNTERACT SPECIFIC ATTACK ELEMENTS AND METHODS THROUGH DEPLOYMENT OF SYMBIOTE TECHNOLOGY ON COMMUNICATIONS EQUIPMENT AND OTHER ESSENTIAL GRID DEVICES.
- PLAYED A KEY ROLE ON BLUE TREAM IN A RED VS. BLUE SIMULATION, AND DEMONSTRATED THE EFFECTIVENESS AND RESPONSIVENESS OF DEPLOYMENTS BOLSTERED BY SYMBIOTE TECHNOLOGY.

CHALLENGE:

BOLSTER THE SECURITY AND RAPID RECOVERY CAPABILITIES OF THE ELECTRICAL GRID — EVEN WHILE CYBER ATTACKERS ARE TRYING TO PREVENT SERVICE RESTORATION.

> *"I would encourage anybody looking to better understand these threats, especially cyber-physical, to move beyond simulators, get out of the lab, and conduct research."*
>
> Walter Weiss, DARPA program manager in the Information Innovation Office (I2O).[1]

SOLUTION:

Red Balloon Security worked closely with device manufacturers, electrical utilities, and US Government agencies to deploy its cybersecurity software on mission-critical devices in the electrical grid, and participated in multiple full-scale exercises, defending an actual test power grid from mock attackers. As part of the multi-year RADICS program, RBS tackled one of the most difficult and relevant challenges facing nations today: how to restart an electrical grid compromised by a cyberattack — while the attackers are trying to stop you. This "black-start recovery" capability became one of the central objectives of the RADICS program.

The RADICS electrical grid comprised of 17 linked substations and three generators, each of which could be targeted by red teams seeking to disable functionality. Red Balloon Security's embedded defense technologies were implemented on switches, controllers, protection relays and other devices critical to maintaining grid communications, operations and monitoring capabilities.

While working onsite at the RADICS deployment, Red Balloon Security's experts also provided unique insights into the security of embedded devices used in the electrical grid, including analysis of the vulnerabilities and the sources of these vulnerabilities across multiple stages of the development process and supply chain. They also participated in multiple, full-scale exercises, in which they assisted in a successful defense of the RADICS-created power grid against mock attackers.

RBS continues to provide DARPA with technology solutions that can minimize the risk of delay between vulnerability disclosure, patching at the manufacturer's level and pushing patches out to grid operators. These solutions have immediate relevance to existing commercial and government-operated grids.

[1] Breaking Defense, "DARPA's Rapid Power Restoration Grid Goes Live," March 4, 2021.