

RED BALLOON SECURITY'S SYMBIOTE TECHNOLOGY STRENGTHENS BMS AND ICS AT THE DEVICE LEVEL.

RESULTS:

- DEPLOYED RED BALLOON SECURITY'S EMBEDDED DEFENSE ON ENTERPRISE-GRADE BMS SYSTEM
- WORKED IN CONJUNCTION WITH MAJOR BMS/INDUSTRIAL CONTROL SYSTEM VENDOR
- INTEGRATED ALERTS WITH EXISTING HMI SYSTEM ACROSS MULTIPLE DEVICES

CHALLENGE:

DEVELOP NEW TECHNOLOGY TO BOLSTER THE CYBERSECURITY DEFENSES OF COMPLEX BUILDING CONTROLLERS AND AUTOMATION SYSTEMS.

“ Building systems typically are not designed with cybersecurity in mind. Installing a robust host-based defense within these embedded devices is critical to ensuring the integrity of their operations. Our research on behalf of DHS has been able to provide an additional tool to address this problem. ”

Dr. Ang Cui, Red Balloon Security CEO and Chief Scientist

SOLUTION:

In 2020 and 2021, Red Balloon Security contracted with the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) on a Phase III SBIR/STTR program. Phase III engagements are structured for small businesses to expand their commercial offerings, based on Phase I and II R&D engagements. This engagement involved an enterprise-scale vendor of building management and control (BMS) and Industrial Control systems.

Since cyberattacks present a growing risk to facilities that depend on embedded devices to automate key functions such as climate control, security and, in the case of U.S. research facilities, biocontainment and decontamination processes, protection of BMS and ICS is a critical goal for the U.S. government and equipment manufacturers.

Red Balloon Security collaborated with the Plum Island Animal Disease Center (PIADC), a Biosafety Level 3 (BSL-3) facility owned and operated by the DHS S&T Office of National Laboratories, on a 12-month deployment to specifically examine and address the types of cyber risks which could impact the safety and security of building control systems.

PIADC's unique internal infrastructure provided an environment conducive for testing and developing new technologies. RBS implemented Symbiote Embedded Defense, which can detect and respond to attacks on building management systems that leverage malware, ransomware or other malicious code or commands. Injected directly to the firmware of BMS embedded devices, Symbiote constantly checks the integrity of static code and data at the device firmware level, and blocks any unauthorized code or commands from executing.

Symbiote's successful demonstrations at PIADC are directly relevant to the commercial market, where it can be used to protect any facility that relies upon embedded devices, including building automation system for hotels and office buildings, and industrial control systems for manufacturing plants, electric utilities, water treatment plants and other critical deployments.