RedBox: Red Team in a Box

Object Security LLC

San Diego, CA
www.objectsecurity.com/otai

Contact:
Susan Farrell
Head of R&D Commercialization
ObjectSecurity LLC
susan@objectsecurity.com

Topic Number: N182-131
SYSCOM: Office of Naval Research (ONR)
www.onr.navy.mil

Program Sponsor: ONR – Cyber Team
Other Potential Programs:
Industrial Software DevSecOps, Red Teams, Industrial Control System Lab Testbeds, Digital Twins

Current TRL: 8
Projected TRL: 9 / Q4 2022

Keywords:
Cyber AI, OT/ICS Cybersecurity, Automated Vulnerability Assessments, Binary Vulnerability Analysis and Reporting, Cyber Security Assessments for ICS, Vulnerability Management, OT Cyber Security, ICS Vulnerability, Air Platform, Ground Sea, Electronics

Innovation Center at 2022 Navy Gold Coast

September 6 – 8, 2022

THE CHALLENGE

A tool to overcome the limitation of human Red Team resources for conducting vulnerability testing and assessments of embedded devices and cyber-physical devices not connected to any internet protocol (IP) network.

THE INNOVATION

The ObjectSecurity OT.AI Platform proactively improves cyber resiliency by preventing cyber-attacks and disruptive production downtime by finding and reporting unpublished, hidden, and exploitable vulnerabilities in the industrial software code of human-machine interfaces (HMIs) and programmable logic controllers (PLCs). ObjectSecurity applies novel binary vulnerability analysis science and Cyber Artificial Intelligence to deliver highly accurate and confident results. The easy-to-use software negates the need for any knowledge of reverse engineering, software vulnerability testing, or industrial control systems (ICS). Offered as a Secure Virtual Machine (VM) in the Cloud or Offline VM, the OT.AI Platform rapidly analyzes the binary code of embedded and cyber-physical devices for published vulnerabilities (CVEs), weaknesses (CWEs), and unpublished Zero-Day threats. Non-expert Sailors or Marines would use the solution to identify vulnerabilities and generate a report.

THE NAVY BENEFIT

NAVSEA, NAVAIR, NAVWAR, warfare, and cyber unit test and evaluation teams can conduct more automated and frequent assessments of the cyber security posture of weapons and hull, mechanical, and electrical (HM&E) systems. A cyber attack can cost an average of $2 million per episode of unplanned production downtime. This solution mitigates cyber risk and threats to national security. Preventative vulnerability analysis translates into increased survivability rates. While a Red Team reverse engineer may need up to three weeks to analyze thousands of lines of industrial software code, the ObjectSecurity OT.AI Platform automates analysis to minutes, saving years of manpower.

THE FUTURE

ObjectSecurity OT.AI Platform technology addresses current and future needs to protect critical industrial infrastructure extending to 5G, Industrial Internet of Things (IIoT), Software-on-Chips, Field Programmable Gate Arrays (FPGAs), SBOM generation, and more. In addition, the ObjectSecurity OT.AI Platform is currently being evaluated for use beyond defense applications to proactively protect operational technology (OT) and ICS of industries including manufacturing, oil and gas, utilities, water treatment, smart cities, air, land, and maritime transportation. ObjectSecurity seeks potential customers, channel partners, and prime contractor relationships.