Mantis Security Corporation

Critical Infrastructure Security

ICS Security Assessment and Vulnerability Remediation

Mantis Security Corporation is a leader in security engineering, penetration testing, and security vulnerability assessment for our nation's critical infrastructure and Industrial Control Systems (ICS). Our security assessors are specialized not only in traditional network and application security testing but are also knowledgeable in the complex architectures, vulnerabilities, functionality and risks of ICS and smart grid systems. We assess the security for Supervisory Control and Data Acquisition (SCADA) and Distributed Grid Management (DGM) systems for DoD and Intelligence Community customers, as well as weapons systems platforms. Mantis Security provides remediation approaches that align with our customers' risk tolerance and mission.

Plan and Assess

We carefully research, plan, and practice the security testing activities for each ICS assessment. Due to the diversity and sensitivity of SCADA systems, our assessors approach each examination with extreme vigilance in order to fully understand the system under test, the risks involved with the test, and the possible consequences associated with the test. Because most SCADA systems are perpetually connected to live industrial equipment, our team leverages SCADA service emulators and virtualized ICS security testing frameworks to safely plan the security tests for user interfaces and control system protocols. For organizations that maintain lab or training environments that safely emulate the operational SCADA system, we use these capabilities to refine our assessment plan. We further examine Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), and ICS communication protocols for known vulnerabilities and architectural weaknesses.

We adhere to the ICS Cyber Security Assessment recommendations per the DHS ICS-CERT, and can assist the owning organization in preparing a security posture self-assessment using the DHS Cyber Security Evaluation Tool (CSET) questionnaire. We plan the scope of the security examination and identify the control families to prepare procedures and tests ahead of time. We follow NIST 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security to

review and evaluate control implementation and countermeasures. These efforts build upon on our team's expertise in IT security assessments for national security systems that follow the NIST Cybersecurity Framework and the NIST 800-137, Risk Management Framework (RMF), as well as tailored security control requirements per Intelligence Community Directives, the Committee on National Security Systems (CNSS), and NIST 800-53 rev 4. The results of these critical, process oriented assessment activities can help determine the best path for the remediation of weaknesses and assist in the modernization of continuous monitoring capabilities.

Remediate and Secure

Following each security assessment, we provide recommendations to remediate any known or identified weaknesses. We provide a summary of weaknesses in reference to NIST 800-82 ICS security architecture recommendations and NIST 800-53 controls. We review IT/Business and SCADA network segmentation and recommend security architecture topologies that help reduce the exposure of the vulnerable SCADA systems. We assist in developing security requirements for vendors, and in providing relevant cybersecurity training for vendor staff, operators, and managers. As necessary, we can assist the organization in the establishment of a Patch and Vulnerability Management Program, as well as recommendations for establishing or improving its Continuous Monitoring capabilities.

Trustworthiness

Our ICS security assessors hold US government security clearances that allow them to assist on national critical infrastructure programs for the DoD and Intelligence Community. We are experts in network security testing and are knowledgeable of the common architectural patterns that tend to enable SCADA systems. We train our security engineers to meet industry ICS/SCADA security engineering requirements, as well as vendor-specific courses, as required. By leveraging our experience in ICS Cybersecurity Engineering we will provide your organization with effective, safe, and responsible support to evaluating and improving the security of these systems.