Carnegie Mellon University
Software Engineering Institute

CYBERSECURITY ASSURANCE

January 2015

Research

Our Cybersecurity Assurance researchers investigate how to improve the ability of organizations to measure and improve their management of cybersecurity risks. Our researchers, engineers, and subject matter experts often lead the national conversation on critical infrastructure protection and supply chain risk management. The collective lessons of years spent measuring and evaluating organizations in all 16 sectors informs our research as well as collaborations with organizations like yours.

Cyber-Physical Systems

We are working to determine if there are management practices and techniques unique to protecting cyber-physical systems, the role sector requirements have in shaping cyber-physical protection strategies, and how organizations can best identify and manage risks resulting from cyber-physical systems.

Cyber-Exercise Diagnostic

We are working to advance the state of the practice of cyber exercise by extending its use as a measurement instrument. We believe cyber exercise can be employed as an effective validation of capabilities in many dimensions.

Next-Gen Penetration Testing

We are developing tools and methods to bring increased value and robust measurement to the performance of technical vulnerability assessment.

Solutions

We create solutions that empower organizations to gain justified confidence in their cybersecurity posture. We use techniques to evaluate the fundamental processes required to manage operational risk and technical safeguards that surround your most important assets. We draw on well-established principles of process measurement, such as the CERT-RMM and leading edge technical vulnerability assessment methods in developing solutions.

Working with our stakeholders, we have created the following comprehensive solutions that help organizations gain justified confidence in their cybersecurity posture.

Cyber Resilience Review (CRR)

Created by the CERT Division for the U.S. Department of Homeland Security (DHS), the CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains (based on CERT-RMM) including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

Risk and Vulnerability Assessment (RVA)

An RVA identifies vulnerabilities and ensures that security implementation actually provides the protection that organizations require and expect. An RVA is conducted collaboratively by CERT subject matter experts and DHS using open source and commercial security tools to conduct vulnerability scanning and manual penetration testing. These scans and tests determine whether, and by what methods, an adversary can defeat security controls on a live or simulated network. The main goals of the RVA are to help secure against known vulnerabilities and threats by providing mitigation strategies to reduce risk, and aggregate vulnerability data so executives can make informed decisions regarding the security and safety of information systems.

External Dependencies Management (EDM) Assessment

The EDM Assessment evaluates an organization's risk management when forming relationships with external entities, ongoing management of third-party relationships, and the ability to sustain services when external entities fail to meet the terms of service or are otherwise disrupted. The EDM Assessment, offered by the DHS Cyber Security Evaluation Program, is a no-cost, voluntary, non-technical assessment to evaluate and communicate the EDM capability of critical infrastructure organizations.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0216