Carnegie Mellon University
Software Engineering Institute

Cybersecurity Assurance: Creating Justified Confidence

HOW DID THIS ATTACK HAPPEN? Are they still in the network? Can we recover our systems? Are we certain they can't come back? These are questions an organization must be able to answer to ensure survival when faced with disruption. A comprehensive and integrated approach to cybersecurity is the only viable path to achieving predictability in uncertain times. Robust measurement of capability maturity coupled with realistic technical vulnerability assessment is required to truly understand your defenses and ability to withstand cyber-attack.

Can your organization survive a disruptive cyber event?

About

The Cybersecurity Assurance team creates tools and methods to 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® Resilience Management Model (CERT®-RMM) and leading-edge technical vulnerability assessment methods in developing solutions. The team has an established and prominent role in protecting our nation's critical infrastructure. Our approach takes assessment beyond the routine compliance checklist and traditional "pen test" and delivers measures of capability.

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 approach. The Cybersecurity Assurance team has worked with organizations of all sizes and composition. Deriving practical tools and methods from the best concepts that academia has to offer and best practices from private industry is at the heart of our work.

Key Capabilities

Process Assessment
Using models and techniques, we understand how to measure the cybersecurity capabilities of an organization.

Technical Vulnerability Assessment
We understand how to examine susceptibility to technical vulnerabilities and cybersecurity exploits.

Supply Chain Risk Management
We understand how to reduce vulnerability, manage risk, and ensure resilience within your supply chain.

Data Analytics & Visualization
We understand how to analyze complex datasets and turn them into practical insights for use by organizations.

Solutions

Working with our stakeholders, we identify and solve problems using comprehensive solutions such as the Cyber Resilience Review, Risk and Vulnerability Assessment, and External Dependencies Management Assessment.

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 eduEvaluation Program, is a no-cost, voluntary, non-technical assessment to evaluate and communicate the EDM capability of critical infrastructure organizations.

Applied Research Areas

Cyber-Physical Systems

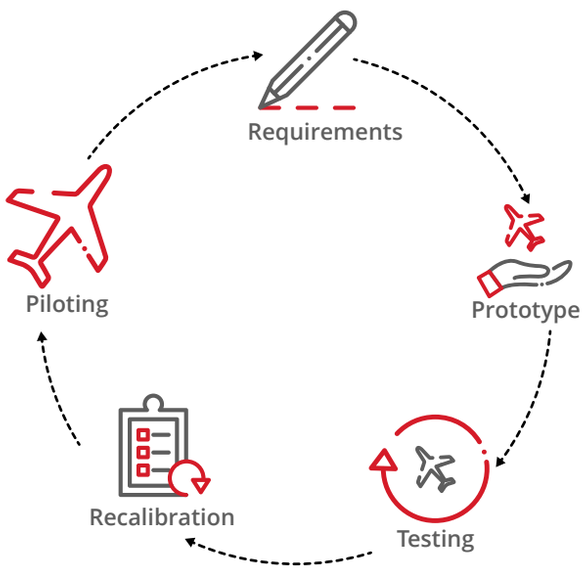
We are working to determine if there are management practices and techniques unique to protecting cyber-physical systems, the role sector requirements have in shaping cyber-physical protection strategies, and how organizations can best identify and manage risks resulting from cyber-physical systems.

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.



About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu