MITRE'S CICAT™

PUT MITRE ATT&CK TO WORK FOR YOUR ORGANIZATION WITH THIS MODELING AND SIMULATION TOOL

MITRE's Critical Infrastructure Cyberspace Analysis Tool (CICAT™) automates generation of cyber attack scenarios based on MITRE ATT&CK® and an infrastructure model representing the target environment. Infrastructure models are imported as Excel spreadsheets and can represent critical infrastructure or cyber physical systems.

CICAT uses attack path analysis to identify attack paths within the infrastructure between specified entry points and targets, and filtering algorithms to select ATT&CK techniques a threat actor could plausibly use to gain entry, laterally move, and deliver effects on targets.

CICAT imports both Enterprise ATT&CK and ATT&CK for ICS to provide seamless threat modeling over IT and OT networks. CICAT can also be extended with supplemental techniques to model hybrid or complex cyber attacks.

CICAT-generated scenarios are collected in a results spreadsheet. Each scenario details the attack path, ATT&CK techniques, potential mitigations, including ATT&CK mitigations or NIST SP 800-53 controls, and CVEs associated with each attack path component.

CICAT results include impact and risk scores calculated for each generated attack path. Other analytics identify hot spots and hot links within the infrastructure model, mitigation usage, and the risk exposure of capabilities, functions, and mission objectives.

CICAT v2.0 is available for license as a standalone python application for Windows, Linux, and MacOS.

CICAT helps evaluate how an adversary might conduct a cyber attack on a system.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Interested in licensing CICAT for your organization's use?
Contact: techtransfer@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™