CALDERA

Use Cases

Github: github.com/mitre/caldera **Web:** caldera.mitre.org **Email:** caldera@mitre.org

Automated Adversary Emulation

- Automated, repeatable evaluation of network and OT systems
- Emulate real world adversaries & threats using their observed tactics, techniques, and procedures
- Generate and evaluate logs for systems under test
- Advanced AI and automated planning for autonomous cyber operations
- Rich mappings to the MITRE ATT&CK™ Matrices

Defensive Cyber Operations

- Test & develop cyber defenses
- Evaluate security products
- Verify SOC analytics
- Plug Caldera into continuous security evaluation pipelines
- Data model & ontology integration

Offensive Cyber Operations

- Develop and test offensive capabilities
- Integrate custom agents, C2 channels, abilities, adversaries, planners etc. into operations platform

Training

- Train computer incident response teams and SOC analysts
- Execute offensive operations with artificial user noise and activity
- Extensive user documentation & interactive tutorials

Research

- Agents
- Abilities (exploits)
- Automated Planning
- Operational Technology
- Noise generation
- (…and more)

ABOUT US

The Caldera team is a group of red teamers, software developers, exploit writers, cyber threat analysts, AI researchers, cyber security engineers and computer scientists who pursue the common goal of building a premier adversary emulation platform for our US sponsors and cyber security defenders around the world. Our mission is to keep pushing the state-of-the-art of using adversary emulation for enhancing cyber security and keeping the good guys many steps ahead of the bad guys.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®