MITRE Caldera

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.

Use Cases/Capabilities

- Automated adversary emulation
- Defensive testing & analytics
- Offensive effects development & cyber ranges
- Enabling advanced red vs. blue research

Public Impact

- GitHub: 4K ⭐ - 300 downloads/week – 2K views/week – MITRE's most popular repo
  - Notable users/proponents: Humana, GitLab, Kali Linux, Otorio
  - Courses created at FIU, Army Cyber School

Resources

- (Web) caldera.mitre.org

- (GitHub) https://github.com/mitre/caldera

- (Blog) https://medium.com/@mitrecaldera

Growth Areas

- AI/Automated Planning
- Cyber Ranges
- OT/ICS
- Continuous Adversary Emulation & Analytic Evaluation Pipelines

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®