# CTE SQUAD EXECUTION STAGE ACTIONS

OVERVIEW

The CTE squad operates within all four stages of CPT execution according to tasking and approving authorities. The CPT operates under two core tasks: transform and rapidly improve cyberspace defenses, and protect the supported owner's critical assets and C-KT. All teams should work with mission partners and their local defenders. The CPT construct reinforces local defenders by mitigating threats when they are detected.

SURVEY

- Coordinate, collect and share threat information
- Prepare threat-emulation plan (TEP) to replicate required threats
- Support participative assessment of existing defenses through coordinated execution of TEP
- Provide recommendations to mission protection to assist risk assessment and inform RMP
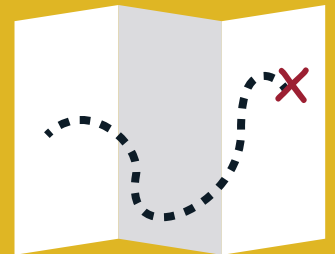
SECURE

- Support non-participative evaluation of deployed risk mitigations
- Generate non-participative, realistic adversary effects
- Provide adversary perspective recommendations to inform MDP

PROTECT

- Receive/share threat updates, observe activity
- Provide adversarial perspective and recommend courses of action for mitigation and preemption
- Assist in ad hoc countermeasure development

RECOVER

- Ensure deliberate transfer of any stay-behind capabilities
- Provide recommendations for inclusion in final report