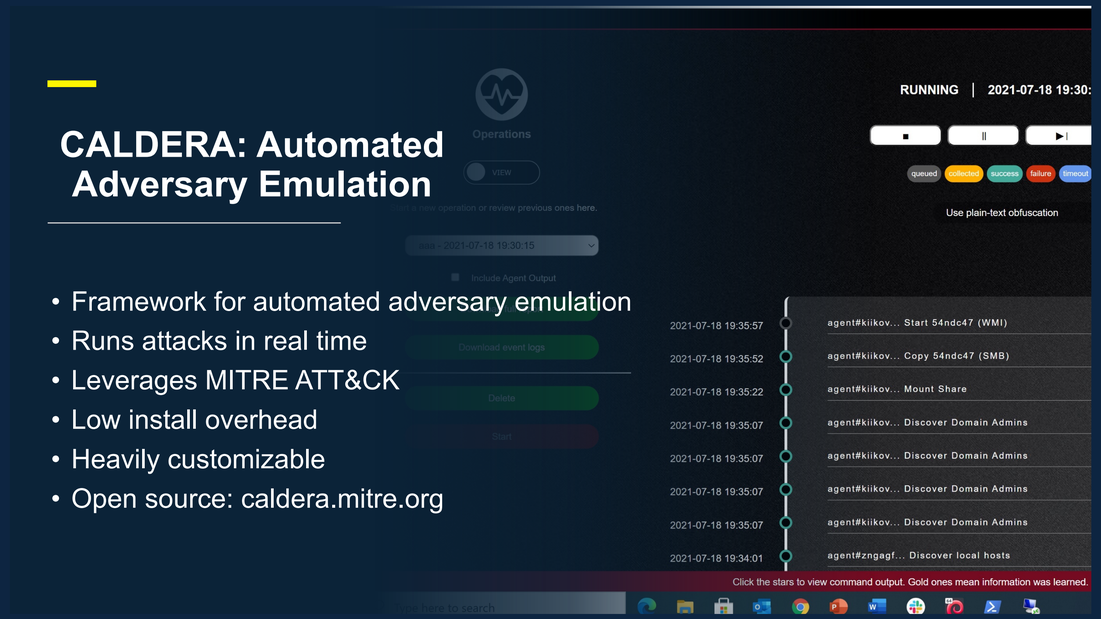
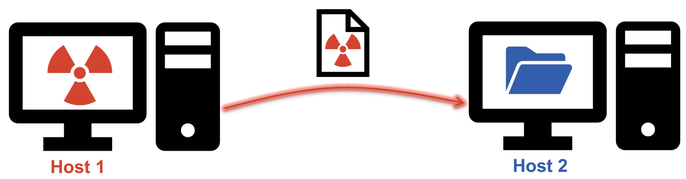
CALDERA: A Red-Blue Cyber Operations Automation Platform

CALDERA: Automated Adversary Emulation

- Framework for automated adversary emulation
- Runs attacks in real time
- Leverages MITRE ATT&CK
- Low install overhead
- Heavily customizable
- Open source: caldera.mitre.org



Analyzing Copying Over a File

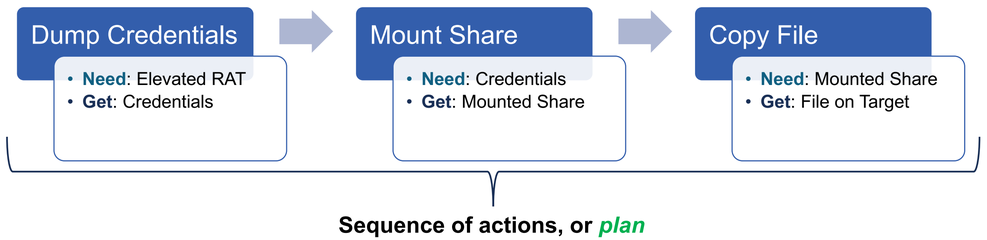


What do we need to do to copy a RAT over?
Working RAT on source host
Mounted file share from target onto source host
Write access to file share

→ **Requirements, or *preconditions***

What happens after copying a RAT over?
There will be a new file on the target host
That file will contain the RAT

→ **Consequences, or *postconditions***



Sequence of actions, or *plan*

THINK LIKE AN ADVERSARY!

Stress test your network by executing a real (controlled) attack
Put your defenses to the test by empirically testing them
See what would happen if an adversary were to breach your network

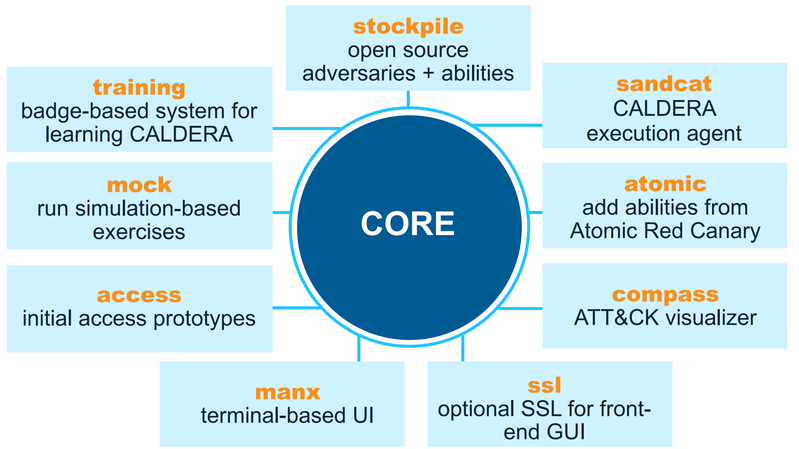
Simulate the goals and actions of a real adversary
Pursue objectives and chain execution like a real attacker
Emulate the techniques of an adversary that's likely to target your network

Evaluate your defenses after the exercises
How far did the attack get?
How much were you able to detect?
What can you do to improve your defenses?

Under the hood

CALDERA's modular plugin architecture

Core system with modular plugin architecture



Impact: can rapidly integrate/ partition code!

response: in-development, automated threat hunting
gameboard: in-development, red vs. blue games