Automated Cyber-Readiness Evaluator
ACE

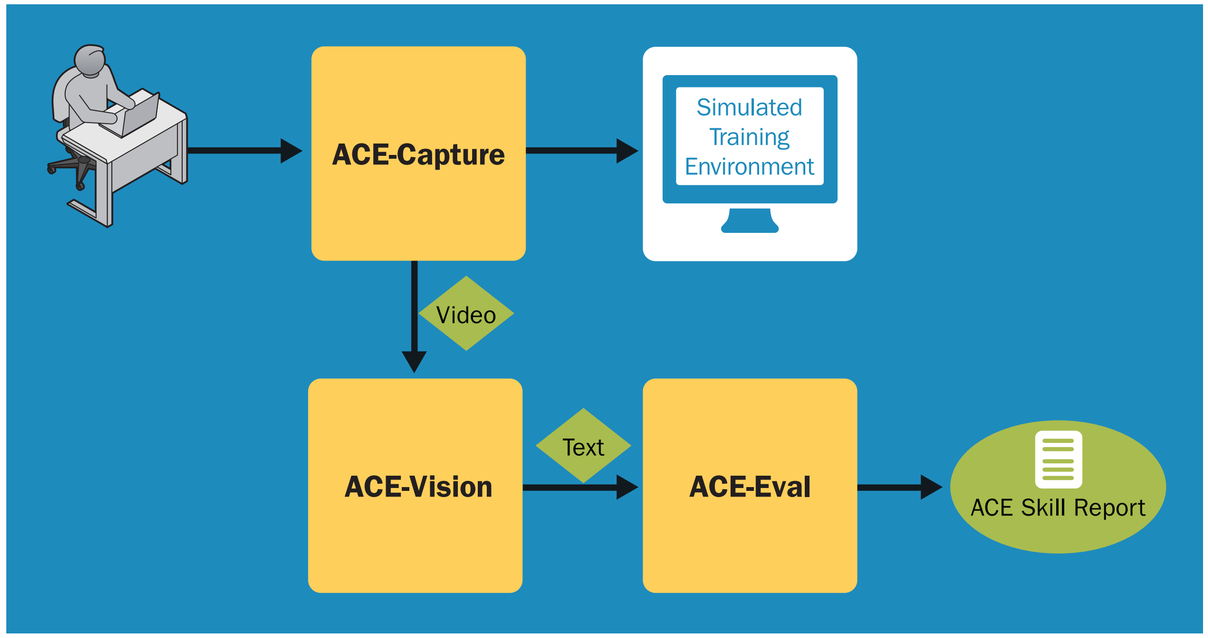
Assessing the mission readiness of all DoD cyber operators is a daunting task that is not achievable using individual one-on-one evaluation techniques. Our project utilizes advanced computer vision and machine learning techniques to evaluate the activity of cyber operators in a realistic scenario in order to determine their mission readiness.

Mission Readiness Assessment

The DoD must assess the capability and capacity of its cyber workforce to support operations conducted in the cyberspace domain and this assessment capability is a key determinant of operational mission readiness. However, because cyber is a relatively new domain for the DoD, it does not yet have a scalable, objective assessment capability that it can use to validate the hands-on, technical knowledge and skills of its cyber workforce.

ACE Philosophy

Current evaluation methods involve checklists of prompted activities or individual assessments. These methods are not reliable, not uniform, and not scalable to DoD requirements. The ACE philosophy is that true mission readiness assessments can only be performed in a realistic environment. ACE users are placed in an environment that mimics their real work environment. Our automated system then observes and understands the actions performed within this environment as users attempt to complete a mission. Based on their activities, our system assesses their knowledge, skills, and abilities.

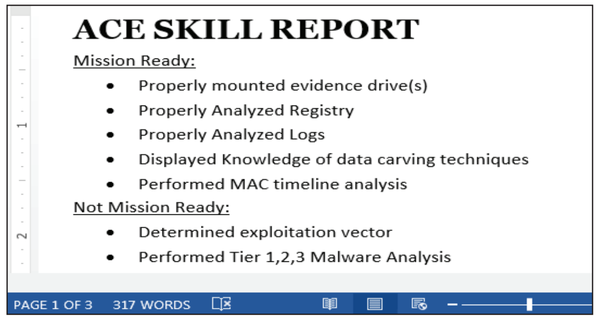


ACE Architecture Overview - User logged into Simulated Training Environment observed using Capture System. Captured video is analyzed and transcribed utilizing ACE-Vision. Vision output is processed by ACE-Eval and used to generate the ACE Skill Report.

ACE-Capture

ACE evaluation scenarios are conducted in the CERT®Simulation, Training, and Exercise Platform (STEP). This platform allows us to push out realistic simulations of real DoD networks through a web browser. The ACE-Capture module has been integrated into the STEP platform, allowing unattended background recording of participants within an evaluation scenario. This recording is performed on the backend servers and consists only of the views we provide to the end users—thus avoiding the possibility of accidentally collecting any personal information that may exists on their personal workstation. Our recording system is highly scalable. It allows us to simultaneously record dozens of users per allocated machine and natively scales with available hardware.

Diagram Title for the Process and Stuff


ACE SKILL REPORT

Mission Ready:

- Properly mounted evidence drive(s)
- Properly Analyzed Registry
- Properly Analyzed Logs
- Displayed Knowledge of data carving techniques
- Performed MAC timeline analysis

Not Mission Ready:

- Determined exploitation vector
- Performed Tier 1,2,3 Malware Analysis

PAGE 1 OF 3 317 WORDS

ACE Skill Reports include an assessment of the capabilities displayed during the evaluation.

ACE-Vision

Video recorded by the ACE-Capture system is processed by a dedicated vision engine that detects a wide array of GUI elements, as well as a set of relevant console commands. These detections (and their associated confidence measures) are generated utilizing a highly optimized, parallelizable algorithm that takes advantage of the unique conditions available within our simulation environment.

ACE-Eval

The detections generated within the ACE-Vision system provide the data for evaluation by ACE-Eval. This system is comprised of two layers. Layer 1 maps groups of detection events with associated higher level activities such as “Opened file examiner_notes.txt for editing in gedit”, “Mounted the evidence drive”, etc. Layer 2 maps these high level activities with the knowledge, skills, and abilities they represent.

ACE Skill Report

The final output of the ACE-Eval system is the ACE Skill Report. This report contains an assessment of the areas in which the participant met or exceeded the requirements for mission-readiness, as well as those areas in which they failed to do so.

By utilizing the automated generation of reliable skill reports, commanders may easily assess the capabilities of their troops, at scale, and with the resources already available.

Contact: Rotem D. Guttman rdguttman@cert.org

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002774