

Previously Unseen Attack Record

Blank engineer form | copy per trial; editable Markdown and JSON are included

Required: at least one novel attack for every assessed critical boundary. Explain novelty against the supplied corpus; do not preselect all attacks from the author's list. Keep every prior failed record.

Evaluator / independence / date	
Campaign / run / version / evidence level	
Exact configuration/source/image hashes	
R / C / B / P IDs; unseen-attack rationale	
Attacker / starting access / budget	
Fault-injector privilege (separate)	
Attack: command, fixture, target	
Opportunity: actual reachable path	
Benign positive controls before / after	
Independent observation / source / shared dependencies	
Control response	
Actual effect	
Result and reason	NOT RUN / PASS / FAIL / INCONCLUSIVE / justified N/A
Raw artifact paths / hashes / external checkpoint	
Time source / uncertainty / sample loss / STOP latency	
Enrolled resources / restart observations	
Limitation; what this proves	
What this does not prove	
Failure ID / class / violated requirement	
Preserved failure -> new version -> regression records	

Attack -> Opportunity -> Independent Observation -> Control Response -> Actual Effect -> Result. Missing opportunity, failed positive control or absent measurement cannot establish a containment pass. Append longer raw evidence and explanations; the editable form has no page limit.