

Host intrusion detection on ADFA-LD

Linux system-call traces from UNSW Canberra, the reference corpus for host intrusion detection. 60 attack sessions against 364 blocks of normal behaviour.

0.9246

session-level ranking AUC, across all attack families, induced on normal behaviour alone

RESULTS

MEASURE	AUC	
Session level, all attack families	0.9246	
Held-out test half, scored once	0.9478	
Per-process trace level	0.8153	
Positive control, re-run 2026-09-23 (documented 0.816)	0.8215	

Bars run 0 to 1 on the ranking scale. The light tick marks 0.5, which is chance.

HOW IT WAS MEASURED

Unit	The session – around twelve process traces, the shape an intrusion actually takes
Atom	The system-call sequence, verbatim
Readout	The probability the machine assigned to the call that actually came next
Learning	Normal traces only. No attack data is used for training

CONDITIONS

Attacks needed for training	None
Hardware	One CPU core
Learn and score 5,118 recordings	7.8 s
Memory	13 MB
Pre-trained artifact	None. Everything is learnt on your own box

THE PASS MARK, FIXED BEFORE THE RUN

Set before the run: session-level AUC at or above 0.85.

LIMITS OF THIS RESULT

ADFA-LD does not group its normal traces into sessions, so a normal session here is a consecutive block of validation traces; this is stated wherever the figure appears. The per-process number, 0.8153, is the honest floor: one process in isolation is a weaker signal than the session it belongs to.

REPRODUCING IT

The dataset is public and the harness is the same binary a customer installs. Ask us for the harness and the exact dataset revision and run it on your own hardware. The run behind this sheet is recorded in `validate/adfa_ld/ADFA_LD_FINDINGS.md`, including the pass mark, every figure, and the results that did not favour us.