Host intrusion detection on ADFA-LD

Linux system-call traces from UNSW Canberra at the Australian Defence Force Academy. The engine learns normal behaviour only and is never shown an attack.

0.9246 session-level ranking AUC (0.924 in the showcase run), 60 attack sessions against 364 blocks of normal operation

Results

Measure	AUC
Session level: host under attack vs normal	**0.9246**
One process judged in isolation	0.8153

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

How it was measured

Measure	AUC, 60 attack sessions against 364 blocks of normal operation; the engine is trained on normal recordings only
Data	ADFA-LD (UNSW Canberra at the Australian Defence Force Academy)

Conditions

Machine	Intel(R) Core(TM) i5-1038NG7 CPU @ 2.00GHz
Physical cores available	4
Cores actually used	1, single-threaded
Memory installed	16 GB
Operating system	macOS 26.6.2
GPU or accelerator used	none
Peak memory used by the engine	13 MB

The pass mark, fixed before the run

> Set before the run: 0.85 or better. Verdict: PASS.

Limits of this result

An intrusion is a session: about 12 processes recorded while the host was under attack, many of them ordinary. Judged one process at a time the score is lower, because roughly a quarter of the processes labelled attack behave exactly like normal ones. Judged as a host, the consensus across its processes separates attack from normal. Normal hosts here are consecutive blocks of 12 held-out normal recordings, because the dataset does not group normal recordings by session. Select any row to see every process inside that unit and the score the engine gave it. Data licence: research use; Creech and Hu 2013, 2014; Xie and Hu 2013, 2014; Haider et al. 2015-2017. On timing: the separation is already present in the first ten system calls of each process (AUC 0.926, against 0.948 using every call), so the decision does not wait for the recording to finish. Recorded in the pre-registered earliness run, ADFA-LD findings amendment 9. What that supports is SPOTTING an intrusion as it happens; on this dataset the result is a ranking, and we do not claim an operating point that could drive automatic blocking here. Blocking in the traffic path, inline and in real time, is the web-request showcase.

Where it is recorded

Showcase run captured 2026-09-19, showcases.senuaai.com/cyber-edge/. The data behind this sheet is published beside it at senuaai.com/evidence/datasheets/.