Log intrusion detection on the AIT Log Data Set

Four mail servers under six days of simulated users, with a real multi-step intrusion injected: scan, brute force, webshell upload and commands.

0.9604 pooled window ranking AUC, with all four servers above 0.95 on their own

Results

Host	Windows	Attack windows	AUC
mail.cup.com	1,485	74	0.9650
mail.insect.com	1,693	76	0.9596
mail.onion.com	819	67	0.9808
mail.spiral.com	1,004	82	0.9571
Pooled	**5,001**	**299**	**0.9604**

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

How it was measured

Unit	A window of 100 consecutive requests, in time order
Atom	The request line only; the client address is excluded
Learning	The first half of each log, which is attack-free on all four hosts

Conditions

Order control	Shuffling requests inside each window costs 0.8886 of AUC
Scanner removed	0.69 to 0.77 across the four hosts
Client address	never seen by the detector

The pass mark, fixed before the run

> Set before the run: pooled AUC at or above 0.75, at least 3 of 4 hosts at 0.70 or better, and a shuffle control that must cost at least 0.05. Verdict: PASS.

Limits of this result

The scanner stage is 93% of labelled attack lines and is detected almost perfectly, which lifts the pooled figure. With the scanner removed the four hosts read 0.69 to 0.77: use that for a quiet intrusion. Single webshell commands are not reliably separated. Apache access logs only.

Where it is recorded

simplex/validate/ait/AIT_FINDINGS.md, simplex/validate/ait/PREREG.md. The data behind this sheet is published beside it at senuaai.com/evidence/datasheets/.