Metrics

(MTTD, MTTR, Dwell Time)

Why metrics matter

Metrics translate security operations into measurable performance:
- How quickly we noticed the incident
- How quickly we acted
- How long the attacker had opportunity before containment

Incident used for metrics

Metrics were calculated on the Feb 27 SSH detection + containment workflow, because it has clear timestamps from SIEM and CrowdSec.

Timeline

T0 (first detection event in SIEM): 11:45:45
T1 (analyst confirmation in SIEM): 11:46:00
T2 (containment executed): 11:51:15 (CrowdSec ban)

Dwell Time

Dwell = T2 − T0
11:51:15 − 11:45:45 = 5 minutes 30 seconds

MTTD

MTTD = T1 − T0
Because ingestion and visibility were near real-time, MTTD is conservatively estimated as 1 minute.

MTTR

MTTR = T2 − T1
11:51:15 − 11:46:00 ≈ 5 minutes

Evidence

Detection screenshot: *screenshots/07_Elastic_Lens_SSH_Virtualisation.png*
Containment screenshot: *screenshots/06_Crowdsec_Decision_List_Ban.png*