

## Rule Report — rule-048a704d

Created: 2025-10-03T08:27:57Z | Threat Level: Critical

**Executive summary:** Detected ARP\_MITM from 172.20.10.3 targeting N/A.

### Technical summary

Field	Value
Rule ID	rule-048a704d
Alert Type	ARP_MITM
Src IP	172.20.10.3
Target IP	N/A
Ports	N/A
CVSS	9.8
Risk score	89.0 (Critical)
Decision	quarantine_mac — ARP spoofing / MITM detected

### Correlation / Related alerts

Related alerts (last 48h): **64**



### Enrichment

Country	N/A
City	N/A
Reputation Score	0.5
IP Info Raw	None

### Evidence

Raw alert: `{"alert_type": "ARP_MITM", "src_ip": "172.20.10.3", "target_ip": "172.20.10.4", "ports": [], "start_time": "Wed Jul 30 16:11:36 2025", "duration": null}`

Capture Time: Wed Jul 30 16:11:36 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 96aeac980d56d68c5c1b35e5166309205cc6703472f9b690ac4485152e281f91