

## Rule Report — rule-aa9ce493

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-aa9ce493
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 15:31:48 2025", "duration": null}

Capture Time: Wed Jul 30 15:31:48 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 127aad7754b44481f41e57347fd50c9e06f668f986afdd1d88fd7d28fabce56f