

# Rule Report — rule-e28077d5

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

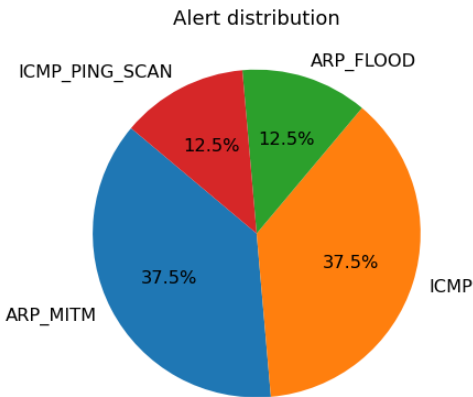
**Executive summary:** Detected ARP\_MITM from 172.20.10.3 targeting N/A.

## Technical summary

Field	Value
Rule ID	rule-e28077d5
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 15:24:16 2025", "duration": null}

Capture Time: Wed Jul 30 15:24:16 2025