Rule Report — rule-ced2674a

Created: 2025-10-03T08:27:58Z | Threat Level: **Critical**

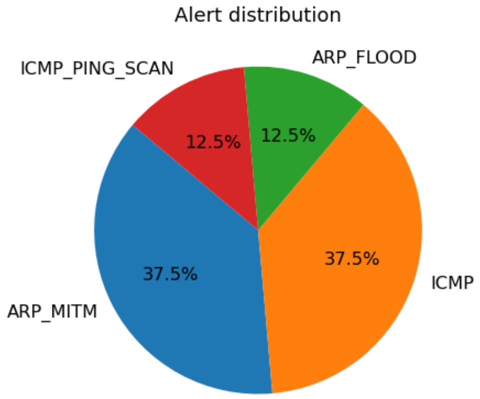
Executive summary: Detected ARP_MITM from 172.20.10.3 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-ced2674a
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: 529d899e6a082b81dd57c9e5b37dc528ca37610d3567c376fb2fdcdc7f1f5cac