Rule Report — rule-4d14b73a

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

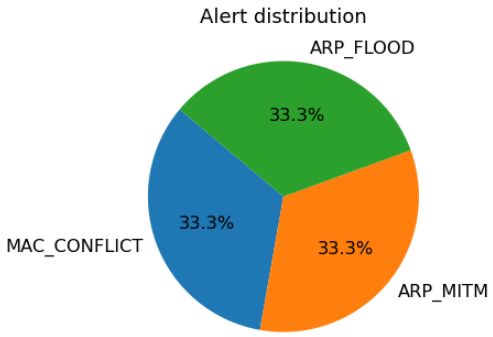
Executive summary: Detected ARP_FLOOD from 172.20.10.1 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-4d14b73a
Alert Type	ARP_FLOOD
Src IP	172.20.10.1
Target IP	N/A
Ports	N/A
CVSS	7.5
Risk score	77.5 (High)
Decision	block_ip — ARP flood detected

Correlation / Related alerts

Related alerts (last 48h): **24**



Enrichment

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

Evidence

Raw alert: `{"alert type":"ARP FLOOD","src ip":"172.20.10.1","target_ip":"172.20.10.4","ports":[],"start_time":"Wed Jul 30 16:01:10 2025","duration":null}`

Capture Time: Wed Jul 30 16:01:10 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: a35f3cbb9f56f61bd1f32eb9b0050bc5f6b0051c1b35592e9498639c909d736a