Rule Report — rule-5395c1b0

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

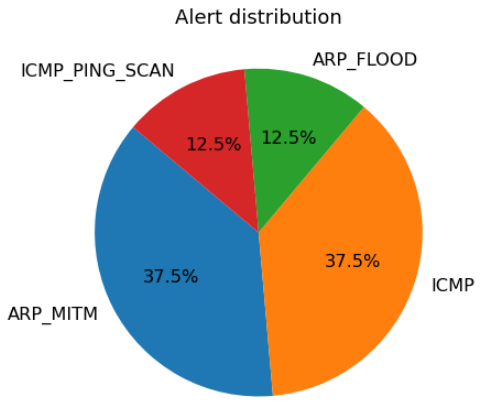
Executive summary: Detected ARP_FLOOD from 172.20.10.3 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-5395c1b0
Alert Type	ARP_FLOOD
Src IP	172.20.10.3
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): **64**



Enrichment

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

Evidence

Raw alert: `{"alert type":"ARP FLOOD","src ip":"172.20.10.3","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