Rule Report — rule-5ebce0b9

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

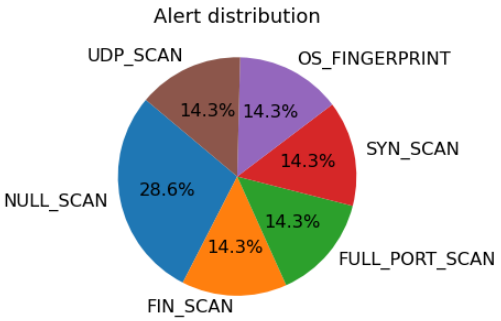
Executive summary: Detected UDP_SCAN from 10.129.5.193 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-5ebce0b9
Alert Type	UDP_SCAN
Src IP	10.129.5.193
Target IP	N/A
Ports	1041, 1049, 1065, 1068, 16896, 17185, 18683, 20360, 20445, 20540, 20791, 21360, 22053, 24644, 28547
CVSS	5.3
Risk score	66.5 (Medium)
Decision	block_ip — UDP Scan detected

Correlation / Related alerts

Related alerts (last 48h): **56**



Enrichment

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

Evidence

Raw alert: `{"alert type":"UDP SCAN","src ip":"10.129.5.193","target ip":null,"ports":["1041","1049","1065","1068","16896","17185","18683","20360","20445","20540","20791","21360","22053","24644","28547"],"capture time":"Mon Jun 2 13:31:00 2025","duration":null}`

Capture Time: Mon Jun 2 13:31:00 2025