

Rule Report — rule-dc4b4f2f

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

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

Technical summary

Field	Value
Rule ID	rule-dc4b4f2f
Alert Type	NULL_SCAN
Src IP	10.129.5.193
Target IP	N/A
Ports	1007, 1025, 1088, 110, 111, 1110, 113, 1141, 135, 139, 143, 1720, 1723, 18101, 1840
CVSS	0.0
Risk score	40.0 (Medium)
Decision	notify — NULL_SCAN detected (low priority - monitoring)

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": "NULL SCAN", "src ip": "10.129.5.193", "target ip": null, "ports": ["1007", "1025", "1088", "110", "111", "1110", "113", "1141", "135", "139", "143", "1720", "1723", "18101", "1840"], "start_time": "Jun 2 13:29:51 2025", "duration": null}`

Capture Time: Mon Jun 2 13:29:51 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: fb5e5ca81b942f57f448b37af9b79084d21c1a1ac8e0c9421f800a9469a4aa39