

Rule Report — rule-fff823ce

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

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

Technical summary

Field	Value
Rule ID	rule-fff823ce
Alert Type	SYN_SCAN
Src IP	10.129.5.193
Target IP	N/A
Ports	10000, 10001, 10002, 10009, 1007, 10180, 1022, 1024, 1025, 1035, 1037, 10566, 1077, 10778, 110
CVSS	5.3
Risk score	66.5 (Medium)
Decision	block_ip — SYN 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": "SYN SCAN", "src ip": "10.129.5.193", "target ip": null, "ports": ["10000", "10001", "10002", "10009", "1007", "10180", "1022", "1024", "1025", "1035", "1037", "10566", "1077", "10778", "110"], "start": "2025-06-02T13:32:45", "end": "2025-06-02T13:32:45", "duration": null}`

Capture Time: Mon Jun 2 13:32:45 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 16efdd42657ca529c55369dd0a36fc3d27c612b2a3157d055611eac49d3c83d6