Rule Report — rule-4b52aa36

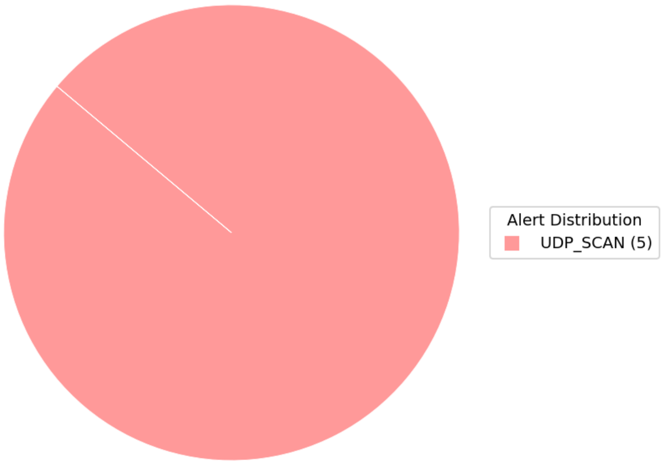
Created: 2025-12-20T16:04:44Z | Threat Level: Medium
Executive summary: Detected UDP_SCAN from 10.35.214.193 targeting 10.35.214.252.

Technical summary

Field	Value
Rule ID	rule-4b52aa36
Alert Type	UDP_SCAN
Src IP	10.35.214.193
Target IP	10.35.214.252
Ports	1025, 1038, 1044, 1059, 1064, 1087, 1419, 1457, 1645, 16573, 16832, 16938, 16974, 17, 17018
CVSS	5.3
Risk score	51.5 (Medium)
Decision	block_ip — UDP Scan detected

Correlation / Related alerts

Related alerts (last 24h): 5
Alert distribution



Enrichment

Country	Private Network
City	Internal
Reputation Score	0.5
IP Info Raw	ip: 10.35.214.193, bogon: True

Evidence

Raw alert: alert_type: UDP_SCAN, src_ip: 10.35.214.193, target_ip: 10.35.214.252, ports: ['1025', '1038', '1044', '1059', '1064', '1087', '1419', '1457', '1645', '16573', '16832', '16938', '16974', '17', '17018'], start_time: Tue Oct 28 09:42:03 2025, duration: null

Capture Time: Tue Oct 28 09:42:03 2025

Created by: rule-generator | Reviewed by: N/A | SHA256:
0c912439d26ae97b6aabfe622de0724318ce44d855fdad4808a8bcfce9809554