

# Rule Report — rule-276987d3

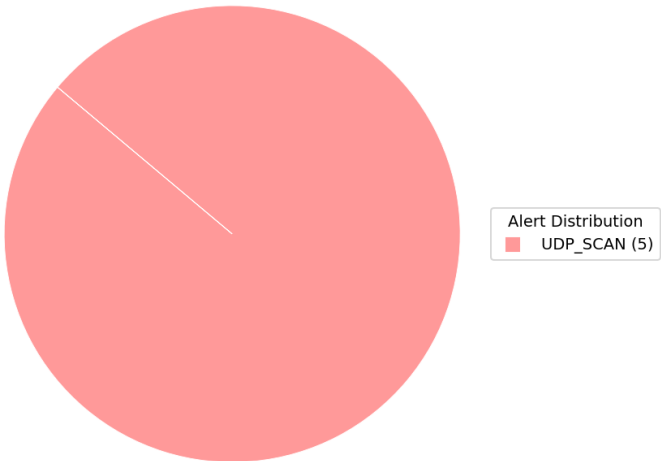
Created: 2025-12-20T16:05:06Z | Threat Level: Medium  
Executive summary: Detected UDP\_SCAN from 10.35.214.193 targeting 10.35.214.252.

## Technical summary

Field	Value
Rule ID	rule-276987d3
Alert Type	UDP_SCAN
Src IP	10.35.214.193
Target IP	10.35.214.252
Ports	1034, 1045, 1046, 1072, 11487, 120, 123, 137, 161, 16402, 16816, 16829, 16862, 16972, 1701
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: ['1034', '1045', '1046', '1072', '11487', '120', '123', '137', '161', '16402', '16816', '16829', '16862', '16972', '1701'], start\_time: Tue Oct 28 09:42:13 2025, duration: null  
Capture Time: Tue Oct 28 09:42:13 2025

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