Rule Report — rule-1a276bd1

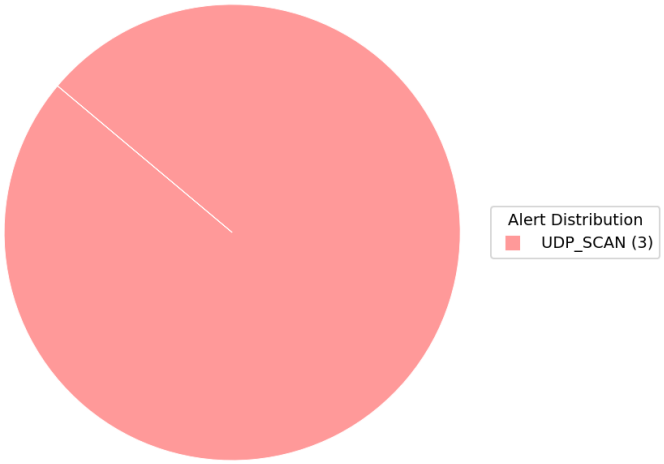
Created: 2025-12-20T16:04:57Z | Threat Level: Medium
Executive summary: Detected UDP_SCAN from 10.35.214.186 targeting 10.35.214.252.

Technical summary

Field	Value
Rule ID	rule-1a276bd1
Alert Type	UDP_SCAN
Src IP	10.35.214.186
Target IP	10.35.214.252
Ports	33704, 34140, 34557, 35328, 35464, 35986, 36159, 36431, 36676, 37773, 38472, 38879, 39209, 40424, 40965
CVSS	5.3
Risk score	45.5 (Medium)
Decision	block_ip — UDP Scan detected

Correlation / Related alerts

Related alerts (last 24h): 3
Alert distribution



Enrichment

Country	Private Network
City	Internal
Reputation Score	0.5
IP Info Raw	ip: 10.35.214.186, bogon: True

Evidence

Raw alert: alert_type: UDP_SCAN, src_ip: 10.35.214.186, target_ip: 10.35.214.252, ports: ['33704', '34140', '34557', '35328', '35464', '35986', '36159', '36431', '36676', '37773', '38472', '38879', '39209', '40424', '40965'], start_time: Tue Oct 28 09:52:58 2025, duration: null

Captured by: rule_generator | Raw log: N/A | SHA256: 0c912439d26ae97b6aabfe622de0724318ce44d855fdad4808a8bcfce9809554