

Rule Report — rule-1ddb9adb

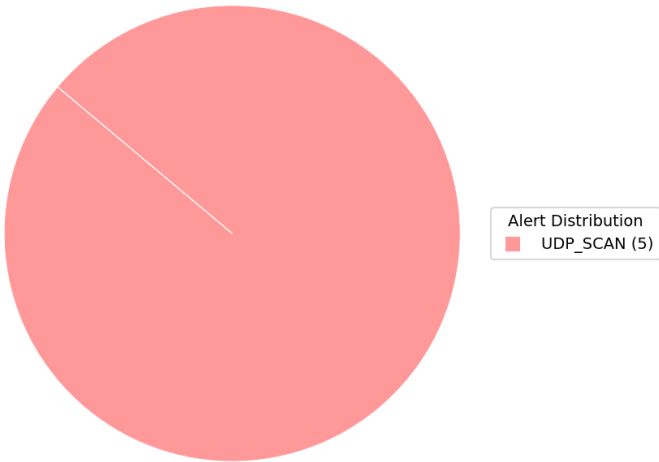
Created: 2025-12-20T15:16:38Z | Threat Level: Medium
Executive summary: Detected UDP_SCAN from 10.35.214.193 targeting 10.35.214.252.

Technical summary

| Field | Value |
|------------|--------------------------------------------------------------------------------------------------|
| Rule ID | rule-1ddb9adb |
| Alert Type | UDP_SCAN |
| Src IP | 10.35.214.193 |
| Target IP | 10.35.214.252 |
| Ports | 1066, 1234, 139, 1484, 16449, 1646, 16545, 16548, 16779, 16829, 16862, 17185, 1719, 17205, 17302 |
| 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: ['1066', '1234', '139', '1484', '16449', '1646', '16545', '16548', '16779', '16829', '16862', '17185', '1719', '17205', '17302'], start_time: Tue Oct 28 09:42:18 2025, duration: null
Created by rule-1ddb9adb | Reviewed by: N/A | SHA256: 0c912439d26ae97b6aabfe622de0724318ce44d855fdad4808a8bcfce9809554