

Rule Report — rule-e4f313e8

Created: 2025-12-20T16:05:00Z | Threat Level: **Medium**

Executive summary: Detected UDP_SCAN from 10.35.214.186 targeting 10.35.214.252.

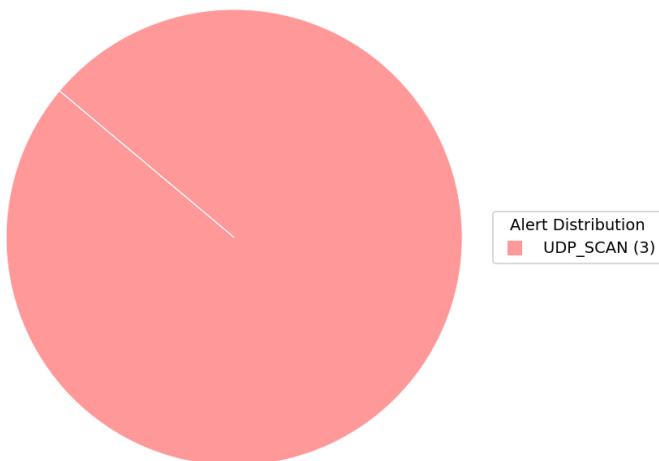
Technical summary

Field	Value
Rule ID	rule-e4f313e8
Alert Type	UDP_SCAN
Src IP	10.35.214.186
Target IP	10.35.214.252
Ports	33044, 33357, 33704, 33740, 34014, 34140, 34557, 34805, 35727, 36042, 36431, 36676, 36994, 37155, 37479
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: ['33044', '33357', '33704', '33740', '34014', '34140', '34557', '34805', '35727', '36042', '36431', '36676', '36994', '37155', '37479'], start_time: Tue Oct 28 09:51:52 2025, duration: null

Captured by rule rule-e4f313e8 on Oct 28 09:51:52 2025: N/A | SHA256: 0c912439d26ae97b6aabfe622de0724318ce44d855fdad4808a8bcfce9809554