

Rule Report — rule-097e6bbc

Created: 2025-10-02T19:38:49Z | Threat Level: Critical

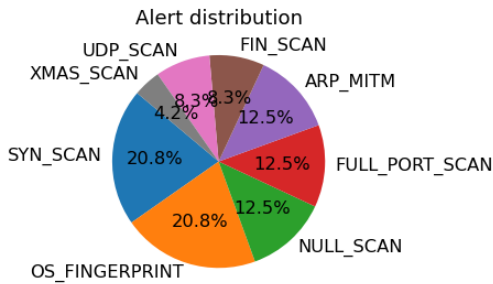
Executive summary: Detected FULL_PORT_SCAN from 10.129.5.193 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-097e6bbc
Alert Type	FULL_PORT_SCAN
Src IP	10.129.5.193
Target IP	N/A
Ports	10000, 10001, 10002, 10009, 1007, 10180, 1022, 1024, 1025, 1035, 1037, 10566, 1077, 10778, 110
CVSS	9.8
Risk score	89.0 (Critical)
Decision	block_ip — Full Port Scan detected

Correlation / Related alerts

Related alerts (last 48h): 24



Enrichment

Country	Private Network
City	Internal
Reputation Score	0.5
IP Info Raw	{'ip': '10.129.5.193', 'bogon': True}

Evidence

Raw alert: {"alert type": "FULL PORT SCAN", "src ip": "10.129.5.193", "target ip": null, "ports": ["10000", "10001", "10002", "10009", "1007", "10180", "1022", "1024", "1025", "1035", "1037", "10566", "1077", "10778", "110"], "st Jun 2 13:32:45 2025", "duration": null}

Capture Time: Mon Jun 2 13:32:45 2025