

Rule Report — rule-9b2b6d40

Created: 2025-10-03T08:27:58Z | Threat Level: Critical

Executive summary: Detected SERVICE_PROBE from 172.20.10.4 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-9b2b6d40
Alert Type	SERVICE_PROBE
Src IP	172.20.10.4
Target IP	N/A
Ports	443, 80
CVSS	9.8
Risk score	89.0 (Critical)
Decision	notify — Service Probe / Reconnaissance

Correlation / Related alerts

Related alerts (last 48h): **128**



Enrichment

Country	N/A
City	N/A
Reputation Score	0.5
IP Info Raw	None

Evidence

Raw alert: `{"alert type": "SERVICE PROBE", "src ip": "172.20.10.4", "target_ip": null, "ports": ["443", "80"], "start_time": "Wed Jul 30 15:31:58 2025", "duration": null}`

Capture Time: Wed Jul 30 15:31:58 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 235fa8421e89c585041076cbfb0c7c10b565f0e645bf4fbff2d796e0aa1f3fe1