

Rule Report — rule-bccafb0a

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-bccafb0a
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 16:11:40 2025", "duration": null}`

Capture Time: Wed Jul 30 16:11:40 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: fa0dd11b01f8692b3a57f7d4cf53739c2d144d8e848e392fac3a4d864bf65640