

Rule Report — rule-ee48eaa4

Created: 2025-10-03T08:27:57Z | Threat Level: Critical

Executive summary: Detected ICMP_PING_SCAN from 172.20.10.3 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-ee48eaa4
Alert Type	ICMP_PING_SCAN
Src IP	172.20.10.3
Target IP	N/A
Ports	N/A
CVSS	9.8
Risk score	89.0 (Critical)
Decision	block_ip — ICMP anomaly

Correlation / Related alerts

Related alerts (last 48h): **64**



Enrichment

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

Evidence

Raw alert: {"alert_type": "ICMP PING SCAN", "src_ip": "172.20.10.3", "target_ip": null, "ports": [], "start_time": "Wed Jul 30 15:31:43 2025", "duration": null}

Capture Time: Wed Jul 30 15:31:43 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 0c0e3353ceebe69c5009b55675489a6cb47a9248a08b3dd7f6d703b5e69ca809