

Rule Report — rule-e332fdc5

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

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

Technical summary

| Field | Value |
|------------|-------------------------|
| Rule ID | rule-e332fdc5 |
| Alert Type | ICMP |
| 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", "src_ip": "172.20.10.3", "target_ip": "172.20.10.4", "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: b606b6a872b35af2905e16b7bc7948184c1e3a7eff87239bb7ff8c396dbb2d49