[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 14d1b72f-9f0e-40c8-a269-67c3a9c6c8ac | Generated: 2026-02-13 03:54:14 UTC

Executive Summary

Verdict: NEEDS_ESCALATION (52.925% confidence) — suspicious activity requiring human review. Key factors: IOC 1.2.3.4 flagged by 2 source(s) (risk score: 64.5). IOC 5.6.7.8 flagged by 1 source(s) (risk score: 33.0).

Verdict

Confidence: 52.9%

Alert Details

Field	Value
Alert Type	generic
Timestamp	2026-02-13T03:53:58.684408
Classification	generic_alert
Initial Severity	MEDIUM
Source IP	1.2.3.4 dest_ip
Destination IP	5.6.7.8

Investigation Timeline

Triage — Complete

Classified as generic_alert. Severity: MEDIUM.

Ioc Extraction — Complete

Extracted 2 IOCs: {'ipv4': 2}

Enrichment — Complete

Enriched 2 IOCs across threat intel sources.

Correlation — Complete

No related investigations found. This appears to be a new, isolated alert.

Att&ck Mapping — Complete

Matched 0 techniques across 0 tactics.

Verdict — Complete

NEEDS_ESCALATION (confidence: 52.9%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
1.2.3.4	🟩	64.5	2 / 5	VT: 2/93 engines flagged as malicious. AS: N/A, Country: AU AbuseIPDB: Abuse confidence 66%, 100 reports. ISP: APNIC Debogon Project, Usage: None, Country: AU OTX: 50 pulses reference this IOC. Tags: zakk, abel, tempdir, rscreateandgo, vima GreyNoise: IP not observed scanning the internet

5.6.7.8	🟩	33.0	1 / 5	VT: 1/93 engines flagged as malicious. AS: Telefonica Germany, Country: DE AbuseIPDB: Abuse confidence 0%, 1 reports. ISP: Telefonica Germany GmbH & Co.OHG, Usage: Fixed Line ISP, Country: DE OTX: 6 pulses reference this IOC. Tags: a cose, zakk, nsview, confusingly, haspasswd GreyNoise: IP not observed scanning the internet

Reasoning Chain

IOC 1.2.3.4 flagged by 2 source(s) (risk score: 64.5).

IOC 5.6.7.8 flagged by 1 source(s) (risk score: 33.0).

No significant behavioral indicators detected.

No historical correlation data available.

No MITRE ATT&CK techniques identified.

Alert occurred during off-hours (03:00). Slightly elevated risk.

Score Breakdown

Component	Score	Weight	Weighted Score

Enrichment	74.5	35.0%	26.1
Behavioral	0.0	25.0%	0.0
Correlation	0.0	20.0%	0.0
Mitre	0.0	15.0%	0.0
Temporal	20.0	5.0%	1.0

Recommended Response Actions

1. Escalate to senior analyst for manual review.

2. Gather additional context from the host and user.

3. Monitor traffic to/from 1.2.3.4 dest_ip for additional indicators.

4. Do not take destructive action until further analysis is complete.

Raw Evidence

```
test alert source_ip=1.2.3.4 dest_ip=5.6.7.8
```

Generated by SOC-AI-Agent | Automated Security Investigation Platform
Report generated at 2026-02-13 03:54:14 UTC