

[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: a3a3538e-105b-4abb-bb37-1a048293519c | Generated: 2026-02-13 04:30:25 UTC

Executive Summary

Verdict: FALSE_POSITIVE (85.638% confidence) — benign activity (false positive). Key factors: IOC 45.33.32.156 flagged by 2 source(s) (risk score: 28.3). IOCs appeared in 2 false positive(s). May reduce malicious confidence.

Verdict

Confidence: 85.6%

Alert Details

Field	Value
Alert Type	generic
Timestamp	2024-01-15T02:01:12.304000+00:00
Classification	data_exfiltration
Initial Severity	HIGH
Source IP	45.33.32.156
Source Host	10.0.1.50

User	mthompson
------	-----------

Investigation Timeline

Triage — Complete

Classified as data_exfiltration. Severity: HIGH.

IoC Extraction — Complete

Extracted 1 IOCs: {'ipv4': 1}

Enrichment — Complete

Enriched 1 IOCs across threat intel sources.

Correlation — Complete

Found 2 related investigation(s). Shared IOCs: 45.33.32.156 (seen 2x). 2 related investigation(s) were previously classified as false positives.

Att&ck Mapping — Complete

Matched 0 techniques across 0 tactics.

Verdict — Complete

FALSE_POSITIVE (confidence: 85.6%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary

				VT: 3/93 engines flagged as malicious. AS: Akamai Connected Cloud, Country: US AbuseIPDB: Abuse confidence 0%, 3 reports. ISP: Linode, Usage: Data Center/Web Hosting/Transit, Country: US OTX: 3 pulses reference this IOC. Tags: sven klemm, ganglia, justin maggard, checks, spam GreyNoise: IP not observed scanning the internet
45.33.32.156		28.3	2 / 5	

Historical Correlation

Found 2 related investigation(s). Shared IOCs: 45.33.32.156 (seen 2x). 2 related investigation(s) were previously classified as false positives.

Alert ID	Type	Verdict	Matching IOC	Date
d03a0eb4...	generic	FALSE_POSITIVE	45.33.32.156	2026-02-13T04:02:00.8818
12c3cace...	generic	FALSE_POSITIVE	45.33.32.156	2026-02-13T04:18:24.2720

Reasoning Chain

IOC 45.33.32.156 flagged by 2 source(s) (risk score: 28.3).

No significant behavioral indicators detected.

IOCs found in 2 previous investigation(s).

IOCs appeared in 2 false positive(s). May reduce malicious confidence.

No MITRE ATT&CK techniques identified.

Alert occurred during off-hours (02:00). Slightly elevated risk.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	28.3	35.0%	9.9
Behavioral	0.0	25.0%	0.0
Correlation	0	20.0%	0.0
Mitre	0.0	15.0%	0.0
Temporal	20.0	5.0%	1.0

Recommended Response Actions

1. No immediate action required.

2. Consider adding to allowlist/exception list if recurring.

3. Document the false positive for tuning detection rules.

Raw Evidence

```
#Fields: timestamp duration src_ip src_port dst_ip dst_port protocol bytes_sent bytes_recv  
packets_sent packets_recv flags #Software: NetFlow v9 Collector #Exporter:  
fw-core-01.corp.acme.local #Date: 2024-01-15 2024-01-15T02:01:12.304Z 45.2 10.0.1.50 49201  
45.33.32.156 443 TCP 52428800 12048 38420 9210 .AP.SF 2024-01-15T02:04:33.518Z 62.8 10.0.1.50  
49202 45.33.32.156 443 TCP 78643200 15872 57540 12104 .AP.SF 2024-01-15T02:08:41.102Z 71.4  
10.0.1.50 49203 45.33.32.156 443 TCP 104857600 18204 76800 13920 .AP.SF  
2024-01-15T02:15:22.891Z 88.1 10.0.1.50 49204 45.33.32.156 443 TCP 125829120 21508 92160 16440
```

.AP.SF 2024-01-15T02:22:08.204Z 95.3 10.0.1.50 49205 45.33.32.156 443 TCP 157286400 24012
115200 18360 .AP.SF 2024-01-15T02:30:44.617Z 102.7 10.0.1.50 49206 45.33.32.156 443 TCP
167772160 26840 122880 20520 .AP.SF 2024-01-15T02:40:11.308Z 110.4 10.0.1.50 49207 45.33.32.156
443 TCP 178257920 29104 130560 22260 .AP.SF 2024-01-15T02:50:02.512Z 98.6 10.0.1.50 49208
45.33.32.156 443 TCP 188743680 31892 138240 24408 .AP.SF 2024-01-15T02:58:18.891Z 115.2
10.0.1.50 49209 45.33.32.156 443 TCP 199229440 33240 146000 25440 .AP.SF
2024-01-15T03:08:42.104Z 121.8 10.0.1.50 49210 45.33.32.156 443 TCP 209715200 35508 153600
27180 .AP.SF 2024-01-15T03:15:33.207Z 108.3 10.0.1.50 49211 45.33.32.156 443 TCP 220200960
37104 161280 28380 .AP.SF 2024-01-15T03:22:01.518Z 126.4 10.0.1.50 49212 45.33.32.156 443 TCP
230686720 39208 169000 30000 .AP.SF 2024-01-15T03:30:48.801Z 134.1 10.0.1.50 49213 45.33.32.156
443 TCP 241172480 41520 176640 31780 .AP.SF 2024-01-15T03:38:22.104Z 118.9 10.0.1.50 49214
45.33.32.156 443 TCP 251658240 43012 184320 32920 .AP.SF 2024-01-15T03:45:11.512Z 141.2
10.0.1.50 49215 45.33.32.156 443 TCP 262144000 45880 192000 35100 .AP.SF
2024-01-15T03:52:44.208Z 128.5 10.0.1.50 49216 45.33.32.156 443 TCP 272629760 47204 199680
36120 .AP.SF 2024-01-15T03:58:01.891Z 137.8 10.0.1.50 49217 45.33.32.156 443 TCP 283115520
49512 207360 37900 .AP.SF 2024-01-15T04:05:33.104Z 145.3 10.0.1.50 49218 45.33.32.156 443 TCP
293601280 51840 215040 39680 .AP.SF 2024-01-15T04:12:08.502Z 131.6 10.0.1.50 49219 45.33.32.156
443 TCP 304087040 53104 222720 40620 .AP.SF 2024-01-15T04:18:44.891Z 148.2 10.0.1.50 49220
45.33.32.156 443 TCP 314572800 55208 230400 42240 .AP.SF # Total bytes exfiltrated: ~2.93 GB
outbound to 45.33.32.156 over 137 minutes during off-hours (02:01-04:18 UTC) # Source host:
10.0.1.50 (FINANCE-WS04.corp.acme.local) - assigned to user mthompson # Destination:
45.33.32.156 - unclassified external IP, no prior baseline traffic