[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 3816a593-8e6f-4896-86e0-293ab57a6704 | Generated: 2026-02-13 03:44:33 UTC

Executive Summary

Verdict: NEEDS_ESCALATION (42.8% confidence) — suspicious activity requiring human review. Key factors: IOC 185.220.101.34 flagged as malicious by 4 sources (risk score: 95.0). Strong indicator of compromise.

Verdict

Confidence: 42.8%

Alert Details

Field	Value
Alert Type	generic
Timestamp	2026-01-15T03:22:01
Classification	generic_alert
Initial Severity	MEDIUM
Source IP	185.220.101.34
User	administrator

Investigation Timeline

Triage — Complete

Classified as generic_alert. Severity: MEDIUM.

Ioc Extraction — Complete

Extracted 1 IOCs: {'ipv4': 1}

Enrichment — Complete

Enriched 1 IOCs across threat intel sources.

Correlation — Complete

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

Att&ck Mapping — Complete

Matched 1 techniques across 1 tactics.

Verdict — Complete

NEEDS_ESCALATION (confidence: 42.8%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary

185.220.101.34	🟩	95.0	4 / 5	VT: 15/93 engines flagged as malicious. AS: Stiftung Erneuerbare Freiheit, Country: DE AbuseIPDB: Abuse confidence 98%, 157 reports. ISP: Network for Tor-Exit traffic., Usage: Fixed Line ISP, Country: DE Shodan: 2 open ports, 0 vulns. Org: Network for Tor-Exit traffic., OS: None, Country: DE OTX: 50 pulses reference this IOC. Tags: OpenCTI, SSH, Brute-Force, malicious, Automated GreyNoise: Classification=malicious, Noise=True, RIOT=False, Name=unknown

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Command and Control	T1090	Proxy	Enrichment tag: tor

Attack chain analysis:
1. **Command and Control**: Proxy (T1090)

Reasoning Chain

IOC 185.220.101.34 flagged as malicious by 4 sources (risk score: 95.0). Strong indicator of compromise.

No significant behavioral indicators detected.

No historical correlation data available.

Matched 1 MITRE ATT&CK technique(s) across 1 tactic(s).

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

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	100	35.0%	35.0
Behavioral	0.0	25.0%	0.0
Correlation	0.0	20.0%	0.0
Mitre	8	15.0%	1.2
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 185.220.101.34 for additional indicators.

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

Raw Evidence

```
Jan 15 03:22:01 prod-ssh-bastion sshd[28401]: Failed password for root from 185.220.101.34 port
44312 ssh2 Jan 15 03:22:03 prod-ssh-bastion sshd[28401]: Failed password for root from
185.220.101.34 port 44312 ssh2 Jan 15 03:22:05 prod-ssh-bastion sshd[28401]: Failed password
for root from 185.220.101.34 port 44312 ssh2 Jan 15 03:22:06 prod-ssh-bastion sshd[28403]:
Failed password for invalid user administrator from 185.220.101.34 port 44398 ssh2 Jan 15
03:22:08 prod-ssh-bastion sshd[28403]: Invalid user administrator from 185.220.101.34 port
44398 Jan 15 03:22:10 prod-ssh-bastion sshd[28405]: Failed password for root from
185.220.101.34 port 44471 ssh2 Jan 15 03:22:12 prod-ssh-bastion sshd[28407]: Failed password
for invalid user test from 185.220.101.34 port 44520 ssh2 Jan 15 03:22:12 prod-ssh-bastion
sshd[28407]: Invalid user test from 185.220.101.34 port 44520 Jan 15 03:22:15 prod-ssh-bastion
sshd[28409]: Failed password for admin from 185.220.101.34 port 44583 ssh2 Jan 15 03:22:17
prod-ssh-bastion sshd[28409]: Failed password for admin from 185.220.101.34 port 44583 ssh2 Jan
15 03:22:19 prod-ssh-bastion sshd[28411]: Failed password for invalid user ubuntu from
185.220.101.34 port 44651 ssh2 Jan 15 03:22:19 prod-ssh-bastion sshd[28411]: Invalid user
ubuntu from 185.220.101.34 port 44651 Jan 15 03:22:22 prod-ssh-bastion sshd[28413]: Failed
password for invalid user postgres from 185.220.101.34 port 44702 ssh2 Jan 15 03:22:22
prod-ssh-bastion sshd[28413]: Invalid user postgres from 185.220.101.34 port 44702 Jan 15
03:22:25 prod-ssh-bastion sshd[28415]: Failed password for root from 185.220.101.34 port 44768
ssh2 Jan 15 03:22:27 prod-ssh-bastion sshd[28417]: Failed password for invalid user oracle from
185.220.101.34 port 44831 ssh2 Jan 15 03:22:27 prod-ssh-bastion sshd[28417]: Invalid user
oracle from 185.220.101.34 port 44831 Jan 15 03:22:30 prod-ssh-bastion sshd[28419]: Failed
password for admin from 185.220.101.34 port 44892 ssh2 Jan 15 03:22:33 prod-ssh-bastion
sshd[28421]: Failed password for invalid user user from 185.220.101.34 port 44955 ssh2 Jan 15
03:22:35 prod-ssh-bastion sshd[28423]: Failed password for invalid user deploy from
185.220.101.34 port 45018 ssh2 Jan 15 03:22:35 prod-ssh-bastion sshd[28423]: Invalid user
deploy from 185.220.101.34 port 45018 Jan 15 03:22:38 prod-ssh-bastion sshd[28425]: Failed
password for root from 185.220.101.34 port 45081 ssh2 Jan 15 03:22:40 prod-ssh-bastion
sshd[28427]: Failed password for admin from 185.220.101.34 port 45144 ssh2 Jan 15 03:22:43
prod-ssh-bastion sshd[28429]: Failed password for invalid user ftpuser from 185.220.101.34 port
45207 ssh2 Jan 15 03:22:43 prod-ssh-bastion sshd[28429]: Invalid user ftpuser from
185.220.101.34 port 45207 Jan 15 03:22:46 prod-ssh-bastion sshd[28431]: Failed password for
invalid user guest from 185.220.101.34 port 45270 ssh2 Jan 15 03:22:46 prod-ssh-bastion
sshd[28431]: Invalid user guest from 185.220.101.34 port 45270 Jan 15 03:22:49 prod-ssh-bastion
sshd[28433]: Failed password for admin from 185.220.101.34 port 45333 ssh2 Jan 15 03:22:52
prod-ssh-bastion sshd[28435]: Failed password for root from 185.220.101.34 port 45396 ssh2 Jan
15 03:22:55 prod-ssh-bastion sshd[28437]: Failed password for invalid user webmaster from
185.220.101.34 port 45459 ssh2 Jan 15 03:22:55 prod-ssh-bastion sshd[28437]: Invalid user
webmaster from 185.220.101.34 port 45459 Jan 15 03:22:58 prod-ssh-bastion sshd[28439]: Failed
password for invalid user pi from 185.220.101.34 port 45522 ssh2 Jan 15 03:22:58
prod-ssh-bastion sshd[28439]: Invalid user pi from 185.220.101.34 port 45522 Jan 15 03:23:01
prod-ssh-bastion sshd[28441]: Failed password for admin from 185.220.101.34 port 45585 ssh2 Jan
15 03:23:04 prod-ssh-bastion sshd[28443]: Failed password for root from 185.220.101.34 port
45648 ssh2 Jan 15 03:23:07 prod-ssh-bastion sshd[28445]: Failed password for admin from
185.220.101.34 port 45711 ssh2 Jan 15 03:23:10 prod-ssh-bastion sshd[28447]: Failed password
for admin from 185.220.101.34 port 45774 ssh2 Jan 15 03:23:13 prod-ssh-bastion sshd[28449]:
Failed password for admin from 185.220.101.34 port 45837 ssh2 Jan 15 03:23:16 prod-ssh-bastion
sshd[28451]: Failed password for admin from 185.220.101.34 port 45900 ssh2 Jan 15 03:23:18
prod-ssh-bastion sshd[28453]: Accepted password for admin from 185.220.101.34 port 45963 ssh2
Jan 15 03:23:18 prod-ssh-bastion sshd[28453]: pam_unix(sshd:session): session opened for user
admin(uid=1001) by (uid=0) Jan 15 03:23:18 prod-ssh-bastion systemd-logind[812]: New session
4827 of user admin.
```

Generated by SOC-AI-Agent | Automated Security Investigation Platform
Report generated at 2026-02-13 03:44:33 UTC