Incident Analysis Report

1. Alarm Information

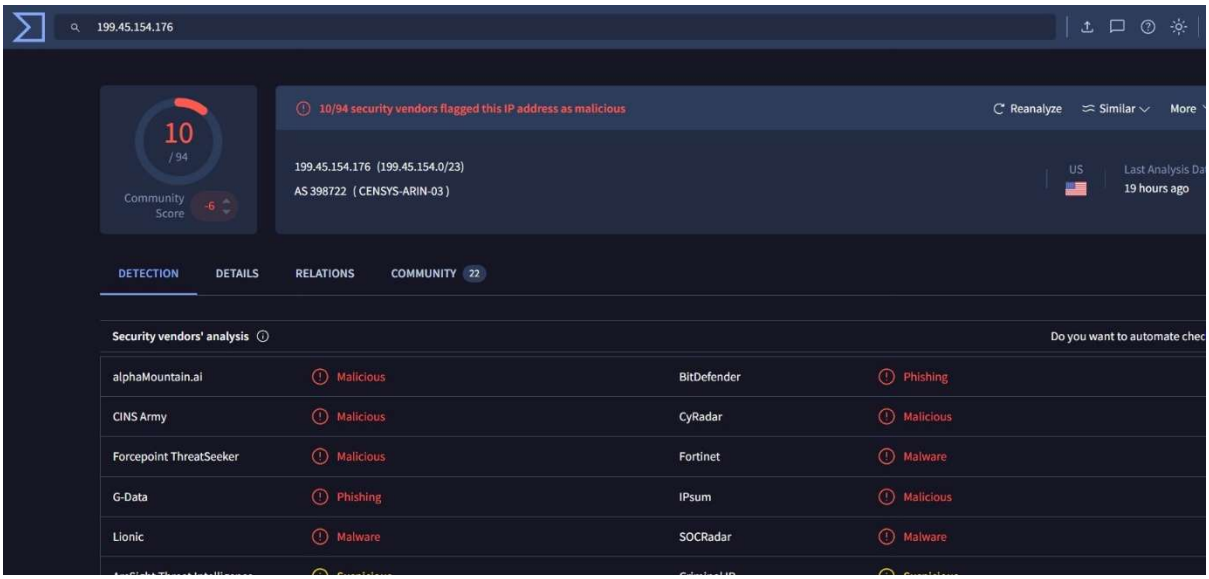
- **Alarm ID / Case No:** 002
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** External Port Scan detected from IP 199.45.154.176
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

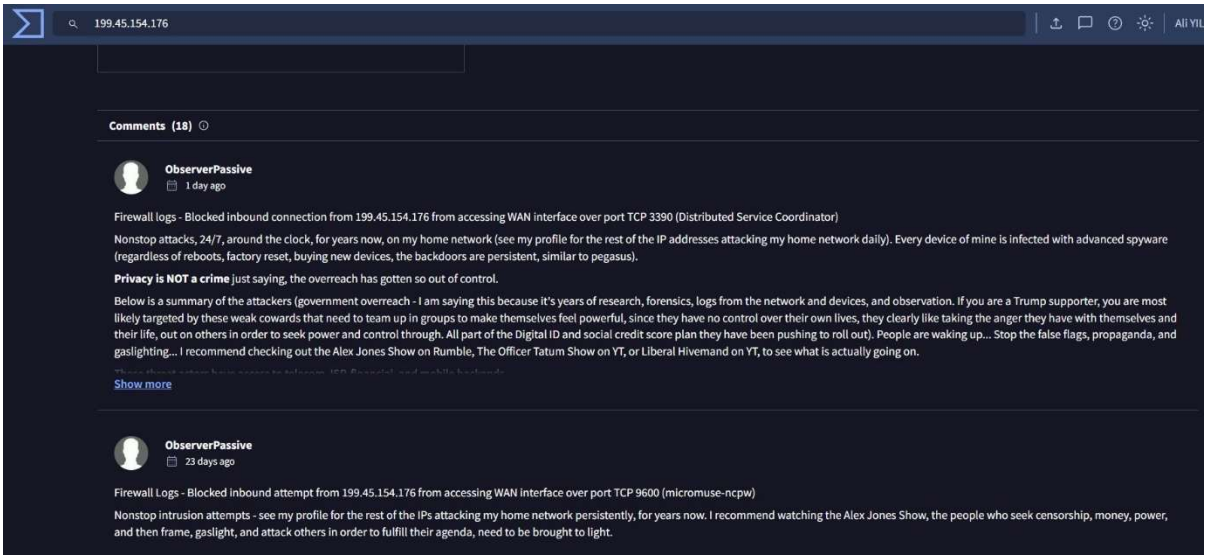
2. IOC Information

- **IOC Type:** IP Address
- **IOC Value:** 199.45.154.176
- **IOC Location:** [USA]

3. OSINT Investigation

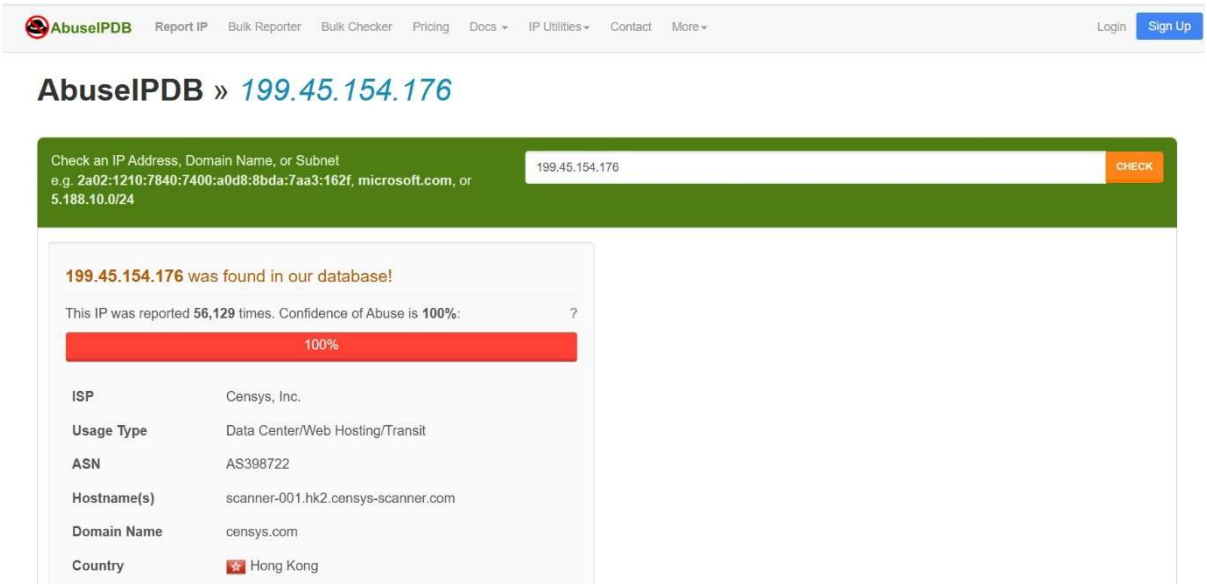
VirusTotal

- Result: Detected by 1 AV engine (low confidence).
- https://www.virustotal.com/gui/ip-address/199.45.154.176
- 

- 

AbuseIPDB

- Result: 100% Abuse Confidence Score – reported for External Port Scan activity.
- https://www.abuseipdb.com/check/199.45.154.176



4. Analysis & Assessment

- VirusTotal result alone is weak evidence.
- AbuseIPDB provides stronger indication of External Port Scan with multiple reports.

5. Conclusion / Decision

- **Decision: ✅ True Positive**

- **Category:** External Port Scan
- **Risk Level:** High (based on organization's classification)

---

6. Recommended Actions

1. Block the IP address on firewall / IPS.
2. Review SIEM logs for additional login attempts from the same source.
3. Correlate failed logins with user accounts for potential compromise attempts.
4. Consider implementing automated blocking rules for IPs with high abuse scores.