Incident Analysis Report

1. Alarm Information

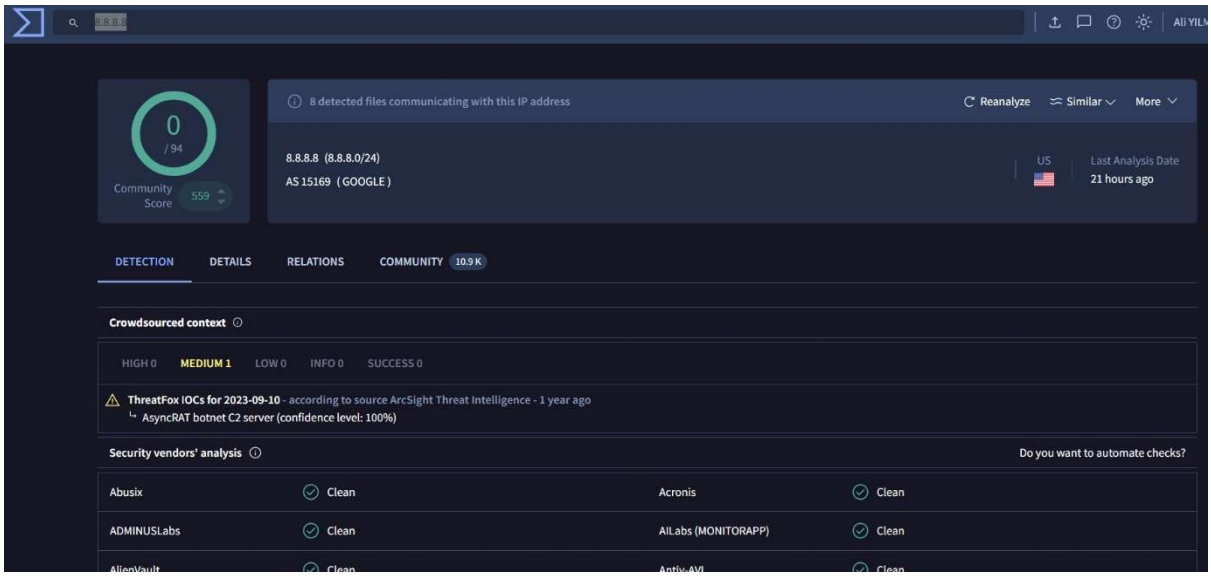
- **Alarm ID / Case No:** 004
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Port Scan detected from IP 8.8.8.8
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** IP Address
- **IOC Value:** 8.8.8.8
- **IOC Location:** [USA]

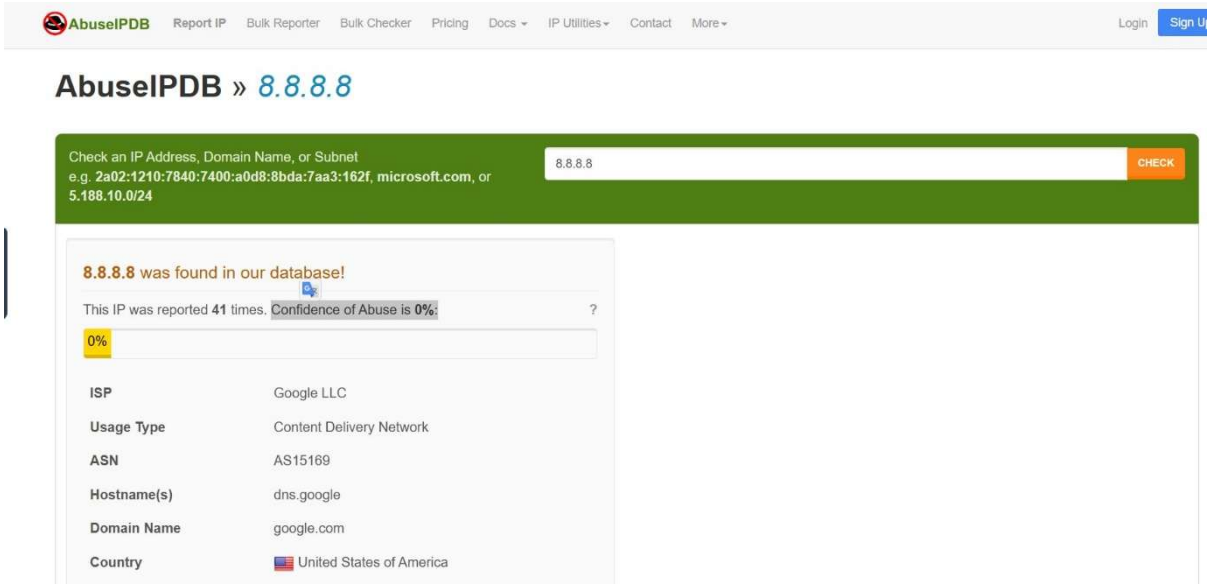
3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (Non confidence).
- https://www.virustotal.com/gui/ip-address/8.8.8.8
- 

AbuseIPDB

- Result: Confidence of Abuse is **0%**
- https://www.abuseipdb.com/check/8.8.8.8

- 

4. Analysis & Assessment

- VirusTotal check returned clean – no malicious classification for this IP
- AbuseIPDB provides Confidence of Abuse is **0%**

5. Conclusion / Decision

- **Decision:** ✅ **False Positive**
- **Category:** Port Scan
- **Risk Level: None** (based on organization's classification)

---

6. Recommended Actions

1 Confirm that the traffic on port 53 to 8.8.8.8 is legitimate DNS resolution activity.

2 Tune SIEM/IDS rule to avoid false positives for standard DNS traffic.

3 Monitor for unusual ports or unexpected destinations in future DNS queries.

4 No blocking action is required for 8.8.8.8.