

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>

The screenshot shows the VirusTotal interface for the IP address 8.8.8.8. At the top, it displays '0 / 94' files communicating with the IP. Below this, the IP is listed as '8.8.8.8 (8.8.8.0/24)' and 'AS 15169 (GOOGLE)'. The 'Community Score' is 559. On the right, there are buttons for 'Reanalyze', 'Similar', 'More', and a map showing the location as 'US' with a 'Last Analysis Date' of '21 hours ago'. Below this, there are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY (10.9 K)'. The 'DETECTION' tab is selected, showing 'CROWDSOURCED CONTEXT' with a 'MEDIUM 1' confidence level. A warning message states: 'ThreatFox IOCs for 2023-09-10 - according to source ArcSight Threat Intelligence - 1 year ago' and '↳ AsyncRAT botnet C2 server (confidence level: 100%)'. The 'SECURITY VENDORS' ANALYSIS' section lists several vendors: Abusix (Clean), ADMINUSLabs (Clean), AlienVault (Clean), Acronis (Clean), AllLabs (MONITORAPP) (Clean), and Antiv-AVI (Clean). There is also a link to 'Do you want to automate checks?'

AbuseIPDB

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

The screenshot shows the AbuselPDB website interface. At the top, there is a navigation bar with links for Report IP, Bulk Reporter, Bulk Checker, Pricing, Docs, IP Utilities, Contact, and More. On the far right, there are Login and Sign Up buttons. Below the navigation bar, the title "AbuselPDB » 8.8.8.8" is displayed. A search bar at the top of the main content area contains the IP address "8.8.8.8" and a "CHECK" button. The main content area displays a message: "8.8.8.8 was found in our database!" followed by a small icon of a person. Below this, it says "This IP was reported 41 times. Confidence of Abuse is 0%." with a question mark link. A progress bar indicates 0%. Below the progress bar, several details are listed in a table-like format:

ISP	Google LLC
Usage Type	Content Delivery Network
ASN	AS15169
Hostname(s)	dns.google
Domain Name	google.com
Country	United States of America

4. Analysis & Assessment

- VirusTotal check returned clean – no malicious classification for this IP
- AbuselPDB 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.