Incident Analysis Report

1. Alarm Information

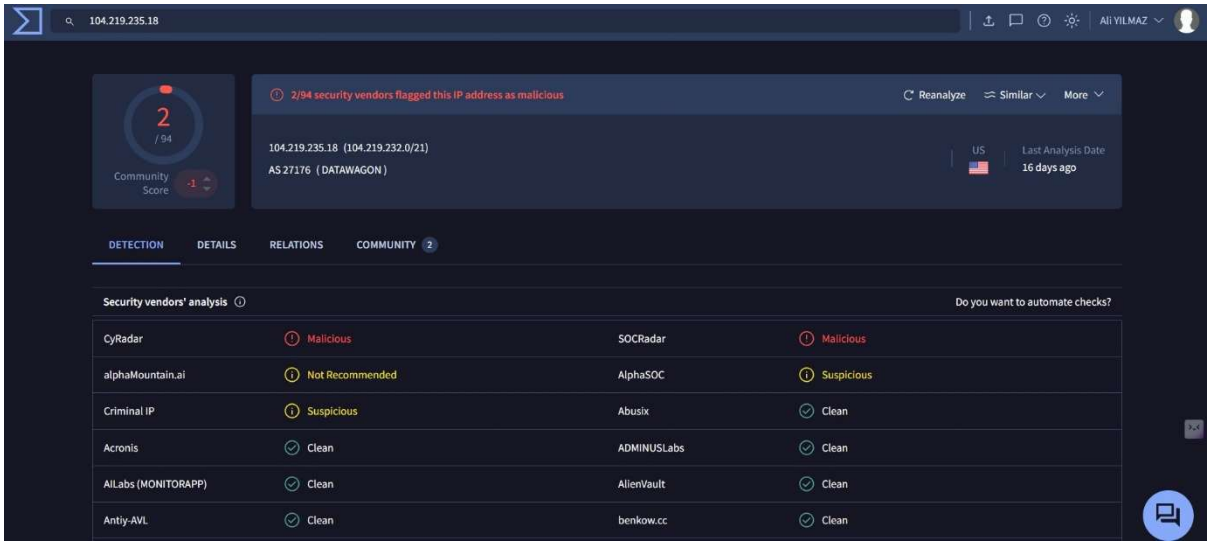
- **Alarm ID / Case No:** 001
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Failed login attempts detected from IP 104[.]219[.]235[.]18
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** IP Address
- **IOC Value:** 104[.]219[.]235[.]18
- **Allowed User Location:** Germany & Netherlands
- **IOC Location:** [USA Maryland]

3. OSINT Investigation

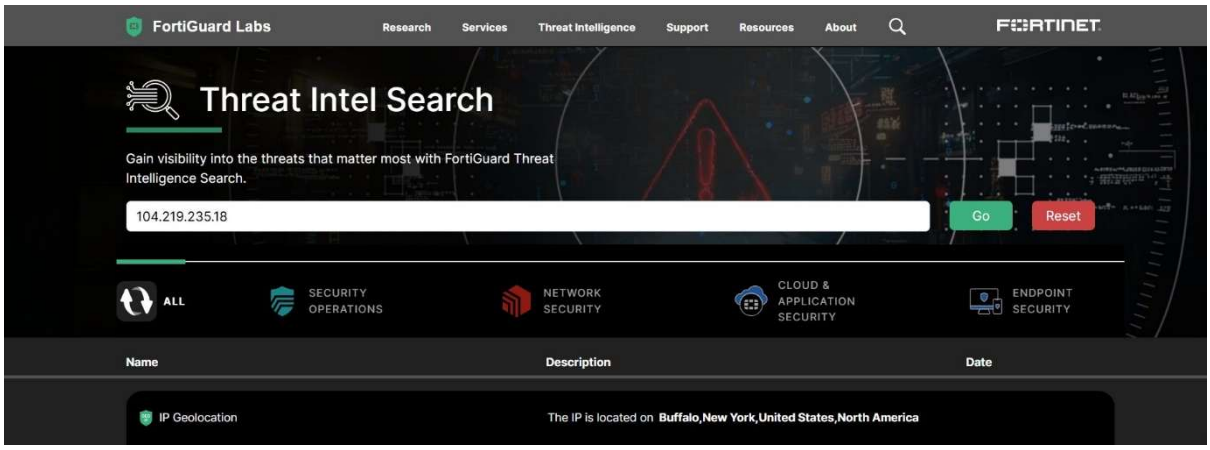
VirusTotal

- Result: Detected by 1 AV engine (low confidence).
- https://www.virustotal.com/gui/ip-address/104.219.235.18
- 

FortiGuard

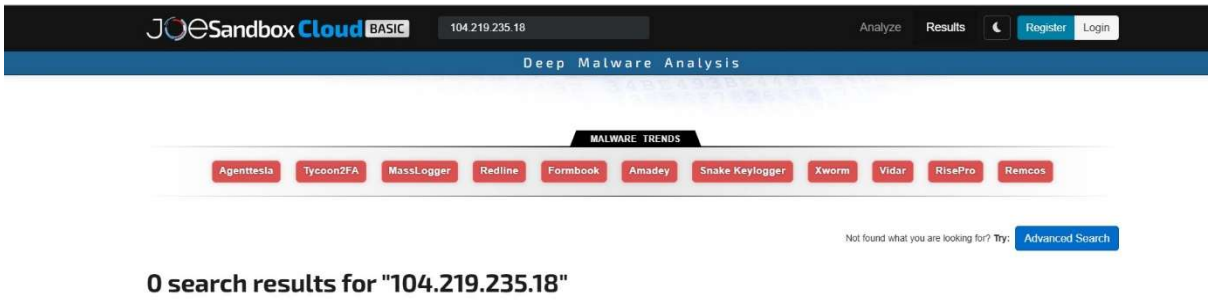
- Result: Clean – no malicious activity found.

- https://www.fortiguard.com/threatintel-search



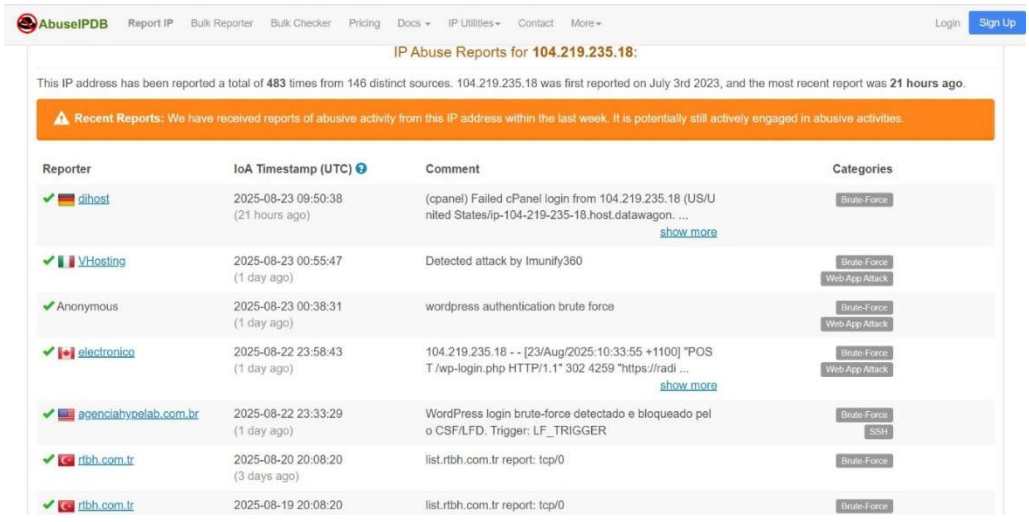
Joe Sandbox / Other Sandbox

- Result: No malicious behavior observed.
- https://www.joesandbox.com/analysis/search?q=104.219.235.18



Joe Sandbox

- Result: 52% Abuse Confidence Score – reported for brute force activity.
- https://www.joesandbox.com/analysis/search?q=104.219.235.18



4. Analysis & Assessment

- VirusTotal result alone is weak evidence.
- FortiGuard and sandbox results show no malware involvement.
- AbuseIPDB provides stronger indication of brute force attempts with multiple reports.
- The IP originates from outside the authorized employee geolocation (Germany/Netherlands).

5. Conclusion / Decision

- **Decision:** ✅ **True Positive**
- **Category:** External Brute Force Attempt
- **Risk Level:** Medium / 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.