

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>

The screenshot shows the VirusTotal interface for the IP address 104.219.235.18. At the top, it displays a 'Community Score' of 2/94, indicating 2 malicious detections out of 94 engines. Below this, the IP is identified as 104.219.235.18 (104.219.232.0/21) and AS 27176 (DATAWAGON). The status bar shows the last analysis date as 16 days ago. The main section, 'DETECTION', lists the results from various security vendors:

Vendor	Result
CyRadar	Malicious
alphaMountain.ai	Not Recommended
Criminal IP	Suspicious
Acronis	Clean
AI Labs (MONITORAPP)	Clean
Anti-AVL	Clean
SOCRadar	Malicious
AlphaSOC	Suspicious
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
benkow.cc	Clean

FortiGuard

- Result: Clean – no malicious activity found.

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

The screenshot shows the FortiGuard Threat Intel Search interface. At the top, there's a search bar with the IP address "104.219.235.18". Below the search bar are several navigation links: ALL, SECURITY OPERATIONS, NETWORK SECURITY, CLOUD & APPLICATION SECURITY, and ENDPOINT SECURITY. A large red warning icon is prominently displayed on the right side of the screen. The main content area displays a table with columns for Name, Description, and Date. One row in the table is highlighted, showing "IP Geolocation" and the note "The IP is located on Buffalo, New York, United States, North America".

Joe Sandbox / Other Sandbox

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

The screenshot shows the Joe Sandbox Cloud BASIC interface. At the top, it displays the IP address "104.219.235.18". Below the IP address are buttons for Analyze, Results, Register, and Login. The main content area is titled "Deep Malware Analysis". It features a "MALWARE TRENDS" section with various threat names like AgentTesla, Tycoon2FA, MassLogger, Redline, Formbook, Amadey, Snake Keylogger, Xworm, Vidar, RisePro, and Remcos. A search bar at the bottom right says "Not found what you are looking for? Try: Advanced Search". Below the trends, a message states "0 search results for '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>

The screenshot shows the AbuseIPDB interface. At the top, it has a navigation bar with links for Report IP, Bulk Reporter, Bulk Checker, Pricing, Docs, IP Utilities, Contact, More, Login, and Sign Up. Below the navigation bar, it says "IP Abuse Reports for 104.219.235.18". A message indicates that the IP address has been reported 483 times from 146 distinct sources. The most recent report was on July 3rd, 2023. A yellow warning box at the top states "Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities." Below this, a table lists recent reports. The columns include Reporter, IoA Timestamp (UTC), Comment, and Categories. Some categories listed are Brute-Force, Web App Attack, and SSH. The table shows multiple reports from various sources, mostly reporting brute-force attacks.

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.