Digital Forensic Incident Report

Case ID: 8cac2c0b

Generated: 2026-01-12 16:39:40 UTC

1. Executive Summary

Integrated narrative for the 2026-01-12 16:34:57 UTC window (all four batches) Overview During a narrow time window around 16:34:57 UTC on 2026-01-12, multiple security-detection signals were recorded across several source IPs. All observed events are denial or detection signals; no explicit successful authentication or data-access events are recorded in these batches. Detected event types include PROTOCOL_ABUSE, WAF_CORRELATION, SQL_INJECTION, and ACCESS_DENIED, with many entries appearing in rapid succession and, in several cases, duplicates of identical events. Key observations consolidated across batches - PROTOCOL_ABUSE, WAF_CORRELATION, SQL_INJECTION, and ACCESS_DENIED events appear across multiple sources and in close temporal proximity. - Several IPs generate more than one type of signal within the same micro-window, particularly WAF_CORRELATION paired with SQL_INJECTION or PROTOCOL_ABUSE. - A number of entries show duplicate reporting of the same event within the same timestamp, indicating duplicate log entries in some cases. - Network-communication observed entries are present across batches, but payload content is not provided in the summaries. Integrated per-source highlights (selected sources of interest) - 216.244.66.199 - Observed across batches with PROTOCOL_ABUSE and WAF_CORRELATION signals. - Reappearing in the later batch timestamps with additional PROTOCOL_ABUSE and repeated WAF_CORRELATION detections, often clustered within the same second. - 204.236.250.147 - PROTOCOL_ABUSE detected (two occurrences) and WAF_CORRELATION detected (two occurrences) within Batch 2, at or near 16:34:57.038022. - 120.233.80.32 - WAF_CORRELATION detected (two duplicates) and SQL_INJECTION detected in Batch 3 (16:34:57.045246+). - 125.75.66.97 - PROTOCOL_ABUSE detected in Batch 3 (16:34:57.043020+). - 204.76.203.212 - PROTOCOL_ABUSE detected in Batch 3 (16:34:57.042022+). - 176.65.149.227 - PROTOCOL_ABUSE detected in Batch 3 (16:34:57.043020+). - 79.124.40.174 - PROTOCOL_ABUSE detected in Batch 1 (two occurrences within the same second). - 198.244.240.150 - WAF_CORRELATION (two occurrences) and SQL_INJECTION (one occurrence) in Batch 1. - 101.72.249.169 - WAF_CORRELATION (two occurrences) and SQL_INJECTION (one occurrence) in Batch 1. - 54.38.147.150 - WAF_CORRELATION (two occurrences) and SQL_INJECTION (one occurrence) in Batch 1. - 92.205.212.128 - ACCESS_DENIED (three occurrences) in Batch 1. - 4.194.99.179 - ACCESS_DENIED (two occurrences) in Batch 1. - 208.167.225.162 - ACCESS_DENIED (multiple occurrences; repeated within the same timestamp) in Batch 1. - 188.164.197.115 - ACCESS_DENIED (seven occurrences) in Batch 2, within the single-second window. - 185.242.226.15 - PROTOCOL_ABUSE (two occurrences) in Batch 2. - 103.152.164.82 - ACCESS_DENIED in Batch 3. - 4.197.100.161 - ACCESS_DENIED in Batch 3. - 216.244.66.199 (note the repeated appearances) - In

Batch 4, WAF_CORRELATION and PROTOCOL_ABUSE are reported for this IP in rapid succession, with multiple timestamps in the same interval. Network observations - Batch 2 records 16 network communications observed in a tight window (16:34:57.039022 and 16:34:57.040021). - Batch 3 and Batch 4 include further lines labeled as “Network communication observed” in quick succession after the other detections, but payload details are not provided in these summaries. - Overall, network activity signals accompany several detection events, but no payload content is described in the provided data. Conservative interpretation (as observed) - The data show clusters of denial and detection signals around 16:34:57 UTC, with multiple detections occurring within microseconds to milliseconds of each other. - No explicit successful access or data exposure is indicated in any batch. - Recurrent appearance of certain IPs across multiple detection types and batches suggests repeated interaction within this narrow time frame, but attribution or conclusions about intent or compromise cannot be drawn from these records alone. - Duplicates in the logs are present for some entries, and some IPs appear in more than one detection category within the same timestamp. Suggested follow-up (conservative) - Correlate the identified IPs across other time windows to determine if this represents a short-lived burst or a broader pattern. - Review firewall/WAF configurations and associated payloads for IPs showing SQL_INJECTION and PROTOCOL_ABUSE signals to confirm the nature of the attempts. - Inspect for repeated ACCESS_DENIED activity from the same IPs to assess if they may represent automated scanning or probing activity. - Cross-check the listed IPs against known-bad lists or external threat intelligence feeds, without drawing attribution. - Verify whether any legitimate traffic could be misclassified due to rule configuration, and validate rule accuracy and thresholds. Bottom line Across the four batches, a coordinated set of detection and denial signals occurred within a very tight time frame. The observations are limited to detections and denial events; no evidence of a successful breach or data access is indicated by the provided data. Further cross-batch correlation and rule-review activities are recommended to determine patterns and validate rule behavior.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-12 16:34:57.031026+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-12 16:34:57.031026+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-12 16:34:57.032026+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-12 16:34:57.032026+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-12 16:34:57.032026+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-12 16:34:57.032026+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-12 16:34:57.033026+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.033026+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.033026+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-12 16:34:57.033026+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.034025+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-12 16:34:57.035024+00:00	ACCESS_DENIED detected from 4.194.99.179
2026-01-12 16:34:57.035024+00:00	WAF_CORRELATION detected from 54.38.147.150
2026-01-12 16:34:57.035024+00:00	WAF_CORRELATION detected from 54.38.147.150
2026-01-12 16:34:57.035024+00:00	SQL_INJECTION detected from 54.38.147.150
2026-01-12 16:34:57.036024+00:00	ACCESS_DENIED detected from 4.194.99.179
2026-01-12 16:34:57.036024+00:00	WAF_CORRELATION detected from 101.72.249.169
2026-01-12 16:34:57.036024+00:00	WAF_CORRELATION detected from 101.72.249.169
2026-01-12 16:34:57.036024+00:00	SQL_INJECTION detected from 101.72.249.169
2026-01-12 16:34:57.037023+00:00	PROTOCOL_ABUSE detected from 185.242.226.15
2026-01-12 16:34:57.037023+00:00	PROTOCOL_ABUSE detected from 185.242.226.15
2026-01-12 16:34:57.037023+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.037023+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.037023+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.037023+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.037023+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.038022+00:00	ACCESS_DENIED detected from 188.164.197.115
2026-01-12 16:34:57.038022+00:00	WAF_CORRELATION detected from 204.236.250.147
2026-01-12 16:34:57.038022+00:00	WAF_CORRELATION detected from 204.236.250.147

Timestamp (UTC)	Observed Event
2026-01-12 16:34:57.038022+00:00	PROTOCOL_ABUSE detected from 204.236.250.147
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.039022+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.040021+00:00	Network communication observed
2026-01-12 16:34:57.041021+00:00	Network communication observed
2026-01-12 16:34:57.041021+00:00	Network communication observed
2026-01-12 16:34:57.042022+00:00	Network communication observed
2026-01-12 16:34:57.042022+00:00	Network communication observed
2026-01-12 16:34:57.042022+00:00	Network communication observed
2026-01-12 16:34:57.042022+00:00	ACCESS_DENIED detected from 103.152.164.82
2026-01-12 16:34:57.042022+00:00	Network communication observed
2026-01-12 16:34:57.042022+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-12 16:34:57.043020+00:00	PROTOCOL_ABUSE detected from 176.65.149.227
2026-01-12 16:34:57.043020+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.043020+00:00	PROTOCOL_ABUSE detected from 125.75.66.97
2026-01-12 16:34:57.043020+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.044245+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-12 16:34:57.044245+00:00	PROTOCOL_ABUSE detected from 125.75.66.97
2026-01-12 16:34:57.044245+00:00	WAF_CORRELATION detected from 120.233.80.32
2026-01-12 16:34:57.044245+00:00	WAF_CORRELATION detected from 120.233.80.32
2026-01-12 16:34:57.045246+00:00	SQL_INJECTION detected from 120.233.80.32
2026-01-12 16:34:57.045246+00:00	ACCESS_DENIED detected from 4.197.100.161
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.045246+00:00	Network communication observed

Timestamp (UTC)	Observed Event
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.045246+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	Network communication observed
2026-01-12 16:34:57.046247+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.047245+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.047245+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-12 16:34:57.047245+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.048243+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.048243+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-12 16:34:57.048243+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.049241+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-12 16:34:57.049241+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-12 16:34:57.049241+00:00	Network communication observed
2026-01-12 16:34:57.049241+00:00	Network communication observed
2026-01-12 16:34:57.049241+00:00	Network communication observed
2026-01-12 16:34:57.049241+00:00	Network communication observed
2026-01-12 16:34:57.049241+00:00	Network communication observed
2026-01-12 16:34:57.050240+00:00	Network communication observed
2026-01-12 16:34:57.050240+00:00	Network communication observed

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
8cac2c0b	T1048	Exfiltration Over Alternative Protocol
3d6dc516	T1046	Network Service Discovery
32804435	T1046	Network Service Discovery
7f023096	T1190	Exploit Public-Facing Application
c011bb59	T1048	Exfiltration Over Alternative Protocol
5bd34808	T1110	Brute Force / Credential Access
92b7d548	T1046	Network Service Discovery
2d143d3b	T1046	Network Service Discovery
3e354986	T1048	Exfiltration Over Alternative Protocol
f6e54392	T1110	Brute Force / Credential Access
14b2bee5	T1110	Brute Force / Credential Access
b9793113	T1110	Brute Force / Credential Access
a92c1294	T1110	Brute Force / Credential Access
9e533f9c	T1110	Brute Force / Credential Access
d7b6c468	T1110	Brute Force / Credential Access
df5a5c34	T1110	Brute Force / Credential Access
3ac8b0c5	T1110	Brute Force / Credential Access
c0fb577a	T1110	Brute Force / Credential Access
81cb0456	T1046	Network Service Discovery
00da6de3	T1046	Network Service Discovery
f87e68a1	T1190	Exploit Public-Facing Application
4076171b	T1110	Brute Force / Credential Access
80756d10	T1046	Network Service Discovery
eecb435e	T1046	Network Service Discovery
7f35d05c	T1190	Exploit Public-Facing Application
7d7935b9	T1048	Exfiltration Over Alternative Protocol
df6f5e36	T1048	Exfiltration Over Alternative Protocol
1421d364	T1110	Brute Force / Credential Access
cad552b4	T1110	Brute Force / Credential Access
3af9d287	T1110	Brute Force / Credential Access
4471dabb	T1110	Brute Force / Credential Access
646ce66a	T1110	Brute Force / Credential Access
4953973d	T1110	Brute Force / Credential Access
553d09c7	T1046	Network Service Discovery
11f1948e	T1046	Network Service Discovery

Artifact ID	Technique ID	Technique Description
137fcc9c	T1048	Exfiltration Over Alternative Protocol
9574c0f2	T1110	Brute Force / Credential Access
fa19742b	T1048	Exfiltration Over Alternative Protocol
869f8f7c	T1048	Exfiltration Over Alternative Protocol
71cfef3d	T1046	Network Service Discovery
623fbba4	T1048	Exfiltration Over Alternative Protocol
c8e65686	T1046	Network Service Discovery
75e83e1f	T1048	Exfiltration Over Alternative Protocol
6534d5ae	T1048	Exfiltration Over Alternative Protocol
a26997f9	T1046	Network Service Discovery
6c41ee65	T1046	Network Service Discovery
6b8bccfc	T1190	Exploit Public-Facing Application
b43b56e6	T1110	Brute Force / Credential Access
895e20e7	T1046	Network Service Discovery
f2850d1f	T1046	Network Service Discovery
f53bf7ff	T1048	Exfiltration Over Alternative Protocol
02fcd46a	T1046	Network Service Discovery
f2dddd66	T1046	Network Service Discovery
4327212f	T1048	Exfiltration Over Alternative Protocol
42fe27df	T1046	Network Service Discovery
62aebaca	T1046	Network Service Discovery
d32c302c	T1048	Exfiltration Over Alternative Protocol

4. Source IP Concentration Analysis

Source IP	Event Count
104.215.26.144	22
4.197.100.161	22
216.244.66.199	15
208.167.225.162	6
188.164.197.115	6
198.244.240.150	3
92.205.212.128	3
54.38.147.150	3
101.72.249.169	3
204.236.250.147	3
120.233.80.32	3
79.124.40.174	2
4.194.99.179	2
185.242.226.15	2
125.75.66.97	2
103.152.164.82	1
204.76.203.212	1
176.65.149.227	1

5. Case Intelligence Summary

Attack Channel	Observed
Web	Yes
Authentication	No
Network	No
Endpoint	No
Cloud	No