Network Log Forensic Investigation Report

Generated on: 2026-01-30 13:32:50.622359

Report Source: reports/timeline_report.txt

```
■ FORENSIC TIMELINE REPORT
======================================================================
Generated At: 2026-01-30 13:13:55
======================================================================
2026-01-30 11:31:49 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:31:49 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:31:57 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:31:57 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:32:04 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:32:04 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:20 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:26 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:33 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:40 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:46 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:39:57 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:58:38 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:58:44 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:58:49 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:58:56 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:03 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:08 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:12 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:17 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:22 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:27 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:33 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
2026-01-30 11:59:42 | TCP | ::1 → 127.0.0.1 | Port 22 | DENY
======================================================================
Total events analyzed: 24
```

Report Source: reports/incident_correlation.txt

```
■ CORRELATED INCIDENT REPORT
============================================================
[INCIDENT] Brute Force Detected
Source IP : ::1
Target Port : 22
Attempts : 5
Time Window : 2026-01-30 11:31:49 → 2026-01-30 11:32:04
------------------------------------------------------------
Total incidents identified: 1
```

Report Source: reports/incident_report.txt

```
■ INCIDENT RESPONSE REPORT
======================================================================
Generated At : 2026-01-30 13:21:05.451821
======================================================================
Incident ID   : INC-2026-001
Attack Type   : SSH Brute Force
Source IP     : ::1
Target Port   : 22
First Seen    : 2026-01-30 11:31:49
Last Seen     : 2026-01-30 11:59:42
Total Attempts: 24
```

Severity   : HIGH
Evidence   : SQLite logs, SSH authentication failures
