Investigation Report

Generated: 2026-02-20 03:21:52

Case Information

Case Name:	case_2
Description:	sample_3
Created:	2026-02-20T00:54:43.587984
Status:	ANALYZED
Total Records:	500

Risk Assessment

Overall Score: 51.2/100 - MEDIUM

Metric	Score
Rule Violations	100.0
Anomaly Detection	28.0
Network Correlation	0.1

Detailed Analysis

Risk Level: MEDIUM (Score: 51.2/100)
Key Findings:
- 124 rule violations detected
- 916 anomalous events identified
- Rule contribution: 100.0
- Anomaly contribution: 28.0
- Network correlation: 0.1
MEDIUM RISK: Some suspicious patterns identified. Monitor closely.

Top Rule Violations

Rule Type	Severity	Description
Midnight Activity	high	Activity detected at 1:00 (off-hours)...
Midnight Activity	high	Activity detected at 2:00 (off-hours)...
Midnight Activity	high	Activity detected at 4:00 (off-hours)...
Midnight Activity	high	Activity detected at 5:00 (off-hours)...
Midnight Activity	high	Activity detected at 5:00 (off-hours)...
Midnight Activity	high	Activity detected at 0:00 (off-hours)...

Midnight Activity	high	Activity detected at 0:00 (off-hours)...
Midnight Activity	high	Activity detected at 0:00 (off-hours)...
Midnight Activity	high	Activity detected at 2:00 (off-hours)...
Midnight Activity	high	Activity detected at 0:00 (off-hours)...

Top Anomalies Detected

Event ID	Anomaly Score	Timestamp
46d199fe-9a97-4d6b-9	1.000	2026-02-20T00:56:46
73e2a6b4-51d7-4a9b-b	1.000	2026-02-20T00:56:46
50e0c05f-17c4-450a-9	1.000	2026-02-20T00:56:46
46815b0f-ef89-470e-8	1.000	2026-02-20T00:56:46
940a5f63-f2d5-4799-b	1.000	2026-02-20T00:56:46
ef1d3430-ed3f-4603-b	1.000	2026-02-20T00:56:46
ced5a6e3-ad5d-455f-9	1.000	2026-02-20T00:56:46
c5f90721-3dd6-4070-8	1.000	2026-02-20T00:56:46
6126f4ee-19bc-426b-a	1.000	2026-02-20T00:56:46
7d61d218-0165-41f2-a	1.000	2026-02-20T00:56:46