Investigation Report

Generated: 2026-02-20 04:39:59

Case Information

Case Name:	case_1
Description:	sample_1
Created:	2026-02-20T03:31:13.216664
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	0.0

Detailed Analysis

Risk Level: MEDIUM (Score: 51.2/100)
Key Findings:
- 124 rule violations detected
- 1374 anomalous events identified
- Rule contribution: 100.0
- Anomaly contribution: 28.0
- Network correlation: 0.0

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
f9ea5d6f-924f-48df-9	1.000	2026-02-20T03:32:01
908a740b-3cd4-4f14-b	1.000	2026-02-20T03:32:01
ebd385b7-1497-4f26-8	1.000	2026-02-20T03:32:01
5cdbe44e-53cf-47c6-b	1.000	2026-02-20T03:32:01
a78d712a-0d38-45b4-9	1.000	2026-02-20T03:32:01
c0d9e30e-a636-45c9-a	1.000	2026-02-20T03:32:01
7be465c8-235d-4049-a	1.000	2026-02-20T03:32:01
f298e7a2-8381-4ad1-a	1.000	2026-02-20T03:32:01
7d06c431-e119-4345-8	1.000	2026-02-20T03:32:01
7cc58e95-45ad-4bf8-8	1.000	2026-02-20T03:32:01