BLACKWALL
SECURITY

BLACKWALL SOC
Incident Report

Prepared for:	Sample Client (Demo Data)
Prepared by:	Christian Chavez — BlackWall Security
Generated:	2026-06-12 01:02:40 UTC
Classification:	CONFIDENTIAL — Internal Use Only

Executive Summary

Metric	Value
Total Events Detected	1
Critical Alerts	1
High Alerts	0
Users Monitored	1
Unique Finding Groups (deduplicated)	1
Automated Responses	1
Connected Agents	1
Geo Locations Tracked	0
Report Generated	2026-06-12 01:02:40

Critical & High Alerts

Origin / Host	Reasons	Count	Max Risk	Severity	Users
WIN-FS01	brute force: 41 failed logons	1	220	CRITICAL	jdoe

Top Risk Users

Username	Max Risk Score	Event Count	Risk Level
jdoe	220	1	CRITICAL

Connected Agents

Agent Host	OS	Last Seen	Events Processed
WIN-FS01	Windows	2026-06-11T10:00:00	1204

Automated Responses Taken

Action	Target	Status	Detail

isolate_host	WIN-FS01	OK	host isolated

Recommendations

1. Immediately investigate and isolate affected hosts from critical alert events.
2. Brute force activity detected — enforce account lockout policies and enable MFA on all accounts.
3. Review all automated response actions taken and verify their effectiveness.
4. Update threat intelligence feeds and review detection rules based on findings in this report.