Sentinel Incident Response Report

Executive Summary

Incident ID: 456
Date: 2025-12-20 13:03:01.185955
Severity: Critical
Type: Data Exfiltration
Status: Active

Incident Details

Target System: user_5
Source IP: 192.168.1.77
Rule Triggered: Rule_754

Technical Context

No detailed system context available.

Mitigation & Response

Automated Actions:
- Incident logged to database.
- Administrators notified (Desktop Alert/Log).
- Containment measures (IP Block/Process Kill) initiated.