

Sentinel Incident Response Report

Executive Summary

Incident ID: 552
Date: 2025-12-20 17:12:04.352982
Severity: Critical
Type: Phishing
Status: Active

Incident Details

Target System: user_3
Source IP: 192.168.1.165
Rule Triggered: Rule_875

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.