Incident Ticket – SOC Case

Title:
[Critical] Ransomware Detected on Server-X

Incident ID:
INC-2025-001

Severity:
Critical

Status:
Open

Reported By:
Wazuh SIEM

Assigned To:
SOC Analyst

Incident Description

Ransomware activity was detected on production system Server-X.
Multiple files were encrypted, and a suspicious executable named `crypto_locker.exe` was identified.
Outbound network communication was observed from the affected host prior to encryption.

Indicators of Compromise (IOCs)

- Malicious File: `crypto_locker.exe`
- Source IP Address: `192.168.1.50`
- Affected Host: Server-X

Impact Assessment

- Production server affected
- Potential data loss and service disruption
- High business impact

Immediate Actions Taken

- Server isolated from the network
- Alert escalated to Tier 2 SOC
- Investigation initiated

Current Status

Incident is under investigation.
Awaiting deeper forensic analysis and recovery actions.