Executive Summary

A ransomware alert was detected on Server-X indicating the presence of a malicious executable. Immediate containment actions were taken to isolate the system and prevent lateral movement.

Timeline

Time	Action
11:00	Alert triggered
11:05	Endpoint isolated
11:20	IOCs identified
11:30	Incident escalated

Impact Analysis

Potential risk of data encryption and service disruption. No evidence of lateral spread observed.

Remediation Steps

- Removed malicious file
- Blocked malicious IP
- Reset affected credentials

Lessons Learned

Early alerting and quick isolation reduced potential impact. Improved phishing awareness is recommended.