



Security Breach Incident Response

Form

Company: [Name of Organization Affected]

Primary Responder: [Name of Primary Responder]

Secondary Responder(s): [Name of Secondary Responder(s)]

Date and Time of Incident:

# Incident

Description of Incident: [What occurred on the device, IOC’s]

Affected Systems/Resources: [Hostnames]

Response Actions: [What actions should client conduct, immediately]

Immediate Response Actions Taken: [What actions had to be taken by ThreatLocker]

Further Investigation Steps: [Steps needed to be taken later by ThreatLocker]

# Post- Incident

Post-Incident Actions:

[Actions the client must take to ensure this doesn't happen again]

Remediation

Remediation Steps:

[List steps taken to address vulnerabilities and prevent similar incidents in the future]

Lessons Learned:

[Document lessons learned from the incident and areas for improvement]