PLAYBOOK / IRONCLAD RESOURCE CENTER

Incident Response & Case Management Playbook

A reusable operating model that helps teams validate, contain, recover from, and learn from security incidents.

Validate and scope

Playbook guidance for building a stronger, more repeatable security operation.

- Confirm the alert and assess severity
- Assign an incident owner and record evidence
- Map affected assets, identities, services, and indicators

Contain and recover

Playbook guidance for building a stronger, more repeatable security operation.

- Preserve evidence while limiting further impact
- Isolate endpoints, reset credentials, and block indicators
- Validate recovery and monitor for recurrence

Improve

Playbook guidance for building a stronger, more repeatable security operation.

- Hold a concise post-incident review
- Tune detections and response procedures
- Assign follow-up actions with clear owners

DECIAN / IRONCLAD SIEM

WORKING PAGE

Action worksheet

Use this page to adapt the resource to your environment and keep the next decision visible.

Topic	Notes
Objective	
Owner	
Key evidence	
Decision / next action	
Review date	