SOLUTION BRIEF / IRONCLAD RESOURCE CENTER

Alert-to-Case Workflow

A clear operating flow for connecting Ironclad SIEM detection with documented DFIR case management.

Detect and validate

Solution Brief guidance for building a stronger, more repeatable security operation.

- Review alert context, severity, and affected assets
- Assign an owner and a communication channel
- Capture the first evidence and working hypothesis

Investigate and contain

Solution Brief guidance for building a stronger, more repeatable security operation.

- Search related endpoints, identities, and indicators
- Track decisions, evidence, and containment actions
- Escalate as scope or business impact changes

Recover and improve

Solution Brief guidance for building a stronger, more repeatable security operation.

- Verify recovery and monitor for recurrence
- Document lessons and follow-up work
- Tune detections and response procedures

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	