WHITEPAPER / IRONCLAD RESOURCE CENTER

AI-Assisted Threat Hunting with Ironclad

A practical approach to using AI-integrated searches to accelerate discovery while retaining analyst validation and control.

Start with a hypothesis

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

- Frame the behavior, asset group, or indicator you need to examine
- Use natural-language prompts to explore related signals
- Keep search scope tied to a meaningful question

Validate the evidence

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

- Correlate AI-assisted findings with raw telemetry
- Check timelines, affected identities, processes, and connections
- Escalate only when context supports a material risk

Turn findings into improvement

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

- Document hunting outcomes and gaps
- Tune detections based on validated behavior
- Share recurring insights with response and engineering teams

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	