CHECKLIST / IRONCLAD RESOURCE CENTER

Ironclad SIEM Evaluation Checklist

A focused framework for evaluating visibility, detection, reporting, retention, and response before selecting or expanding a SIEM program.

Data coverage and compatibility

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

- Windows, macOS, and Linux endpoint telemetry
- Firewall, cloud, email security, and identity integrations
- Retention aligned to operations and compliance

Detection and investigation

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

- Cross-source correlation for suspicious patterns
- AI-assisted search and guided investigation workflows
- Threat-hunting views that connect alerts to context

Response and operational fit

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

- Meaningful alerts with clear triage context
- Evidence, containment, and remediation tracking
- Reporting for operations, leadership, and compliance

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	