

GUIDE / IRONCLAD RESOURCE CENTER

# Security Logging & Retention Planning Guide

A practical planning guide for choosing source coverage, retention periods, owners, and review habits.

## Plan source coverage

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

- Identify systems that hold critical business or security context
- Map endpoint, identity, cloud, firewall, and email telemetry
- Document source owners and expected event quality

## Set retention intentionally

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

- Align log retention with investigations and compliance needs
- Protect evidence integrity and accessibility
- Review storage and retention decisions on a schedule

## Operate and improve

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

- Monitor source health and ingestion gaps
- Review alert quality and investigation value
- Update ownership as the environment changes

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            |       |