ARCUSDATA | IT / OT SECURITY
SPLUNK & CRIBL PARTNER

Data Onboarding Checklist

NERC CIP-Regulated Environments

Configuration practices aligned to Splunk Lantern

USE THIS WHEN	GOAL	OWNER SIGN-OFF
Adding any new data source to a Splunk / Cribl pipeline that touches BES Cyber Systems.	Clean parsing and right-sized volume, with logging and audit evidence that satisfy CIP.	Requester, Splunk admin, CIP compliance. Sign off before promotion to production.

1 Intake & Scoping

SPLUNK LANTERN · REQUEST + DEFINE USE CASE

- [ ] Capture concrete source facts: hostnames / IPs, path or location, access method, and a plain description of what the data represents.
- [ ] Record the retention requirement and estimated daily volume. Verify volume by inspecting the source yourself, not just the requester's estimate.
- [ ] Define the use case before ingest: name the security or observability question this data will answer.
- [ ] **CIP-002** Assign BES impact rating (High / Medium / Low) and asset type (BCA, PCA, EACMS, PACS, EAP); flag if the source is or contains BCSI.

2 Authorization & Change Control

CIP GOVERNANCE LAYER

- [ ] **CIP-004** Confirm need-to-know access to both the data and the onboarding tooling; apply least privilege on the target index.
- [ ] **CIP-010** Open a documented change and capture the current baseline configuration before modifying anything.
- [ ] **CIP-010** Build and test the source type in a dev / non-production index before promoting to production.
- [ ] **CIP-005/011** Keep the data path inside the authorized ESP. Confirm forwarder / Cribl routing does not egress BCSI to an unapproved destination.

3 Source Type Config: the "Great Eight"

ARCUS BLOG: THE GREAT EIGHT · SET IN PROPS.CONF

- [ ] `LINE_BREAKER` anchored to the event-start pattern, not the default newline.
- [ ] `SHOULD_LINEMERGE = false`
- [ ] `TRUNCATE` tuned to max event length +10%. Never 0.
- [ ] `EVENT_BREAKER_ENABLE = true` and `EVENT_BREAKER` matches `LINE_BREAKER` (UF 6.5+).
- [ ] `TIME_PREFIX` anchored to the timestamp.
- [ ] `MAX_TIMESTAMP_LOOKAHEAD` = exact timestamp length.
- [ ] `TIME_FORMAT` set with strptime syntax.
- [ ] Optional: `CHARSET`, `ANNOTATE_PUNCT = false`.
- [ ] Name it `vendor:product:technology:format`; prefer a Splunk-certified / CIM add-on; deploy via a custom app, not system/local.

4 Validation

SPLUNK LANTERN · DATA QUALITY GATE

- [ ] Format correctness: timestamps, numeric and string fields parse exactly as expected.
- [ ] Completeness: required fields present and populated; no truncation or gaps.
- [ ] Standards: naming conventions and CIM field mapping conform.
- [ ] Enrichment / transformation output validated against the source.
- [ ] **CIP-007 R4.1** Confirm required security events are captured: successful and failed authentication, account management, object access, detected malicious code, and access attempts at Electronic Access Points.

5 Retention, Alerting & Audit

ARCUS BLOG + CIP-007 R4

- [ ] **CIP-007 R4.3** Index retention (`frozenTimePeriodInSecs`) holds event logs for at least 90 consecutive calendar days.
- [ ] **CIP-007 R4.2** Real-time alerts fire on detected security events; monitor for logging / ingest failures and data gaps.
- [ ] **CIP-007 R4.4** Schedule review of a summarization or sample of logged events at intervals no greater than 15 days.
- [ ] **CIP-010** Keep `props.conf`, `inputs.conf` and onboarding scripts under Git version control: who changed what, and when.
- [ ] Retain audit evidence that 90 days were held historically, separate from the live logs.
- [ ] Baseline ingest volume and set data-quality / latency monitoring to catch drift.

6 Communicate & Hand Off

SPLUNK LANTERN · CLOSE THE LOOP

- [ ] Notify stakeholders the data is available; publish index, sourcetype, retention, and data owner.
- [ ] Update the data catalog / onboarding register and close the change record.

SOURCES & FURTHER READING

Splunk Lantern: Data onboarding workflow | Configuring new source types | Data onboarding best practices | Onboarding data to Splunk ES

Arcus Data blog: The Great Eight (props.conf) | Onboarding without the rework | Onboarding under NERC CIP | OT Security & NERC CIP

CIP QUICK REFERENCE

CIP-002 asset classification · **CIP-004** access & need-to-know · **CIP-005** electronic security perimeter · **CIP-007 R4** security event monitoring, alerting & log retention · **CIP-010** baseline & change management · **CIP-011** BES Cyber System Information protection.

Arcus Data, LLC | 11335 NE 122nd Way Suite 105 Kirkland, WA 98034 | www.arcusdata.io | Automation | Cloud | Analytics