MACHINE DATA INSIGHTS

CIM Normalization Pipeline

Turn raw machine data into validated, deploy-ready content for Splunk® ES & ITSI - faster, with AI-accelerated tooling and repeatable methods.

There's Gold In That Data!®

THE FOUNDATION

What is CIM Normalization?

CIM normalization aligns security and operational data from every vendor to Splunk's standard schemas - so **one detection, dashboard, or KPI works across all of them**, instead of a custom search per technology.

- **Map** vendor-specific fields to common CIM fields.
- Create **tags** that link those events to the accelerated data models Splunk ES & ITSI run on.
- Create **eventtypes** that identify significant security and operational events.
- Make every source **analyzable consistently** - firewall, endpoint, identity, cloud, email, PLC, SCADA, IoT.

WHY IT MATTERS

What CIM Normalization Unlocks in Splunk ES & ITSI

Normalized data is what lets a **single detection, KPI, or dashboard span every vendor**, run at data-model speed, and use the content Splunk ships. ITSI KPIs and entity rules want the same thing: **consistent fields and identifiers**. Miss it and nothing errors - you just pay for coverage one search at a time.

FOR SPLUNK ES

- One correlation search covers **every vendor** in a data model - not one per technology.
- Out-of-the-box **Security Content** works as shipped.
- Better detection accuracy, **fewer false positives**, faster investigations.
- Asset & identity enrichment keys on **CIM fields**.

FOR SPLUNK ITSI

- One **KPI** definition measures every vendor's tier the same way.
- Consistent identifiers mean **entity rules match** - hosts don't drop out of services.
- **Content packs** depend on well-built add-ons; the pipeline produces them.
- Service health scores you can **actually trust**.

The MDI CIM Normalization Pipeline

You run the client-side tools; the encrypted exchange hands data to MDI; MDI runs the engine.

01 · ASSESS

CAT

CIM Assessment Toolkit

Free, open-source Splunkbase app that scores CIM compliance by dataset and sourcetype - exposing the gaps that break Splunk ES correlation searches.

Free & Open Source | Dataset-Level | Acceleration Health

02 · SANITIZE

Paydirt

Log Scrubber

Free, open-source scrubber for CUI, PII, PHI & credentials. Runs fully on your machine - no install, no network calls. CMMC, HIPAA & GDPR aware.

Free & Open Source | Runs Offline | No Install

03 · SECURE HANDOFF

Secure Exchange

Encrypted Data Transfer

A private, encrypted cloud channel per engagement - clients upload source data, collect signed deliverables. Isolated, encrypted, fully logged.

Encrypted | Per-Client Isolation | Audit Trail

04 · BUILD

Data Refinery

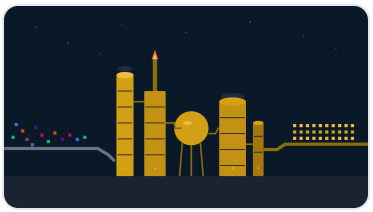
Normalization Engine

The MDI engine that builds the fix an assessment finds: validated, CIM-compliant Splunk TAs and Cribl packs - AppInspect-checked and deploy-ready.

CIM-Validated | AppInspect-Checked | TAs + Cribl Packs

One Validated Output, Two Deployment Paths

Data Refinery
CIM-validated output



→

Splunk CIM TAs

props, transforms, eventtypes & tags - normalize vendor fields to CIM at search / index time. Drop-in for Splunk ES.

Cribl Packs

normalize *and* reduce in-stream - cut ingest and license cost before data ever lands.

Let's turn your data into detection.

MDI delivers CIM normalization, data-volume reduction, and CIM macro & correlation-search optimization - with AI-accelerated tooling that cuts time-to-value and consulting cost.

CIM Normalization | Data-Volume Reduction | Correlation-Search Optimization | CIM Macro Optimization | AI-Accelerated

SCAN TO EXPLORE

hello@machinedatainsights.com machinedatainsights.com