DATA SHEET

Cribl Detect™

Turn telemetry into defense.

Cribl

The **AI Platform** for Telemetry

Cribl Detect is a complete detection, investigation, and response solution with an open architecture that accelerates AI-driven security operations. Security teams can continuously monitor their posture, expand data and detection coverage, detect in the pipeline, and drive investigations and threat hunts across any data, wherever it lives.

Eliminate the tradeoff between visibility and cost with a SIEM built for the AI era. Cribl brings security closer to the data and gives you control over the telemetry driving security outcomes.

Cribl Detect is powered by:

Tiered routing and storage with the Cribl platform

- Context-driven pipelines: with Stream and Lake, route high-value data to high-performance storage, send the rest to low-cost object storage.
- Long-term retention: keep years of full-fidelity logs in open, cost-effective storage, without paying premiums to index data that doesn't need it.
- Open architecture: store data where it makes sense: Cribl Lake, S3, or other storage. No proprietary formats or lock-in.

Posture management and high-fidelity detections

- MITRE mapping: map your coverage to ATT&CK to identify where you're lacking detections, or the telemetry to power them.
- In-stream detection: Apply detection logic as logs move through the pipeline for immediate response signals.
- Correlation searches: chain single event detections together to uncover slow-burn attacks that simple detections miss.
- Continuously optimized rules: pull from a catalog of 8,000+ production-ready detections, tailor them to your environment and tune them for noise. Find and fix broken rules before threats go unnoticed.

AI-Powered investigation across the full IT and security estate

- Federated search: use KQL to query telemetry wherever it lives–in Cribl, other data lakes and object storage, or even other SIEMs–without duplicating and centralizing it first.
- Natural language investigations: ask questions of data directly, without query language expertise. AI reasons across telemetry and environmental context to move from alert to containment.

Signals before storage

Apply detection logic in the pipeline, before data is ingested, indexed and stored.

Cut wasteful SIEM costs

Stop paying premiums for every log. Route high-value data to high-performance storage, retain full-fidelity telemetry in open, low-cost storage.

Close coverage gaps

Detection posture management shows where you lack detections for key threats, and what telemetry is missing.

Accelerate investigations

Get context and answers for fast response. AI-powered federated search reasons across your full estate.

Modernize at your pace

Run Cribl Detect alongside your existing stack. Onboard what you need, when you need it.

Product Features

OPEN ARCHITECTURE

- **Composability.** Each layer–pipeline, detection, correlation, search, and storage–is Cribl-native and AI-ready, but none of it is mandatory. Adopt what you need, expand as you grow.
- **OCSF & KQL.** Telemetry is normalized on write to OCSF, an open, consistent schema. Queries are in KQL, a powerful, widely used query language, powering detection, correlation, and security analytics across sources while keeping your data flexible and open.
- **Multi-store support.** Flexible architecture supports storage in Cribl Lake, other data lakes, object stores, and even other SIEMs.

HIGH-FIDELITY DETECTIONS

- **In-stream detection:** security analytics are embedded in the pipeline, generating real-time signals.
- **Correlation.** Connect individual signals and behaviors into chains of related findings, piecing together the full context of slow-burn attacks to give analysts everything they need to quickly contain threats.
- **Rule templates:** Start from a library of 8,000+ rules that cover a wide range of key threat detection use cases, and quickly tailor them to your environment.
- **AI-assisted rule development.** Build, validate, and tune detections with the Detection Lab: a familiar AI chat interface built around in-depth detection engineering knowledge foundations.

COVERAGE & POSTURE MANAGEMENT

- **MITRE mapping:** View current detection coverage against the ATT&CK framework to see where key TTPs lack corresponding detections.
- **Drift detection.** Pinpoint configuration and schema drift issues that cause rules to break and create false positives–or false negatives that let threats go unnoticed. Get recommendations on how to fix issues with detection logic and upstream telemetry.
- **Prioritized recommendations:** Get targeted insights on where to fill gaps with new detections, based on your threat model and priority APTs.

INVESTIGATION

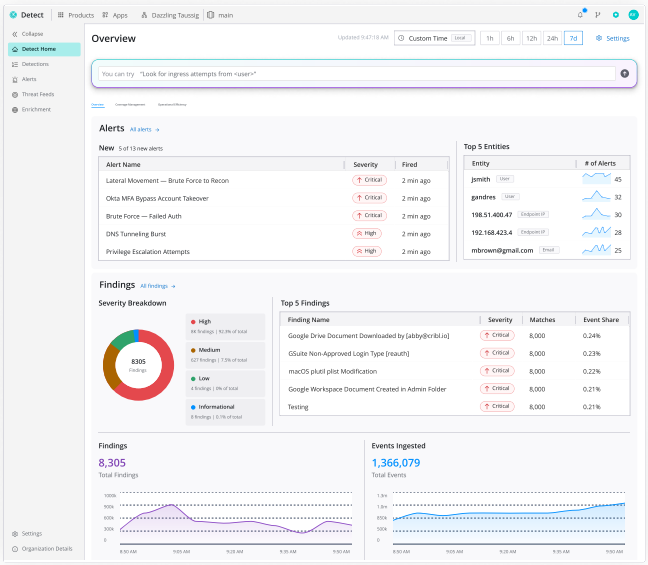
- **Federated search.** Run queries across Cribl infrastructure, other data lakes and object storage, and other SIEMs. No re-indexing or data migration required.
- **Guided AI exploration.** An intuitive AI copilot surfaces related evidence and suggests next steps, without requiring deep query language expertise.
- **Collaborative notebooks.** Combine searches, findings, and notes into shareable investigation workflows.

RESPONSE

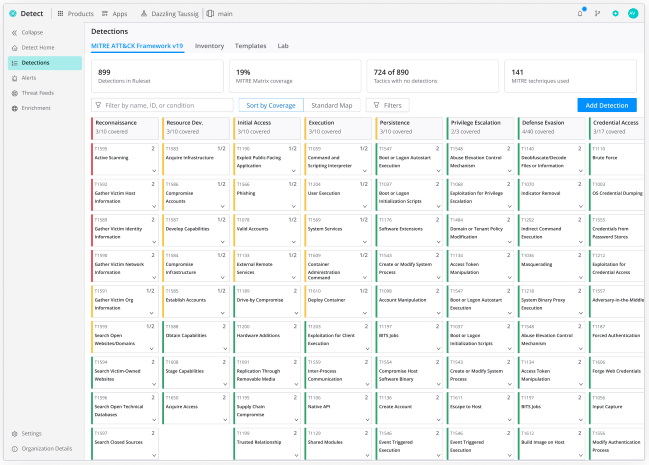
- **Automated triage.** AI-driven alert analysis separates genuine threats from noise, escalating only what matters.
- **Alert aggregation.** Related signals are grouped into streamlined, detailed alert views instead of scattered raw events.
- **SOAR integration.** Enable automated response actions and runbooks to align with existing SOAR workflows.
- **Flexible notifications.** Send alert notifications to Slack, PagerDuty, or any other downstream channel.

THREAT INTELLIGENCE & ENRICHMENT

- **External threat intel.** Enrich alerts with current context on emerging APT activity, new CVEs, and evolving adversary tactics.
- **Internal enrichment.** Add critical contextual information on specific user identities, endpoints, assets and systems in your environment.
- **Embedded context.** Accelerate response with threat intel and enrichment built into response and investigation workflows—no manual pivoting across tools required.



Overview Dashboard offers a quick snapshot of key alerts, findings, and coverage.



MITRE map shows your current coverage and highlights gaps.

Cribl

The AI Platform for Telemetry

Learn more at cribl.io | Join our Slack community
Try Cribl Sandboxes | Follow us on LinkedIn and X

DS-0010-EN-1-0926