Proof of Concept: Comparison Between Trivy CLI and Clair Scanner

Criteria	Trivy CLI	Clair Scanner
Installation & Setup	Trivy requires minimal setup; a single binary that works across multiple platforms and can be run immediately after installation.	Clair requires more configuration, including setting up a PostgreSQL database for storing vulnerability data.
Ease of Use	Simple command-line interface (`trivy image <image-name>`). Easy to run and does not require additional components to start scanning.	Requires running a service that listens for API requests, making it more complex to get started.
Performance	Faster scanning with a smaller database footprint. Trivy's local vulnerability database updates quickly, and scanning times are optimized.	Scanning times can be slower due to Clair's reliance on a larger backend infrastructure (PostgreSQL database).
Supported Platforms	Supports scanning for a wide variety of platforms (Docker, Kubernetes, AWS Lambda, GitHub Actions, etc.).	Mostly used for scanning container images. Support for other platforms is limited.
Reporting	Trivy offers human-readable output, JSON, and various formats, including HTML and JUnit XML for integration with CI/CD pipelines.	Clair requires manual effort to convert API responses into readable formats.

		The reporting is less flexible and requires custom development for certain formats.
Community Support	Large, active community with frequent updates and support from Aqua Security. Trivy is widely adopted across various industries.	Clair has good community support but is more focused on enterprise container registries, and the development is slower compared to Trivy.