



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Securing the AI/ML Lifecycle with MLSecOps: Open-Source Best Practices

Presenters: Andrey Shorov & Bahaulddin Shammary

Co-authored with: Elif U. Soykan & Sarah Evans

In collaboration with: OpenSSF



Agenda & Audience

Agenda:

- Visual lifecycle models: MLOps → MLSecOps
- Personas, threats, controls and tools by stage
- Open-source building blocks: Sigstore · Scorecard · SLSA
- End-to-end ML systems recommendations

Audience:

- Developers and cloud-native professionals incorporating AI/ML
- Open-source contributors in the AI/ML security space
- Security engineers and IT teams expanding governance to ML systems
- AI/ML engineers, data scientists, and MLOps teams

Why MLSecOps Exists



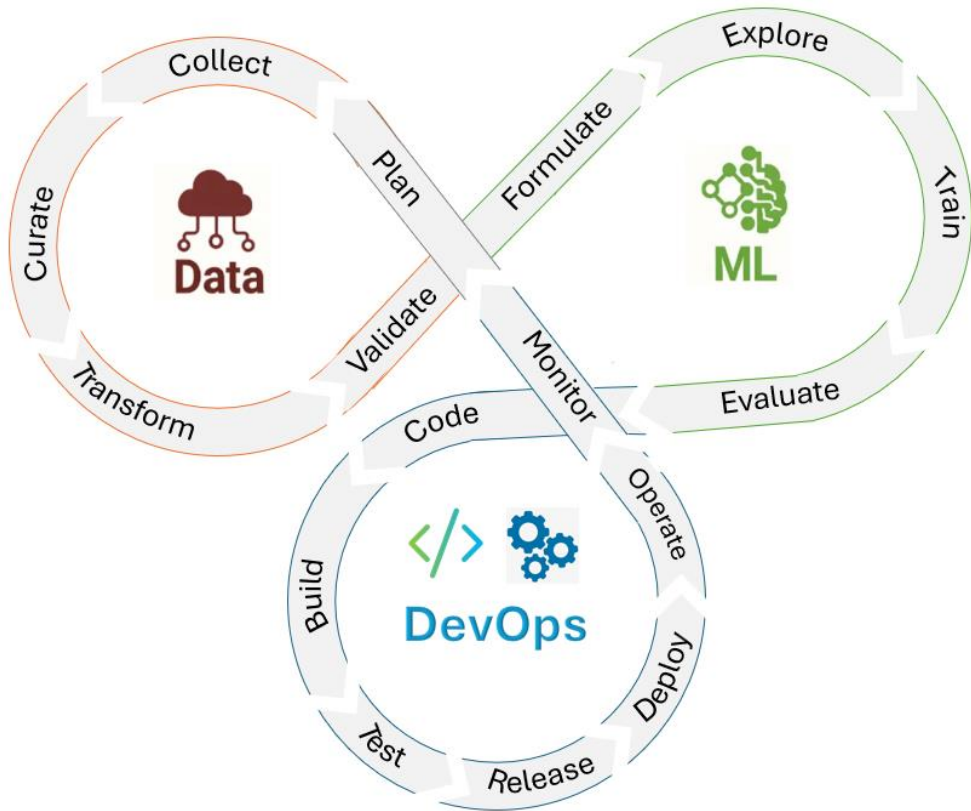
KubeCon



CloudNativeCon

Europe 2026

- **DevSecOps**: security woven into delivery pipelines
- **MLOps**: adds data dependency, drift, non-determinism
- **MLSecOps**: security across the full ML lifecycle (data + models + pipelines)



Mapping the stages to lifecycle



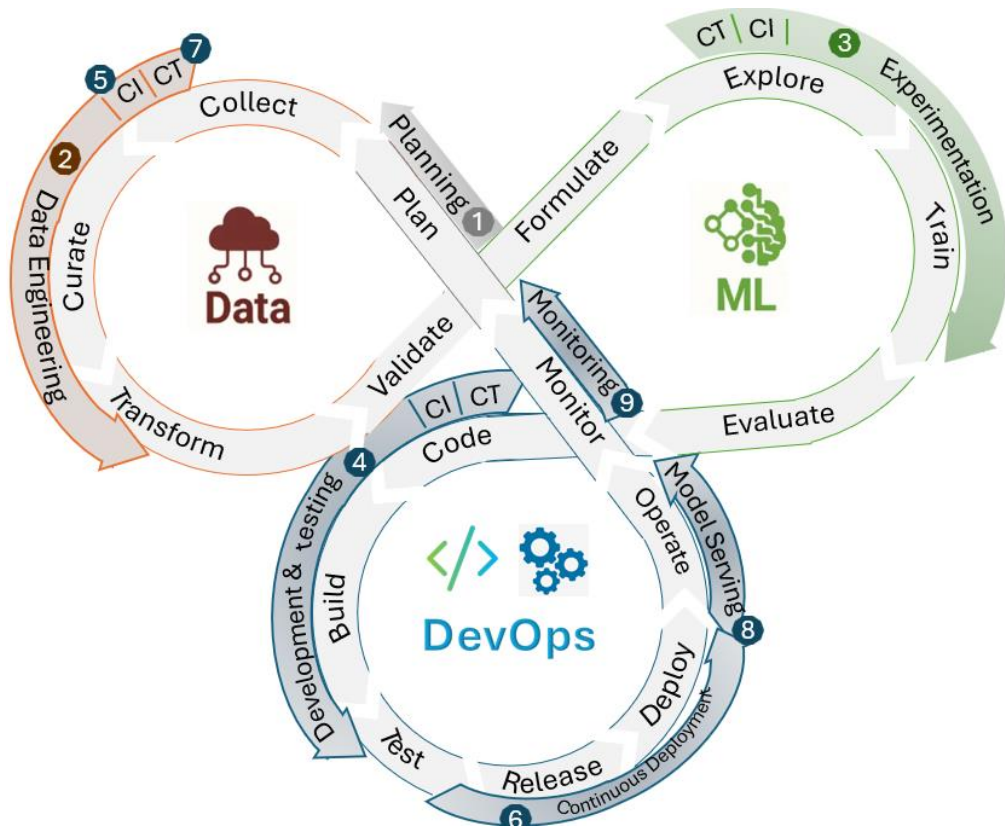
KubeCon



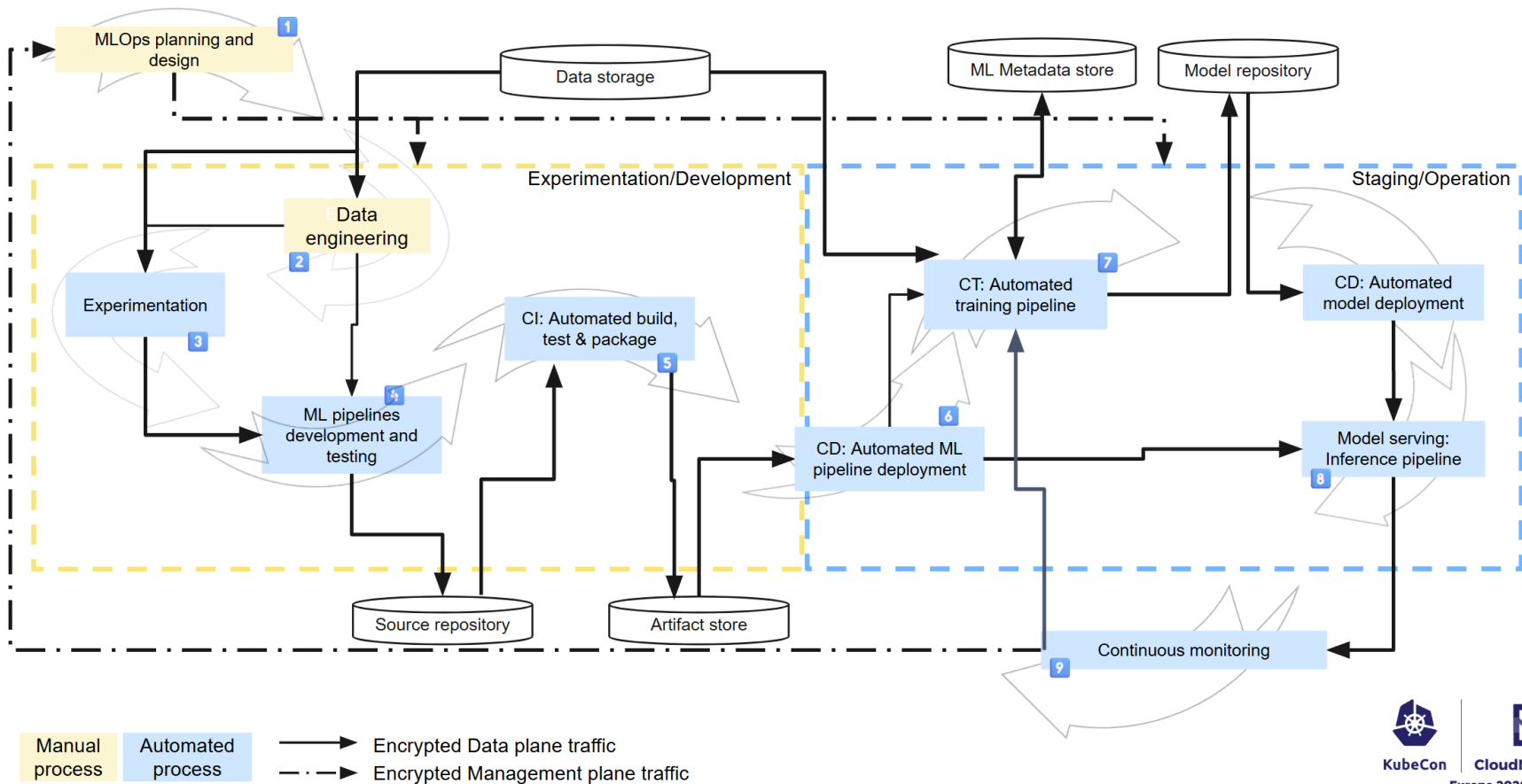
CloudNativeCon

Europe 2026

- Same loop, now with 9 stages
- Turns lifecycle into security control points
- Basis for connecting the Infinity loop to MLSecOps reference architecture



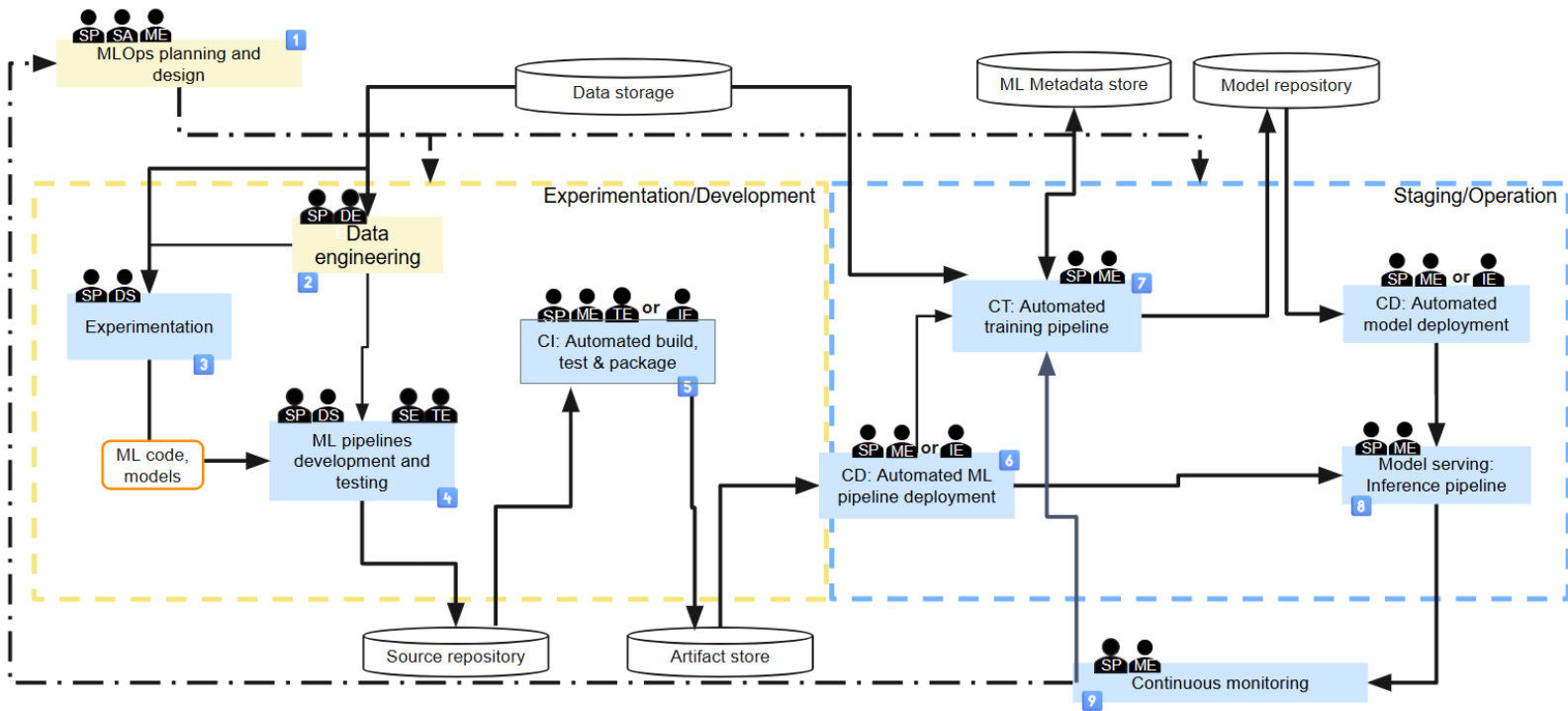
MLOps Reference Architecture



Personas in MLSecOps: Who Secures ML Lifecycle?

- MLSecOps is a team sport
 - Data, ML, software, security, and platform roles must collaborate
- Personas clarify who owns what across the ML lifecycle
 - data → models → deployment → monitoring
- Extends classic DevSecOps roles with AI/ML-specific responsibilities
- Examples of key personas:
 - MLOps Engineer: builds and operates training/serving pipelines
 - Data Scientist: designs and trains models, needs privacy/robustness-aware
 - Security Practitioner: embeds security controls into CI/CD and ML workflows

Personas within MLOps



Manual
process

Automated
process



Encrypted Data plane traffic



Encrypted Management plane
traffic

SP: Security practitioner

DE: Data engineer

DS: Data scientist

IE: Infrastructure Engineer

SA: Solution architect

SE: Software engineer

TE: Test engineer

ME: MLOps engineer



KubeCon



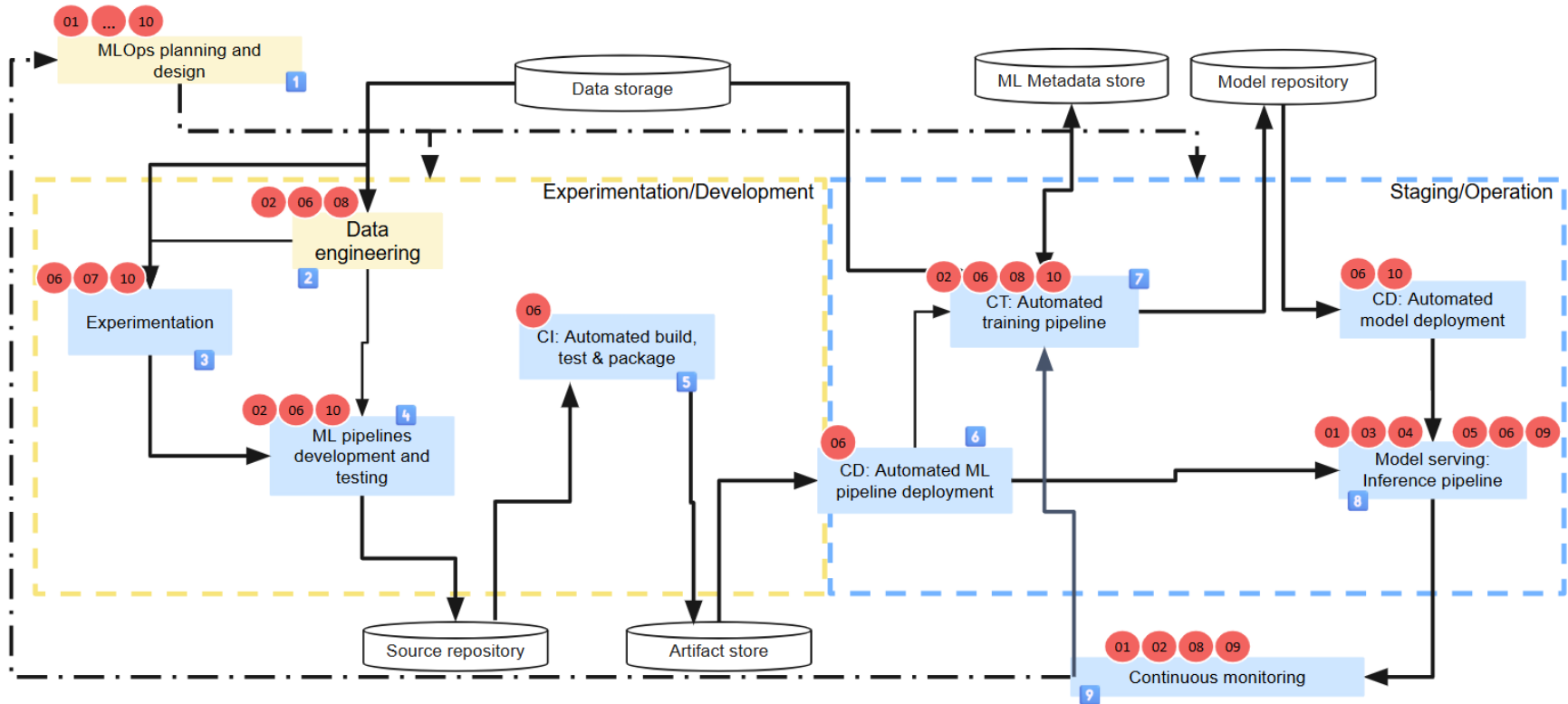
CloudNativeCon

Europe 2026

Risks to ML lifecycle

- ML introduces different risks than traditional software
 - data-driven behavior, non-determinism, continuous retraining
- Threats can emerge at every stage of the MLOps lifecycle
 - from data collection and experimentation to CI/CD, serving, and monitoring
- Security work often fragmented (only code scans, only infra hardening) and misses:
 - Attacks on training data, models, and feedback loops
 - Privacy leakage and model misuse through APIs
 - ML-specific supply chain compromises (datasets, pre-trained models, notebooks, libraries)
- OWASP ML Security Top 10 provides a shared baseline for these risks, teams can:
 - Threat-model ML systems systematically
 - Prioritize controls and monitoring where it matters most
 - Align MLSecOps practices across data, ML, security, and platform teams

Risks mapped to MLOps



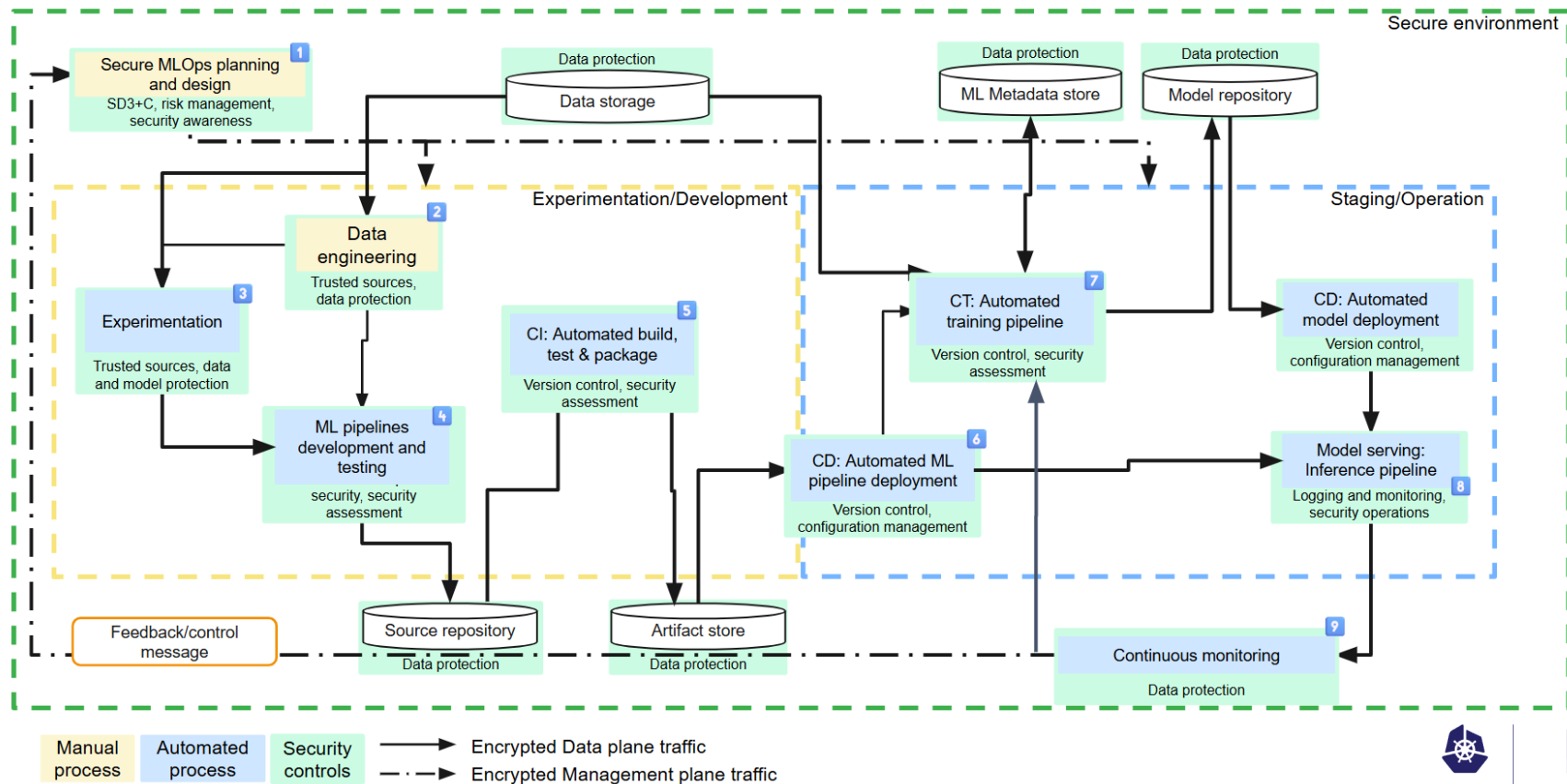
KubeCon



CloudNativeCon

Europe 2026

MLSecOps: Adding Security Layer to MLOps



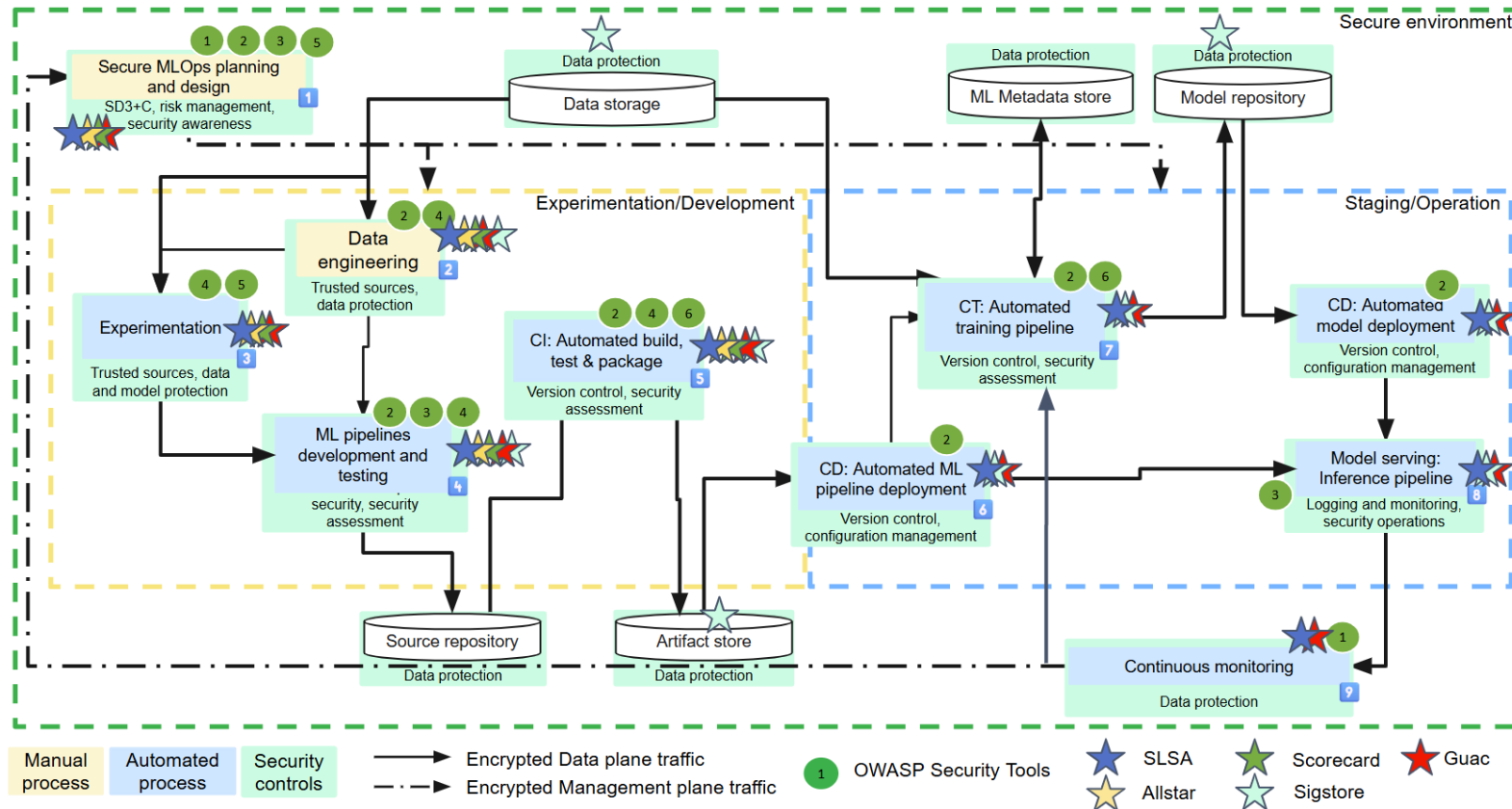
KubeCon



CloudNativeCon

Europe 2026

MLSecOps: OWASP/OPENSSEF Tools added



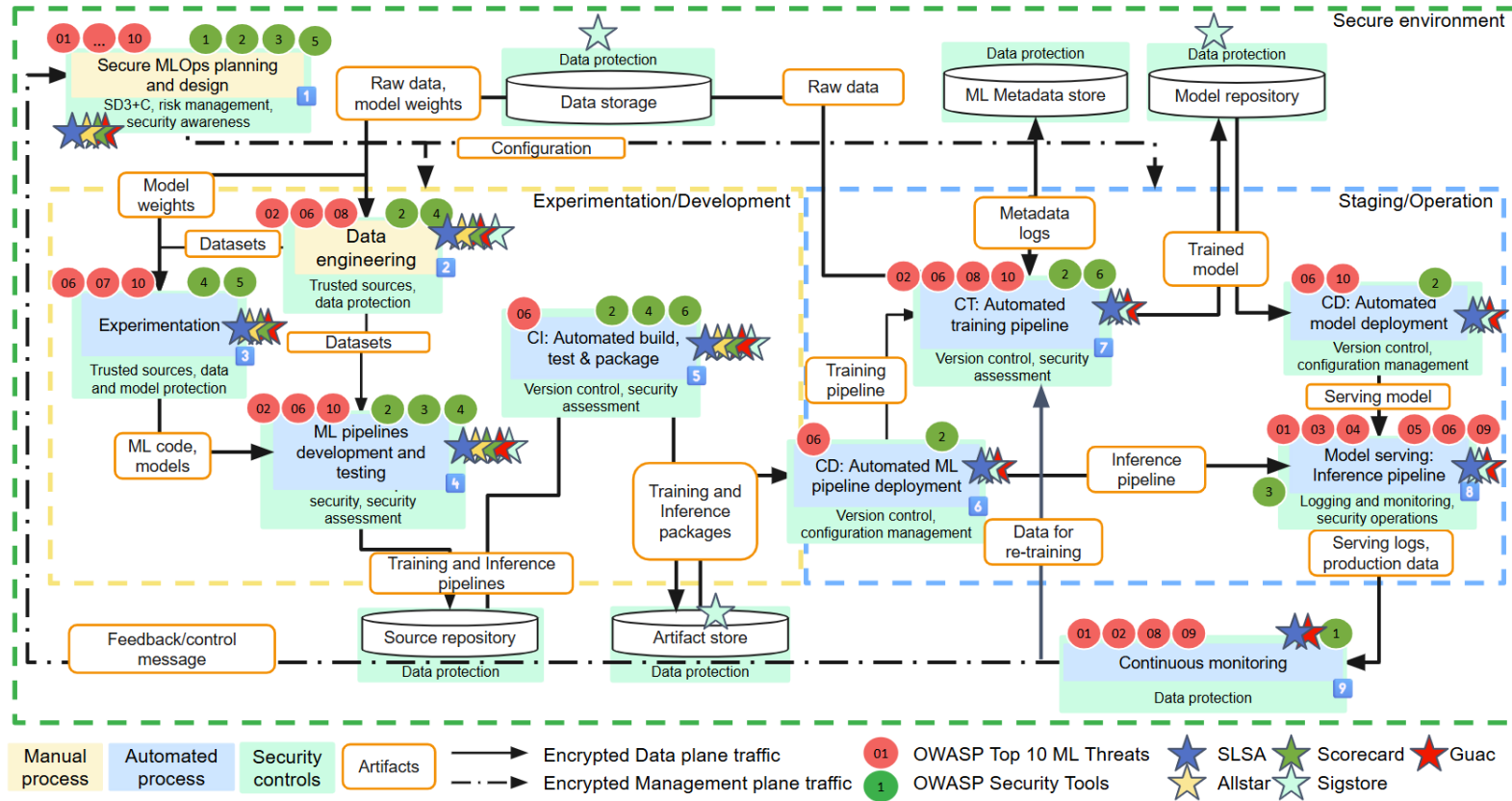
KubeCon



CloudNativeCon

Europe 2026

MLSecOps: OWASP/OPENSSF Tools added



Conclusion

Challenges

- ML-specific threats (poisoning, theft, adversarial)
- Retraining creates new risks
- Opaque models hinder audits
- Provenance + reproducibility gaps

Recommendations

- Automate security controls across CI/CD/CT
- Version datasets, models, and environments
- Embed security roles within MLOps teams

Lessons Learned

- MLSecOps complements existing security
- Security is shared across all teams
- Early integration reduces remediation cost
- Training investment closes the skills gap



KubeCon



CloudNativeCon

Europe 2026

<https://openssf.org/resources/visualizing-secure-mlops-mlsecops-a-practical-guide-for-building-robust-ai-ml-pipeline-security/>



Read Paper

Q&A



Sarah Evans

sarah.evans@dell.com



Bahaulddin Shammary

bshammary@opentext.com



Andrey Shorov

andrey.shorov@ericsson.com



Elif Ustundag Soykan

elif.ustundag.soykan@ericsson.com

