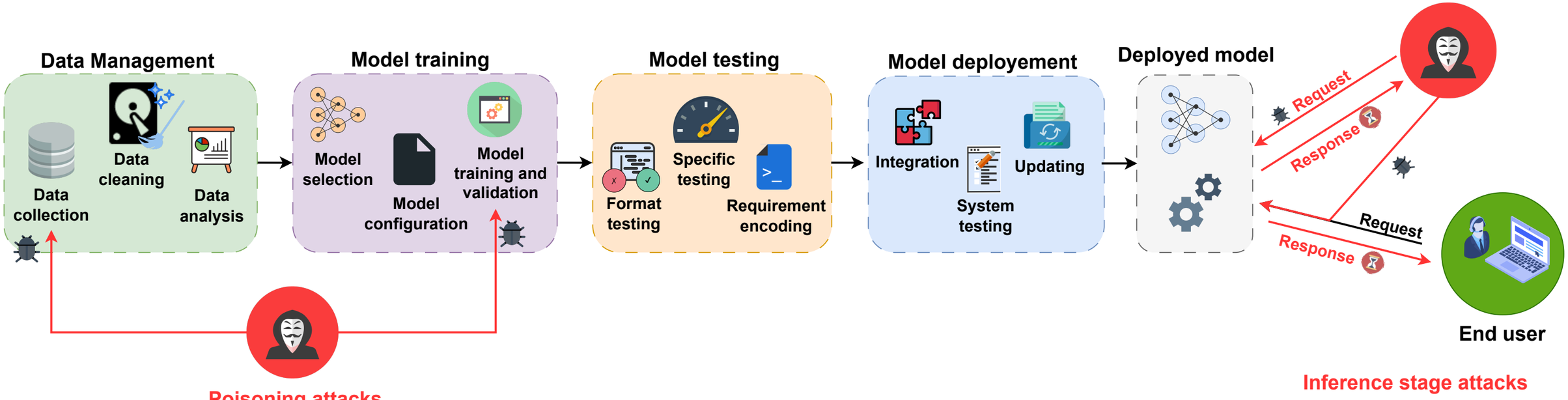
Data Management
Data collection
Data cleaning
Data analysis
Model training
Model selection
Model configuration
Model training and validation
Model testing
Format testing
Specific testing
Requirement encoding
Model deployement
Integration
System testing
Updating
Deployed model
Request
Response
Request
Response
End user
Poisoning attacks
(Training stage)
Inference stage attacks