Evaluate ElastAlert for IT-DB use cases

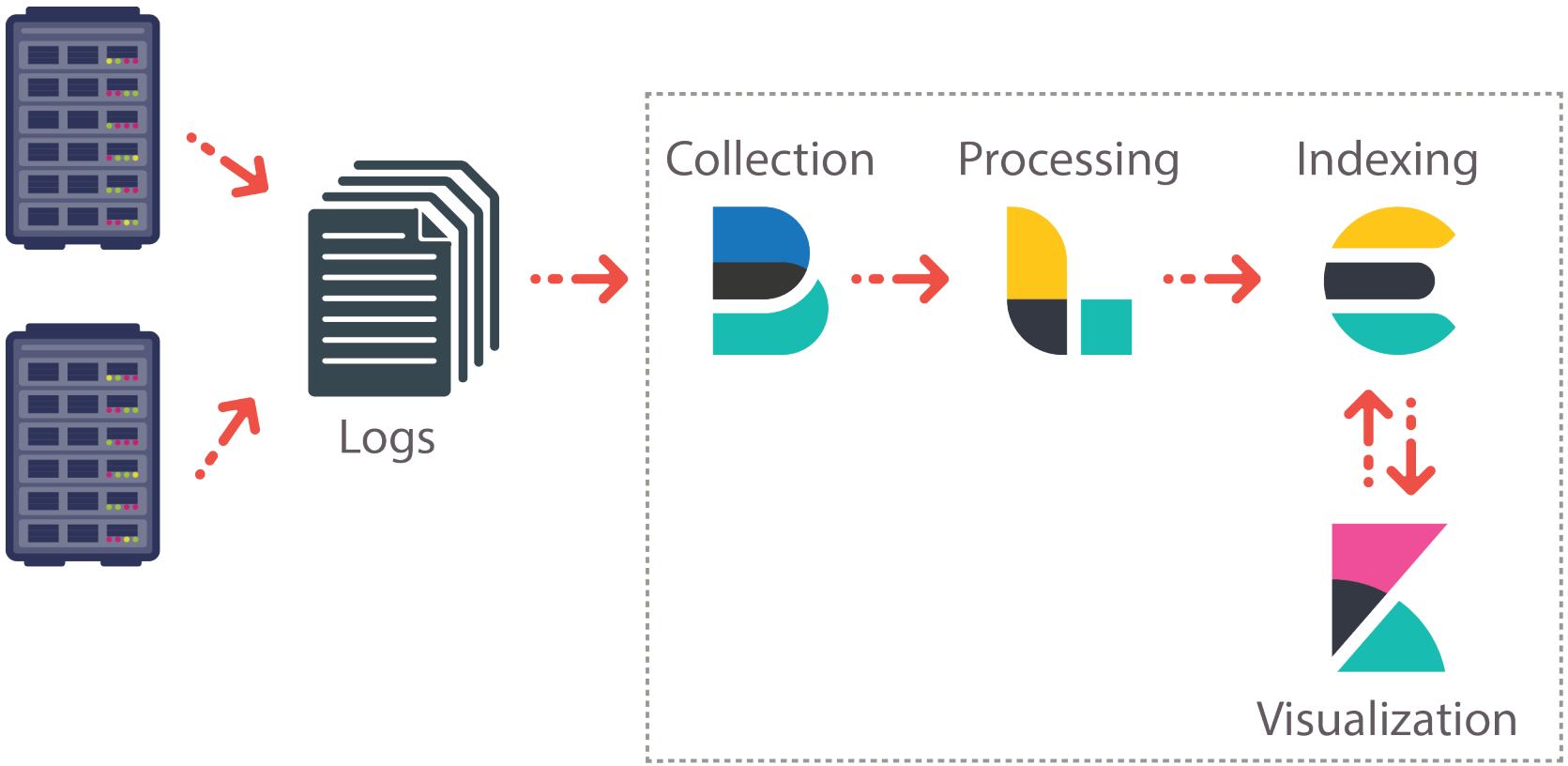
Dimitra Chatzichrysou

CERN IT Department – Database Group – Infrastructure & Automation

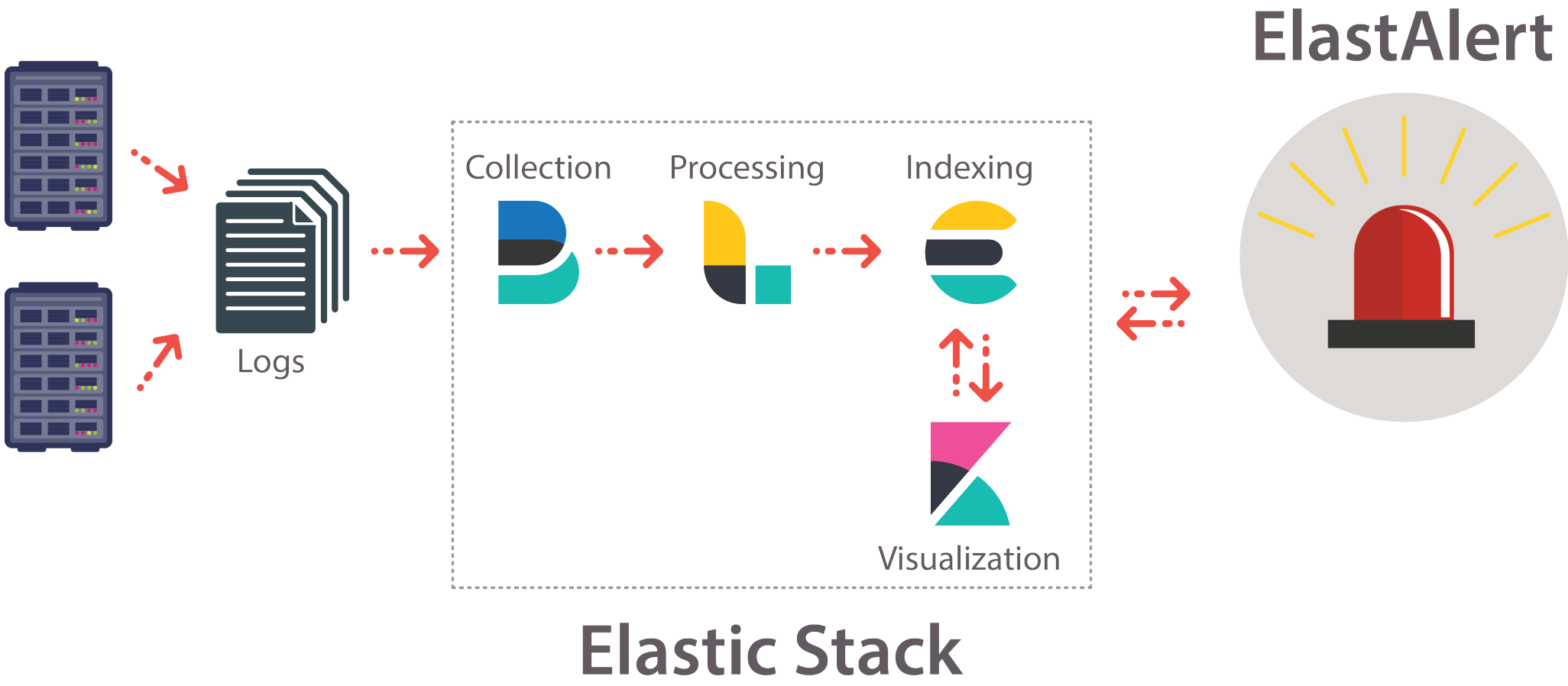
Supervisors: Aimilios Tsouvelekakis, Ignacio Coterillo Coz

15/08/2019

Log management currently in IT-DB



Monitoring with ElastAlert

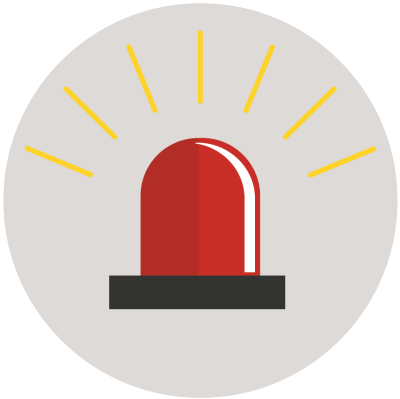


How ElastAlert works

Rules

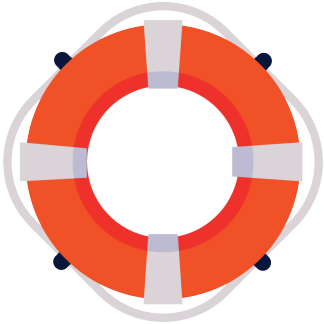
Config file

ElastAlert



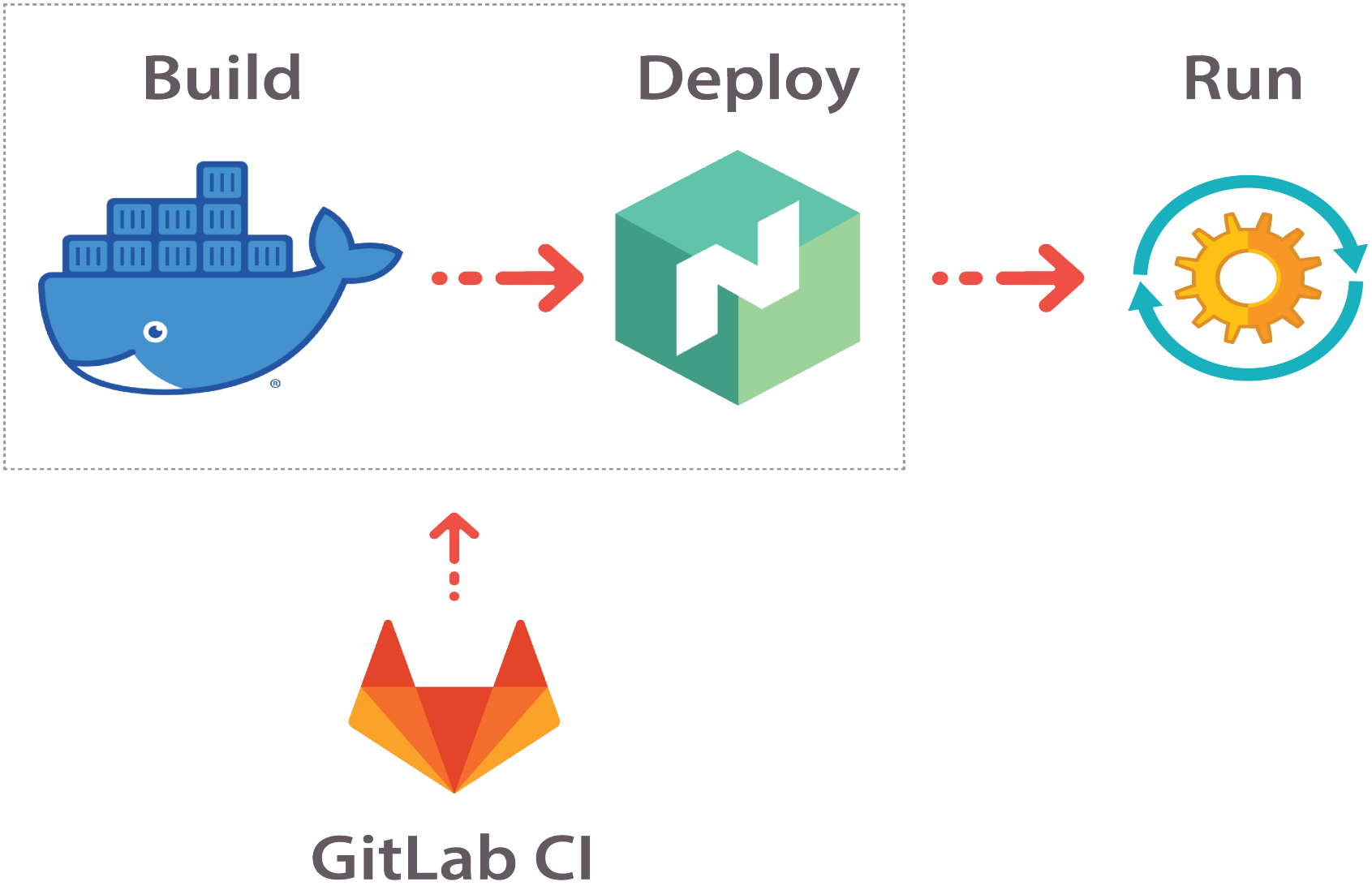
Match

ServiceNow



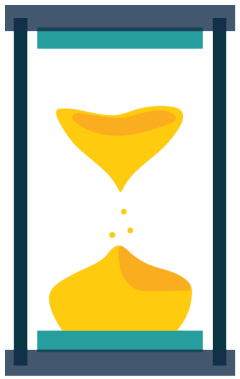
e-mail

How ElastAlert runs

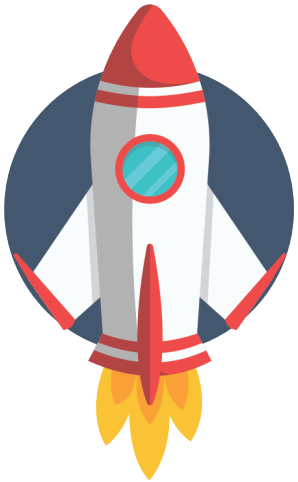


https://www.docker.com
https://www.nomadproject.io
https://about.gitlab.com
This diagram has been designed using resources from Freepik.com

Next Steps



Migration to Python 3



Run ElastAlert on production

Thank you!

Email: dimie.chatz@gmail.com | LinkedIn: Dimitra Chatzihrysou | Twitter: @DimieChatz