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

Elastic Stack

https://www.elastic.co
This diagram has been designed using resources from Freepik.com
Monitoring with ElastAlert

ElastAlert

Elastic Stack

Collection → Processing → Indexing → Visualization

Logs

https://www.elastic.co
This diagram has been designed using resources from Freepik.com
How ElastAlert works

1. Rules
2. Config file
3. ElastAlert
4. Match
5. ServiceNow
6. e-mail
How ElastAlert runs
Next Steps

Migration to Python 3

Run ElastAlert on production
Thank you!

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