CI/CS WORKSHOP

THE COMMUNITY TOGETHER

ResearchSOC | CI CoE PILOT

Valerio Pascucci & Yarden Livnat

SCIENTIFIC COMPUTING AND IMAGING INSTITUTE | University of Utah
https://www.sci.utah.edu/

Questions

- Managing a lot of logs, over 50M/day
- Assuming no or very little budget, what visualizations are the biggest wins at the SOC (incident-focused), CISO (security-focused), and Executive (organization-focused) levels?
- How much is the responsibility of the user vs the presentation layer of a data discovery tool?
- I will be interested to learn how to visualize the security events as network map