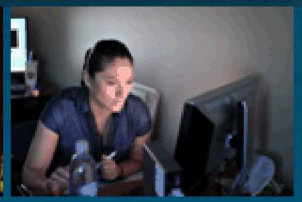
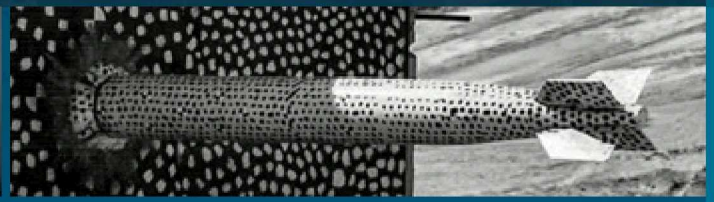
SAND2018-10079C

Containers on Production HPC Systems





PRESENTED BY

Aron Warren, SNL HPC Systems

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Overview of Containers at Sandia

- Containers are primarily built on unclassified networks then moved to classified networks via automated transfers.
- Cybersecurity approvals necessary to run containers on unclassified and classified networks.
- Security controls used in running containers on HPC systems.

Automated Transfer Services to Classified Networks

- Overview of available services
- Challenges of automated transfers
  - Size – 5GB-10GB are ideal
  - Integrity – md5 is enough
  - Availability – who are you competing against?
  - Transfer policies – executables, code, etc.
- Takeaway: Containers will fully work with automated transfers.

Container Software Approvals

- Operating Systems Approval
- Container Software Approval
- Security Plan Requirements

- Takeaway: Containers using SNL approved OS and applications don't require additional software approval.

HPC Systems Security Controls

- Singularity's privilege elevation via setuid
- Container Monitoring via Splunk Universal Forwarder and Splunk Addon for Unix/Linux

- Takeaway: Singularity containers + Monitoring + A few additional host security measures = SNL HPC security approval*