Building a science lab

with ContainerSSH

It’s colorful, but it’s not a sales presentation. ContainerSSH is fully open source.
What is ContainerSSH?
ContainerSSH
Launch containers on demand
ContainerSSH in a nutshell

- It’s an SSH server
- When someone connects, it starts a container
- It doesn’t run in the container
- You can configure it dynamically with webhooks
Auth & Config Server

NFS server
Why ContainerSSH?

- Ease of access
- Simple resource-constrained environments
- Automatic cleanup
- It can record a detailed audit log
- … and it’s fully open source!
Where can I get it?

- Quick start tutorials, reference guide, and development documentation are available at containerssh.io
- Click the Slack link on the website for quick help or guidance.
- The source code is available at github.com/ContainerSSH
ContainerSSH @ CERN
LxPlus Service @ CERN

- LxPlus: Linux Public Login User Service
- Set of Linux machines with SSH access
- Used for code writing, job submission and file operations on remote file systems
- ~100 VMs, ~2000 logged in users at any moment
Investigating ContainerSSH integration
Developed and contributed upstream native AD/Kerberos integration
Pilot service has already been set up
Why containerize?

- Privilege escalation vulnerabilities are common
- Shared resources like /tmp and network interfaces provide a big attack surface
- Resource fair-share is problematic
Authentication flow via Kerberos
Authorization & Configuration
What is the future of ContainerSSH?
OAuth 2.0 authentication for SSH

- **Passwordless** login using a browser
- Works with **most SSH clients**
- Coming in **ContainerSSH 0.5**
Stop! **Demo time!**
Demos

- ContainerSSH with normal credentials
- Auditing in honeypot mode
  *(Audience participation!)*
- Logging in via GitHub (oAuth2)
Questions?