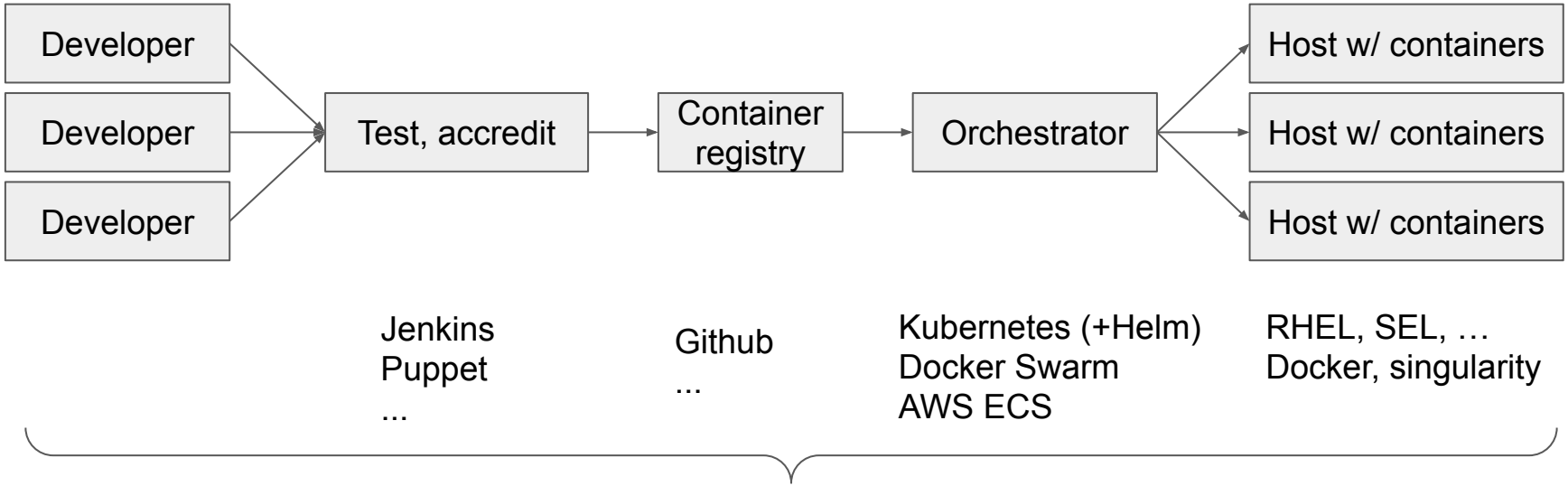
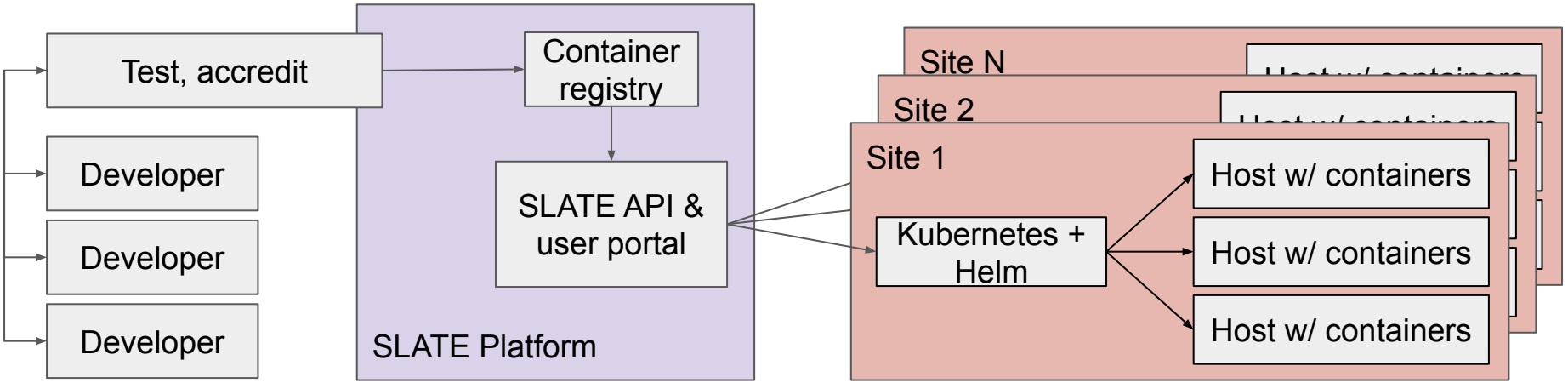
Security for Federated Operations: SLATE and SCI v2

Tom Barton
UChicago

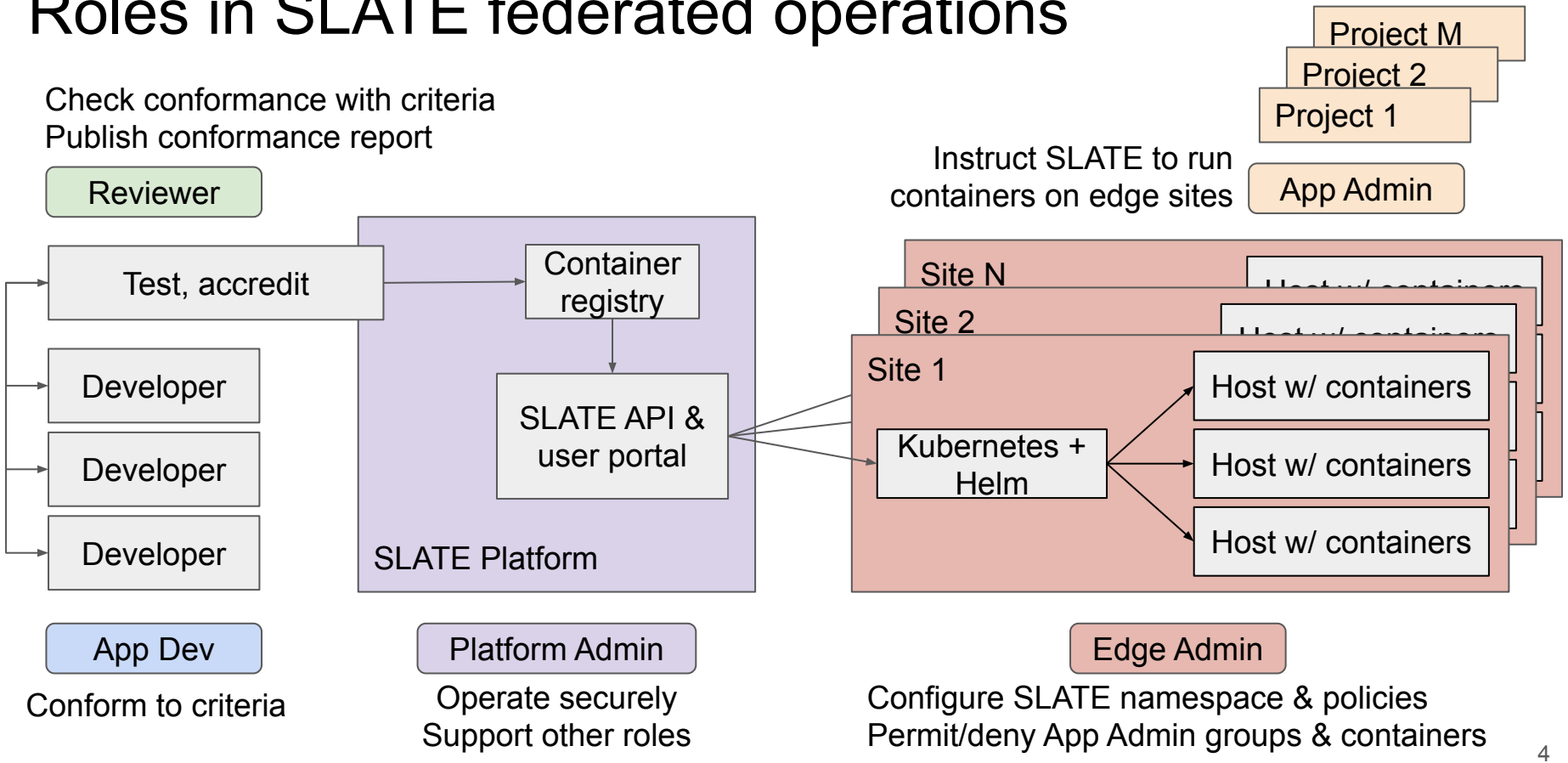
Private cloud operation - DevOps basics



SLATE: federated DevOps



Roles in SLATE federated operations



The Edge Admin’s trust problem

How can I remain responsible for the security of my site if I permit others to run things in it?

- SCI is designed to address this concern, at least enough to address cooperation in managing security incidents, by listing criteria for adequate security of collaborating organisations

SLATE’s federated operations further complicates this problem in two ways

- Prospect of SLATE itself giving unauthorised access
- Prospect of SLATE-installed containers creating security issues for the site

Prospect of SLATE itself giving unauthorised access

- Community-reviewed security documentation
  - TrustedCI early engagement
  - Address all criteria in SCI v2
  - WLCG Federated Operations WG
  - OSG security leads
  - All review is welcome!
- “Overview of SLATE Platform Internals and Security” doc
- Clarity of role obligations and SLATE Platform Admins’ support of them

Extension of SCI v2 criteria to the federated operations context was accomplished through per-role Obligations documents

Security of SLATE-installed containers

Top container misconfiguration security risks*

> RBAC; Secrets; Network policies; Privilege levels; Resource limits/requests; Read-only root file systems; Annotations, labels; Sensitive host mount and access; Image configuration, including provenance

We are currently determining additions to the per-role Obligations documents, application review criteria and procedures, and installation defaults, to address these concerns

Fundamental goal: to report each container's adherence to application review criteria so that Edge Admins can better understand the risk

*State of Container and Kubernetes Security, Fall 2020, StackRox

What SCI v2 did and didn’t do for SLATE

Did

Each of its specifications informed aspects of one or more of the various SLATE security documents

Extension to the federated operations context was pretty straightforward through use of per-role Obligations documents

Didn’t

Help address container security

Provide guidance on its use in a federated operations context

OS3 and OS4 don’t really address the upstream DevOps technologies and processes that can have ***more impact*** on the resultant security of a running container than its host’s own security configuration

SLATE security policy areas and documents

Area	Documents	Status
Foundational policy	Master Information Security Policy and Procedures	In progress
Definition of SLATE Platform	"Overview of SLATE Platform Internals and Security"	Done
Risk Assessment	Asset Inventory	Done
Acceptable Use	Acceptable Use Policy	Done
User Data Handling	Privacy Policy	Done
Incident Response	Incident Response Policy	Done
Obligations for each Role	Edge Admin. Obligations, App. Admin. Obligations, App. Dev. Obligations, App. Reviewer Obligations	Done
Application Review Process	Application Review Procedures	In progress
Access Control	Access Control Policy	Pending
Traceability	Traceability Policy	Pending
Change Management	Change Management Policy	Pending