Security for Federated Operations: SLATE and SCI v2

Tom Barton
UChicago
Private cloud operation - DevOps basics

A single organization manages everything
SLATE: federated DevOps
Roles in SLATE federated operations

Check conformance with criteria
Publish conformance report

Reviewer

Test, accredit

Developer

Developer

Developer

App Dev

Conform to criteria

SLATE Platform

Container registry

SLATE API & user portal

Platform Admin

Operate securely
Support other roles

App Admin

Instruct SLATE to run containers on edge sites

Project M
Project 2
Project 1

Edge Admin

Configure SLATE namespace & policies
Permit/deny App Admin groups & containers
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

<table>
<thead>
<tr>
<th>Did</th>
<th>Didn’t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each of its specifications informed aspects of one or more of the various SLATE security documents</td>
<td>Help address container security</td>
</tr>
<tr>
<td>Extension to the federated operations context was pretty straightforward through use of per-role Obligations documents</td>
<td>Provide guidance on its use in a federated operations context</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Area</th>
<th>Documents</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foundational policy</td>
<td>Master Information Security Policy and Procedures</td>
<td>In progress</td>
</tr>
<tr>
<td>Definition of SLATE Platform</td>
<td>&quot;Overview of SLATE Platform Internals and Security&quot;</td>
<td>Done</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Asset Inventory</td>
<td>Done</td>
</tr>
<tr>
<td>Acceptable Use</td>
<td>Acceptable Use Policy</td>
<td>Done</td>
</tr>
<tr>
<td>User Data Handling</td>
<td>Privacy Policy</td>
<td>Done</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Incident Response Policy</td>
<td>Done</td>
</tr>
<tr>
<td>Application Review Process</td>
<td>Application Review Procedures</td>
<td>In progress</td>
</tr>
<tr>
<td>Access Control</td>
<td>Access Control Policy</td>
<td>Pending</td>
</tr>
<tr>
<td>Traceability</td>
<td>Traceability Policy</td>
<td>Pending</td>
</tr>
<tr>
<td>Change Management</td>
<td>Change Management Policy</td>
<td>Pending</td>
</tr>
</tbody>
</table>