UXL CI PoC Update

Aaron Dron – Codeplay Software Ltd

July 2024

Who Am I?

- VP Infrastructure at Codeplay Software Ltd
- Responsible for all Infrastructure, systems, security, and testing
- Over a decade managing test systems
- Ran continuous integration systems with hugely varied hardware, including GPUs, embedded devices, laptops, games consoles, cell phones, FPGAs etc
- Lots of experience as a very small company working with huge companies

UXL CI PoC Goals

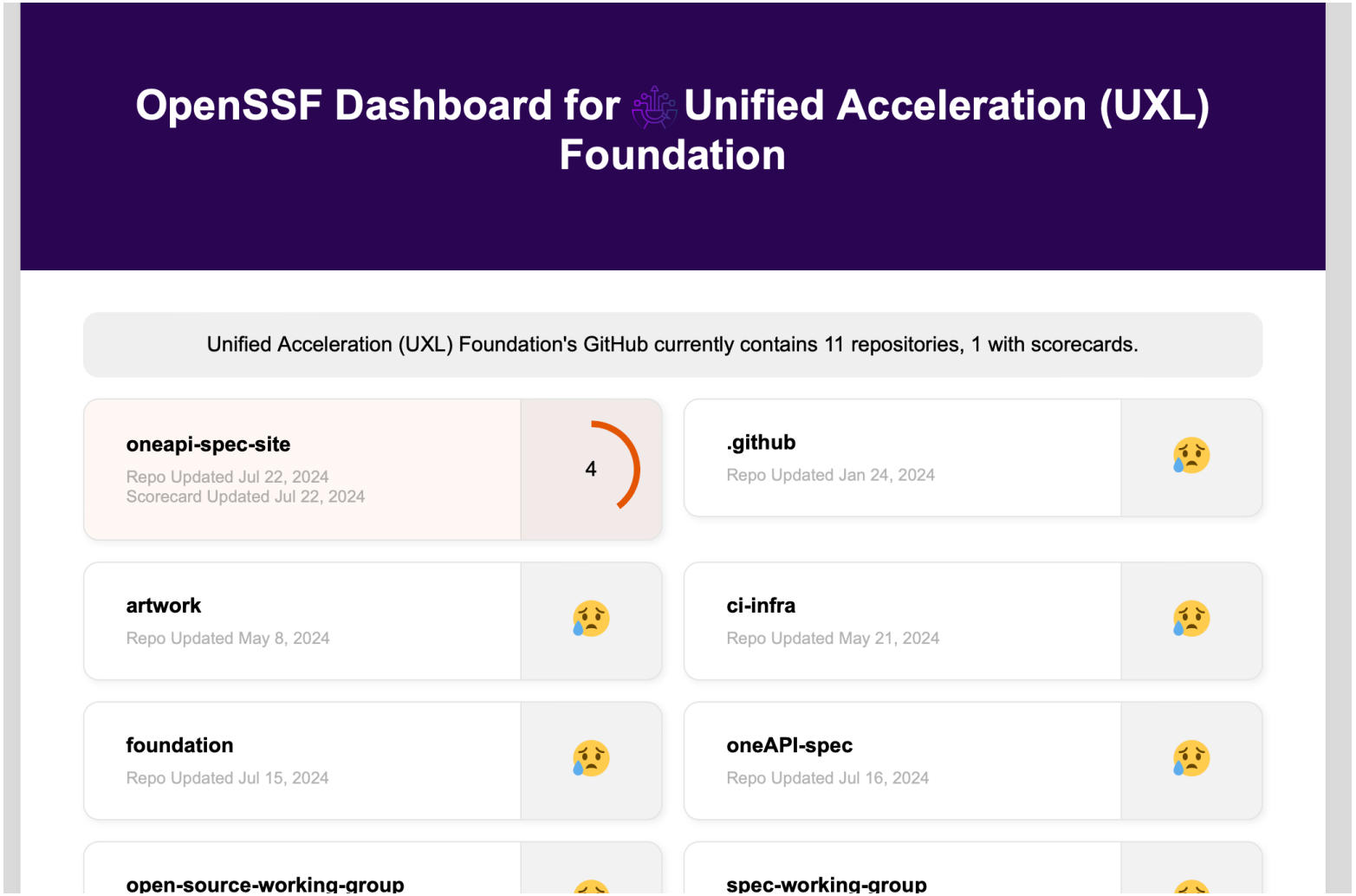
- Enable community contributions
  - Ideally at least a set of smoke tests should be performed on all contributions
- Enable members to enrol and support self-hosted test hardware
  - Having testing across multiple hardware vendors and compute platforms is critical
- Encourage members to develop in UXL repos directly, rather than in private internal repositories
  - This will help avoid large PRs etc
- Where possible prove viability of UXL projects with thorough, public testing

UXL GitHub Organisation

We are now admins of the UXL org and will support for the remainder of 2024 (2025 TBC)

We've begun adding OpenSSF Scorecard functionality to existing UXL repos – many improvements to come

We've set up an OpenSSF Dashboard to track progress

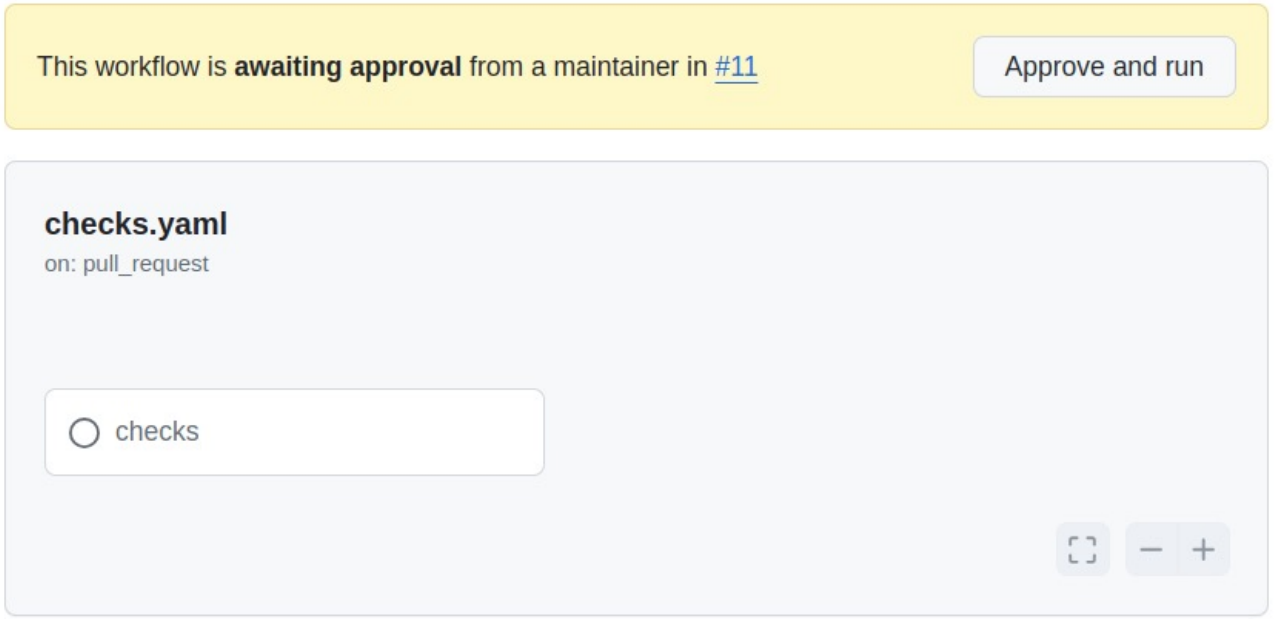


GitHub Actions Security Best Practices

Enabling security configuration best practices on the organisation and relevant repositories

Requiring approvals for any external contributions, to help protect self-hosted runners from malicious contributions

Documenting safeguards and mitigations for GitHub Actions Injection attacks



Self-Hosted Runners

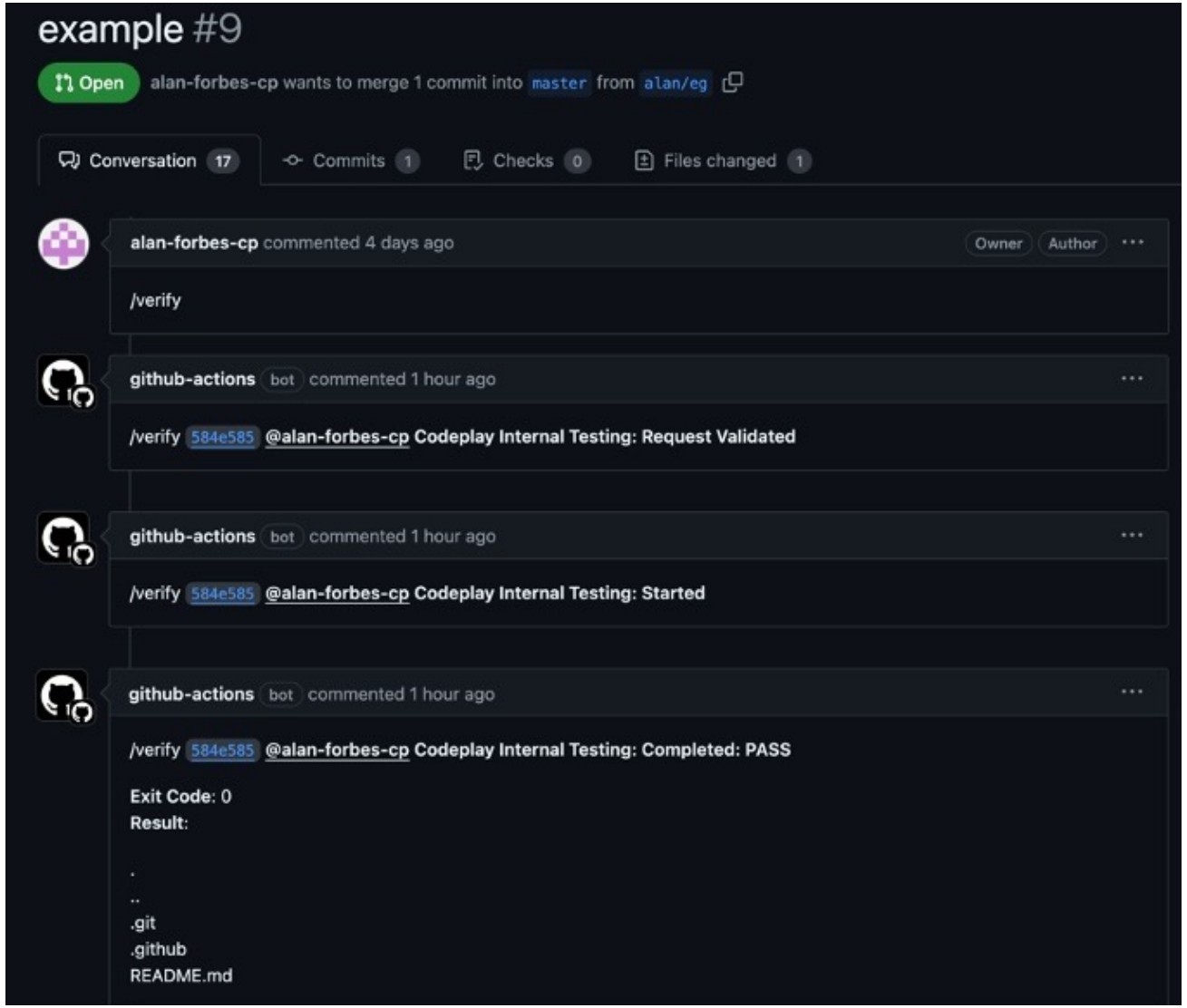
- **Very** conscious of security concerns related to self-hosted hardware in public repositories
- Completed proof of concept self-hosted ephemeral runner using Docker
  - Working on additional PoC ephemeral runners using Kubernetes and virtualisation (w/ PCIe passthrough)
- Guidance and tips for creating security-conscious runners will be in our member documentation
- Working with Intel Tiber Developer Cloud to gain access to GPU Max systems to use as UXL runners
  - They have committed to provide 16 GPUs for our PoC, and may be able to provide further systems (GPU and CPU-only) if there is sufficient demand

Supporting Ancillary Test Systems Hosted by Members

Working on solutions to support test systems that members may host internally for additional / confidential verification testing

Some experimentation with comment triggers and webhooks – some security concerns around them still

Built a PoC self-hostable bot to execute internal test runs on GitHub PRs with safety precautions and comment posts



Ancillary Test Systems and UXL Workflows

- Based on our experiences we would caution against PR workflows that indefinitely block approvals / merges based on private results on Member Hosted Test Systems, as this may discourage contributions from the open-source community
- We would instead recommend that private test results with undesired results (e.g. performance issues on internal hardware) could lead to affected members simply asking for a reasonable amount of time to fix related internal issues before the merge

Not (Currently) Part of the CI PoC

- Migrating Intel oneAPI repositories to UXL Organisation
  - The exception potentially being oneMKL's migration
- Providing and maintaining runner systems
  - Aside from those directly connected to the PoC
- Building functionality to support Just-In-Time cloud-based runners
  - E.g. efforts to minimise AWS costs
- Creation and maintenance of build environments / containers
  - E.g. handling drivers, software stacks, etc
- Releases and artifact management

What we need

- Member feedback
- A location for private members documentation, best practices, etc
- Solutions for secret management

Reach out:

- aaron@codeplay.com
- aaron.dron@intel.com
- UXL Slack