Transparency Report

2025 SECURITY SLAM AT KCCN EUROPE

CLOUD NATIVE
COMPUTING FOUNDATION

2025 SECURITY SLAM

The Security Slam at KubeCon+CloudNativeCon Europe was a stark change in style and structure compared to the previous events run by CNCF's Security Technical Advisory Group (TAG Security).

For starters, this was the first time the event was ever restricted to a subset of projects — which we'll look at more closely throughout this article.

This year's events were a far cry from the 2022 Security Slam, which targeted maintainers with a 30-day period with a $30,000 prize pool in the form of Diversity Scholarship Fund donations made in the name of each project.

And again this was unlike the 2023 Security Slam — a month-long period with plaques, badges, and buckets of swag for participating project maintainers.

In a way, this year's events were more similar to the Kubernetes Lightning Round, which was a 48-hour focus period of targeted collaboration between maintainers and new contributors.

Still, this year's efforts were largely experimental. At the direction of CNCF's events team, TAG Security and members of the CNCF Technical Oversight Committee (TOC) together identified four projects which were given a 45-minute period to collaborate with maintainers on the Project Pavilion stage in London.

Four projects of various maturity levels were selected: Flux, OpenTelemetry, Meshery, and OSCAL Compass.

Similar to Contribfest or the Kubernetes Lightning Round, anyone and everyone was invited to participate alongside maintainers in the event. At the end of the week, four prizes sponsored by Sonatype were issued to the most impactful contributors.

While maintainers were encouraged to create their own backlog of tasks, driven by the project's current goals, a recurring theme was the controls defined in the Open Source Project Security Baseline.

FLUX

Flux and its maintainer team has seen no shortage of obstacles in the past year, and yet the adoption of this graduated project continues to rise at astonishing rates. With Flux contributors already integrated into the TAG Security community, it was a natural fit to participate in this year's Security Slam.

Maintainers from the project, including Stefan Prodan and Matheus Pimenta, rallied around the Slam to create a highly refined backlog for new contributors — and the entire team showed a forceful presence on the Project Pavilion during the event!

> *In the Flux project we had people working on all of the issues we added to the Security Slam backlog! Three pull requests were merged during the event, with two of them effectively improving the security of our CI. We saw solid contributions for our Security Insights files, and a single person worked with the maintainers to draft an entire Self Assessment! We need more of those slams!*
>
> \- Matheus Pimenta

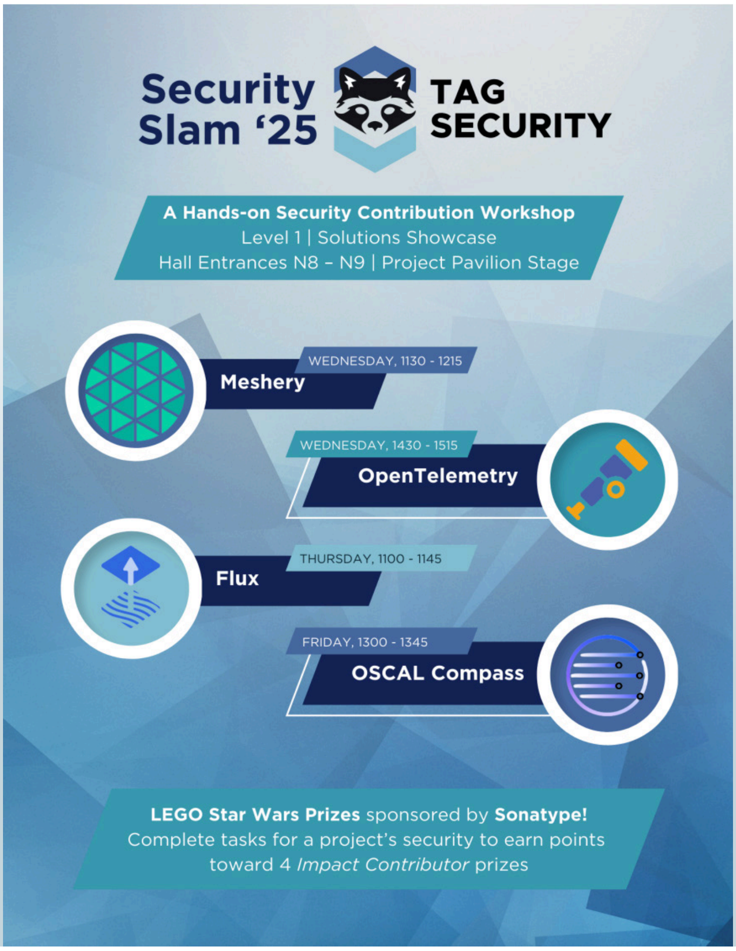
Matheus Pimenta and Stephan Prodan welcoming contributors to the Flux Security Slam.

OPENTELEMETRY

The OpenTelemetry project is among the most popular projects in the CNCF ecosystem. After completing a security self-assessment through TAG Security, maintainers Austin Parker and Trask Stalnaker accepted an invitation to join the Security Slam.

The project made excellent strides to improve their 70+ repositories during the event, but none as much as the revival of the special interest group dedicated specifically to project security. If you are interested in contributing to the security of OpenTelemetry, read more here about how you can join the SIG!

> *Working with TAG Security to prepare for the Security Slam helped us consolidate our goals and reflect on our current security posture. In addition to the work done by KubeCon participants, we have taken advantage of this momentum to re-launch the Open Telemetry Security SIG!*
>
> \- Trask Stalnaker



Security Slam '25

TAG SECURITY

A Hands-on Security Contribution Workshop
Level 1 | Solutions Showcase
Hall Entrances N8 – N9 | Project Pavilion Stage

WEDNESDAY, 1130 - 1215
Meshery

WEDNESDAY, 1430 - 1515
OpenTelemetry

THURSDAY, 1100 - 1145
Flux

FRIDAY, 1300 - 1345
OSCAL Compass

LEGO Star Wars Prizes sponsored by **Sonatype!**
Complete tasks for a project's security to earn points
toward 4 *Impact Contributor* prizes

MESHERY

Meshery is one of two Sandbox projects that were invited to this Security Slam on a recommendation from the Technical Oversight Committee, to help bolster its application for promotion to Incubation status.

Several Meshery project maintainers and contributors from across the community showed enthusiastic participation during the participation phase, as they used scanning tools and best practices guides to create a backlog of improvements for the 10 project repos. The project also issued special “Security Sentinel” badges for both remote and in-person participants!

> *Meshery’s participation in Security Slam wasn’t just a session, but was the community and maintainers rolling up their sleeves together, turning shared knowledge into tangible security improvements for the project right at KubeCon. It was inspiring to see contributors and maintainers unite, earning their Security Sentinel badges while making Meshery stronger for everyone. Events like this push the community forward—not just in code, but in culture.*
>
> - Lee Calcote

Sangram Rath issuing prize to impact contributor Alberto Barbaro

OSCAL COMPASS

The second Sandbox project that was recommended for the Security Slam by the CNCF TOC was OSCAL Compass, home of the Trestle compliance tool.

Though it was last on the schedule, with the least time for participants to qualify for a prize, multiple tasks were completed and four pull requests were merged during the session! The completed work included the setup of OpenSSF Scorecard scanning, security improvements for the project's CI/CD workflows, and significant progress on the project's security self assessment.

> *The preparation period was really valuable and helped us gain deeper knowledge of the OSPS baseline requirements and associated assessment tooling. We were able to get security insights files in place for several repositories and are now in a place where we can automatically assess our project repositories against OSPS baseline Maturity 1 controls.*
>
> - Jennifer Power

Anca Sailer issuing prize to impact contributor Jeremy Sollars

LESSONS LEARNED

Similar to previous years, maintainers have reported finding value in the preparation period, where opportunities for improvement were identified and brainstormed with members of TAG Security.

While the event was a success, there were several lessons learned that we believe will help similar events in the future.

1. In spite of an attempt to phrase the event description as a hands-on session in the KubeCon schedule, every session had nearly 90% of the audience appearing to be surprised by the structure.
2. Constricting the event to a 45-minute collaboration block reduced the capacity for maintainers to effectively support contributors, reducing the impact significantly compared to previous years.
3. The Project Pavillion proved to be an ineffective location for this event. Distractions and tech failures were prevalent, and — in all four events — the start time was delayed by anywhere from 7 to 12 minutes. This delay resulted in decreased energy levels, rushed introductions, and general confusion for participants who then had 25% less time with maintainers.

NEXT STEPS

This event coincided with the reorganization of CNCF’s technical advisory groups, and as such it is the final event that will ever be run by TAG Security. The emerging *TAG Security & Compliance* will have a new charter, leadership, and goals, which may or may not include a continuation of the Security Slam.

In the event that future Security Slams are run by TAG Security & Compliance, the lessons here suggest a return to long-form remote events with highly targeted in-person activities, similar to the massively successful 2023 Security Slam.

If you would like to be part of future Security Slam events as a project maintainer, contributor, or sponsor, be sure to reach out to the TAG or TOC!

THANK YOU!

CLOUD NATIVE
COMPUTING FOUNDATION