OC3 SCHEDULE

12 March 2026

Stage 1

Stage 2

16:00–16:15 (CET)
08:00–08:15 (PT)

Introduction

OC3 2026 Opening introduction

Felix Schuster
Edgeless Systems

Keynote
16:15–16:45 (CET)
08:15–08:45 (PT)

On building a global cloud champion – with confidential computing done right

Octave Klaba
OVHcloud

Ecosystem & foundations
16:45–17:15 (CET)
08:45–09:15 (PT)

Regulations and standards for Confidential Computing

Mike Bursell
Confidential Computing Consortium

AI
17:15–17:30 (CET)
09:15–09:30 (PT)

Building the Trust Fabric for AI Agents

Ivan Petrov & Patrick McGrath
Google Deepmind

AI
17:30–17:45 (CET)
09:30–09:45 (PT)

Privatemode: Lessons learned from one year of running confidential AI in production

Moritz Eckert
Edgeless Systems

Ecosystem & foundations
16:15–16:45 (CET)
08:15–08:45 (PT)

Transparency for the Web using Confidential Computing

Shabsi Walfish
Google

Ecosystem & foundations
16:45–17:15 (CET)
08:45–09:15 (PT)

Azure confidential computing in the sovereign cloud era: Tech advances, customer uptake, and workload patterns

Vikas Bhatia
Microsoft

AI
17:15–17:45 (CET)
09:15–09:45 (PT)

Confidentiality in the Era of Generative and Agentic AI

Mengmei Ye, Hubertus Franke, Marcio Silva & Apoorve Mohan
IBM Research

Break
17:45–18:00 (CET)
09:45–10:00 (PT)

Break
17:45–17:50 (CET)
09:45–09:50 (PT)

Keynote
18:00–18:30 (CET)
10:00–10:30 (PT)

Memory Interposer Attacks: Out of scope, but not out of mind

Simon Johnson
Intel

Keynote
18:30–18:45 (CET)
10:30–10:45 (PT)

Pushing the Boundaries of AI Workloads to Where

Daniel Rohrer
NVIDIA

Attestation
18:45–19:15 (CET)
10:45–11:15 (PT)

Remote Attestation of Imutable Operating Systems built on systemd

Lennart Poettering
Amutable

Ecosystem & foundations
19:15–19:45 (CET)
11:15 –11:45 (PT)

AWS EC2 Confidential Compute Options: Choosing the Right Protection for Your Workloads

Alexander Graf & J.D. Bean
AWS

Ecosystem & foundations
19:45–20:00 (CET)
11:45 –12:00 (PT)

COCONUT – Beyond Secure Service Modules

Jörg Rödel
AMD

Keynote
17:50–18:20 (CET)
09:50–10:20 (PT)

Confidential Computing at Google Scale: An Inside Look

Will Grannis
Google Cloud

Attestation
18:20–18:50 (CET)
10:20–10:50 (PT)

Proof of Cloud: Data Center Execution Assurance for Confidential VMs

Filip Rezabek
Flashbots

Apps & Solutions
18:50–19:20 (CET)
10:50–11:20 (PT)

TEEs in Web3: Powering Rollups, Consensus, and Real-World Exchange Infrastructure

Giovanni Mazzeo
Trillion

AI
19:20–19:50 (CET)
11:20–11:50 (PT)

An IT-Security view on privacy-preserving, LLM-based systems with provider exclusion

Ivan Gudymenko & Andrey Ruzhanskiy
Telekom

AI
19:50–20:05 (CET)
11:50–12:05 (PT)

The Weakest Link in AI: Hardening MCP Servers with Confidential Computing

Pawan Khandavilli
Microsoft

Break
20:00–20:45 (CET)
12:00–12:45 (PT)

Break
20:05–20:10 (CET)
12:05–12:10 (PT)

20:10–20:25 (CET)
12:10–12:25 (PT)

Ecosystem & foundations

OpenCCA: An Open Framework to Enable Arm CCA Research

Andrin Bertschi
ETH Zürich

Panel Discussion
20:45–21:15 (CET)
12:45–13:15 (PT)

Tech Leaders Panel

Daniel Rohrer, Anand Pashupathy
Ravi Kuppuswamy, Mark Russinovich
NVIDIA, Intel, AMD, Microsoft Azure

Apps & Solutions
21:15–21:30 (CET)
13:15–13:30 (PT)

Hermetik - An "Operating System" for Cross-Company Collaboration

Sven Trieflinger
Bosch

Keynote
21:30–21:45 (CET)
13:30–13:45 (PT)

Confidential Computing on the Scaling Laws Curve

Jason Clinton
Anthropic

Attestation
21:45–22:15 (CET)
13:45–14:15 (PT)

Device Attestation, Confidential Identity, and Generic vTPM Support in Trustee

Tobin Feldmann-Fitzthum
NVIDIA

20:55–21:25 (CET)
12:55–13:25 (PT)

Ecosystem & foundations

Full disk encryption for Confidential Computing guests

Vitaly Kuznetsov & Emanuele Esposito
RedHat

21:25–21:40 (CET)
13:25–13:40 (PT)

Ecosystem & foundations

Creating Global Standards for Confidential Computing

Rachel Wan
Confidential Computing Consortium

21:40–22:10 (CET)
13:40–14:10 (PT)

Attestation

Toward ownership-aware attestation: Contrast meets Platform Ownership Endorsement

Benny Fuhry & Markus Rudy
Intel & Edgeless Systems

22:10–22:25 (CET)
14:10–14:25 (PT)

AI

From Build to Runtime: Enabling Trusted and Transparent LLM Service Pipelines with TDX

Edmund Song
Intel

The End