OPERATIONAL TECHNOLOGY CYBERSECURITY HACKATHON

DATES
24–27 August 2026

LOCATION
Dhahran Techno Valley

TEAM SIZE
Groups of 5

PRIZE POOL
SAR 200,000

GLOBAL CYBERSECURITY FORUM | CENTER OF EXCELLENCE OPERATIONAL TECHNOLOGY CYBERSECURITY | aramco

JOIN THE OT CYBERSECURITY HACKATHON

An initiative by the Operational Technology Cybersecurity Center of Excellence (OTC-CoE) in collaboration with Aramco

WHAT IS THE OTC CENTER OF EXCELLENCE (OTC-COE)?

The OTC-CoE was established by the Global Cybersecurity Forum (GCF) and Aramco in 2023 to catalyze collaboration to address increasingly complex OT cybersecurity challenges. Under the leadership of GCF and Aramco, alongside a diverse and growing membership spanning the entire OT cybersecurity value chain, the OTC-CoE serves as a platform for advancing the maturity of global OT cybersecurity through capability development, standardization and policy advocacy, research and innovation, and knowledge exchange.

WHAT IS THE OT CYBERSECURITY HACKATHON?

Participants are challenged to solve real-world OT security challenges, working in teams to develop innovative ideas and strategies for safeguarding critical infrastructure. Over four days, teams will work together to transform their ideas into impactful solutions and present them to a panel of industry judges. All ideas will be reviewed after the Hackathon to inform real-world industry application.

WHY IT MATTERS

OT cybersecurity is one of the most important emerging fields, protecting the industrial control systems that operate our critical infrastructure, including the production and distribution of energy, water, and electricity. A cyber threat to critical infrastructure disrupts industries, essential services, and the daily lives of millions of people.

IS THE OT CYBERSECURITY HACKATHON FOR YOU?

It is open to professionals or students across the industry, including:

Employees from oil, gas, and utilities operators and vendors worldwide

Experts from cybersecurity or related consulting firms

Students, researchers, and faculty from universities and research institutions

WHY PARTICIPATE?

Solve real-world challenges
Apply your expertise to real-world OT security challenges facing critical infrastructure

Collaborate widely
Work alongside industry peers from across the OT sector

Gain access to mentorship
Mentors and instructors will be on hand to support your thinking

Showcase to experts
Present to, and be evaluated by, a jury of experienced OT industry professionals

Compete for a prize pool
The four winning teams will share a total prize pool of SAR 200,000

See your ideas go further
All submitted solutions will be reviewed by the OTC-CoE Technical Review Committee after the event and further developed to inform real-world solutions

WHAT TO EXPECT

Four OT cybersecurity challenges will each be tackled by up to ten groups of five members each. Supported by instructors with global subject-matter experience, participants will develop final presentations showcasing their solutions. Days 1–3 run from 8am–4pm, with ample time to exchange ideas and a one-hour lunch and networking break at noon. Day 4 runs from 1–3:30pm, featuring Hackathon highlights and the award ceremony, followed by lunch.

ABOUT THE JURY

Our Hackathon judges are an exceptional group of experienced, certified professionals from across the OT industry and its disciplines, including technology and innovation, research, governance, and consultancy.

THE FOUR CHALLENGE TRACKS

Groups will each tackle one of four OT cybersecurity challenges:

1. **Reconnaissance in OT**
   Develop secure approaches for asset discovery and reconnaissance in OT environments while addressing the challenges of legacy systems, limited computing resources, vendor limitations, and impact on operations

2. **Security Monitoring of Operations Data**
   Enhance cybersecurity monitoring by integrating cybersecurity data with process and operational data to improve detection and situational awareness. Improve visibility across diverse and segmented OT environments by collecting control system application logs and monitoring system application logs

3. **Change Detection Constraints**
   Develop solutions to distinguish authorized changes from unauthorized modifications and maintain a defensible change history, including logic, project files, firmware, recipes, setpoints, HMI configurations, network configurations, and safety system SIS changes

4. **Securing Legacy Systems**
   Address the cybersecurity challenges of legacy OT systems that are no longer supported by vendors and manufacturers by identifying alternative approaches to securing these systems

EVENT LOCATION

The Hackathon will take place at Dhahran Techno Valley – a regional OT innovation hub.

Dhahran Techno Valley, Dhahran. Saudi Arabia

Confirm your place by 23 August:

REGISTER NOW

GLOBAL CYBERSECURITY FORUM

CENTER OF EXCELLENCE
OPERATIONAL TECHNOLOGY CYBERSECURITY

aramco

Follow us for updates:

For questions or enquiries:

OT-CoE@gcforum.org