# Thematic CERN School of Computing on Security 2022

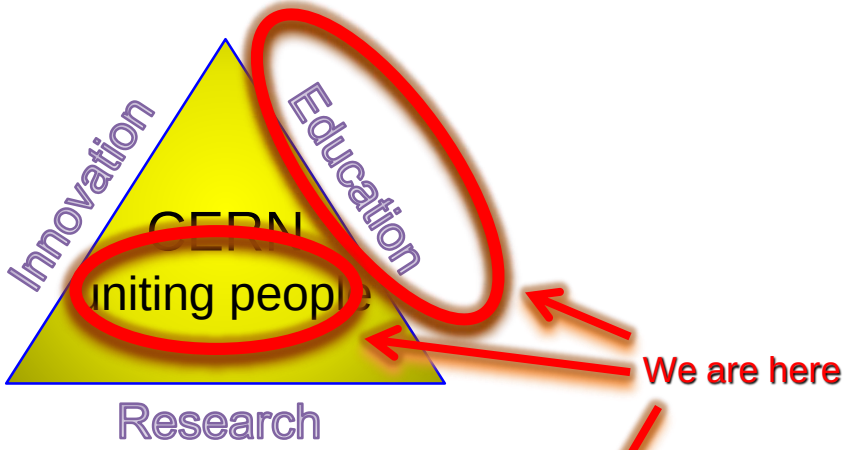
https://indico.cern.ch/e/tCSC-Security-2022

*Sebastian Łopieński*
*CERN School of Computing director*

**GDB meeting, 13 July 2022**
https://indico.cern.ch/event/1096032/

# Introduction to CERN School of Computing

# CERN's mission




Accelerating beams
(accelerators)

Detecting particles
(experiments)

Large-scale computing
(analysis)

Discovery

# A school with a long history

- The school was created in 1970
  - 43rd edition in 2022


- 2900 students of ~80 different nationalities have followed the school
  - usually 60-80 per year
  - alumni web site: https://cern.ch/CSC/history/alumni/


- The school has visited 22 countries
  - https://cern.ch/CSC/history/past-schools/
  - recent: France, Romania, Croatia, Israel, Spain, Belgium, Greece, Portugal, Cyprus

# Bridging science and computing

- Technological evolution in computing empowers science
  - especially in data-intensive domains such as High Energy Physics
  - computing is the main strategy for many scientific fields to do research efficiently on a large scale

- It is nowadays essential that:
  - scientists master computing technologies as a main tool for their research
  - computer engineers understand the scientific needs in order to deliver computing services to research projects

# Academic dimension

CERN School of Computing…

- is not a conference
  - lecturers do not present their work or promote their projects
- is not a training session
  - not a replication of training courses available at home institutes or online
  - focus on persistent knowledge, less on know-how


# Three CERN Schools of Computing

## tCSC 2022

Thematic School 10th edition, will take place at Cargèse, Corse-du-Sud (FR), from 1 to 7 May 2022 – Applications are now closed

## tCSC security 2022

Thematic School on Security, will take place in Split, Croatia (HR), from 19 to 25 June 2022 – Applications are now closed

## CSC 2022

Main School 2022 43rd edition will take place in Krakow (PL), from 4 to 17 September 2022 – Apply!

# Thematic CSC on Security 2022

# Security CSC 2022

- **Applications → student selection**
- **June 19-25, 2022** (Sunday to Saturday) at MEDILS institute, **Split, Croatia**
  - **Sunday afternoon:** arrival and informal welcome, visit of Split city
  - **Monday to Friday:** official opening, lectures and exercises
  - **Wednesday afternoon**: excursion / outdoor acitivty
  - **Saturday morning:** departure
- **Lectures and hands-on exercises:** ~30 hours in total
  - including a guest lecture, student lightning talks etc.
- **Exam → diploma**
- **Optional social and sport activities**
- **Registration fee**: 550-750 EUR (covers acommodation, meals, tuition, activities)
  - depending on the accommodation (twin vs. single rooms, place)

# Programme committee

https://indico.cern.ch/event/1106023/page/24209-programme-committee

| | |
|---|---|
| • Ian Collier | UKRI-STFC |
| • David Crooks | UKRI-STFC / EGI CSIRT / IRIS CSIRT |
| • Sven Gabriel | Nikhef / EGI CSIRT |
| • David Groep | Nikhef |
| • David Kelsey | UKRI-STFC |
| • Sebastian Lopienski | CERN / CSC |
| • Hannah Short | CERN / GÉANT GN4-3 |
| • Romain Wartel | CERN / WLCG |

# Topic and target audience

CERN School of Computing "**Security of research computing infrastructures**"

The programme of this school is targeted at **people working in academia and research institutes**, who as part of their job need to **ensure security and resilience of computing resources** they manage, and want to be prepared to **detect and handle possible security incidents**:

- **service managers and service providers** of distributed scientific computing infrastructures, both from IT departments and from experiments,
- **people in charge of deploying cloud services** used by scientists,
- **security professionals**, who would like to expand their knowledge in a more holistic fashion.

# Lecturers

https://indico.cern.ch/event/1106023/page/23919-lecturers

Stefan Lüders
CERN

Sebastian Łopieński
CERN

Sven Gabriel
Nikhef, the Netherlands

Hannah Short
CERN

Barbara Krašovec
ISJ, Slovenia

Daniel Kouřil
CESNET, Czech Republic

David Crooks
UKRI-STFC, UK

Romain Wartel
CERN

# Programme

https://indico.cern.ch/event/1106023/program

| | |
|---|---|
| **Introduction** | Security in research and scientific computing<br>Security operations |
| **Track 1: Protection and prevention** | Identity, authentication, authorisation<br>Security architecture<br>Vulnerability management<br>Application security and penetration testing |
| **Track 2: Detection** | Logging and traceability<br>Intrusion detection with SOC |
| **Track 3: Response** | Introduction to forensics<br>Incident response<br>Coordination of security incidents |

**30 class hours**

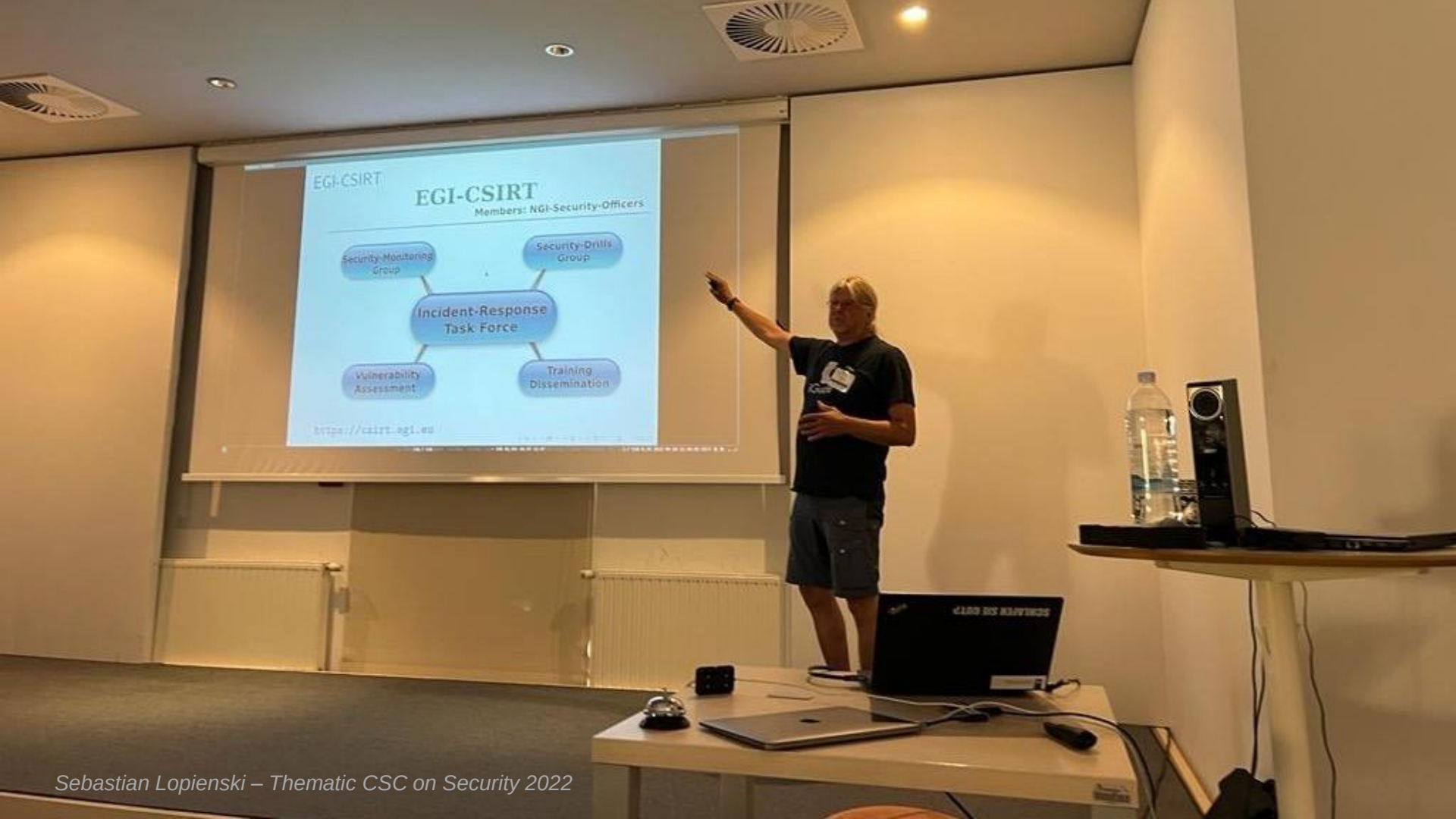
**Lectures** and **exercises,** but also **group discussions** and **role-playing**

| Monday, 20 June 2022 | Tuesday, 21 June 2022 | Wednesday, 22 June 2022 | Thursday, 23 June 2022 | Friday, 24 June 2022 |
|---|---|---|---|---|
| 08:45 **Opening Session** - Sebastian Lopienski | 08:45 **Vulnerability management** - Sven Gabriel | 08:45 **Container security** - Daniel Kouřil | 08:45 **Introduction to forensics - lecture 1** - Daniel Kouřil | 08:45 **Introduction to forensics - exercises** - Daniel Kouřil |
| 09:45 **Security in research and scientific computing** - Stefan Lueders | 09:45 **Virtualization security** - Barbara Krašovec | 09:45 **Container security - exercises** - Daniel Kouřil | 09:45 **Incident response - lecture 1** - Romain Wartel | 10:15 **Coffee break** |
| 10:45 **Coffee break** | 10:45 **Coffee break** | 10:45 **Coffee break** | 10:45 **Coffee break** | 10:30 **Introduction to forensics - exercises** |
| 11:15 **Announcements** | 11:15 **Announcements** | 11:15 **Announcements** | 11:15 **Announcements** | 11:45 **Announcements** |
| 11:30 **Security operations - lecture 1** - Sven Gabriel | 11:30 **Logging and traceability** - David Crooks | 11:30 **Intrusion detection with SOC - lecture 2** - David Crooks | 11:30 **Introduction to forensics - lecture 2** - Daniel Kouřil | 12:00 **Penetration testing - ex...** |
| 12:45 **Lunch** | 12:45 **Lunch** | 12:45 **Lunch** | 12:45 **Lunch** | 12:45 **Lunch** |
| 13:30 **Study time and/or daily sports** | 13:30 **Study time and/or daily sports** | 13:30 **Outdoor excursion** | 13:30 **Study time and/or daily sports** | 13:30 **Study time** |
| 14:45 **Security operations - lecture 2** - Sven Gabriel | 14:45 **School photo** | | 14:45 **Incident response - lecture 2** - Romain Wartel | 14:15 **Exam** |
| 15:45 **Coffee break** | 14:50 **Student lightning talks** | | 15:45 **Coffee break** | 15:00 **Coffee break** |
| 16:00 **Identity, authentication, authorisation** - Hannah Short | 15:45 **Coffee break** | | 16:00 **Intrusion detection with SOC - exercises** - David Crooks | 15:15 **Incident response - exercise** - Romain Wartel |
| 17:00 **Security architecture** - Barbara Krašovec | 16:00 **Intrusion detection with SOC - lecture 1** - David Crooks | | | 18:30 **Closing Session** - Sebastian Lopienski |
| 18:00 **Security architecture - exercise** - Barbara Krašovec | 17:00 **Application security an...** | | | 19:45 **Outside Closing Dinner** |
| 19:15 **Dinner at MEDILS** | 17:30 **Penetration testing - exercises** - Sebastian Lopienski | 19:15 **Outside dinner** | 19:15 **Dinner at MEDILS** | |
| | 19:15 **Dinner at MEDILS** | | 20:00 **Special evening talk: Ransomware - and much more!** | |

nputing


*Sebastian Lopienski – Thematic CSC on Security 2022*


*Sebastian Lopienski – Thematic CSC on Security 2022*




*Sebastian Lopienski – Thematic CSC on Security 2022*


Intrusion detection with SOCs: Part 1
threat intelligence, monitoring, integration and processes
David Crooks
UKRI STFC
EGI CSIRT/IRIS Security team
david.crooks@stfc.ac.uk


Network topology example
DMZ
ZONE 1
ZONE 2
PRIVATE

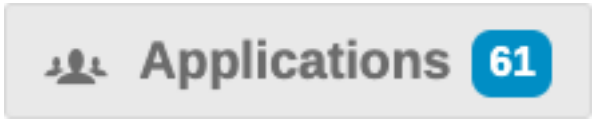

Putting the Pieces Together
LINKIN PARK
Putting the Pieces Together


OpenSearch
ILLABONG


Coca-Cola

# Participants

https://indico.cern.ch/e/1106023/page/23920-participants




- 27 different nationalities
- 9 female applicants
- 32 different institutes from 20 countries

36 students selected and invited
(minus 3 late withdrawal)

- 18 different nationalities
- 5 female participants
- 20 different institutes from 14 countries

**Diverse, talented, passionate about science and technology**


Nikhef

UTA
THE UNIVERSITY OF TEXAS
AT ARLINGTON

Technion
Israel Institute of Technology

CERN
School of Computing

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Stony Brook University

HUMBOLDT-UNIVERSITÄT
ZU BERLIN

University of
Zagreb

CERN

KIT
Karlsruher Institut für Technologie

IGFAE
Instituto Galego de Física de Altas Enerxías

UNIVERSITÉ
Clermont
Auvergne

UNIVERSITÀ DEGLI STUDI DI MILANO
BICOCCA

Lancaster
University

Fermilab

IFAE
Institut de Física d'Altes Energies

UNIVERSITY OF
COPENHAGEN

UNIVERSITÄTSMEDIZIN
GÖTTINGEN
UMG

SWITCH

LIP
LABORATÓRIO DE INSTRUMENTAÇÃO
E FÍSICA EXPERIMENTAL DE PARTÍCULAS

# Self-presentation session

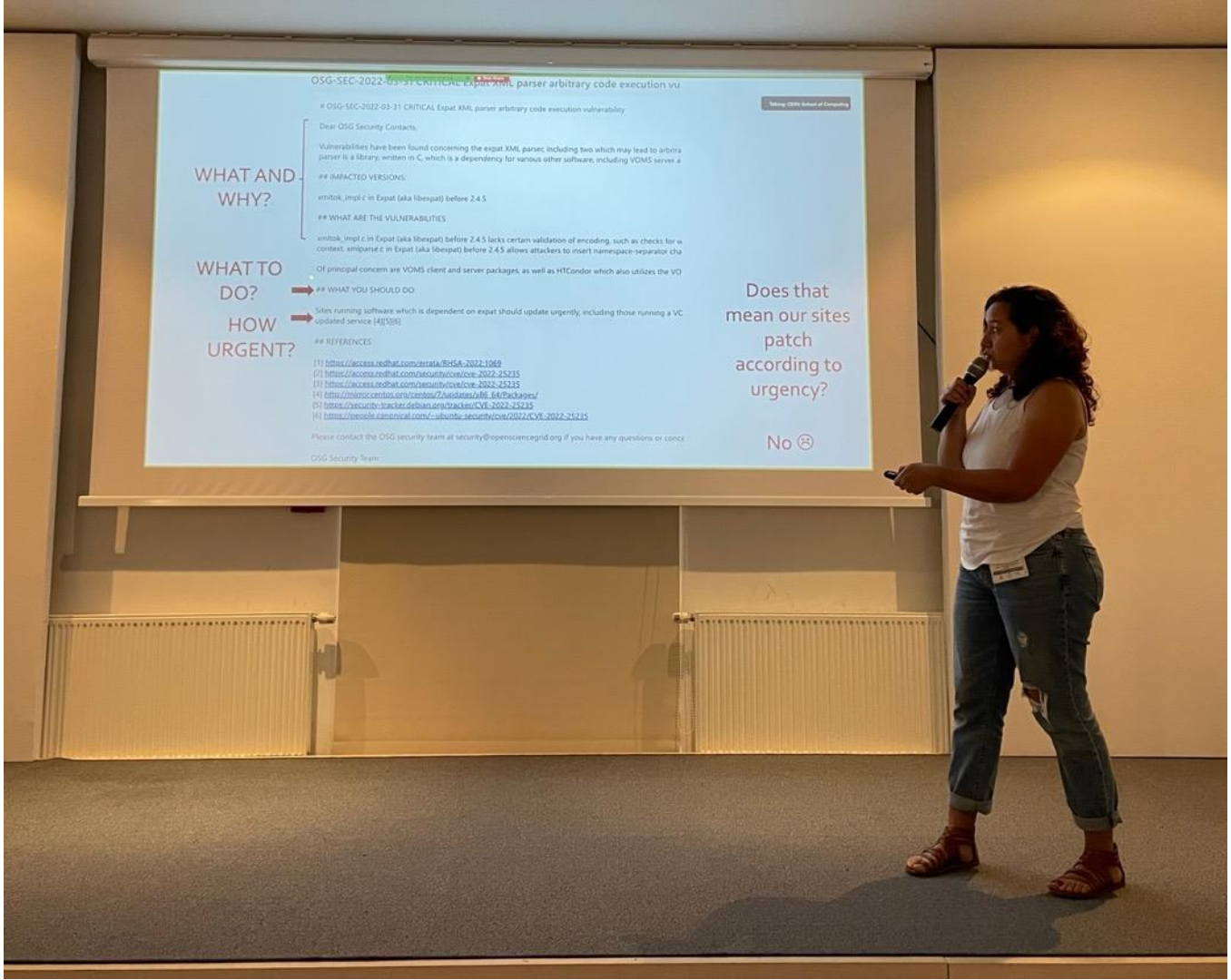


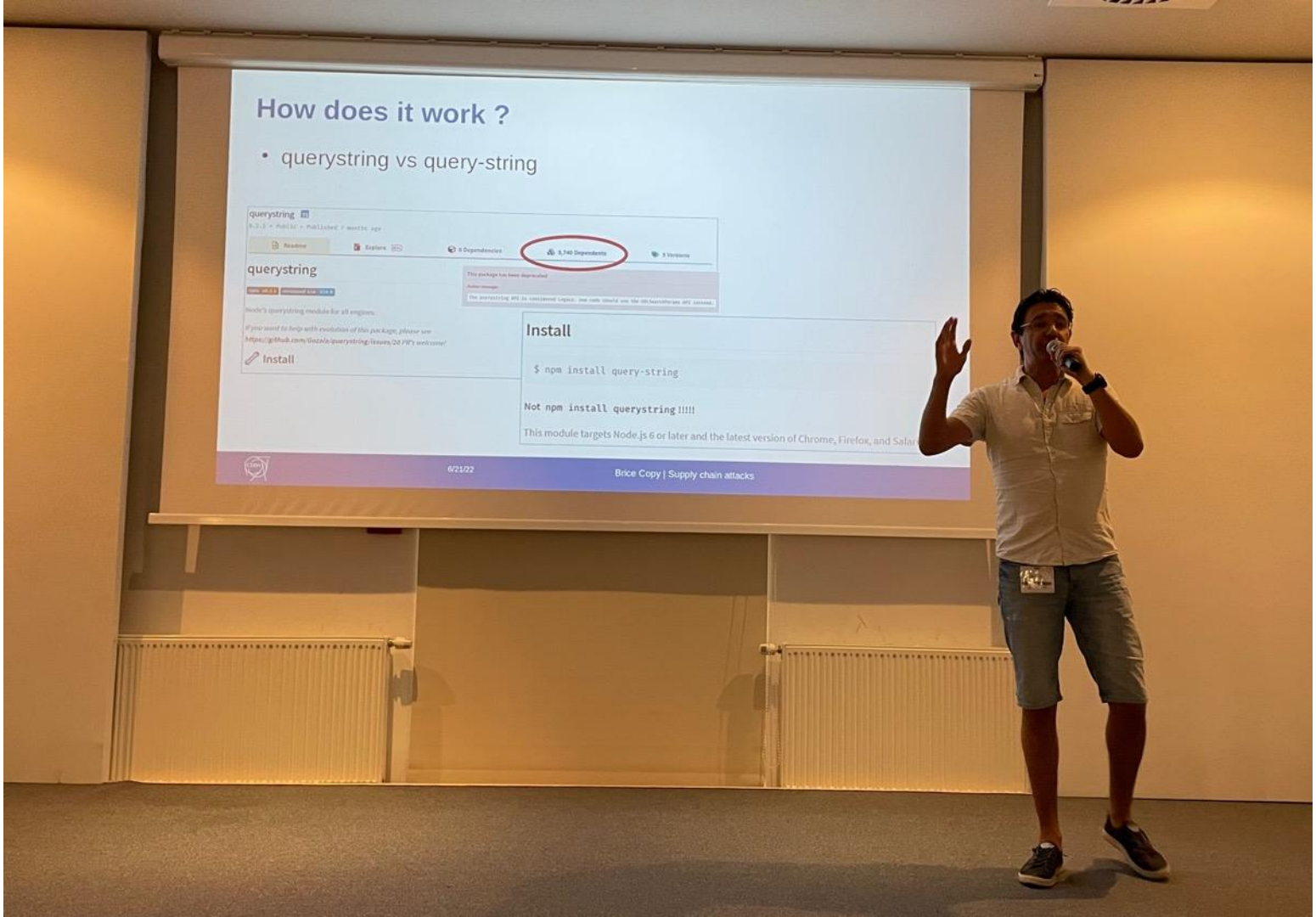
# Security tCSC 2022 participants

# tCSC on security 2022: Student lightning talks

CERN School of Computing

- Björn Leder (Humboldt University of Berlin, Germany)
  *"Why to hack your vacuum cleaner?"*
- Jack Henschel (CERN)
  *"Pulumi: Infrastrucutre-As-Actual-Code"*
- Jeny Teheran (Fermi National Accelerator Laboratory, US)
  *"Compute node scanning tool for Open Science Grid"*
- Brice Copy (CERN)
  *"Software supply chain security"*
- Luca Giommi (University of Bologna and INFN, Italy)
  *"Machine Learning as a Service for High Energy Physics"*
- Pau Cutrina Vilalta (CERN)
  *"Cyber threat vectors in the space industry"*
- Andrei Dumitru (CERN)
  *"Dark Patterns"*


OSG-SEC-2022-03-31 CRITICAL Expat XML parser arbitrary code execution vu
# OSG-SEC-2022-03-31 CRITICAL Expat XML parser arbitrary code execution vulnerability
Dear OSG Security Contacts,
Vulnerabilities have been found concerning the expat XML parser, including two which may lead to arbitra
parser is a library, written in C, which is a dependency for various other software, including VOMS server a
## IMPACTED VERSIONS:
xmltok_impl.c in Expat (aka libexpat) before 2.4.5
## WHAT ARE THE VULNERABILITIES
xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for w
context. xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator cha
Of principal concern are VOMS client and server packages, as well as HTCondor which also utilizes the VO
## WHAT YOU SHOULD DO
Sites running software which is dependent on expat should update urgently, including those running a VC
updated service [4][5][6]
## REFERENCES
[1] https://access.redhat.com/errata/RHSA-2022:1069
[2] https://access.redhat.com/security/cve/cve-2022-25235
[3] https://access.redhat.com/security/cve/cve-2022-25235
[4] http://mirror.centos.org/centos/7/updates/x86_64/Packages/
[5] https://security-tracker.debian.org/tracker/CVE-2022-25235
[6] https://people.canonical.com/~ubuntu-security/cve/2022/CVE-2022-25235
Please contact the OSG security team at security@opensciencegrid.org if you have any questions or conce
OSG Security Team
WHAT AND WHY?
WHAT TO DO?
HOW URGENT?
Does that mean our sites patch according to urgency?
No ☹


How does it work ?
querystring vs query-string
querystring
Readme
Explore
0 Dependencies
3,740 Dependents
3 Versions
querystring
This package has been deprecated
Node's querystring module for all engines.
Install
Install
$ npm install query-string
Not npm install querystring !!!!!
This module targets Node.js 6 or later and the latest version of Chrome, Firefox, and Safa
6/21/22
Brice Copy | Supply chain attacks


TIBHAR 5000


Juicy
100%

# Summary

- The first Thematic CSC on Security
- An ambitious and exciting academic programme
- Lots of interest from the community (HEP and outside)
  - 2 x more applications than places available
- Lots of interactions, discussions and networking
  - between the students and with lecturers
- Very good feedback (programme, format etc.)

- The plan is to organize this school regularly
  - every year, or every two years (depending on the resources)


CERN