https://indico.cern.ch/event/1297500/

Sebastian Lopienski, Kristina Gunne and David Crooks
On behalf of the school organisers

GDB meeting, 8 November 2023
https://indico.cern.ch/event/1225118/
A school with a long history

- The school was created in **1970**
  - 43\textsuperscript{rd} edition in 2022

- **2900** students of \textasciitilde80 different nationalities have followed the school
  - usually 60-80 per year
  - alumni web site: [https://cern.ch/CSC/history/alumni/](https://cern.ch/CSC/history/alumni/)

- The school has visited **22 countries**
  - [https://cern.ch/CSC/history/past-schools/](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
Thematic CSC on Security 2023
CERN Organizers

Kristina Gunne
Administrator

Andrzej Nowicki
Technical Manager

Alberto Pace
Director
No more support for external activities

All bookings, payments etc directly handled with the service providers (restaurants, transport, excursions etc)
Security CSC 2023

• **Applications → student selection**
• **October 8-14, 2023** (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 activity
  – **Saturday morning**: departure
• **Lectures and hands-on exercises**: ~30 hours in total
  – including student lightning talks etc.
• **Exam → diploma**
• **Optional social and sport activities**
• **Registration fee**: covers accommodation, meals, tuition, activities
  – depending on the accommodation (twin vs. single rooms, places)
Programme committee

https://indico.cern.ch/event/1297500/page/30008-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
- Ralph Niederberger
  - Forschungszentrum Jülich
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/1297500/page/30668-lecturers

Stefan Lüders
CERN

Sebastian Łopieński
CERN

Sven Gabriel
Nikhef, the Netherlands

Tom Dack
UKRI-STFC, UK

Barbara Krašovec
IJS, Slovenia

Daniel Kouřil
CESNET, Czech Republic

David Crooks
UKRI-STFC, UK
### Programme

https://indico.cern.ch/event/1297500/page/30007-academic-programme

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

- **30 class hours**
- **Lectures and exercises, but also group discussions and role-playing**
Programme

https://indico.cern.ch/event/1297500/page/30007-academic-programme

• Programme predominantly the same as last year
  – Some small tweaks including new tutors taking over where appropriate
• Allows for a gradual evolution of the programme over time
<table>
<thead>
<tr>
<th>Time</th>
<th>Monday, 9 October 2023</th>
<th>Tuesday, 10 October 2023</th>
<th>Wednesday, 11 October 2023</th>
<th>Thursday, 12 October 2023</th>
<th>Friday, 13 October 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00</td>
<td>Opening Session - Alberto Pace (CERN) Mie Dziewia (University of Split) Ivica Puljak (Mayor of Split)</td>
<td>Virtualisation and cloud security - Barbara Kralovec (US)</td>
<td>Container security - Daniel Koull (CESNET)</td>
<td>Digital forensics: essentials and data acquisition - Daniel Koull (CESNET)</td>
<td>Digital forensics - exercises - Daniel Koull (CESNET)</td>
</tr>
<tr>
<td>08:45</td>
<td>Security in research and scientific computing - Stefan Lupers (CERN)</td>
<td>Risk and vulnerability management - Sven Gabriel</td>
<td>Container security - exercises - Daniel Koull (CESNET)</td>
<td>Defensible security architecture: how to implement security principles - Barbara Kralovec (US)</td>
<td>Coffee break</td>
</tr>
<tr>
<td>09:45</td>
<td>Announcements</td>
<td>Announcements</td>
<td>Announcements</td>
<td>Announcements</td>
<td>Introduction to forensics - exercises - Daniel Koull</td>
</tr>
<tr>
<td>10:00</td>
<td>Coffee break</td>
<td>School photo</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10:06</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10:30</td>
<td>Identity, authentication, authorisation - Tom Dack (Science and Technology Facilities Council STFC (GB))</td>
<td>Logging and traceability - David Crooks (UKRI STFC)</td>
<td>Intrusion detection with SOC: deployment and operation - David Crooks (UKRI STFC)</td>
<td>Digital forensics: data analysis - Daniel Koull (CESNET)</td>
<td>penetration testing - exercise debriefing - Expedient Events</td>
</tr>
<tr>
<td>11:30</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
</tr>
<tr>
<td>12:15</td>
<td>Study time and/or daily sports</td>
<td>Study time and/or daily sports</td>
<td>Study time and/or daily sports</td>
<td>Study time and/or daily sports</td>
<td>Study time</td>
</tr>
<tr>
<td>13:45</td>
<td>Security architecture fundamentals - Barbara Kralovec (US)</td>
<td>Intrusion detection with SOC: threat intelligence, monitoring, integration and processes - David Crooks (UKRI STFC)</td>
<td>Incident response management - Barbara Kralovec (US)</td>
<td>Incident response - exercise - David Crooks (UKRI STFC) Sebastian Luperski (CERN) Tom Dack (Science and Technology Facilities Council STFC (GB))</td>
<td>Exam</td>
</tr>
<tr>
<td>14:00</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Incident response - exercise - Tom Dack (Science and Technology Facilities Council STFC (GB)) Sebastian Luperski (CERN) Romain Wertel (CERN)</td>
</tr>
<tr>
<td>15:15</td>
<td>Security operations - lecture 1 - Sven Gabriel</td>
<td>Student lightning talks</td>
<td>Intrusion detection with SOC and AAI - exercises - David Crooks (UKRI STFC) Tom Dack (Science and Technology Facilities Council STFC (GB))</td>
<td>Intrusion detection with SOC and AAI - exercises - David Crooks (UKRI STFC) Tom Dack (Science and Technology Facilities Council STFC (GB))</td>
<td>Incident response - exercise - David Crooks (UKRI STFC)</td>
</tr>
<tr>
<td>16:15</td>
<td>Security operations - lecture 2 - Sven Gabriel</td>
<td>Introduction to web penetration testing - Sebastian Luperski (CERN)</td>
<td>Incident response management - Daniel Koull (CESNET)</td>
<td>Incident response - exercise - David Crooks (UKRI STFC) Sebastian Luperski (CERN) Romain Wertel (CERN)</td>
<td>Incident response - exercise - David Crooks (UKRI STFC)</td>
</tr>
<tr>
<td>17:15</td>
<td>Network design - exercise - Barbara Kralovec (SU)</td>
<td>Penetration testing - exercises - Sebastian Luperski (CERN)</td>
<td>Incident response management - Daniel Koull (CESNET)</td>
<td>Incident response - exercise - David Crooks (UKRI STFC) Sebastian Luperski (CERN) Romain Wertel (CERN)</td>
<td>Incident response - exercise - David Crooks (UKRI STFC)</td>
</tr>
<tr>
<td>18:15</td>
<td>Dinner at MEDILS</td>
<td>Dinner at MEDILS</td>
<td>Dinner at MEDILS</td>
<td>Dinner at MEDILS</td>
<td>Walk to the restaurant</td>
</tr>
<tr>
<td>19:45</td>
<td>Outside dinner at Kaestl Sianica, Omis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18:30</td>
<td>Outside Closing Dinner at Kavanazone (Zona restaurant)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Participants

https://indico.cern.ch/event/1297500/page/30975-student-participants

26 students invited out of 29 applicants

• 6 female participants
• 11 different institutes,
• 13 nationalities (Belgium, Bulgaria, Canada, Estonia, Germany, Greece, India, Italy, Portugal, Romania, Spain, Ukraine, United Kingdom)
  – One sponsored student cancelled due to travel funds

Diverse, talented, passionate about science and technology
Lectures and exercises
Evening activities....
Excursion on the Cetina river
Excursion on the Cetina river – calm version
tCSC on security 2023: Student lightning talks

- Benedikt Bieringer (University of Münster) "Reverse engineering USB drivers (with PyUSB)"
- Robin Hofsaess (Steinbuch Centre for Computing) "Nelson Mandela"
- Roberta Miccoli (INFN CNAF) "An overview of the INDIGO IAM service"
- Elizaveta Ragozina (CERN) "Quantum Computing and Cybersecurity: Preparing for Tomorrow"
- Diogo Santos (CERN) "Model Security in Federated Learning"
- Shrija Rajen Sheth (CERN) "Dark web and Cyber Security"
- Roman Sumailov (CERN) "OSINT: What you post online” + “Privacy in modern cars”
- Leon Welchert (WWU Münster) "Encrypting Secrets with SOPS"
Feedback and reflections

- Feedback from the students was very constructive and useful
- Overall feedback was very positive
  - Maintained level from first iteration
- Need to process as we work towards the next iteration
  - Planned for the same time next year
  - Feedback included interest in material on dev-sec-ops, secure coding, etc…
- Topics we’re thinking about include the demographic of the cohort and how this factors into the evolution of the syllabus
Summary

• Second Thematic CSC on Security
• Predominantly similar programme with slight adjustments
• Lots of interactions, discussions and networking
  – between the students and with lecturers
• Maintained level of feedback from first time

• Next iteration planned for October 2024