

# tCSC on Security 2022: Back to (Security) School

Matt Doidge  
GridPP48  
August 31st 2022

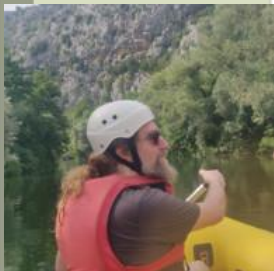
# The Thematic CERN School of Computing

- A branch of the long running CERN School of Computing
  - Covering specific themes (!)
  - This was the first school specifically on the theme of Security.
- Hosted at the Mediterranean Institute for Life Sciences (MedILS) in Split, Croatia.
- Over 30 students from lots of countries and many career-stages, 8 Lecturers, 30 hours (plus change) of classes, and an exam.
  - And a tour of the old city, a set of great lightning talks, a bunch of nice meals out and an afternoon of river rafting.

# So why did we send Matt here?

- Useful to get a “Student Eye’s View”.
- Aim was to crib notes for our own security training syllabus
  - What areas are useful to teach? What areas can you “get away” with point at some documentation?
  - How to frame subjects?
  - How best to present them?
  - What is relevant to **our** needs
    - Where **our** in this case is some superimposition of GridPP/IRIS/STFC/UKRI

# Timetable

Sunday, 19 June 2022	Monday, 20 June 2022	Tuesday, 21 June 2022	Wednesday, 22 June 2022	Thursday, 23 June 2022	Friday, 24 June 2022
	07:45 <b>Opening Session</b> - Sebastian Lopienski (CERN)	07:45 <b>Risk and vulnerability management</b> - Sven Gabriel (Nikhef)	07:45 <b>Container security</b> - Daniel Kouřil (CESNET)	07:45 <b>Digital forensics: essentials and data acquisition</b> - Daniel Kouřil (CESNET)	07:45 <b>Digital forensics - exercises</b> - Daniel Kouřil (CESNET)
	08:45 <b>Security in research and scientific computing</b> - Stefan Lueders (CERN)	08:45 <b>Virtualisation and cloud security</b> - Barbara Krašovec (ISJ)	08:45 <b>Container security - exercises</b> - Daniel Kouřil (CESNET)	08:45 <b>Incident response: policies and procedures</b> - Romain Wartel (CERN)	09:15 <b>Coffee break</b>
	09:45 <b>Coffee break</b>	09:45 <b>School photo</b>	09:45 <b>Coffee break</b>	09:45 <b>Coffee break</b>	09:30 <b>Introduction to forensics - exercises</b>
10:00 <b>Registration</b>	10:15 <b>Announcements</b>	09:50 <b>Coffee break</b>	10:15 <b>Announcements</b>	10:15 <b>Announcements</b>	
	10:30 <b>Security operations - lecture 1</b> - Sven Gabriel (Nikhef)	10:15 <b>Announcements</b>	10:30 <b>Intrusion detection with SOC: deployment and operation</b> - David Crooks (UKRI STFC)	10:30 <b>Digital forensics: data analysis</b> - Daniel Kouřil (CESNET)	10:45 <b>Announcements</b>
		10:30 <b>Logging and traceability</b> - David Crooks (UKRI STFC)			11:00 <b>Penetration testing - exercise debriefing</b>
11:45 <b>Lunch</b>	11:45 <b>Lunch</b>	11:45 <b>Lunch</b>	11:45 <b>Lunch</b>	11:45 <b>Lunch</b>	11:45 <b>Lunch</b>
	12:30 <b>Study time and/or daily sports</b>	12:30 <b>Study time and/or daily sports</b>	12:30 <b>Outdoor excursion</b>	12:30 <b>Study time and/or daily sports</b>	12:30 <b>Study time</b>
13:00 <b>Registration</b>					13:15 <b>Exam</b>
	13:45 <b>Security operations - lecture 2</b> - Sven Gabriel (Nikhef)	13:45 <b>Student lightning talks</b>		13:45 <b>Responding to security incidents as a community</b> - Romain Wartel (CERN)	14:00 <b>Coffee break</b>
15:00 <b>Welcome to the CERN School of Computing</b>	14:45 <b>Coffee break</b>	14:45 <b>Coffee break</b>		14:45 <b>Coffee break</b>	14:15 <b>Incident response - exercise</b> - Romain Wartel (CERN)
15:20 <b>Self-presentation: 1 minute per person</b>	15:00 <b>Identity, authentication, authorisation</b> - Hannah Short (CERN)	15:00 <b>Intrusion detection with SOC: threat intelligence, monitoring, integration and processes</b> - David Crooks (UKRI STFC)		15:00 <b>Intrusion detection with SOC - exercises</b> - David Crooks (UKRI STFC)	
16:15 <b>Visit of Split old town</b>	16:00 <b>Security architecture</b> - Barbara Krašovec (ISJ)	16:00 <b>Introduction to web penetration testing</b> - Sebastian Lopienski (CERN)			17:30 <b>Closing Session</b> - Sebastian Lopienski (CERN)
	17:00 <b>Network design - exercise</b> - Barbara Krašovec (ISJ)	17:00 <b>Penetration testing - exercises</b> - Sebastian Lopienski (CERN)			18:45 <b>Outside Closing Dinner</b>
18:15 <b>Outside Welcome Dinner</b>	18:15 <b>Dinner at MEDILS</b>	18:15 <b>Dinner at MEDILS</b>	18:15 <b>Outside dinner</b>	18:15 <b>Dinner at MEDILS</b>	
				19:00 <b>Special evening talk: Ransomware - and much more!</b> - Romain Wartel (CERN)	

We went rafting!

The 1-minute intro talks really set up the week.

# How to go over a week long course in 20 minutes?

- Most of the slides are [online](#) so I will focus on each lecturer and their subjects (with a link to the slides where I could get one), and pick out any prime points I've gleaned - focuses touched on in the talks, a few personal epiphanies or items I think particularly relevant to future training.



Hopefully I won't end up out of my depth!

# Security in Research and Computing - Stefan Lüders

Stefan's talk was an interesting and engaging framing of the security landscape and the problems we face on this front - and sadly weren't included in indico. Among the slides were some (depressing) results from some phishing tests at CERN - which is probably why the slides aren't public.

One thing that stuck with me was the recommended reading list:

- Who Moved My Cheese? (Spencer Johnson)
- Animal Farm (George Orwell)
- The Art of War (Sun Tzu)

No “Firewalls for Dummies” or “How to spot a Root-Hack”. Emphasis that your mindset is more important than your knowledge base.

# Security Operations - Sven Gabriel

- Covering CSIRTs and Security Teams, and their role and preparedness for Incident Response
  - CSIRT setup
  - Incident Response Preparation
    - Checklists!
    - (redundant) Infrastructure (as one of the examples showed)
    - Simulation
  - Audit Frameworks
    - ISO 27k, SIM3
  - CSIRT communities
    - TF-CSIRT
    - FIRST
- One of the points emphasised was the Importance of a **Mandate** (which in turn comes from Senior Management buy-in).
  - This sets goals, defines boundaries and “allows” authority.

## Identity, Authorisation, Authentication - Hannah Short

One of the best primers on the subject I've seen.

I'd encourage these slides becoming a first stop for anyone starting with AAI, or interested in, AAI.



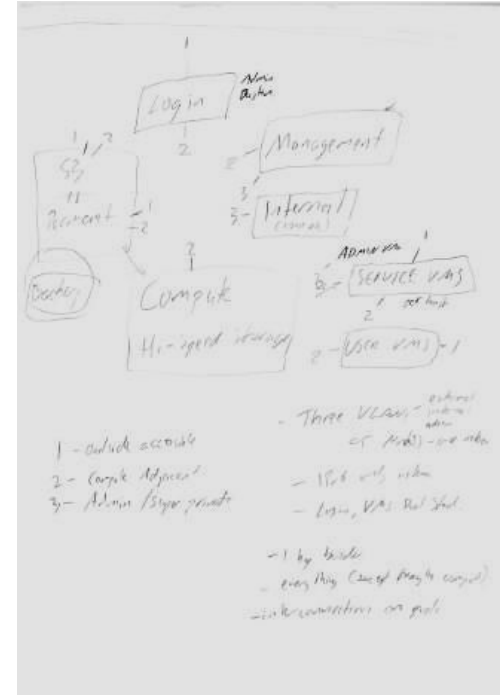
# Security Architecture - Barbara Krašovec

- If there was one session I had a recording of and could just play it back to you it is this one.
  - This is the foundation, the bones, the tofu-and-potatoes of good security practice, applicable to all.
- Security should be baked in from the start, with views on:
  - Defence in Depth
  - Zero Trust/Least Privilege design.
  - Risks/Threat Assessment
  - Location/Hardware/Network/OS Security
- Concept of CIS (or Critical Security) controls, developed by the Center for Internet Security
  - Implemented by many vendors.
  - Benchmarks available to turn these actions to configuration guidelines

# Network Design Exercise - Barbara Krašovec

A small hands on exercise where we were given a brief, then split into groups to design a network topology to fit that brief.

- This was very engaging exercise for everyone, but seemed especially useful for the earlier-career students who hadn't considered such problems before.
  - I would encourage a similar exercise for any new starter.
  - “Group Hypotheticals” seem like a very good way of creating engaging exercises without needing the infrastructure of other security exercises.



Although it appears I encrypted out team's design with my own handwriting.

# Risk and Vulnerability Management - Sven Gabriel

- The other “these are the fundamentals!” subject.
- STRIDE model of what can go wrong (Spoof, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).
- Risk Analysis is an ongoing process (like documentation maintenance).
  - But need to keep within your **mandate**.
  - Asset valuation-> Threat/Vulnerability Mapping -> Risk Calculation -> Risk Mitigation
  - There are various ways of codifying and quantifying these steps.
- Vulnerability management was done from an EGI/Linux perspective.
  - Scope is also important here.
  - Also an ongoing, cyclic process.
  - Policies are important - they grant guidance and give authority.

# Virtualisation and Cloud Security - Barbara Krašovec

A whistle stop tour of the challenges of securing a virtualised environment.

- “Plain” virtualisation or IaaS Cloud
- A lot of the principles in the earlier session apply.
  - The obvious problem is that users might roll out infrastructure that don't abide by (or even know of) these principles.
  - Emphasis on hardening, monitoring and containing.
    - Protect against breakouts and cross contamination.
    - Monitor for weird behaviour and user machines doing silly things.
    - Segment networks virtually and encrypt as much internal traffic as possible.
  - Of course education of the IaaS user base can help!

## Logging and Traceability - David Crooks

- Overview of logging - from the basics, to the importance of central logging, to Data Protection considerations (David is not a lawyer).
  - The latter is important when it comes to log retention.
- Moves on to the interlocking concept of traceability
  - A lot of cross-referencing between talks.
- Tools to consider beyond rsyslog - ossec/wazzuh, osquery.
- And onto network tracing - netflow/sflow, and then Zeek (a bit of a spoiler for David's later talks).

This is another set of “101” slides, the material is relevant to all.

# Intrusion Detection with SOC ([part 1](#) and [part2](#))- David Crooks

- Split between a more generic introduction to the processes and the “MISP/Zeek” specific deployment and operation scenario.
- Introduction to Threat Intelligence and “responsible sharing” (TLP, Chatham House rules).
- Rolls in concepts from the Logging and Traceability session.
- Explains SOC using the RAL Zeek instance as a base, and how it rolls into MISPs.
  - Baseline to Build Your Own.

TBH I’ve probably gone over these slides more then I needed, as hopefully David will give us all a repeat showing at a future UK training session.

# Introduction to Web Penetration Testing + Exercises - Sebastian Lopienski

- Some classic web testing material - proceeded by some all important ethics and rules (in a crude nutshell, make sure you're being a "White Hat").
  - The mandate thing comes in again.
- A reminder of the importance of keeping our web interfaces secure.
  - Even if an attacker can't do any real damage to your systems, these incidents almost always lead to reputational damage.
- A lot of classic techniques are explained - from specific tools to just using the browser's features.
- Also a nice list of top 10 attack vectors.

The exercises were a lot of fun - but I felt this was "specifically useful" but not "generically useful" - which is a conclusion I came to a few times.

## Container Security + Exercises - Daniel Kouřil

- The material is also a good primer on containerisation.
- “Container escape” is one of the prime threats, and one of the focuses of the exercises.
- The importance of keeping things patched (and correctly configured) has an even stronger emphasis when dealing with containers.
  - Applies to the host, containerisation and the images.
- (Naturally) Strong call back to the Virtualisation & Cloud Security session.

Daniel’s exercises were presented using a “Capture the Flag” style, where each exercise provided the key to the next (with a inbuilt hint system). This was a very popular format among the students.



# Digital Forensics: [Essentials and Data Acquisition](#), [Analysis](#), [Exercises](#) - Daniel Kouřil

This was split into multiple sections - the essentials, data acquisition and data analysis. Then followed up by practical exercises.

- The section on Data Acquisition is the most vital for everyone - it covers acquiring data for forensics in a way that causes minimal possible disruption or corruption of the data.
  - The data analysis portion of a real event could (likely should) be handed off to “experts”.
- Emphasis that in case of emergency don't panic!

Again the exercises use the “Capture the Flag” format, which again proved very popular and user friendly.

# Incident Response and Responding to Incidents as a Community - Romain Wartel

- One of the first points Romain stressed was the importance of maintaining an Address Book.
  - Not just of formal contact points, but of informal, **trusted** contacts (like the kind you make at a Security Training week).
- Another emphasis is preparation ahead of time - policies and procedures.
  - “When” not “If”.
- Moves on to responding as a community.
- The final section on “Handling Severe Cases” was quite sobering.

## Intrusion Detection with SOC Exercises - David Crooks

- First thing - Portainer is really cool.

For these exercises David guided us through setting up a interconnected mini-SOC (MISP and Zeek with an Opensearch dashboard) using Portainer Containers.

It was an incredibly useful exercise, especially for helping visualise what goes on in a SOC and with threat intelligence sharing.

Again hoping for an “in-house” repeat performance at a future UK event.

# Incident Response Exercise - Romain Wartel

I'm not going to spoiler this one as for one we might want to repeat it in the UK, this was the closing session of the week.

We split into teams, each team playing a role involved in an incident (from local admins to various level of Security Team, and others). All teams were partially anonymised by the use of code names. Each team brief only had the role, their goal, and the “identities” of a few other teams. Communication between teams was restricted to using mattermost alone.

A bit of time crunch made things quite frantic! It was useful, insightful, and fun.

# Conclusions

- It was a fantastic, useful week, which could have easily been a fortnight.
  - Every session was an exceptionally dense whistlestop tour of the subject matter.
  - Credit to the lecturers and organisers that they still kept things interesting and useful.
- I see fairly firm boundaries between subjects that are essential for all, and subjects that are essential for some.
  - By all I mean all - or at least anyone who opens a terminal at least semi-regularly.
  - By some I mean skills that need to be present in a community, but not possessed by all.
- The “Essential for all” list would include:
  - Security Architecture Awareness (from firewalls to central logging).
  - Vulnerability and Risk Assessment.
  - Basics of Digital Forensic capture.
  - Incident Response Procedures and Policies.

# A Final Thought

- There is a lot to be said for the benefits of running courses such as this in a face-to-face setting.
  - There's the usual benefits of the increased bandwidth.
  - But the added benefit, particularly for a security community, is the increased trust simply garnered from meeting people in a physical setting.
    - And it helps if that's a nice physical setting :-)

