



WLCG OTF Security: Prevention, Detection Architecture & Risk

David Crooks



Agenda



- Prevention
 - CERN School on Security
- Detection
 - SOC Working Group
- Architecture and Risk
 - Token-based workflows

Prevention: Skills and Training



- Providing our users/researchers, service providers and cybersecurity professionals the right training is essential
 - Including building effective cybersecurity culture
- Focus here on system managers expected to be involved with security at some level
- If you are deploying a service, what do you need to consider for security?

Thematic CERN School: Security



- Third instance of this school
 - 2022 and 2023 in Split, Croatia
 - 2025 in Abingdon, UK
- Follow same overall structure as before
 - Protection and Prevention
 - Detection
 - Response

Thematic CERN School: Security



Thematic CERN School of Computing on Security 2023 from Sunday 8 October 2023 (11:00) to Saturday 14 October 2023 (11:00)						
Sunday 8 October 2023	Monday 9 October 2023	Tuesday 10 October 2023	Wednesday 11 October 2023	Thursday 12 October 2023	Friday 13 October 2023	Saturday 14 October 2023
	09:00 Opening Session	08:45 Virtualisation and cloud security - Barbara Krašovec (IJS)	08:45 Container security - Daniel Kouřil (CESNET)	08:45 Digital forensics: essentials and data acquisition - Daniel Kouřil (CESNET)	08:45 Digital forensics - exercises - Daniel Kouřil (CESNET)	08:45 Departure
	09:45 Security in research and scientific computing - Stefan Lueders (CERN)	09:45 Risk and vulnerability management - Sven Gabriel	09:45 Container security - exercises - Daniel Kouřil (CESNET)	09:45 Defensible security architecture: how to implement security principles	10:15 Coffee break	
	10:45 Announcements	10:45 Announcements	10:45 Announcements	10:45 Announcements	10:30 Introduction to forensics - exercises - Daniel Kouřil	
	11:00 Coffee break	11:00 School photo	11:00 Coffee break	11:00 Coffee break	11:45 Announcements	
	11:30 Identity, authentication, authorisation	11:05 Coffee break	11:30 Intrusion detection with SOC: deployment and operation - David Crooks (UKRI STFC)	11:30 Digital forensics: data analysis - Daniel Kouřil (CESNET)	12:00 Penetration testing - exerci...	
	12:30 Lunch	11:30 Coffee break	12:30 Lunch	12:30 Lunch	12:30 Lunch	
12:45 Lunch	13:15 Study time and/or daily sports	12:30 Lunch	13:15 Outdoor excursion	13:15 Study time and/or daily sports	13:15 Study time	
14:00 Registration	14:45 Security architecture fundamentals - Barbara Krašovec (IJS)	13:15 Study time and/or daily sports		14:45 Incident response management - Barbara Krašovec (IJS)	14:15 Exam	
	16:00 Self-presentation: 1 minute per person	14:45 Intrusion detection with SOC: threat intelligence, monitoring, integration and processes		15:45 Coffee break	15:00 Incident response - exercise	
	16:40 Welcome to the CERN Sc...	15:45 Coffee break		16:15 Intrusion detection with SOC and AAI - exercises - David Crooks (UKRI STFC) Tom Dack (Science and Technology Facilities Council STFC (GB))	16:30 Coffee break	
	17:00 Transport to Split	16:15 Security operations - lecture 1 - Sven Gabriel		18:45 Outside dinner at Kastil Stanica, Omis	16:45 Incident response - exercise	
	17:15 Security operations - lecture 2 - Sven Gabriel	16:15 Student lightning talks			18:00 Closing Session - Alberto Pace (CERN)	
	18:15 Network design - exercise - Barbara Krašovec (ISJ)	17:15 Introduction to web penetration testing - Sebastian Lopienski (CERN)			19:00 Walk to the restaurant	
	19:15 Dinner at MEDILS	18:15 Penetration testing - exercises - Sebastian Lopienski (CERN)			19:30 Outside Closing Dinner at Kavanazona (Zona restaurant)	
		19:15 Dinner at MEDILS				

2023
timetable

Thematic CERN School: Security



- Follow lifecycle of service deployment through initial architecture and consideration of risk and service hardening
- Lectures and hands-on exercises
- Allow syllabus for security training to be established and evolved over time

Detection: SOC WG

- SOC working group focuses on developing reference designs for Security Operations Centres for R&E organisations
 - Aggregation of security monitoring data correlated with threat intelligence
- Last year a total of three hackathons!
 - March @ CERN:
 - <https://indico.cern.ch/event/1370544/>
 - HEPiX:
 - <https://indico.cern.ch/event/1450798/>
 - December @ Jisc offices, UK:
 - <https://indico.cern.ch/event/1441326/>



Detection: SOC WG

- Consolidate documentation and guidance:
 - <https://wlcg-soc-wg-doc.web.cern.ch>
- WLCG focus on how we can allow broad range of sites to benefit from threat intelligence
 - "80% SOC"
 - pDNSSOC, originally developed by CERN Security Team
 - Correlation of DNS data with threat intelligence and flexible deployments
 - Testing underway

Architecture and Risk: Token Workflows



- Extensive work ongoing to establish Token-based workflows involving Experiments, Software Developers, IAM team...
- As these approaches develop, important to have collective view of landscape including range of perspectives from different stakeholders
 - Including operational security
 - Establish requirements to support security development of architectures and approach

Architecture and Risk: Token Workflows



- Following dedicated operational security for token workflows sessions at EUGridPMA meeting at CERN last week
 - Including representation from CERN IAM team and ATLAS
- Propose focused, time-limited piece of work to create a white paper (or similar), gathering perspectives from stakeholders to support ongoing, risk-based decision making
 - Very early stages
 - Anticipate using existing vehicles to work on this
 - Focus on bringing in different viewpoints to inform collective whole