

Incident Handling

Monday, 22 March 2021 11:00 (1h 30m)

With the uptake of different virtualization technologies also in traditional data processing workflows the security landscape gets increasingly heterogeneous. Container technology allows users and user communities to easily ship complex data processing environments to the federated resources. While using containers adds a lot of flexibility for the resource usage, it also increases the possible attack surface of the infrastructure. The goal of this training session is to discuss selected aspects related to containers and present potential security threats. We will focus mainly on Docker and its typical use-cases. The main principles, however, will be applicable also for other container technologies. The workshop is not meant as an exhaustive training session covering every possible aspect of the technology. Its purpose is to point out some typical problems that are important to consider, some of which are inspired by real-world security incidents.

The workshop will be organized as a mixture of technical presentations, interleaved with shorter sessions where attendees will be able to practice the ongoing topics on a couple of hands-on exercises.

Presenter: Dr KOURIL, Daniel (Masaryk University)

Session Classification: Security Workshop