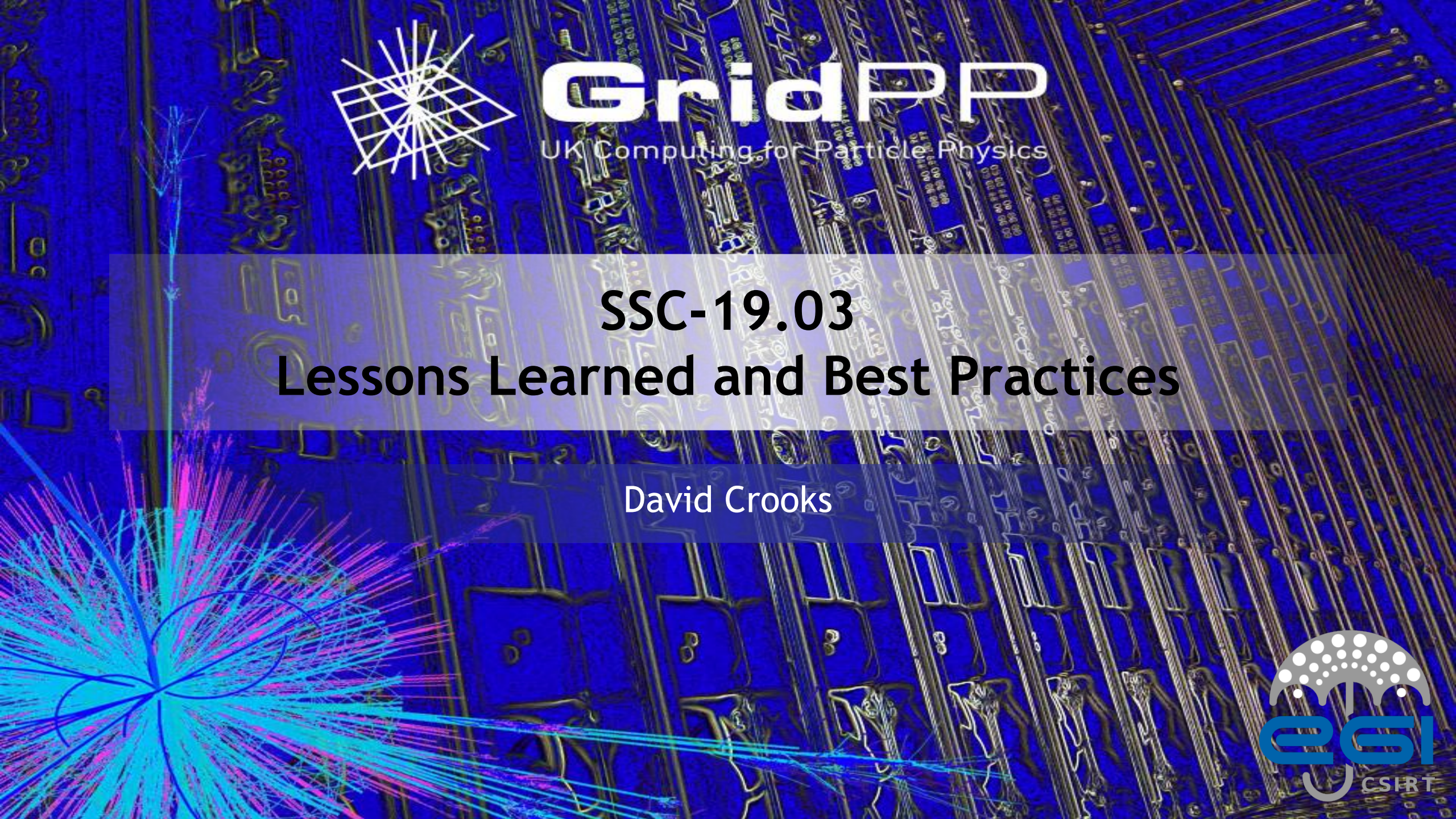
GridPP
UK Computing for Particle Physics
SSC-19.03
Lessons Learned and Best Practices
David Crooks
CSIRT

GridPP
UK Computing for Particle Physics

Overview

- Quick recap of SSC
- Outcomes from reports
- Ongoing work

EGI CSIRT

SSC Recap

- Discussed in Abingdon
- Malware injected via LHCb DIRAC, forming botnet throughout EGI Infrastructure
- Suspension on CE and SE measured independently
- 62 resource centres took part, 17 in the UK

Overall status

- All sites engaged well and appropriately, and acted as a credit to GridPP

SSC reports

- Three sections:
  - Reporting/Communications
  - Containment/Operations
  - Forensics

- Scores are formative/diagnostic; *i.e.* may include other elements as well as site response
  - Behaviour of software
  - SSC framework
  - Other parts of SSC

Common elements

- T_0 is the broadcast on afternoon of Friday 15th (in all cases)
- Calculations are based on working hours
  - Uses timezones recorded in GOC DB
  - Assumes 0900 – 1700

$$Score = Min\left(100, DONE \times 100 \times \frac{Target}{Actual}\right)$$

- Forensics does not use time for calculation

Reporting/Communications

- In this case, based entirely on the first report to the CSIRT from a site
- Any communication before broadcast gives “Actual” time as zero
  - Sites responding early get some bragging rights, but scoring is based on the broadcast
- Average 94/100 (mean 73)
  - Most sites responded within 4 working hours
  - Remainder on Monday afternoon, within ~1 working day
  - Excellent results

- Key requirement – **please respond to CSIRT emails**
  - If this is to say “I’m swamped, but I’ve seen your email”, that’s perfect

Containment/Operations

- Suspension measured by independent process checking CEs and SEs every 30 minutes

- User suspended (CE)
  - Average 94 (mean 92)
  - Identified a couple of issues to run down

- User suspended (SE)
  - Average 48 (mean 62)
  - certainly down to DPM issues; non-DPM sites were better
  - Followed up during challenge (Sam/Raul)

Containment/Operations

- Bot last seen
  - Average 98 (mean 90)
  - Good containment!
- Bot last seen also detects if payload ran at site

- Key requirement: **Check deployment of, and test, suspension methods**
  - Task for both sites and security teams (see later)

Forensics

- Details of payload running at site
- Found user
- Found Job IDs
  - Via DIRAC or direct submission (cream only)
- Found UUID in binary (filename, etc.)
- Found inner (memory) UUID
  - Generated at runtime, only findable in memory dump
  - We believe no site found this (or at least reported it)

- Average 26 (mean 27)
  - However, health warning!

Forensics

- As we know, timing of challenge meant that many jobs died over weekend, thus robbing many sites of opportunity to perform forensics

- This area is different in that we don't expect all sites to do all the forensics
- Communications and containment are the most important
- CSIRT making the malware available ~now to allow sites to take another look
  - recommend that UK sites take up this offer where appropriate

- Key requirement: **Sites need to be able to trace jobs from different submission methods**
  - Significant task for training and documentation

Lessons learned

- Timing was not great, either for sites or VO (undergoing operational upgrade that week).
  - Entirely likely that incidents occur/are reported late on Friday or overnight, but balance this with making challenge useful
- First response time was excellent
- CE suspension results suggest that this is generally in good shape
- SE suspension results suggest that work is needed
  - Good documentation on suspension process for different storage types
  - Resolve DPM issue or use workaround

- Generally, structured testing of suspension systems is essential

Lessons learned (CSIRT)

- Timing
- VO CSIRT communications didn't work as well as it should
  - Some procedural improvements on VO side
- Important in new split traceability world
  - Applies to *all VOs*
  - What to do in UK for VOs who may not have security team?
    - IC act as proxy for information available in GridPP DIRAC?
- Handling the large volume of tickets
- Some refinement of communication templates

Ongoing work

- Training at HEPSYSMAN
  - https://indico.cern.ch/event/721692/
  - Also has links to all forensics slide decks used, including on SSC malware
- Intention to make malware available to sites
  - Particularly for sites that didn't see it/didn't have a chance to analyse in place
  - Already spoken to some, if interested please talk to me so that we can coordinate/check if we want anything in place beforehand
- Generally, most important parts are not elaborate
  - Documentation, Procedures, Training, Awareness
- Suspension testing
  - As discussed over the summer, starting up suspension testing on CEs
  - SEs coming soon
  - Manual testing first with a view to regular, structured testing

Key requirements

- Please respond to CSIRT emails
- Check deployment and test suspension methods
- Sites need to be able to trace jobs from different submission methods

This week

- Please talk to me about your results/if you would like to have access to the malware at your site

- Questions?