Open CSIRT Foundation

CCoP : CSIRT Code of Practice

Don Stikvoort, TF-CSIRT/TI Associate Member

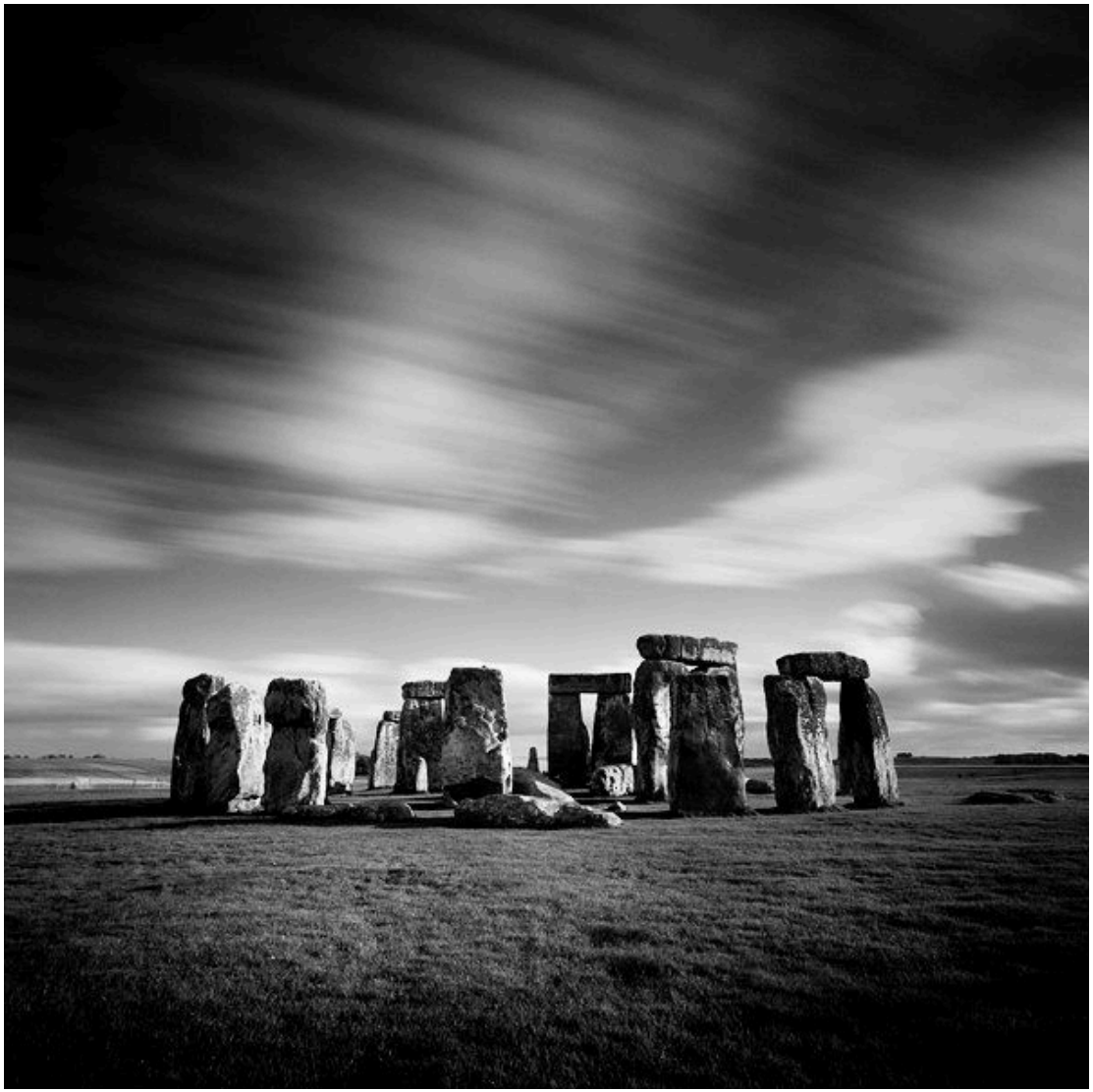
CCoP version 2.3 final draft

Monday 15 May 2017

CCoP background

- Our ethics are not all the same
- People will do weird things, by all standards
- People will do weird things, by professional standards
- But what are the standards?

- Parker/Cormack/Maj/Stikvoort drafted CCoP
- 2005 ➔ Version 2.1 approved by TI accredited teams
- SHOULD criterion = strong recommendation
- 2009 ➔ SIM3 parameter H-1 : Code of Conduct/Practice/Ethics
- Starting point for discussion



v2.1 of 2005 needed update

- The world and the net are a different place
- Team who wanted to charge a peer for basic CSIRT work
  - Not in the CCoP
- Time for an update anyway
  - Experience from setting up teams and doing certifications

- Update started in 2016
  - Dave Parker ➔ Klaus-Peter Kossakowski
- Excellent suggestions, but :
- KISS

v2.1 → v2.3 final draft

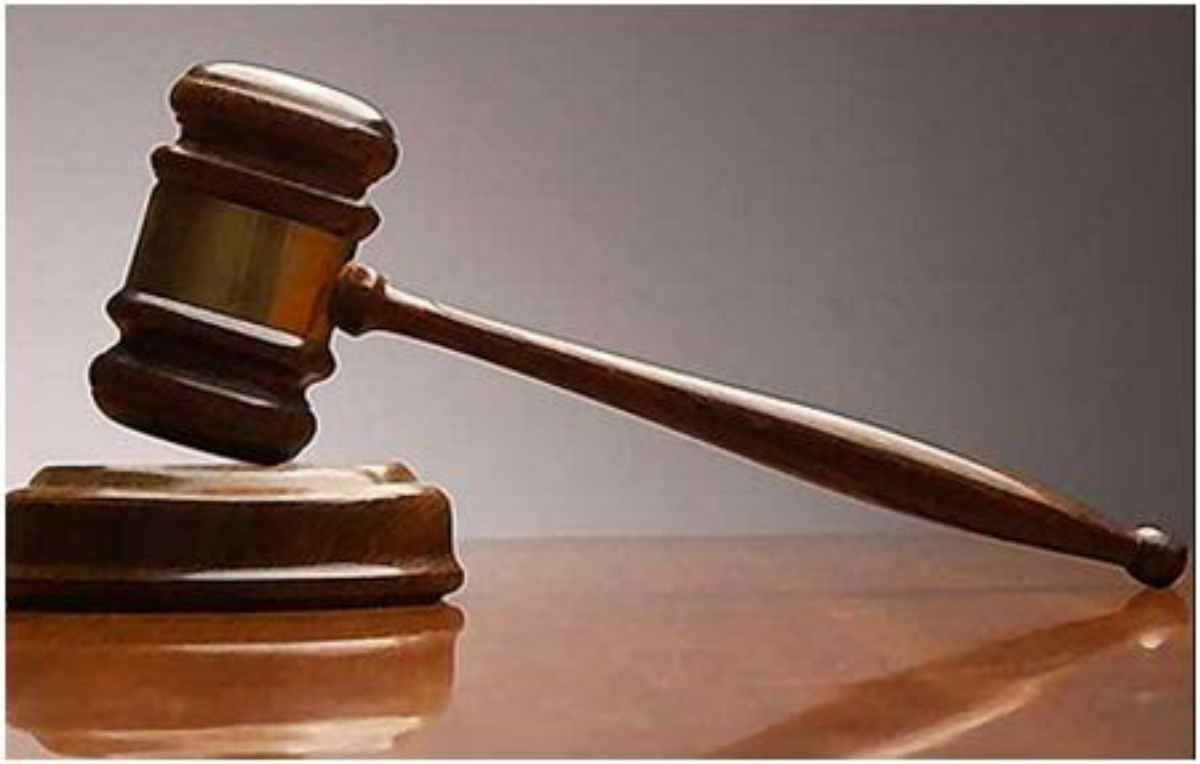
- "Definitions"
  - Added "vulnerability", "CSIRT" and "team members"
  - CSIRT more widely defined, including PSIRTs and SOCs
  - Using literal RfC-2119 definitions for MUST and SHOULD
- Add "Starting Points"
  - CSIRTs work peer-to-peer with due care and without cost recovery
  - Clarification of "peer" = other members of the CSIRT cooperations the team is a member of
    - "with the exception of the case where a cooperation is explicitly based on different standards"
  - Benefit of the doubt for valid reporters
    - "any CSIRT or party acting as such" … "with the exception of the case where the relationship between both is different and bound by agreement."

v2.1 ➔ v2.3 final draft

- "The Team"
  - Added: "The team will, considering its stated services towards its constituency, take appropriate incident management action when it is notified of an incident in its constituency."
- "Team Members"
  - No changes except change throughout of staff ➔ team members
- "Information Handling"
  - Terminology improvements only
- "Service Specific Requirements"
  - Modular approach dropped, content kept and improved ➔
  - "Vulnerability Handling Requirements"

v2.1 → v2.3 final draft

- "Vulnerability Handling Requirements"
  - New: introduction of *responsible* disclosure
  - New: "The team SHOULD publish their responsible disclosure practice, or spread it on a need-to-know basis, and encourage the adoption and use thereof. "
  - New: "Any public disclosure of what could be considered critical vulnerabilities should not only follow the guideline of 7.4, but also the team SHOULD seek to achieve a coordinated effort within the CSIRT community – and especially any such disclosure should be done as a concerted and synchronised effort."
    - 7.4 : "Where appropriate, and considering the team's security requirements, the details of the vulnerability and any associated research MUST be provided to the relevant vendor(s) for assessment and remediation at the earliest opportunity."



Next steps

- Version 2.3 final draft will be sent round 16 May
  - Request for final comments < 21 June
- Consolidation of comments into version 3.0
- Version 3.0 will be sent to Accredited teams < 21 August
- Proposal to vote in Stockholm 21-22 September :
  - Keep adherence to CCoP as SHOULD for Accreditation
  - Change CCoP v2.1 into v3.0

[Draft and final version will also be shared in new Ethics SIG of FIRST]

THANK YOU FOR YOUR ATTENTION