Some Key Terms for Incident Management

draft-davis-nmop-incident-terminology

Nigel Davis (ndavis@ciena.com)
Adrian Farrel (adrian@olddog.co.uk)

NMOP Working Group : IETF-119 : Brisbane : March 2024

Why and What?

- Clarity, consistency, portability - all documents on incident management in IETF need to
  - Use the same key terms
  - Have a common understanding of these key terms
  - Have single common definition to ensure shared clarity of meaning for each term
- Do need:
  - A small set of key terms
  - Simple definition to clarify meanings
  - No dependency on undefined terms
  - No circular definitions!
- Don’t need:
  - All possible terms
  - Very detailed explanations
- Would help to be consistent with other SDOs and forums, but…
  - Beware when they are not all consistent between SDOs and within single SDOs!
  - Good to use established IETF terms if they exist
  - It may help to show mapping between terminologies in some cases

A Stake in the Ground

- Revision -00 is only a first attempt
  - Fully expect to have to make changes
  - Comments already received on list
- Next steps
  - Adapt definitions based on comments received
    - What is missing *that is needed*
    - Hope for more comments and opinions
  - Do more serious review of other work
  - Think about the scope
    - Network only?
    - Add security, applications, protocols?
  - Sharpen the stake

Those key terms

- Resource
- State, Condition, Change, Occurrence
- Event, Incident, Problem, Cause
- Detect, Alert, Notification, Alarm
- Transient, Intermittent

What the authors think…

- The authors think that this is foundational for the working group
- We hope other drafts will align themselves
- We think it would be wise to adopt this into the WG and polish it
  - It *could* be merged into another document, but we think this is not wise