Using incidents to develop expertise

Nora Jones

How do you know when an incident is occurring?

How do you know when an incident is occurring?

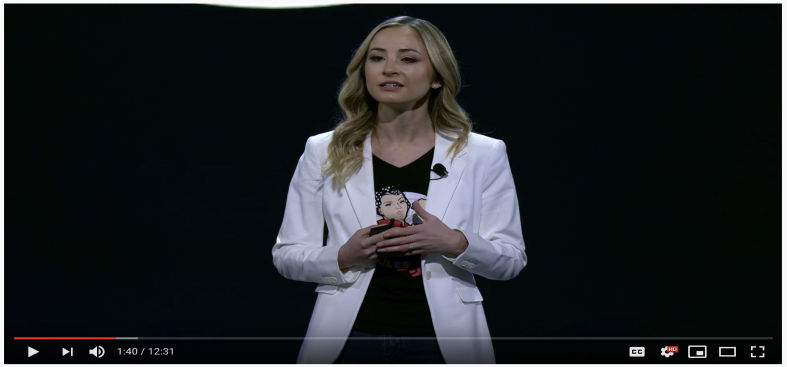
You observe it.

How do you know what actions to take when an incident is occuring?

Human Factors & System Safety

FACULTY OF ENGINEERING, LTH

MSc Programme | Learning Laboratories | FAQ | Lund | Staff | Videos



AWS re:Invent 2017 - Nora Jones Describes Why We Need More Chaos - Chaos Engineering, That Is

@nora_js

Human Factors and Systems Safety

Aren’t you all just the “no” people on Twitter?

Hopefully not!

“Resilience is not about reducing errors. It’s about enhancing the positive capabilities of people and organizations that allow them to adapt effectively and safely under pressure”

- Dekker, Woods, Cook

John Allspaw’s Heuristics

Heuristic 1: “What is the first thing you ask yourself in an incident?”

“What changed?”

Heuristic 2: Widen the search

Heuristic 3: Convergence Searching

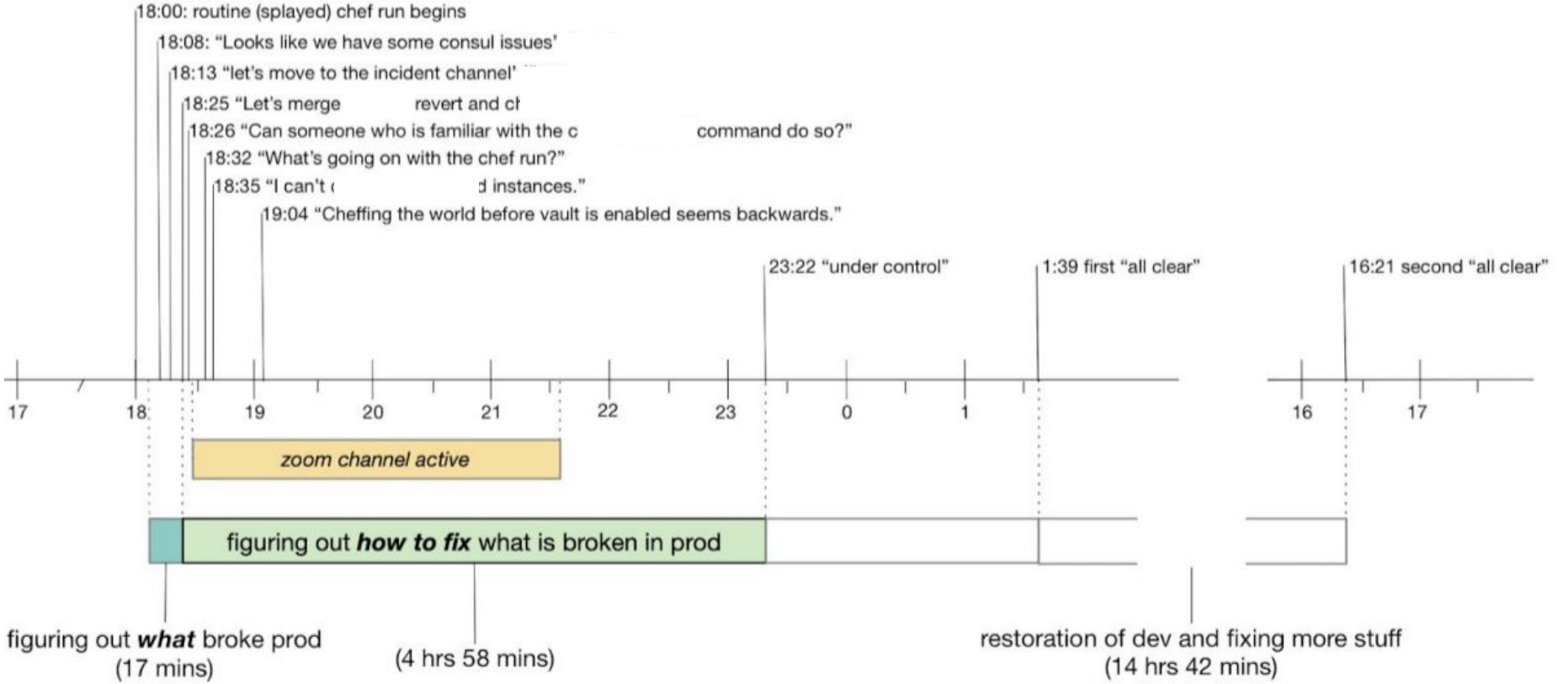
How do you know what to do when an incident is occuring?

Experts use their knowledge base to recognize typicality.

“I’ve been here before” phenomenon

A case: Unexpected Self-Inflicted DDoS of service discovery infrastructure

How do people work when everything is underwater?


18:00: routine (splayed) chef run begins
18:08: "Looks like we have some consul issues'
18:13 "let's move to the incident channel'
18:25 "Let's merge revert and cl
18:26 "Can someone who is familiar with the c command do so?"
18:32 "What's going on with the chef run?"
18:35 "I can't (d instances."
19:04 "Cheffing the world before vault is enabled seems backwards."
23:22 "under control"
1:39 first "all clear"
16:21 second "all clear"
17
18
19
20
21
22
23
0
1
16
17
zoom channel active
figuring out how to fix what is broken in prod
figuring out what broke prod
(17 mins)
(4 hrs 58 mins)
restoration of dev and fixing more stuff
(14 hrs 42 mins)

Key Questions after every “charged” incident

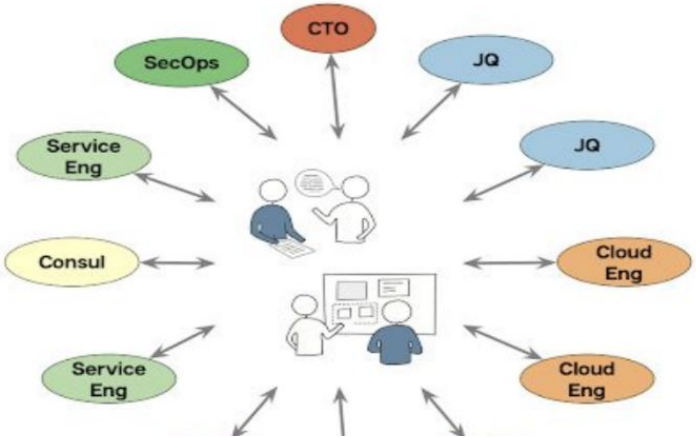
- Who to interview?
- What to focus on in those interviews?
- What to focus on in a report?
- Who to share this report with?

incident

Slack transcripts

#incd-xxxx
#devel-yyyy
#zzzz
etc.

Initial analysis of incident channel(s) to identify opportunities and initial interviewees.



Individual Interviews...

- what their understanding of the event was
- what stood out for them as important
- what stood out for them as confusing/ambiguous/unclear
- what they believe they know about the event and how things *actually* work that they believe others don't
- etc.

Cognitive Interviews

Knowledge and perspective gleaned in early interviews can point to important new topics to continue exploring:

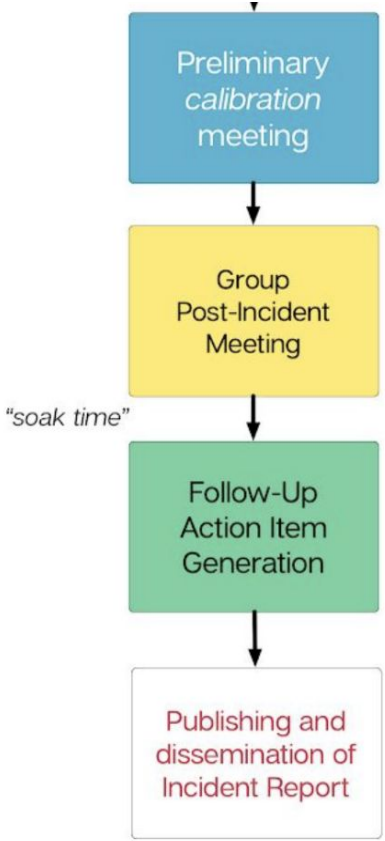
- Relevant ongoing projects
- Past incidents
- Past experiences

Iteratively informed and contrasted the results of the cognitive interviews with other sources of data.

My biggest finding?

Expertise on the service discovery infrastructure was **scattered and limited** throughout the organization.

How I formatted the after-incident “process”



Re-playing what was heard/understood in the analysis thus far with experts, re-calibrating understanding with discussion/diagrams

Focused and facilitated discussion on central themes/observations of the case with broader groups

Focused and facilitated discussion on diverse sets of ideas/notions/tasks to address future needs based on what’s been understood, including those already taken at this juncture.

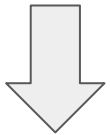
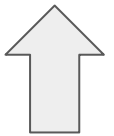
Synthesizing analysis, findings, and discussion points into a collection that is intended to have *lasting value* beyond this specific incident.

Used the report as an opportunity to teach the organization about this piece of infrastructure.

Experts in the audience?

“With experience, a person gains the ability to visualize how a situation **developed** and can imagine how it’s going to turn out. Experts can see **what is not there.**”

- **Seeing the Invisible (Klein and Hoffman)**

Performance Improvement = Errors  + Insights 

Seeing What Others Don't - Gary Klein

Incident Analysis can fuel this insight generation.

Actual examples from how incident analysis fueled insight generation.

“By the time, as the reader, that I get to the "Impact of Change" section (pg15), it's like hearing different pieces of a symphony and finally hearing them all together. Really awesome to get to this point and have a better understanding.”

“I left the document feeling like a satisfied customer who walked into a butchershop to ask the butcher how the sausage is made.”

“Never have I ever seen such an in-depth analysis of any software system that I've had the pleasure to work with. Anyone who will read this document should come out more informed and even have a better understanding of the services that started off as having 1 or 2 persons understanding. This is a beautiful educational piece that anyone who plans on using $X should read.”

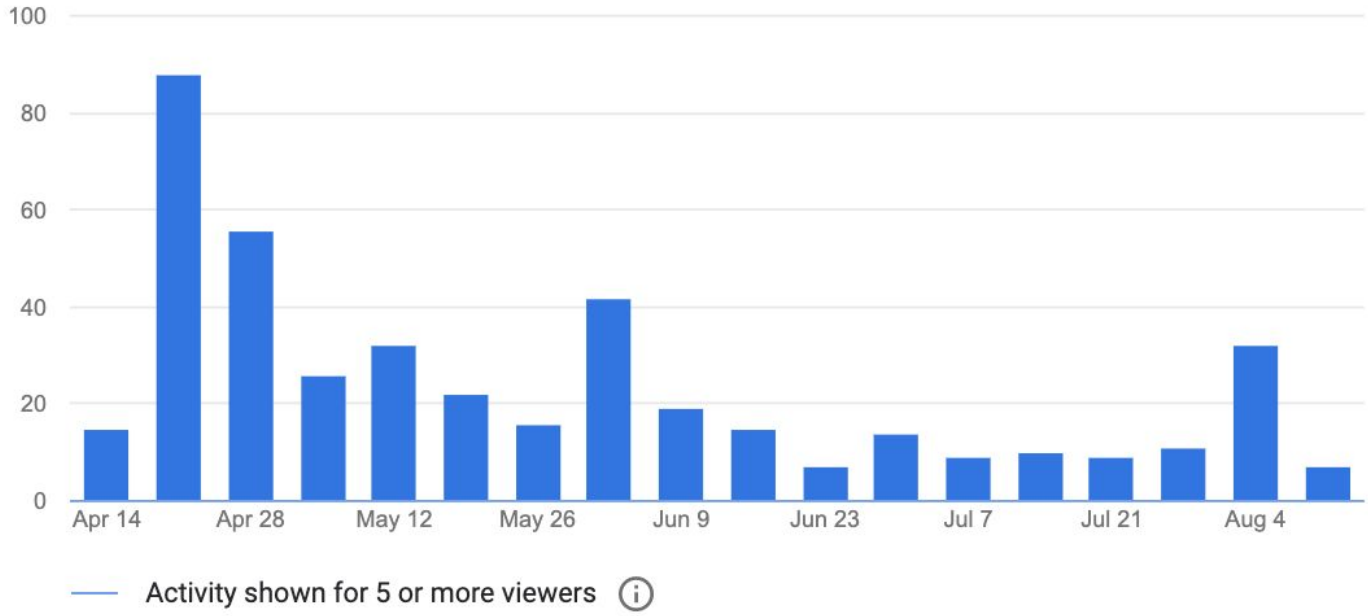
"I just changed the way I was proposing to use $X in a design as a result of reading this document"

I really appreciate how the document is written with so much context and definitions of terminology provided. It's very accessible. Sometimes reading postmortem docs when I have a cursory familiarity with the terminology but it's not actually defined, my incorrect mental model warps my reading of the document. I hope people take the time to read it, given its length. It was very much worth my time to do so.

Total **202** unique viewers

All time

Weekly unique viewers



Are your incident reports written to be filed or written to be read?

Questions you can ask to elicit feedback

- Was there something in this that strikes you as different from the 'normal' way you've seen postmortem write-ups?
- Any information we should add?
- Will we get pushback on things in there?
- Will we get pushback on things not in there?
- Anything in here that you didn't know before about $X?
- Is it easy enough to read that it keeps your interest after the summary bits at the top? (if not, what might make it more compelling?)
- Does this write-up lead you to ask more/different questions about various bits that are involved? (if so, what are they?)

“Expertise takes time and space.

Create that time and space.”

- J. Paul Reed

Despite all the automation in the world and all the testing — we will never get to zero incidents, we will always have surprises.

Those **surprises will be costly** if organizations don’t invest time in developing and honing the adaptive capacity of each engineer in the organization.

So, my challenge and question to you is, how are you developing this?