Incident Response

How I learned to stop worrying when everything is on fire

Michael Ansel
Who is this guy?

- **Pratt** 2011, ECE/CS
- **NetApp**, Solutions Architect for storage appliances
- **Box**, Site Reliability Engineer for cloud storage
- **Twitch**, Security Engineer for live streaming -> Management
STORY TIME
Why is incident response important?
The best solution is avoiding the problem, right?
Space shuttle
Challenger/Columbia Disasters

Okay, but just, like, fix it and move on.
ONE DOES NOT SIMPLY

FIX THE ISSUE
Spaceteam
How do you make incidents less difficult?

- Write down what is happening
- Fix the Failure not the Fault
Write down what is happening
Fix the **Failure** not the **Fault**
Error Propagation
https://pld.ttu.ee/IAF0530/16/avi1.pdf
Moore County Substation
Moore County power outage

- Fault: a bullet was fired at a transformer
- Error: oil leaked out of the radiator
- Error: transformer overheated
- Error: transformer entered emergency shutdown
- Failure: power lines were de-energized
Star Wars Episode I: The Phantom Menace (2009)
Mitigate the impact
Retrospective
Postmortem
Post-Incident Analysis
After Action Report
Correction of Errors
B-17 Flying Fortress
B-17 Instrument Panel
https://www.ncsc.gov.uk/blog-post/so-long-thanks-for-all-the-bits
How can you fix this problem?
Shape Coding
https://www.ncsc.gov.uk/blog-post/so-long-thanks-for-all-the-bits
737 MAX
https://commons.wikimedia.org/wiki/File:EGLF_-_Boeing_737_Max_-_N120IS_(43406207022).jpg
Not just What, but Why
Mitigate the impact
Fix the root cause
Defend against it happening again
Getting ready for next time
Rewrite history
Optimize the system for Future You
Build better duct tape
Thank you

Signed,
Future You
It was about security the whole time
Conclusion

- IR is important, unavoidable, and difficult.
- IR takes practice and is a lot of fun.
- Write down what is happening
- Fix the Failure, not the Fault
- Review every dimension once the dust settles
- Do Future You a favor
Questions?

Michael Ansel

erss2023@anselcomputers.com

I’m here until they kick me out

Slides & Links: https://links.anselcomputers.com/erss2023