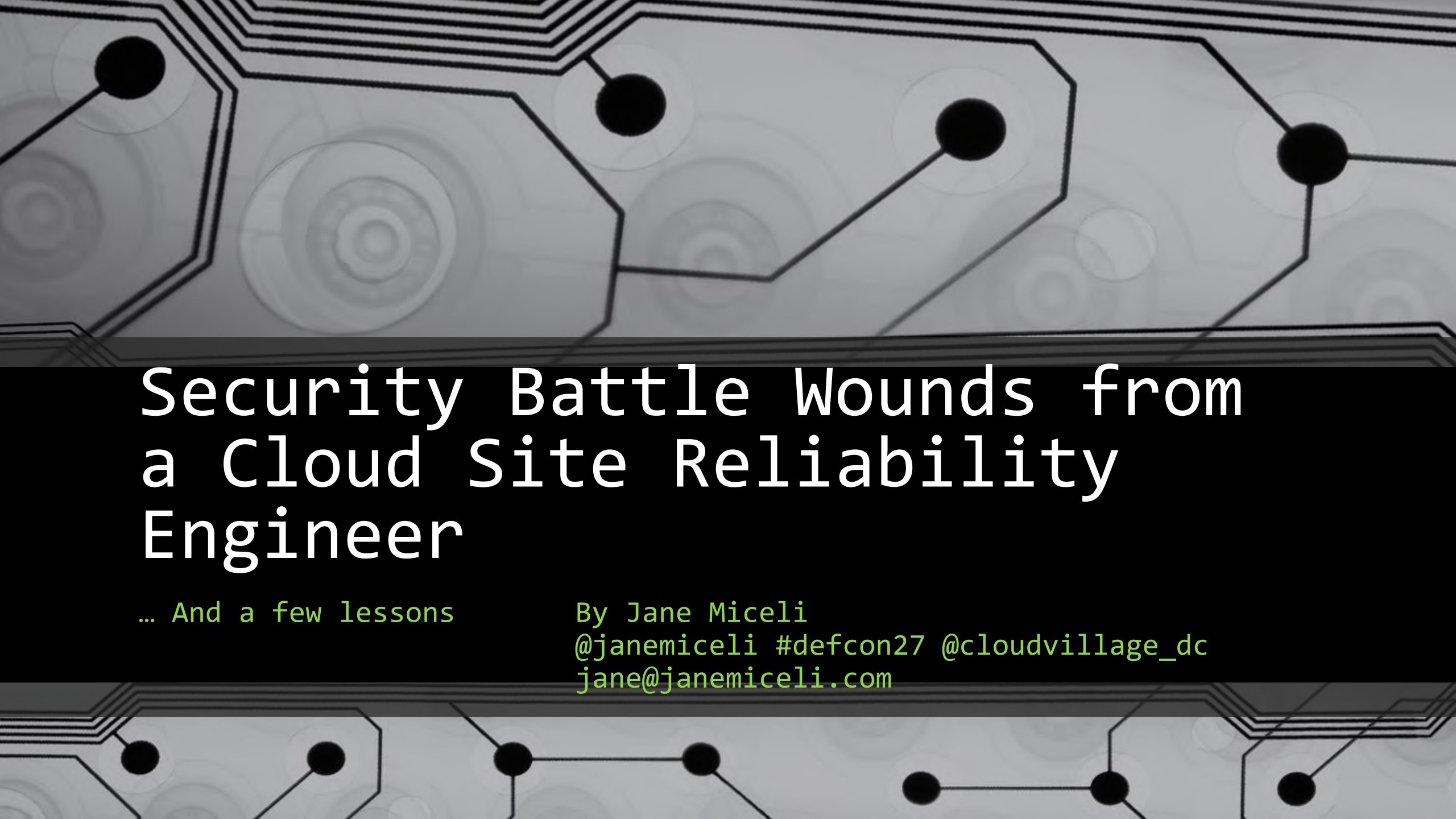


Security Battle Wounds from a Cloud Site Reliability Engineer

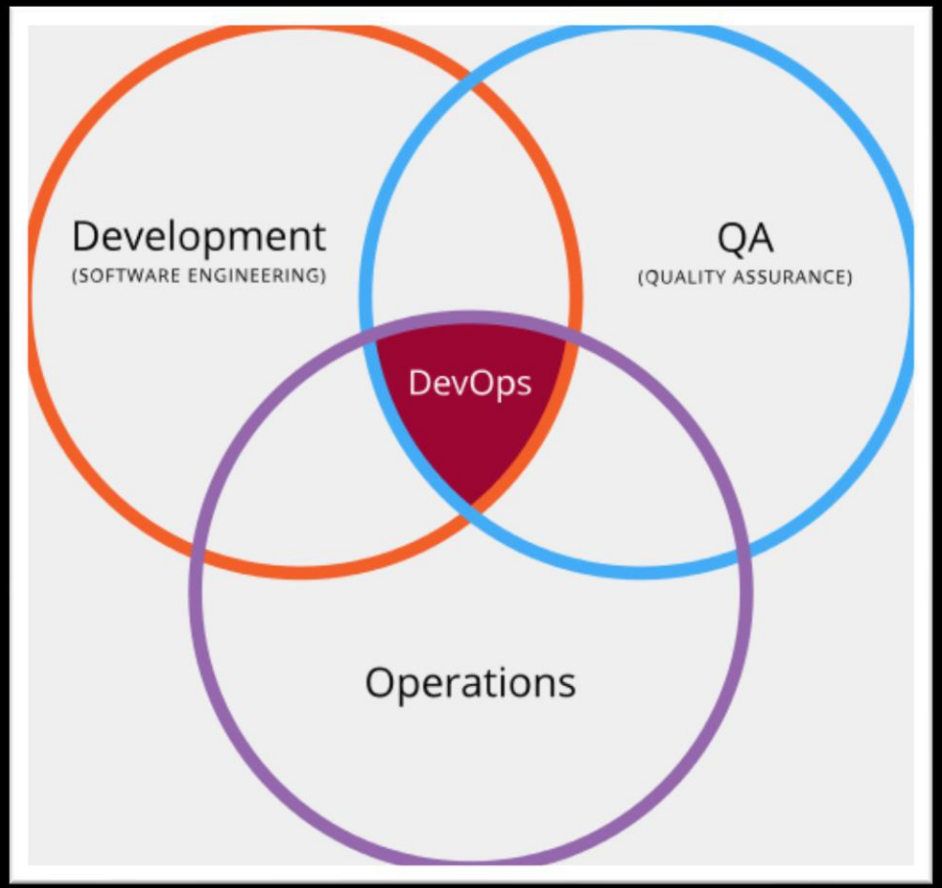
… And a few lessons

By Jane Miceli
@janemiceli #defcon27 @cloudvillage_dc
jane@janemiceli.com

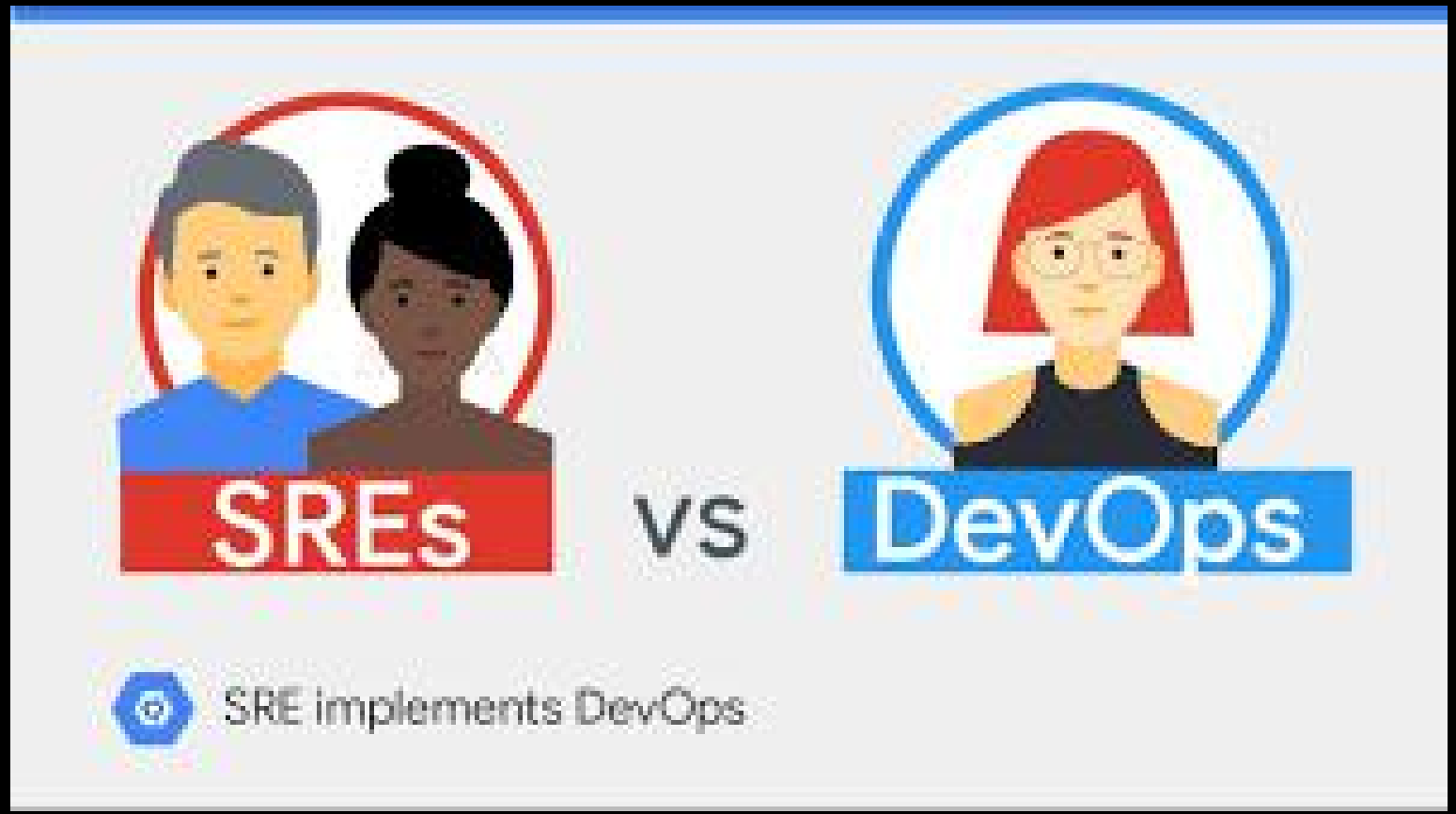
Agenda

- Background information
- Battles
- Lessons learned
- Questions?

What is DevOps anyways?



SRE vs DevOps

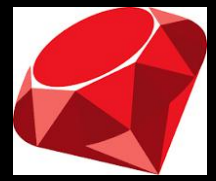


What technologies used?











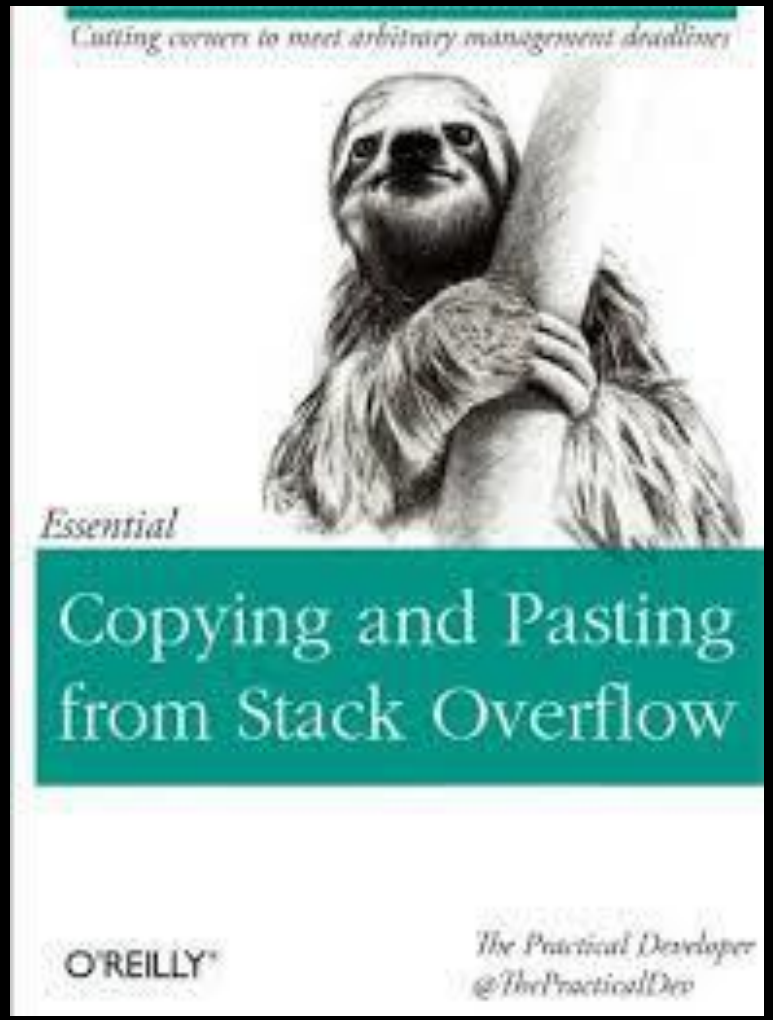

@janemiceli #devops27 #cloudvillage #cloud #security

Battles: The mindset of developers

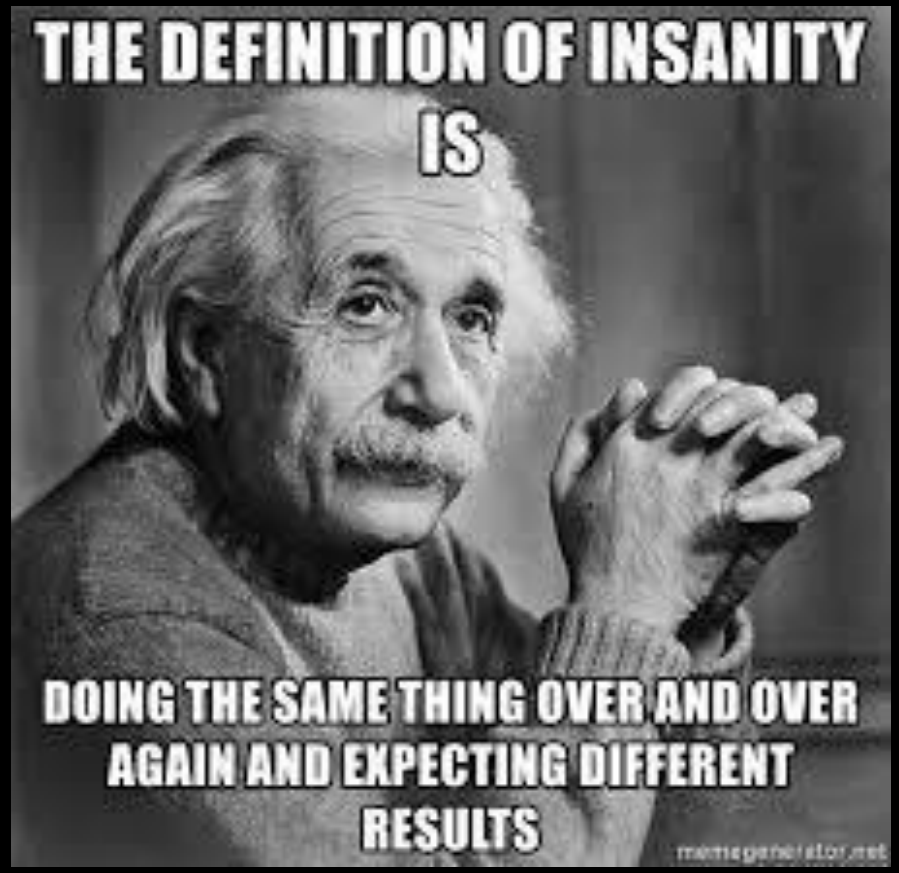
Battles: The mindset of managers

Battles: The view of security

Battles: The view from security

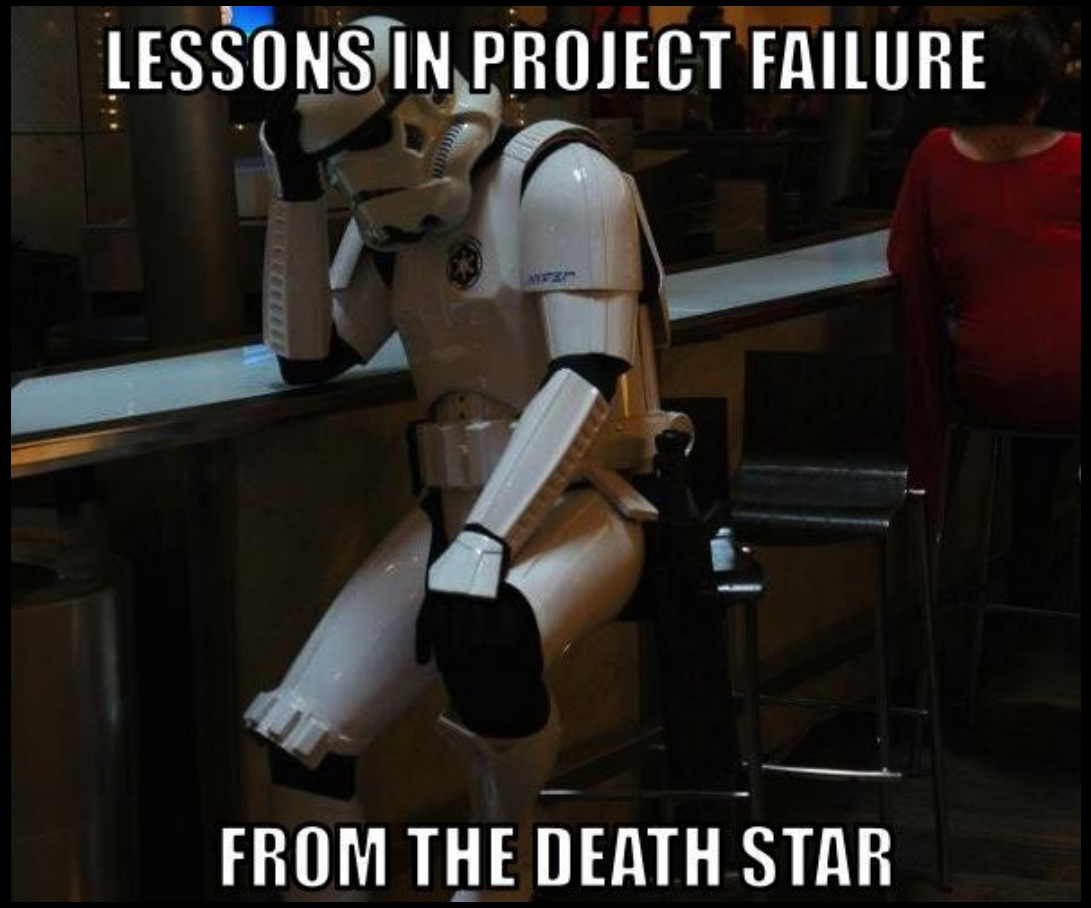


Battles: My own secrets vault means faster, “I’m cool”, no software purchase.



Battles: The accumulation of insecure technical debt

Fubar



Advice for CyberSecurity

- Developers/Engineers/coders need you
- If it's hard to understand, it won't get fixed.
- Don't send reports of scans, help them investigate the and recommend mitigation.
- Learn some coding, learn to show security coding/using libraries, do code reviews.
- Turn around answers quickly – its an opportunity to influence.
- Use simple and concise security policies that everyone can understand and obey.
- Tell them no when appropriate, but give alternatives to enable.
- Involve coders to join an investigation, so the impact is well understood.

Advise for Developers/Engineers/Programmers

- Security is your friend, secure coding is not new.
- Plain text, base 64 encoding, is not OK
- Use good random generators.
- You *don't* need production access.
- Take in-depth security training, Don't take the easy way out.
- Cleanup is important, as well as least privilege, reducing attack vector
  - If that doesn't mean sense, take a week long security class
- Don't roll your own vaulting mechanism/ cryptography AND Git is not for secrets!
- POCs turn into production really fast.
- Vet all the libraries and even those plugins on approved apps.
- Try not to get the security exception for being "business critical".

Lessons Learned

Questions?

Twitter: @janemiceli #defcon27 @cloudvillage_dc #cloud #security

Web: www.janemiceli.com

Email: jane@janemiceli.com