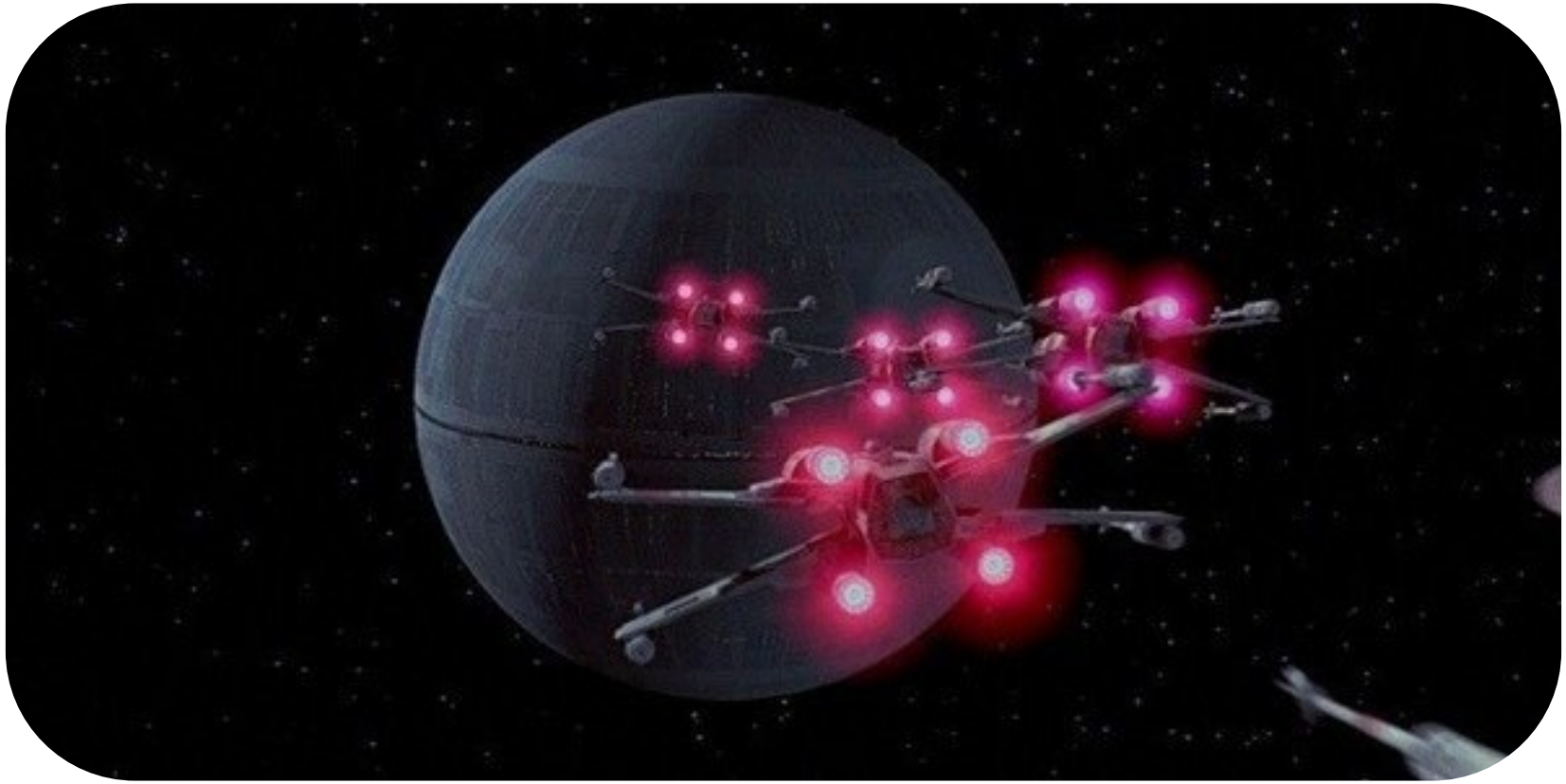
California Community Colleges

Vulnerability Management

Stephen Heath
Amir Khan
Omer Usmani

5/6/2021

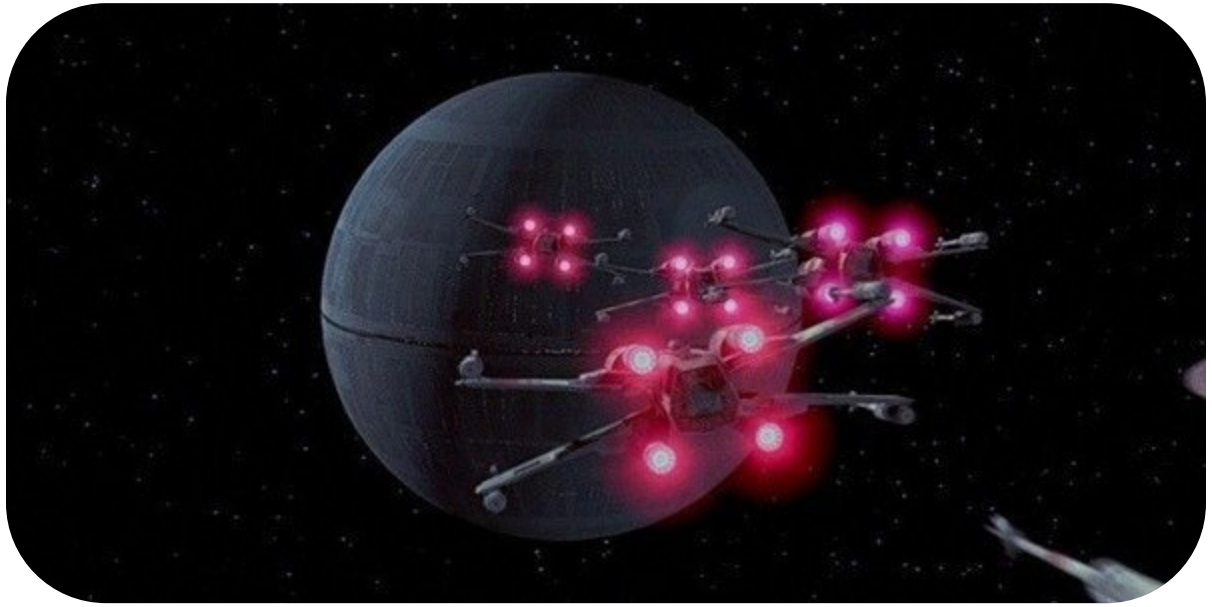
What is the most infamous vulnerability?



California Community Colleges

What is the most infamous vulnerability?

- Intentional design flaw
- Exploit stolen during a data breach
- Management knew it was a problem
- Hackers exploited for political reasons
- Built another, put in prod before hardening



California Community Colleges

Agenda

- Background info on vulnerabilities
- Keys to vulnerability management
- Demo of TechCenter tools to identify and track vulnerabilities

California Community Colleges

Vulnerability lifecycle – “0-day phase”

- Software/hardware company itself discovers
  - Create a patch and release

- Security Researcher / Hacker discovers
  - Keep it for themselves
  - Release it to the world
  - Disclose to the company
  - Disclose through a third party
  - Disclose through a bug bounty program
  - Sold through an exploit broker

Vulnerability lifecycle – “1+ day phase”

- After a patch is released
  - Security researchers being to reverse engineer
  - Try to replicate
  - Publish a PoC
  - Hackers weaponize and use in the wild

- System admins race to patch

Keys to vulnerability management

1) Know what you have
2) Have a regular patch cycle
3) Monitor and confirm

California Community Colleges

Handling exceptions – Out-of-band patching

Yellow flag: Monitor and consider patching early

- High CVE score 9.0+
- Includes “Remote Command Execution” or “RCE”

Red flag: Patch immediately!

- “Actively being exploited in the wild”
- “Weaponized”
- “PoC released”

California Community Colleges

Handling exceptions – Unable to patch

What if I can’t patch it?

- Segment
- Filtering rules
- Application whitelisting

California Community Colleges