CI/CS WORKSHOP

THE COMMUNITY TOGETHER

ResearchSOC | CI CoE PILOT

CI/CS WORKSHOP TALK 1, TRACK A

Patching Patch Management

Joshua Drake
Senior Security Analyst, Indiana University Center for Applied Cybersecurity Research

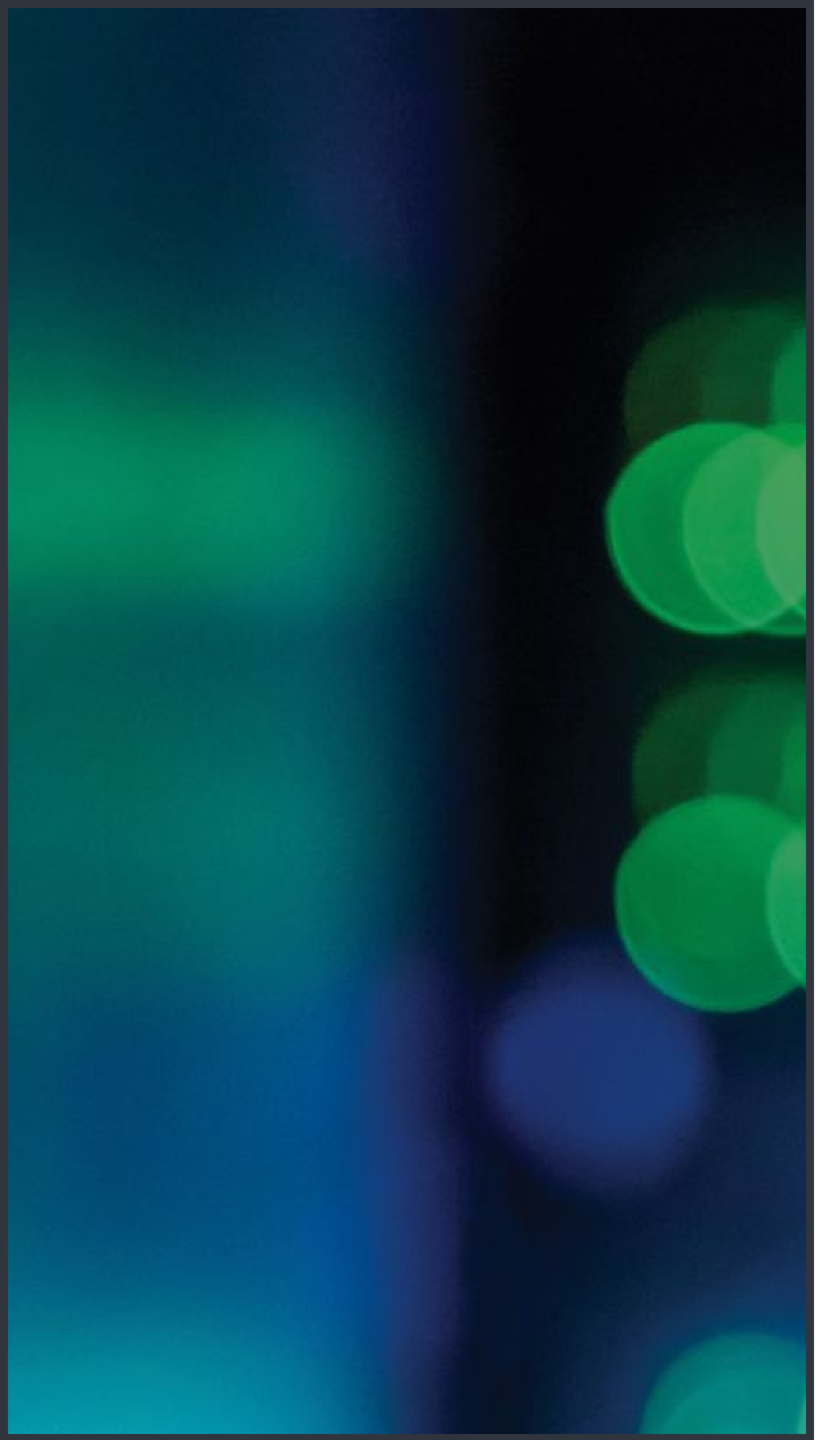
About Me

- Security Analyst at CACR since 2019
- Fifteen years experience in IT

  Applications support, systems analysis, systems administration, network administration and data center management

- Worked in several industries for organizations large and small

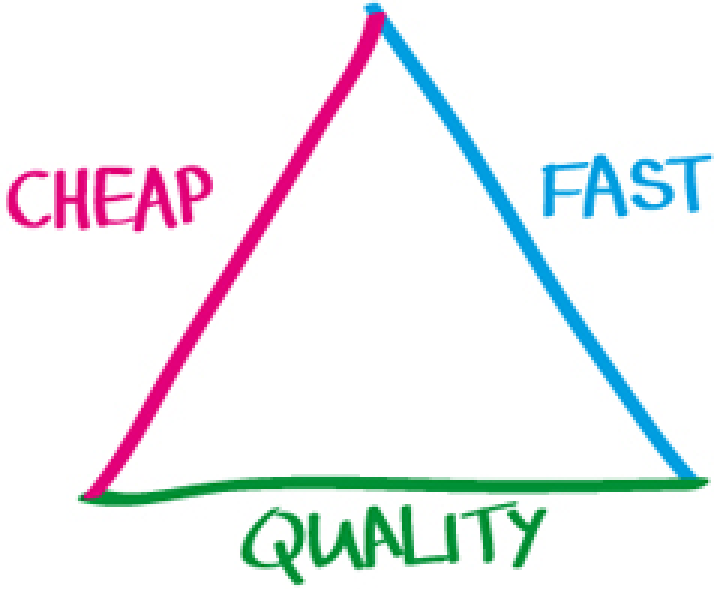
  Healthcare companies with hundreds of IT staff, municipal government with tight budgets and limited resources, and small businesses with one person IT shops



Expectations

- Not going to get in depth on technical topics
- Rather, trying to provide a mental model for thinking about patch management like a security engineer

THE TRIANGLE OF TRUTH



YOU CAN ONLY EVER HAVE 2 SIDES

ResearchSOC

CI CoE PILOT

Poll 1

What are you patching?

How to think about patch management like a security engineer

The Information Security Practice Principles

https://cacr.iu.edu/principles/ispp.html

- **Comprehensivity**

  Am I covering all my bases?

- **Opportunity**

  Am I taking advantage of my environment?

- **Rigor**

  What is correct behavior and how am I enforcing it?

- **Minimization**

  Can this be a smaller target?

- **Compartmentation**

  Is this made of distinct parts with limited interaction?

- **Fault Tolerance / Proportionality**

  What happens if this fails?

  Is it worth it?

Comprehensivity

- Question:

  Do I know about all the assets I'm meant to be patching? Am I taking adequate steps to ensure they are receiving patches?

- Solution: Hardware Asset Inventory
  - Cheap/Good: PDQ, Snipe-IT
  - Good/Fast: SCCM, Solarwinds, Goverlan Reach

Opportunity

- ## Question:

  What tools and information are available to me?

- ## Solution: Gather threat intelligence

  - Vendors - subscribe to feeds for your major vendors
  - CSIRT - find general and industry specific CSIRTs who issue alerts on relevant software
  - ISAC - join and participate in communities to share information and ask questions

Threat Intel Resources

- us-cert.cisa.gov
- www.ren-isac.net/public-resources/csirt.html
- www.microsoft.com/en-us/msrc/technical-security-notifications

Rigor

- Question:

  Can I identify what hosts are missing which patches? What does my infrastructure look like to an attacker?

- Solution: Test and Verify
  - Software Inventory Tools: PDQ, SCCM, Goverlan, etc
  - Security Exercises
  - Vulnerability Scanners

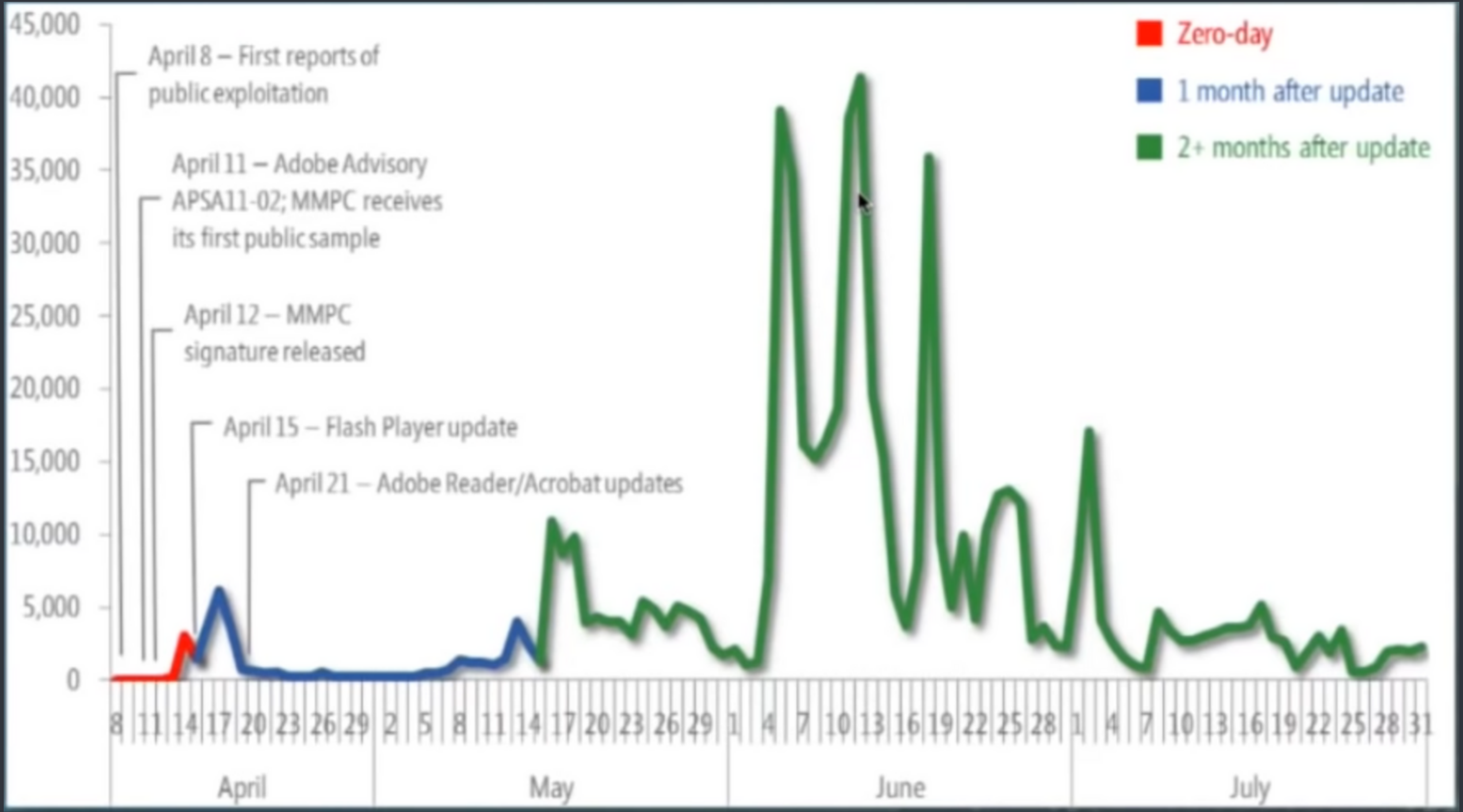
Minimization

- Question:

  Am I remediating ALL of my external facing vulnerabilities in a timely manner?

- Solution:
  - Prioritize patching different areas of your infrastructure (DMZ/Servers)
  - Stage Patches using SLA type model (Critical 24 hrs, High 48 hrs, etc)
  - Do whatever you have to do ensure you have regular maintenance windows

Zero-day exploits Lifecycle



Compartmentation

- Question:

  Are my internal assets being patched in a timely manner?

- Solution:
  - Endpoints should have regular maintenance windows as well
  - Set and enforce deadlines (if your toolset allows it)
  - Linux Admins: Don't trust your users!

ResearchSOC

CI CoE PILOT

Poll 2

Endpoints

Taking things to the next level

Automation

- Everyone should be using some form of automation!
- Paid tools (SCCM, PDQ, Goverlan, SALT, Satellite, etc)

  Typically lower tech barrier to entry, GUI based

  Can be expensive!

- FOSS or low cost options

  Windows Admins - Use WSUS and get familiar with Powershell!

  Linux admins - chron jobs, distro specific manager

- System Configuration Tools

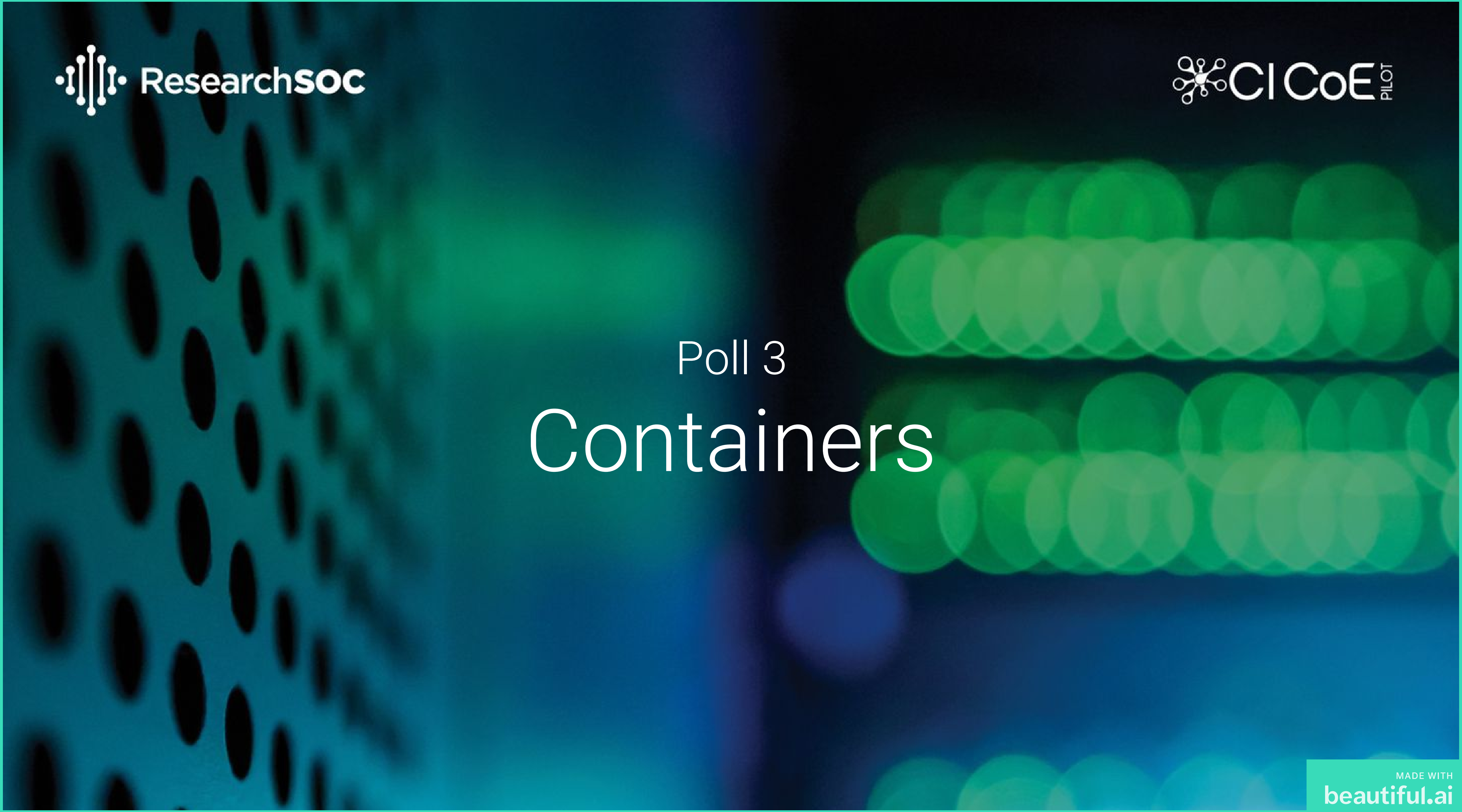
  Ansible - requires yaml, no client deployment, pull model

  Chef/Puppet - more setup required, push model, diff compliance

Running Services in Containers

- Make sure to use latest image when building container
- Have a policy and use an automated process to relaunch containers regularly
- Sample Policy

  Open Science Grid Container Policy



Poll 3

Containers

Questions?

Thank you!

Josh Drake | Sr Security Analyst | IU CACR

@ drakejc@iu.edu

🌐 cacr.iu.edu