RISE 2030

Observability: Fixing problems before the pager rings.

Replacing Guesswork with Clarity

Presented by Matt Hohmeister

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- A multitude of solutions exist to provide for observability.
- Monitoring for a system in a normal vs a trouble state is based on a parameter such as responding to pings or certain ports, such as 80 and 443 for a typical Web server.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- When a system goes into a trouble state, the monitoring system creates an alert, then hands it to the alerting system if we had previously determined it worth a “push” alert.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- When we receive an alert during business hours (or otherwise), it becomes an “outage until proven otherwise”: we solve the outage if it exists, then we demonstrate to ourselves that the outage is no longer—or if it’s a false alarm, gather notes about why.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- Conventional monitoring pitfalls:
  - While we may receive an instant reactive notification of a problem, the problem already happened…
  - …and we now must find the symptom, starting with close to zero knowledge, all during customer downtime: stressful.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- Observability involves moving from external monitoring to internal monitoring.
  - An observability agent is installed on the target server as a service to locate problems that aren’t visible to external monitors or customers.
  - Log viewing may be consolidated into a single pane of glass.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- Cloud-based observability
  - Fewer on-premise servers to maintain just for observability.
  - Maintain observability, even in a hard failure such as an outside line cut.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- Synthetic monitoring
  - Traditional:
    - Test redcap.med.fsu.edu, ports 80 and 443
  - Synthetic:
    - Repeat hourly
      - Go to https://redcap.med.fsu.edu/.
      - Type username “redcap.monitoring” and password “12345”.
      - Click “Log In”.
      - If the resultant page does not contain the word “Project”, alert.

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- What else can we monitor?
  - Services on servers with no immediate customer impact, but we should know.
    - Did the CrowdStrike service fail?
    - Are any services not there that should be?
    - Are there any services that should have been removed, such as formerly-used monitoring agents or endpoint protection?

RISE 2030

Observability

The College of Medicine Office of Information Technology is moving beyond monitoring (the "what") and investing in observability (the "why").

- What else can we monitor?
  - Third-party websites used by our customers.
    - “We just found example.com down. Let’s notify customers proactively and contact example.com tech support.”

RISE 2030

Observability

"Fixing Problems Before the Pager Rings"

RISE 2030

Observability

"Fixing Problems Before the Pager Rings"

- Paged at 0200?
- Paged out of a concert?
- Customer reports an issue that happens "sometimes", but you never actually see it?

RISE 2030

Observability

"Fixing Problems Before the Pager Rings"

- Service monitoring: see a service fail before it becomes an issue or noticed by a customer.
- Consolidated logging: view logs from a single pane of glass, narrowing down based on known parameters like timestamp.

RISE 2030

Observability

"Fixing Problems Before the Pager Rings"

- Solve many problems before they happen.
  - Prevent that late-night call.
- Solve problems much faster, using real data to narrow down the symptom.
  - If there *is* a late-night call, what data do you want presented to you?

RISE 2030

Observability

"Fixing Problems Before the Pager Rings"

- Less "hero work".
- More boring reliability. ☺

RISE 2030

Observability

The helpdesk can benefit too.

- Helpdesk personnel can receive endpoint issues before they impact the customers.
- Helpdesk is better equipped == less escalation—and more accurate escalation.

RISE 2030

Observability

The helpdesk can benefit too.

- Post-incident review and reflection.
  - Not everything requires a formal PIR.
  - Was this preventable? How?
  - Be better prepared for next time.
  - Write it all down!

RISE 2030

Observability

The helpdesk can benefit too.

- You can do this!
  - Proper system recommended—not required.
  - Scheduled tasks and cronjobs.

RISE 2030

Observability

The helpdesk can benefit too.

- What's in it for you?
  - Less time "putting out fires".
  - More time focusing on work that will improve things or meet requirements.

Thank you!

Thanks for coming to this presentation! We hope that you were able to garner helpful information. Feel free to contact me with further questions.

Also, thanks to my supervisor and teammates for help in putting this together.

Matt Hohmeister

matt.hohmeister@med.fsu.edu

850-645-0544

- College of Medicine, Office of Information Technology, Infrastructure Operations (IOPS)
  - Dan Bennett
  - Matt Hohmeister
  - Tim Smith
  - Tyler Teagle