Chainguard

The Pain of Software Vulnerability: 900 minutes of interviews in 15 minutes of presentation :)

John Speed Meyers (jsmeyers@chainguard.dev)
September 12, 2023
Chainguard Labs

How much time do organizations* spend on vulnerability management?

And why is vulnerability management* so painful?

* Organizations that build or operate container-based applications.
* Identifying, triaging, and remediating known vulnerabilities in containers.

Methodology

~10 interviews with software professionals

- All interviewees do vulnerability management as part of their day-to-day job.
- All interviewees work at organizations that build or operate containers.
- 3 pre-interviews. 9 full interviews.
- 60-90 minutes.
- Recorded. Rewatched.
- Analyzed for themes.
- Paid interviewees a flat fee.

ACKNOWLEDGEMENT: Accurately understanding how software professionals spend their time is a software engineering research holy grail. I have not found this particular holy grail :)

Some companies spend A LOT of time on vulnerability management. But not all.

Company	Estimated # of Employees	Estimate of Total Annual Direct Staff Hours Spent on Vulnerability Management
European Logistics	10,000s	~20,000 hours
U.S. Military Organization	100s	~15,000
Software provider	1000s	~1250 hours
Software provider	100s	~1000
Software provider	100s	~1000 hours
Software provider	1000s	~200
Software provider	10s	~100 hours
Software provider	100s	~150

Vulnerability Management Pain Points
(a few of them)

1. App developers impose “externalities” on platform team when choosing base images.

2. False positives are annoying. Interviewees expressed interest organically in VEX.

3. Vulnerability management affects software consumers AND producers.

Should organizations analyze their vulnerabilities? Or try to reduce them? (Or both?)

Chainguard

The Pain of Software Vulnerability: 900 minutes of interviews in 15 minutes of presentation :)

John Speed Meyers (jsmeyers@chainguard.dev)
September 12, 2023
Chainguard Labs

https://www.chainguard.dev/contact