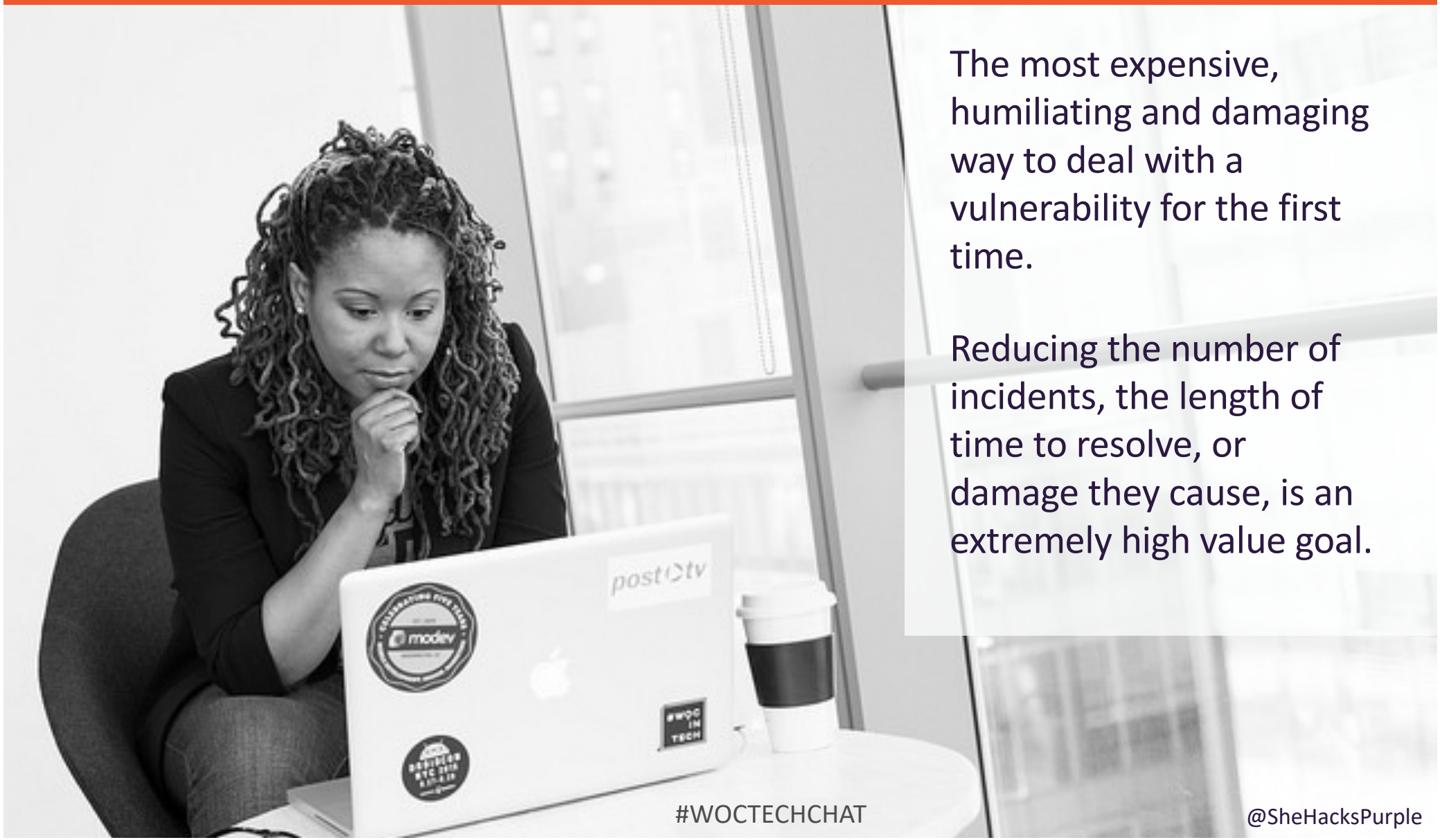
Security Metrics *That Matter*

- Time to detection
- Time to remediation and/or patch
- Baseline security posture, how close are you to your goals? How much closer 3, 6, 12 months later?
- Are **you** meeting your SLAs with developers and ops?
- Average number of vulnerabilities per system or app, and does this go down over time?
- Detecting the same types of vulns? Reduction in #s?
- Are you now able to detect new types of vulns?
- After education on specific topics do instances decline?
- After targeting specific vulns do they decline?

Security Incidents



The most expensive, humiliating and damaging way to deal with a vulnerability for the first time.

Reducing the number of incidents, the length of time to resolve, or damage they cause, is an extremely high value goal.

Incident Metrics *That Matter*

Measuring Incidents

- Time to resolve
- Time to detect
- Time to diagnose as incident or just event (triage)
- Types/categories of incidents
- Process is/is not followed
- Cost & damage
- Types repeated, or new types found
- Other teams understand what to do/cooperative
- Post-mortem performed *every single time*?
- Quarterly review of incident stats
- Time between incidents (if there's no recovery time that's an issue) – Note on resting your staff
- Access and tooling was/was not available