The 5 stages of grief with Vulnerability Management

Vulnerability management is hard, especially when there are issues such as alert fatigue, lack of visibility, and manual processes. In this infographic, we explore how a typical vulnerability management process looks from detection to remediation. Without the right tools that help provide contextual and actionable insights, vulnerability management teams can easily fall into all five stages of grief when dealing with this never-ending cycle.

Stage 1: Alert on new vulnerability
- Do I need to handle it?
  - No: Dismiss
  - Yes: Do I need to handle it now?
    - No: Delay
    - Yes: What is the root cause of the alert?

Stage 2: When do I need to handle it by?
- Do I need to handle it now?
  - No: Is it a duplicate alert? Is it a false positive? Too complicated No resources Need to ask someone
      - No: Root cause found
      - Yes: Found the fix

Stage 3: Who is responsible for this alert?
- What is the root cause?
  - Who is responsible?
    - No: Look it up in system
    - Yes: I know the fix

Stage 4: How do I remediate it?
- How do I remediate?
  - No: Google it
  - Yes: Remediates it

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 35 percent of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenslopes, Lightspeed and Agilab. Visit https://www.wiz.io/ for more information.