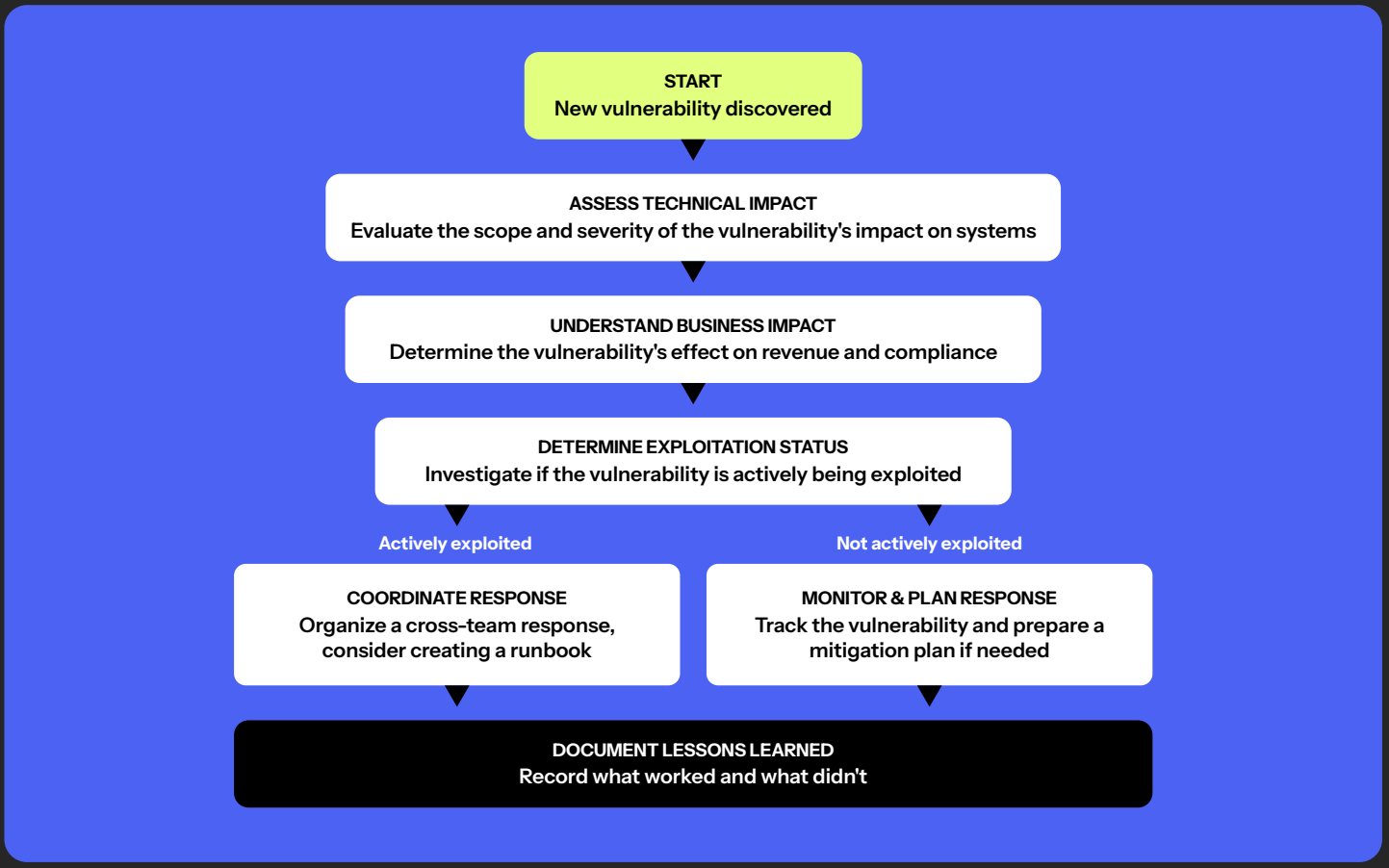
Axonius

Should I escalate a vulnerability?

A decision flowchart



Questions to assess real-time risk

1. **Is this being actively exploited?**
   - Have attackers already weaponized it?
   - Do threat intel reports confirm real-world exploitation?
2. **How easy is it to exploit?**
   - Does the vulnerability require specialized knowledge and resources, or can it be exploited using publicly available tools?
   - Can it be exploited remotely, or does it need local access?
3. **What's the blast radius?**
   - Does it impact business-critical systems, regulated data, or production environments?
   - Could it cause operational downtime, financial loss, or reputational damage?
   - Do you have mitigating controls?

Criteria to determine if a zero-day can wait

Your team should adopt a structured approach to determine whether an urgent response is needed or if temporary mitigations can be implemented until a patch is released.

Here's how to determine if a zero-day can wait:

- **It's mitigated by existing security controls.** (Network segmentation, Web Application Firewall, or Intrusion Prevention System rule protecting against that specific threat)
- **It's already scheduled in an upcoming patch cycle.** (No need for emergency intervention)
- **There's no evidence of exploitation in the wild.** (High severity ≠ active attack)
- **The impact is isolated.** (A low-risk internal system vs. a public-facing customer database)

Learn more ↗