RedHelm

ACTION GUIDE:

HOW TO PRIORITIZE VULNERABILITIES THAT ACTUALLY MATTER

Step 1:

Build Continuous Visibility

Identify vulnerabilities across:

- Endpoints
- Servers
- Cloud infrastructure
- Applications
- Network devices
- Internet-facing assets
- Remote infrastructure
- Business-critical systems

Organizations cannot prioritize exposures they do not know exist.

Step 2:

Add Asset Context

Connect vulnerabilities to the systems they affect.

Ask:

- What does this asset support?
- Is it business-critical?
- What information does it contain?
- Is it externally accessible?
- What would happen if it became unavailable or compromised?

This transforms vulnerability data into business context.

Step 3:

Evaluate Exploitability and Threat Activity

Determine whether:

- Exploit code exists
- Exploitation is occurring in the wild
- Threat actors are actively targeting the vulnerability
- CISA or other authoritative sources have identified active exploitation
- The vulnerability could provide meaningful attacker access

Prioritize based on realistic attack potential rather than severity alone.

Step 4:

Determine Exposure

Evaluate how reachable the vulnerable asset is.

Consider:

- Internet exposure
- Network segmentation
- Authentication requirements
- User access
- Existing security controls
- Potential attack paths

A vulnerability attackers cannot easily reach may warrant different treatment than one directly exposed to the internet.

RedHelm

Step 8:

Measure Whether Risk Is Declining

Track whether high-risk exposures are being addressed faster and whether vulnerability backlogs are becoming more manageable. The objective should be measurable risk reduction, not simply remediation activity.

Step 7:

Validate the Fix

Do not assume a closed ticket means the vulnerability is gone. Rescan or otherwise validate that remediation successfully removed or reduced the exposure.

Step 6:

Remediate or Mitigate

Determine the appropriate response:

Consider:

- Patch
- Upgrade
- Reconfigure
- Restrict access
- Segment
- Monitor
- Apply compensating controls
- Accept documented risk

Not every vulnerability requires the same remediation strategy.

Step 5:

Prioritize Based on Business Risk

Combine:

Severity + Exploitability + Exposure + Asset Criticality + Business Impact

This provides a stronger foundation for cyber risk prioritization than relying on a technical score alone.