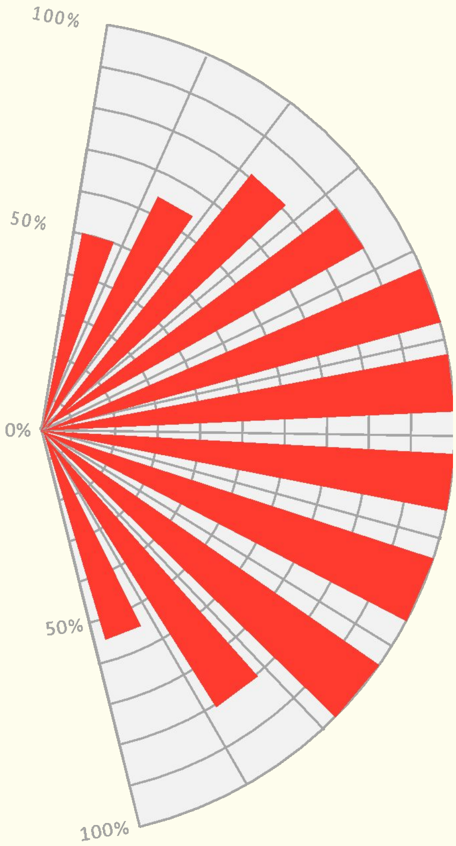
The 11 Ways We Sabotage Our Own Vulnerability Management



Balbix®

Based on an analysis of several hundred conversations with Balbix prospects and customers through 2023

#1

Confusing risk of CVE instances vs risk of CVEs

Implication:

Wasted resources and effort addressing non-risky vulnerabilities on less critical assets while more risky instances of other CVEs ones remain unaddressed

#2

Ignoring EOL systems

Implication:

Increased risk of breaches and vulnerabilities due to the lack of security updates and support for EOL systems

#3

Not understanding and using superseding patches

Implication:

Spending excessive time and effort in applying patches for individual CVEs in lieu of using a single superseding patch

#4

Picking too many vulnerabilities to resolve in a single patching project

Implication:

Wasted resources spent in testing and applying patches for CVE instances that do not matter, and more reasons why the project goes slowly

#5

Lack of fixed asset scope for remediation project

Implication:

Can lead to projects becoming unmanageable, with unclear goals and outcomes, making it difficult to measure progress and effectiveness.

#6

No alignment on patch SLAs

Implication:

Lack of consistency in remediation speed make it impossible to maintain an acceptable level of risk

#7

SLAs that are too loose or not measured

Implication:

Risky vulnerabilities may not be addressed promptly or effectively, causing security risks to escalate beyond acceptable levels

#8

Focus on new critical and high severity CVEs vs the growing backlog

Implication:

Lack of holistic vulnerability management leaves older vulnerabilities unaddressed, and security gaps

#9

Relying on ticketing systems to indicate resolutions

Implication:

Significant risk of overlooking CVE instances that may not have been properly addressed

#10

Lack of root cause analysis when fixes are not successfully applied

Implication:

Persistence of underlying issues can continue to pose a hidden threat

#11

Not forcing system reboots and application restarts

Implication:

May leave systems vulnerable, as security patches require a reboot/restart to become effective