50 Cyber AI Prompts Cheat Sheet

Balbix®

⚠ **WARNING:** These prompts will not work on ChatGPT. Use BIX.

Exposure, Risk and Prioritization

1 What is our cyber risk exposure in dollars?

2 Which vulnerabilities pose the highest financial risk to us?

3 What are the top cyber risks I should present to the board this quarter?

4 Which assets contribute most to our overall cyber risk exposure?

5 Which vulnerabilities in our environment have critical exposure?

6 What percentage of critical vulnerabilities remain unpatched after 30, 60, or 90 days?

7 Which critical vulnerabilities have active exploits in the wild?

8 What are the key actions that drive better vulnerability management outcomes?

9 How do I become a vulnerability management expert?

10 Which vulnerabilities from the latest Patch Tuesday apply to our environment?

Security Posture (Quantified)

11 What is the risk of a major ransomware incident?

12 How does our cyber risk compare across different business units?

13 What are the top 5 security gaps impacting our compliance posture?

14 Which security misconfigurations are driving the most risk in our environment?

15 What is the financial impact of vulnerabilities affecting our top 5 critical assets?

16 Which compliance frameworks are we currently at risk of violating?

17 What is the dollar impact of our unpatched vulnerabilities across all assets?

18 Which security controls would provide the highest ROI in risk reduction?

19 What is our total cyber risk exposure by business unit?

20 What are the highest-risk security gaps across our infrastructure?

Unpatched and EOL Systems

21 Which endpoints have unpatched critical vulnerabilities?

22 Which assets are running an unsupported or end-of-life (EOL) operating system?

23 How many Windows, Linux, and macOS devices are out-of-date by more than 12 months?

24 Which assets have outdated or vulnerable versions of Log4j?

25 What percentage of our asset fleet is running EOL software or browsers?

26 Which applications are running outdated versions that pose security risks?

27 What is the total risk exposure from outdated or unsupported systems?

28 How many critical vulnerabilities remain unpatched despite available fixes?

29 Which devices are missing endpoint detection and response (EDR) coverage?

30 Which assets are most at risk from zero-day vulnerabilities?

Attack Surface and Asset Visibility

31 How many total assets do we have across the enterprise?

32 What is the distribution of assets by type (e.g., servers, endpoints, IoT, cloud workloads)?

33 Which assets are classified as mission-critical, and who owns them?

34 How many cloud workloads do we have, and what is their security posture?

35 Which servers, applications, or end-user assets have the highest business impact?

36 What is the distribution of assets across different geographic locations?

37 Which business applications contribute most to our cyber risk exposure?

38 How many new assets were discovered in the last 7 days?

39 How many assets were decommissioned last month?

40 What is the security posture of our cloud assets versus our on-premises infrastructure?

Remediation Performance

41 How has our Mean Time to Remediate (MTTR) changed over the last 30 days?

42 What has been our average MTTR over the past 60 days?

43 Which business units have the fastest remediation response times?

44 Which security teams are closing vulnerabilities the fastest?

45 Which assets have the longest outstanding unpatched vulnerabilities?

46 What percentage of high-risk vulnerabilities have been remediated in the last 90 days?

47 Which vulnerabilities remain open despite remediation being assigned?

48 Which teams or departments are falling behind in meeting patching SLAs?

49 Can you create a weekly performance report for my team and summarize it in two lines for an executive?

50 Create a leaderboard of the top 25 vulnerability owners based on their performance against critical and high exposures and email it to vuln-owners@mycompany.com every Friday afternoon.