20

Proven tactics to help you quickly reduce your cyber risk

Show them to me ☛

Presented by Balbix

1

Strategic Deadline-Driven Fixes

Align patches or fix deadlines with key upcoming product launches, major sales events, or audits.

Why it works

By syncing remediation with major organizational milestones, security becomes impossible to ignore. Teams feel compelled to address critical issues before they can derail high-impact events.

How to implement

Gather up-to-date vulnerability data, correlate it with upcoming launches or events, and set remediation deadlines aligned to those milestones. Automate tracking and reminders.

2

Revenue-Driven Prioritization

Prioritize fixes for systems directly tied to risk to revenue streams and critical IP assets.

Why it works

Highlighting the financial impact of unresolved vulnerabilities for critical assets (e.g., e-commerce, payment gateways) makes it crystal clear why certain fixes jump the queue. Executives and dev teams naturally align on preventing disruption.

How to implement

Identify which applications, services, or data sources are at greatest impact risk. Pinpoint their exposures and enforce shorter remediation windows. Track progress in a visible report.

3

Daily Risk Huddle

Conduct a brief (15-30 minute) daily standup where teams flag any blockers for top-priority fixes.

Why it works

Short, focused meetings maintain momentum on critical remediation tasks. They also provide a quick forum for escalating issues or resource gaps that might otherwise linger.

How to implement

Invite key stakeholders, security leads, developers, and product owners to a recurring quick session. Use a simple agenda: (1) critical fixes in progress, (2) any blockers, (3) immediate next steps. Keep a shared list or Kanban board to track updates and prevent duplicate efforts.

4

External Asset Tracking

Track all externally facing assets then stack rank them by potential impact.

Why it works

Many breaches start through internet-facing assets. By systematically mapping every asset and assigning owners, teams can more clearly track high-risk assets.

How to implement

Create or update your asset inventory, tagging each external asset with owners. Remember, all end-user systems are externally facing. Engage owners with SLAs for critical vulnerabilities and monitor progress in a shared dashboard.

5

Immediate EOL Endpoints Triage

Address end-of-life (EOL) operating systems and other software.

Why it works

Unsupported systems are magnets for exploitation since they don’t receive official patches. Fixing or retiring these immediately provides a major risk reduction.

How to implement

Inventory all operating systems and browser versions in your environment. Flag any that have exceeded their end-of-support timeline. Develop a fast-track plan to patch, upgrade, or decommission these systems. If none of this is possible, then isolate these systems with airgaps and restricted network segments.

6

GenAI-Enhanced Weekly Summaries

Use a generative AI tool to summarize your weekly cyber risk report and propose an actionable plan.

Why it works

Cut through dense security data with an easily digestible summary that helps teams and execs focus on urgent items.

How to implement

Feed your vulnerability scans and threat intel into a secure GenAI system. Use the prompt, “Review critical vulnerabilities, correlate with threat intelligence and asset criticality, and recommend an action plan for next week. Include reasons why these need to be resolved.”

Avg. Time Open for Critical & High

Rather than counting the number of vulnerabilities, measure how long critical and high vulnerabilities remain open.

Why it works

A pure vulnerability count can be misleading. Closing 100 low-severity issues might look great, but it doesn’t reduce risk. Tracking open days for critical and high issues highlights the true impact.

How to implement

Define a metric (e.g., “Mean Time Open for Critical/High Exposures”). Adopt a sound way of calculating scores for each vulnerability instance that considers severity, exploits, attack paths, mitigating controls, and asset criticality. Track how many days those vulnerabilities remain unpatched, from discovery to remediation.

8

Monthly BAS/KEV Remediation

Schedule remediation specifically for findings flagged by BAS tools that also appear on CISA’s KEV catalog.

Why it works

Focusing on vulnerabilities already exploited in the wild (as per KEV) and validated by Breach and Attack Simulation (BAS) ensures you’re tackling the most dangerous threats. This combo approach directly addresses real-world attack paths.

How to implement

Review your BAS reports. Cross-reference vulnerabilities with the KEV list. Consolidate them into a dedicated “must-fix” queue for the monthly remediation cycle. Track closure rates and re-run BAS to confirm these high-risk issues are resolved.

Monthly Remediation Competition

Establish a competition where business units or teams earn points for fixing critical exposures. Offer rewards.

Why it works

Gamifying security fosters friendly competition. Teams race to resolve vulnerabilities, boosting morale and collaboration while driving down risk in a fun, tangible way.

How to implement

Define scoring: e.g., each critical fix = 5 points, each high fix = 3 points. Track results in a shared leaderboard at month’s end. Reward winning teams with items like T-shirts, stickers, or a mention in the company newsletter. Rotate each month's focus (e.g., critical web app bugs, and server misconfigurations) to keep it fresh.

Achievement Badges for Fixes

Award badges for meeting timely goals, like remediating vulnerabilities on mission-critical assets.

Why it works

Similar to online gaming achievements, badges tap into social recognition. By celebrating progress, you encourage ongoing engagement with the remediation process.

How to implement

Define clear criteria: e.g., fix 5 critical vulnerabilities in under 7 days for a “Rapid Responder” badge. Track achievements automatically in your ticketing or reporting system. Showcase them on team channels or a company-wide dashboard for maximum visibility.

Remediation Hackathon Blitz

Dedicate a day exclusively to addressing vulnerabilities and misconfigurations with critical exposure scores.

Why it works

Inspired by hackathon culture, people set aside their usual work and rally around solving security problems. Friendly competition, pizza and the celebratory atmosphere keep teams motivated.

How to implement

Pick a date when critical projects allow dev/security teams to focus. Provide a common scoreboard and live metrics. Encourage cross-team collaboration for complex fixes. At the event's conclusion, celebrate top performers with awards or recognition.

Fix-Lag Dashboard

Publish a dashboard showing how long exposures have been unaddressed for critical applications or assets.

Why it works

Aging exposures and vulnerabilities are easy to overlook if there’s no visibility. A “fix lag” leaderboard creates gentle pressure for teams to tackle older issues and helps leadership spot persistent laggards.

How to implement

Automate the extraction of open vulnerabilities from your ticketing/scanning tool. Sort them by days since the discovery and highlight the ones with the longest open durations. Publish the dashboard to provide a powerful nudge to resolve stale items.

13

Complete “Fix Journey” Guidance

Provide context for each vulnerability with patch links, config changes, and an explanation of impact.

Why it works

When dev or IT teams understand how to remediate a vulnerability and why it matters, they fix it faster. Clear instructions remove the guesswork and reduce error rates.

How to implement

Automate or manually attach “fix journey” notes to each vulnerability ticket. Include links to vendor patches, relevant code snippets, or config settings. If possible, briefly note the financial, reputational, or operational risks of leaving it unpatched (in dollars).

GenAI for Cyber Insurance Negotiation

Use an AI tool to analyze key metrics such as MTTR and suggest talking points for negotiating.

Why it works

Demonstrating a robust security posture can reduce insurance costs. GenAI can quickly highlight the specific data points (e.g., improved average patch time, and lower open days for high-severity flaws) that insurers care about.

How to implement

Collect data on your remediation metrics, especially around critical or high vulnerabilities. Prompt a GenAI system to produce an executive-friendly summary of risk reduction and consistent improvements. Use these insights in renewal discussions with insurers.

15

Exposure Improvement Leaderboard

Build an internal dashboard that ranks business units based on average exposure score improvements.

Why it works

A leaderboard that shows how teams track against MTTR-CH (Mean Time to Remediate Critical & High exposures) and patch compliance builds public recognition and fuels motivation for lagging departments to improve.

How to implement

Create an “exposure score” for each department. Update the leaderboard monthly or quarterly. Highlight the best performers and share specific actions or practices they use so others can learn.

Quarterly Ownership Checks

Conduct quarterly audits to ensure every asset-vulnerability pair has a valid, accountable owner.

Why it works

Vulnerabilities can easily become “orphaned” if employees change roles or leave. Regular ownership checks prevent issues from slipping through the cracks.

How to implement

Export a list of active vulnerabilities and their assigned owners. Verify each owner’s contact info, department, and role. If data is missing or outdated, escalate to team leads or managers to fill the gap. Maintain a clean, up-to-date record.

Security Buddy Program

Pair each business unit with a dedicated security buddy who translates technical CVEs into business impact and unblocks them.

Why it works

Close collaboration erases the knowledge gap between security and business units. It also fosters a direct line of communication, ensuring vulnerabilities are handled swiftly.

How to implement

Identify at least one security point person (the “buddy”) for each department. They attend relevant standups, review active issues, and help manage escalations. Encourage building a rapport so teams naturally ask for help when something seems off.

Rotating Patch Blitz Windows

Rather than holding one big patch day, rotate short, intense “patch blitz” windows across different products or teams over a month.

Why it works

Staggering these blitzes spreads resource demands, reducing the risk of an “all or nothing” patch event. Smaller, focused sprints maintain momentum and allow teams to fix more thoroughly.

How to implement

Create a schedule (e.g., Week 1 for Team A, Week 2 for Team B). Gather vulnerability data, highlight top exposure issues, and coordinate with developers or system admins for each window. Focus on clearing the backlog of critical and high-exposure issues.

GenAI-Driven Executive Summaries

Use an AI tool to digest your cyber risk KPIs and craft an executive narrative for budget approvals.

Why it works

Clear, data-backed storytelling resonates with leadership. An AI-generated summary with metrics such as breach likelihood and impact can quickly translate complex security metrics into compelling insights, improving your odds of securing resources.

How to implement

Feed your KPI data (dashboards, reports) into a generative AI solution. Direct it to highlight trends, wins, challenges, and budget justifications in an executive-friendly format. Review and polish for accuracy, then present in quarterly reviews or budget meetings.

Designated Hot Zones

Identify specific “hot zones” that historically yield the highest impact or exploit activity.

Why it Works

Focusing on areas (e.g., database servers, external-facing apps) with a proven track record of high-impact or frequent attacks ensures that attention is not spread too thin. It also gives teams a clear sense of where to concentrate limited resources.

How to implement

Analyze vulnerability scan logs to find patterns of exploitation or frequent misconfigurations. Classify these components as “hot zones” and enforce tighter patch SLAs, additional monitoring, or regular pen tests specifically for them.