KUDELSKI SECURITY

PODIUM-READY RBVM

What Does a Winning Programme Look Like?

Executive Summary

Exposure management is a race against risk. The only way to win is to discover, prioritise, fix, and validate controls faster than adversaries can exploit weaknesses.

This eBook shows what good looks like in risk-based vulnerability management, how to benchmark your current qualifying position, and how to move up the grid every quarter with a team that can run the programme end-to-end. You will leave with a clear operating model, the metrics that travel to the board, and practical next steps that compound over time.

XPOSURE TEAM

Why This Matters Now

A Attackers are getting faster & more focused

CrowdStrike reports[1] that adversaries continue to compress the time between initial access and lateral movement. The fastest observed breakout time in the latest report is measured in minutes, not hours.

B Exploitation is not random

CISA's Known Exploited Vulnerabilities catalogue[2] lists flaws that attackers are using right now. If you align your queue to KEV, you'll focus on the risks that matter most.

C The cost of losing even a single race is real

MGM Resorts International forecast a $100M quarterly hit after its 2023 breach[5]. That's a figure that brings the business risk into sharp focus for any board, highlighting the real financial impact of cyber incidents.

D Healthcare offers another clear lesson

In 2024, the Change Healthcare attack[3] disrupted claims and pharmacy operations across the United States. Senate testimony[4] confirmed that the initial access path lacked multi-factor authentication.

What this means

The takeaway is straightforward. Don't try to fix everything at once. Focus on the issues that matter most, resolve them before adversaries can weaponize them, and show leadership that exposure is falling quarter by quarter.

What a Winning RBVM Programme Looks Like

2

A strong RBVM programme looks and feels like operations. People know their part. Context guides the queue. The cadence has to be repeatable.

Programmes falter when severity scores drive everything, when service expectations are unclear, and when platforms sit apart from IT service management.

A risk-based approach corrects this by focusing on what truly matters, routing work to named owners, validating outcomes, and showing measurable reduction over time.

The RBVM Workflow

1

Discover

Continuously discover vulnerabilities across your estate, including cloud, web applications, and access management.

2

Prioritise with context

Start with your most critical systems, anything internet facing, and vulnerabilities that are being exploited right now.

3

Remediate

Assign named owners and service level expectations that reflect the realities of each asset class.

4

Validate controls

Controls should be validated before closure so that a green tick means a real reduction in exposure.

5

Report

Trends executives understand (exposure time, KEV MTTR on critical assets, exception rates).

Start with business criticality

The systems that keep the organisation running get attention first. Add signals that show what is being exploited in the wild, such as entries from the Known Exploited Vulnerabilities list. Factor in whether an asset is exposed to the internet or shielded by strong controls.

With those inputs, you can focus on the small set of issues that truly matter, route them to named owners with clear timeframes, and use light automation to reduce friction and keep the queue moving.

A risk-based approach works because it turns vulnerability data into meaningful tasks.

The result is less noise, faster resolution, and a measurable reduction in exposure.

XPOSURE TEAM

The Team Advantage

Think of the platform as the car, and the expert operators as the pit crew. World-class programmes rely on a team that tunes the signals, maintains data quality, coaches owners, and sustains the operating cadence.

Risk-based vulnerability management is not a one-time purchase. It's a programme that matures quarter by quarter through consistent execution. The team keeps prioritisation honest, integrates the workflow into service management, validates outcomes, and presents precise results to leadership.

That's how scanner output becomes real risk reduction

Benchmark Yourself
‘Where Do We Qualify Today?’

3

Before you tune the programme, you need to establish where you are today. That’s how progress becomes visible to leadership and repeatable for the team. Use the checklist to get a clear read on four things: ownership, context, workflow, and proof.

The score is not a judgment. It’s a baseline. Once you have it, you can agree on the two or three moves that will matter most in the next ninety days, set simple targets, and measure against the same scale each quarter.

Answer each statement with yes or no. It should take only a few minutes, and you can review it with key stakeholders.

YES	NO	
☐	☐	Asset criticality is defined with the business and used in prioritisation.
☐	☐	Internet-exposed assets are tracked as a living set.
☐	☐	KEV-first: actively exploited CVEs influence your queue.
☐	☐	Threat intelligence informs prioritisation.
☐	☐	SLAs by asset class (not a one-size 48-hour promise).
☐	☐	Full ITSM integration: tickets include owner, impact, and recommended fix.
☐	☐	Exceptions have expiry and review dates.
☐	☐	Validation is standard (re-scan/control check) before closure.
☐	☐	The exec dashboard shows trends, not counts.
☐	☐	OT/ICS constraints are handled with segmentation/monitoring when patching isn’t viable.
☐	☐	A quarterly Plan-Run-Validate-Show ritual is in place.
☐	☐	Named owners for crown-jewel services (business accountability).

Sum up the **YES** to know your position!

11–12 points	9–10 points	5-8 points	0-4 points
Podium-Ready	Front Row	Midfield	Back of the Grid

Move Up the Grid With a 90-Day Cadence

4

Elite teams improve their qualifying position every quarter. The pattern is simple, predictable, and effective. Begin with a focused scope, such as internet-facing assets.

As data quality and ways of working mature, widen the field with confidence rather than noise.

PLAN

Weeks 0–2

Choose three moves that will change outcomes, not just activity.

Common starting points include using Known Exploited Vulnerabilities as a primary signal, enriching asset context for your most critical services, redesigning service levels by asset class, and automating validation where it is safe to do so.

Establish a baseline for a small set of metrics. Share the plan with the people who will do the work, so ownership is clear before you start.

RUN

Weeks 3–10

Choose three moves that will change outcomes, not just activity.

Common starting points include using Known Exploited Vulnerabilities[6] as a primary signal, enriching asset context for your most critical services, redesigning service levels by asset class, and automating validation where it is safe to do so.

Establish a baseline for a small set of metrics, and track progress consistently to demonstrate measurable improvement over time.

VALIDATE

Weeks 11–12

Confirm that fixes are in place or that compensating controls are working as intended. Close only when validation is recorded.

Prepare a one-page executive readout that shows the baseline, the current position, the risk removed, and the two or three moves planned for the next quarter.

Repeat this rhythm. The consistency matters as much as the content. A steady cadence turns intent into measurable progress and gives leadership a clear sight of improvement from quarter to quarter.

Metrics That Prove Risk Reduction

5

Leaders want a clear view that exposure is coming down. Operators need signals that guide the next hour of work. The right metrics do both jobs. They connect your daily queue to outcomes that matter in the boardroom, and they do it with evidence rather than volume.

QUARTERLY

Executive scorecard

Start with proof that you are racing the real field. Show the percentage of open and closed findings that appear on the Known Exploited Vulnerabilities (KEV) list and show the time to remediate those items on critical assets. This links your effort to live adversary behaviour rather than to theoretical severity.

Add a simple time-at-risk view for your crown-jewel services. Use median days to close to show direction without letting outliers dominate the story. Include the current exception rate for critical assets, and make it clear that exceptions expire and are reviewed on schedule. Close with a ninety-day exposure trend, so leadership sees momentum rather than snapshots.

Make the scorecard simple. Show four headline metrics and two trend lines. If a number slips, call it out and state what you will do differently in the next cycle.

DAY-TO-DAY

Your RBVM operator dashboard

Put the work where action happens. Show the queue by business service and by named owner. Break time to remediate down by asset class, such as servers, workstations, web applications, and OT systems. Track validation rate so that closure means reduction, not just status changes. For systems that cannot be patched, show that a tested control is in place and monitored.

Use the same north stars that drives the executive scorecard. Make KEV visible in the operator view and highlight items with active exploitation or credible threat intelligence.

CrowdStrike reports[7] that adversaries can move from a first foothold to lateral movement in minutes at the fastest end, and in around an hour on average. This means your dashboard must focus on what matters now.

How these measures fit together

The executive scorecard shows direction and builds trust with leadership. The operator dashboard shows what to do next and keeps momentum with the teams who do the work. Both rely on the same inputs.

They use live exploitation signals from CISA KEV. They use sensible measures such as time at risk and validation rate. They keep numbers small and meaningful so that everyone can act on them.

When the two views tell the same story, the programme feels coherent, and progress is easier to sustain.

An Architecture That Produces Results

6

A programme only works when its parts work together. Think of your RBVM architecture as a clear flow from signal to action to proof. When those connections are weak, RBVM becomes a reporting exercise. When they are strong, it becomes an operating model.

On one side, you have the sources that tell you what exists and what is vulnerable.

In the middle, you have a system that turns those signals into a single, prioritised view of risk.

On the other side, you have the platforms where work is assigned, tracked, completed, and evidenced.

Sources of truth

This is where raw findings become a workable queue. The platform links findings to your asset inventory, removes duplicates so the same issue is not counted twice, and adds the context needed to decide what matters most.

That context includes business criticality, whether the system is internet facing, whether the vulnerability is being exploited in the wild, and what controls are already in place. With that in place, the platform can rank work in a way that is clear, defensible, and focused on real exposure.

Service and configuration management

This is where action happens. The configuration database helps confirm what systems exist and who owns them. The service platform is where remediation work should live, because it is where teams already manage operational tasks.

The RBVM programme should create well-formed work items in the service platform that name an owner, explain the impact, and recommend a fix. Status should flow back automatically so reporting reflects reality. Closure should not be based on a status change alone. It should be based on validation that the exposure has actually dropped.

Closing the loop

Signals flow into the programme and evidence flows back out. Discovery identifies issues. Prioritisation selects what matters. Remediation addresses the problem. Validation confirms it is no longer present or that a compensating control is working.

That validation is what turns activity into proof. Without it, you only know what was planned. With it, you know what changed.

WEB APPLICATIONS

How to Make Findings Actionable

Web applications need a slightly different approach because they change often, sit close to customers, and can expose data quickly when something slips. The goal is the same as anywhere else. Turn signals into clear work, get fixes shipped predictably, and confirm the exposure has dropped.

1

Start

Start with authenticated scanning, which simply means scanning with the right access so you see what a real user can reach.

Tune the findings so teams are not buried in noise.

2

Then

Then route remediation work into your normal release cycle so fixes land in planned deployments, not last-minute fire drills.

Each work item should have a named owner, a clear reason to act, and a simple definition of done.

3

Close

Close the loop with validation. For web applications, that can be a clean re scan, a targeted retest, or verification that the vulnerable component has been updated and is no longer reachable.

When validation is built into closure, your reporting reflects what changed in the real world, not what someone hoped was fixed.

Team Over Tool: Why Managed RBVM Scales

6

Powerful machines do not win on their own. They win because a skilled crew keeps them fast, steady, and safe from the first lap to the last. Risk-based vulnerability management is the same.

A strong crew runs the programme

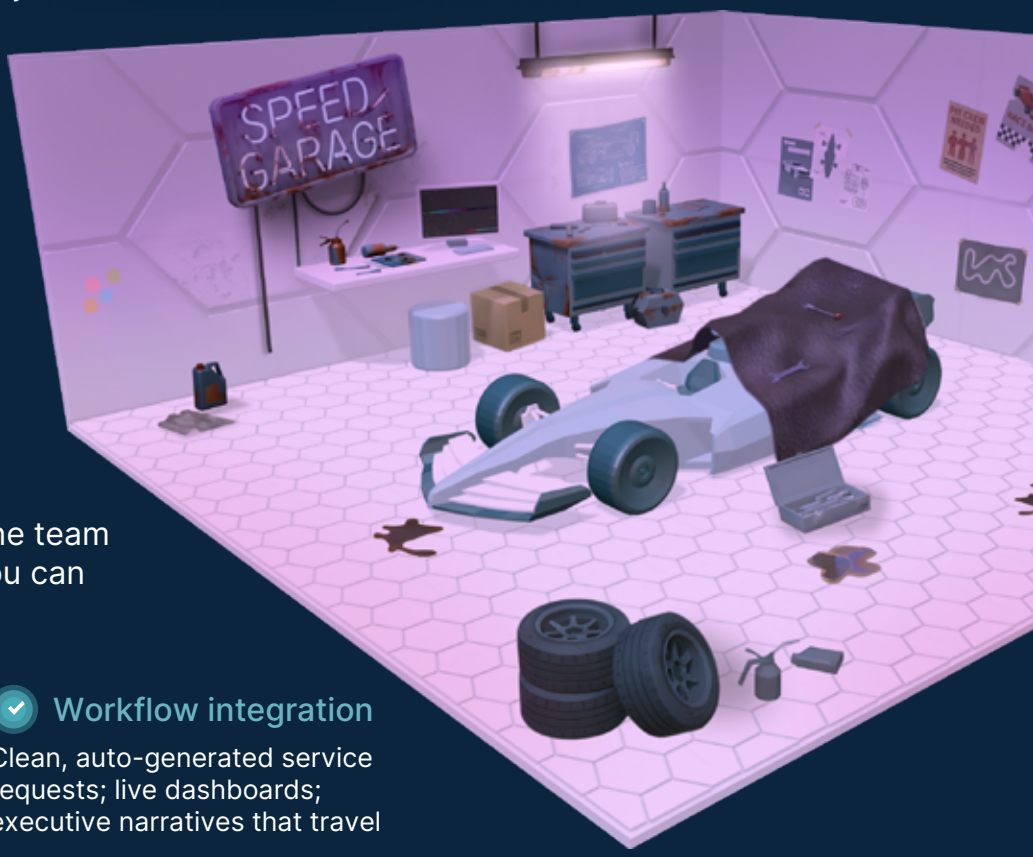
They tune prioritisation so that business-criticality, internet exposure, and live exploitation sit at the top of the queue. They blend data so each asset has one story and one owner. Workflows through service management, not side channels, and every ticket names an owner, explains the risk, and recommends a fix. Closure only happens after validation.

The rhythm is simple and repeatable

Plan the quarter. Run the work. Validate the outcome. Show the results. Start with the exposed perimeter and the services that matter most. Expand coverage as confidence grows, adding external attack surface monitoring and web application scanning when teams are ready to absorb the findings.

The benefits are practical

Owners get fewer remediation tasks, and each one makes sense. Leaders see time at risk falling on critical services and faster remediation on actively exploited vulnerabilities. Everyone sees the same story on screen and in the board pack. That is how tools become outcomes and how maturity climbs quarter by quarter.



What an expert pit-crew adds

The platform gives you power. The team turns that power into progress you can prove.

Prioritisation tuning

Blending KEV, threat intelligence, and asset criticality to make the queue workable

Workflow integration

Clean, auto-generated service requests; live dashboards; executive narratives that travel

Cross-client playbooks

Bring proven patterns so you skip the learning curve

Options as you mature

EASM and web app scanning to extend coverage without chaos

Cadence and coaching

Weekly ops, quarterly reviews, and unblockers

How Winning Teams Run RBVM

7

Winning teams treat RBVM as risk operations, not as a scan schedule. They set clear owners and service levels, and they work to a pace that never slips.

A

They start with live evidence

If a vulnerability is being exploited in the wild and the asset is critical or internet-facing, it goes to the top of the queue. Severity alone does not decide. Real-world exploitation and business impact do.

B

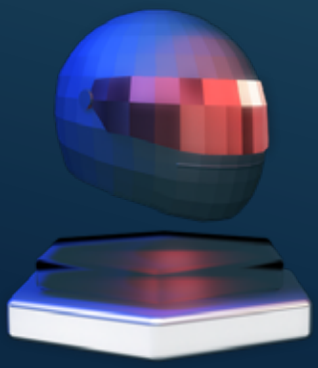
They add context to every item

Each piece of vulnerability data names the business service at risk, the accountable owner, and the recommended fix. Workflows through service management, so action and status are visible to everyone. Exceptions expire by default and are reviewed on time.

C

Validation is part of closure, not an afterthought

Closure only happens when there is evidence that risk has actually dropped. That evidence can be a clean re-scan on the affected asset, a verified compensating control that is live and monitored, or a targeted re-test that proves the exploit no longer works. Treat this as a definition of done. Build it into the workflow so every remediation task includes the validation method, the owner, and the timestamped result. Record the outcome in the same system that tracks the work so the dashboard and the board pack reflect reality, not intention.



What good looks like in practice

When validation sits inside the process, leaders see time at risk falling on critical services and faster remediation where attackers are active. The programme earns trust because every “closed” item is backed by proof.

- Re-scan results attached to the work item for patchable systems.
- Control verification for unpatchable cases, for example segmentation confirmed and monitored.
- Targeted functional tests for web applications, ideally tied to the release that delivered the fix.
- Expiring risk acceptances with a next review date and a named approver.
- Light sampling or peer review to keep quality high without slowing the programme.

RBVM CHAMPIONSHIP

Winning takes more than fast tools

You win by reaching the right risks first

That is how teams move from the chasing pack to podium

READY TO RACE?

If you want help benchmarking a starting position or shaping a ninety-day plan, speak with Kudelski Security, and we'll outline a clear path to a podium-ready RBVM programme.

Contact Us

Endnotes

1 https://www.crowdstrike.com/en-us/global-threat-report/

2 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

3 https://apnews.com/article/change-healthcare-cyberattack-unitedhealth-senate-9e2fff70ce4f93566043210bdd347a1f

4 https://www.cnbc.com/2024/03/27/unitedhealth-group-paid-over-3-billion-to-providers-since-cyberattack.html

5 https://www.bbc.com/news/articles/cy9pdld4y81o

6 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

7 https://www.crowdstrike.com/en-us/global-threat-report/