edgescan™

FEATURE OVERVIEW

Edgescan Remediation Playbook

Your vulnerability. Your environment. Your remediation plan.

Turn an individual vulnerability finding into a dated response plan, with technical instructions, containment steps, and a direct route to requesting an Edgescan retest.

Because "just patch it" isn't much of a plan

Your security team has found the vulnerability. Now someone has to decide what happens first, work out what needs to change, and check that the fix worked.

Every Edgescan finding comes with remediation guidance on how to address that type of vulnerability. The Edgescan Remediation Playbook complements that guidance; this AI feature uses the selected finding's actual asset details and evidence to generate a response plan for that specific instance on your system.

Less Preparation. Clearer Action

Give engineers a head start: Start with technical instructions for the affected system so engineers can spend less time researching how to apply the guidance

Act while the fix is being prepared: Identify steps to reduce exposure while the permanent fix is pending. For web-facing findings, the containment phase points to the Edgescan WAF Rule Generator

Look beyond the patch where relevant: Get steps to investigate whether the vulnerability may already have been exploited.

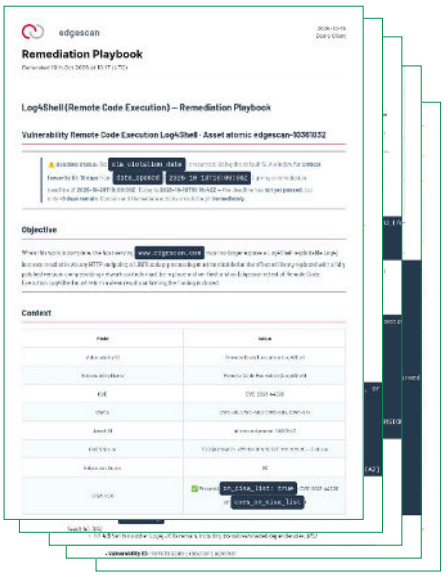
Keep the SLA in sight: Work from dated actions with overdue findings flagged so the team can see what needs immediate action.

Reduce the planning load on security: Give the system owner a plan they can review and work from without asking security to write every technical step

Support AI-assisted development: If your team works with AI coding agents, choose a specification they can pass on to their coding tool to help apply the fix.

Check the fix with an Edgescan retest

Every playbook includes an API call to request an Edgescan retest of that specific vulnerability. Use your Edgescan API token to make the request. The call is included in the on-screen playbook and the copied or downloaded version.



When the finding is clear but the next step isn't

Use the Remediation Playbook when:

Engineers need more detail before they can start a fix

Security is repeatedly preparing technical instructions for system owners

A permanent fix needs time, but exposure needs attention now

The team needs a clear plan for applying and checking a change

From first check to Edgescan retest

Each playbook covers four core phases. Where a compromise assessment applies, it appears between containment and the fix.

1 Validate

Steps to confirm the issue is real and still present

2 Contain

Actions to reduce exposure while the permanent fix is prepared

Check for compromise, where relevant

The playbook includes investigation steps when the vulnerability is listed in CISA's Known Exploited Vulnerabilities Catalog, is linked to known ransomware use, or allows remote code execution.

3 Fix

Technical instructions and copy-paste commands for engineers to review and use

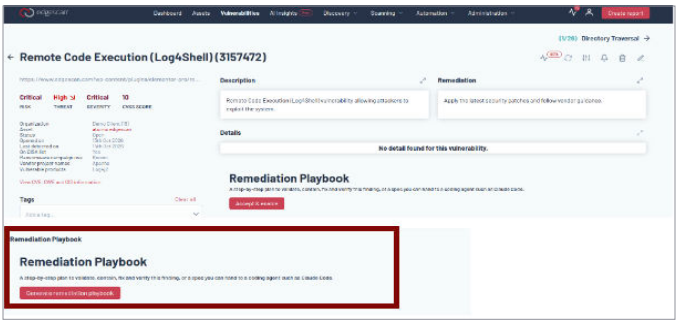
4 Verify

Steps and commands to check that the fix works, plus the API call to request an Edgescan retest

Where to find it in the Edgescan Platform

Open the vulnerability detail page and go to Remediation Playbook, directly below the Description and Remediation. Select Generate remediation playbook and choose your output format.

Your organization must accept the AI Insights data-sharing agreement before generating a playbook. Edgescan masks passwords, tokens and other secrets it detects in the evidence before sending it to the AI



Key Feature	What it means to your team
Details from the actual finding	The plan uses the affected asset's name, location, ports, protocols, and supporting evidence. Each playbook covers one finding
SLA- or risk-based target dates	Each phase has a target date. The fix deadline uses the finding's SLA violation date where available. Otherwise, Edgescan uses its default windows by risk: Critical 15 days, High 30, Medium 90, and Low 180. The playbook shows which basis it used. If a finding is overdue, the plan flags it and calls for containment and remediation to start immediately.
Recognized guidance and stated assumptions	The playbook follows NIST SP 800-40r4, NIST SP 800-61r3 and the CISA Vulnerability Response Playbook. The AI is instructed to state its assumptions and avoid inventing version numbers, advisory IDs or file paths, and link only to NVD, MITRE CWE, the CISA KEV catalog, the OWASP Cheat Sheet Series and the vendor's security page.
Two ways to use the output	Generate a remediation playbook for your team or a specification for an AI coding agent. Either output can be copied or downloaded in Markdown

Give your team more than a finding; give them a plan.

The playbook gives your team AI-generated instructions for review. Your team approves, applies, and tests changes through its own change control process. Target dates are set when the playbook is generated and stay fixed for that version.

Talk to your Edgescan representative today and see how you can utilize the remediation playbook.

sales@edgescan.com

edgescan

IRELAND | Unit 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26
UNITED STATES | 445 Park Avenue, 9th Floor, New York, NY 10022

edgescan.com | Copyright© 2026 Edgescan. All rights reserved.