SECURE CODE REVIEW
Hands-On Analysis for your Applications

Every programming language has its unique properties. Python is designed for readability and C applications handle their own memory management. Similarly, each language has security quirks which must be considered during a thorough source code audit.

Rhino Security Labs has application security experts well-versed in a wide range of languages, from Assembly and C code up to high-level scripting languages. A review with language-specific security expertise can mean the difference between identifying critical flaws and having a major data breach.

Penetration testing on production applications provides invaluable awareness of current vulnerabilities and potential damage if exploited.

TARGETED AUDITS FOR YOUR MOST IMPORTANT SOFTWARE

Using a hybrid approach, Rhino Security Labs consultants utilize best-in-class code review tools to scan full codebase and deep manual examination for areas of critical importance.

These select functions, such as user authentication and client-supplied parameters, contain the majority of security flaws– so that's where we perform the deep dive.

INTEGRATE CODE REVIEW INTO YOUR SDLC

Rhino Security Labs offers both stand-alone source audits and integrated code review as an ongoing part of a client's development process.

When incorporated into the regular SDLC, our application experts become a seamless part of your development team, ensuring each code push has been thoroughly reviewed by qualified security authorities. This enables you to:

- Identify flaws earlier in the development lifecycle
- Address bugs before they get pushed to production apps
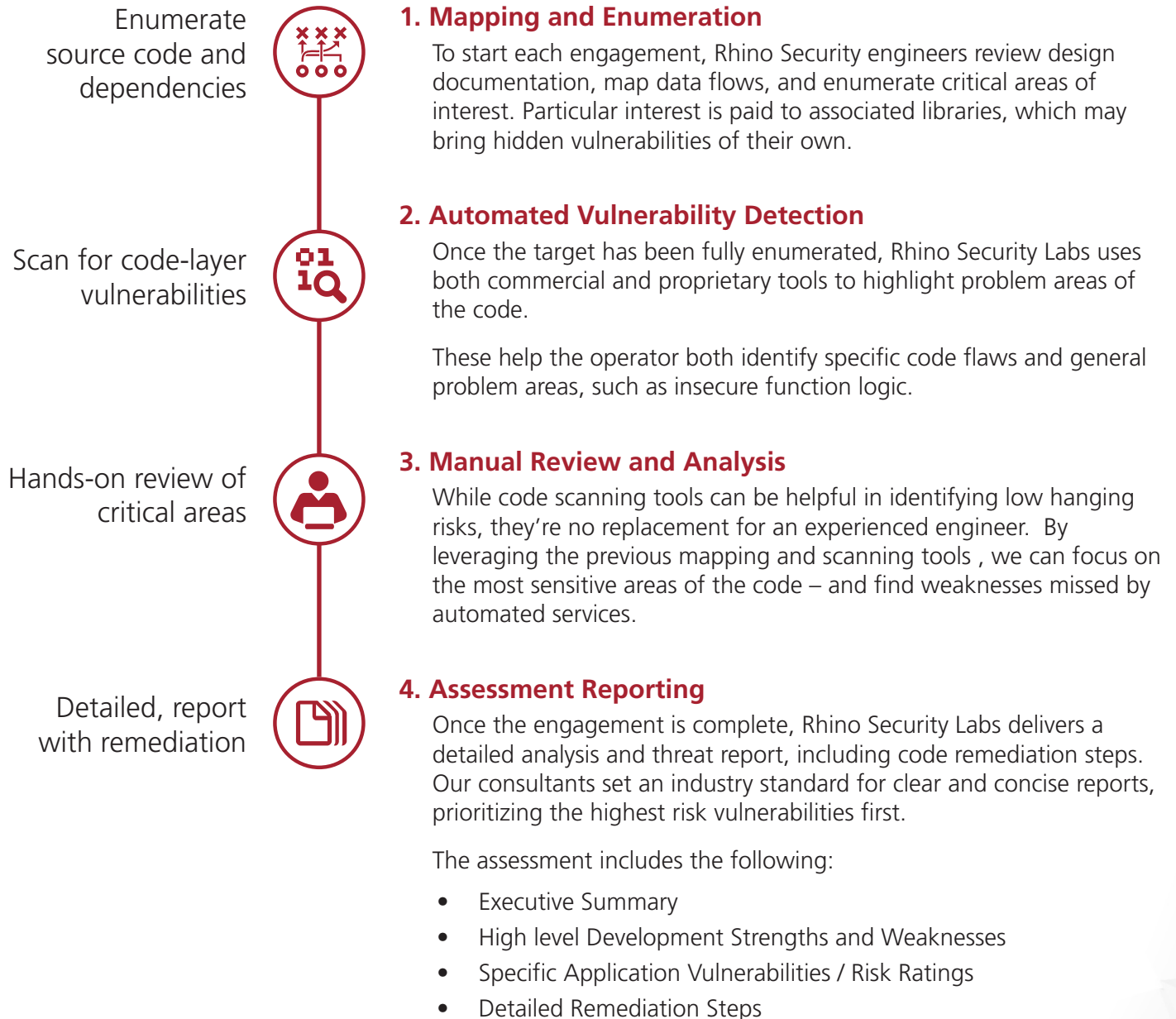- Target audits to your most important software

> *Rhino Security Labs found vulnerabilities and risks several other vendors had missed*
>
> **– Top 10 Financial Firm**

ASSESSMENT DETAILS AND METHODOLOGY

At Rhino Security Labs, each secure code review follows a proven methodology to ensure highly targeted, consistent engagements. Each engagement is executed with the following steps:

Enumerate source code and dependencies

1. Mapping and Enumeration

To start each engagement, Rhino Security engineers review design documentation, map data flows, and enumerate critical areas of interest. Particular interest is paid to associated libraries, which may bring hidden vulnerabilities of their own.

Scan for code-layer vulnerabilities

2. Automated Vulnerability Detection

Once the target has been fully enumerated, Rhino Security Labs uses both commercial and proprietary tools to highlight problem areas of the code.

These help the operator both identify specific code flaws and general problem areas, such as insecure function logic.

Hands-on review of critical areas

3. Manual Review and Analysis

While code scanning tools can be helpful in identifying low hanging risks, they're no replacement for an experienced engineer. By leveraging the previous mapping and scanning tools , we can focus on the most sensitive areas of the code – and find weaknesses missed by automated services.

Detailed, report with remediation

4. Assessment Reporting

Once the engagement is complete, Rhino Security Labs delivers a detailed analysis and threat report, including code remediation steps. Our consultants set an industry standard for clear and concise reports, prioritizing the highest risk vulnerabilities first.

The assessment includes the following:

- Executive Summary
- High level Development Strengths and Weaknesses
- Specific Application Vulnerabilities / Risk Ratings
- Detailed Remediation Steps

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.