Each programming language has its own unique properties. Python is optimized for readability, and C programs perform their own memory protection. Similarly, each language has security quirks that must be considered during a rigorous source code audit.

Infopercept has program security specialists well versed in a broad variety of languages, from Assembly and C programming to high-level scripting languages. An analysis of language-specific security experience may mean a difference between the identification of crucial vulnerabilities and a significant breach of records.

Penetration monitoring on production applications offers an indispensable understanding of existing flaws and future harm if abused.

**Targeted Audits for Your Most Important Software**

Using a mixed approach, Infopercept uses best-in-class code analysis software to search the entire codebase and deep manual scan for critical areas.

These select features, such as user authentication and client-supplied parameters, include much of the security bugs – so that’s where we take a deep dive.

**Integrate Code Review into Your SDLC**

Infopercept provides both stand-alone source checks and automated code analysis as part of the continuing implementation phase of the client.

When inserted into the daily SDLC, our application specialists become integral members of the production team, ensuring that any code push has been carefully checked by trained security authorities.

- Identify vulnerabilities early in the life cycle of production
- Address bugs before being moved to the development apps
- Target audits on the most relevant apps
Assessment Details and Methodology

At Infopercept, each safe code analysis follows a validated approach to ensure highly selective, reliable commitments. Each engagement shall be conducted in the following steps:

Enumerate source code and dependencies

1. Mapping and Enumeration

To begin each engagement, Infopercept engineers review the concept documents, chart data flows, and list essential areas of interest. Particular attention is given to affiliated repositories, which can give rise to hidden vulnerabilities of their own.

Scan for code-layer vulnerabilities

2. Automated Vulnerability Detection

If the goal has been thoroughly listed, Infopercept uses both commercial and proprietary software to illustrate the issue areas of the code.

This helps the operator to distinguish individual code bugs and general problem areas, such as unsafe functional logic.

Hands-on review of critical areas

3. Manual Review and Analysis

Although code scanning tools may be helpful in detecting low-hanging threats, they are no substitute for professional engineers. By using the previous mapping and scanning techniques, we will concentrate on the most vulnerable areas of the code – and discover weaknesses that automated services have overlooked.

Detailed, report with remediation

4. Assessment Reporting

If the engagement has been completed, Infopercept will include a full review and threat study, including code remediation. Our advisors set industry standards for transparent and succinct reviews, prioritizing the highest risk vulnerabilities.

The assessment must include the following:

- Executive Summary.
- High-level development of strengths and weaknesses.
- Specific application Vulnerabilities/Risk rating.
- Detailed remedial steps.
About INFOPERCEPT

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd. 2021

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Offices
UNITED STATES OF AMERICA
+1 516 713 5040
UNITED KINGDOM
+44 2035002056
SRI LANKA
+94 702 958 909
KUWAIT
+965 6099 1177
INDIA
+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd’s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.