Trail of Bits Security Review

Make informed decisions about your risk

Whether you need due diligence on a small codebase or have a complex platform that requires higher assurance, get a comprehensive understanding of your system's security posture through Trail of Bits' software assurance practice. A penetration test won't cut it, as false negatives aren't an option; you need a team that will find more subtle and complex bugs, that understands code-level flaws can lead to full system compromise.

Trail of Bits has unmatched skill at assessing your software and system security and digs deeper than other companies because we programmatically focus on identifying root causes and building foundational tools.

Leaders in technology, finance, and defense choose Trail of Bits

Trail of Bits combines high-end security research with a real-world attacker mentality to secure some of the world's most targeted organizations and products. Our security audits allow our clients to make informed decisions about risk and the security-relevant modifications necessary for a secure deployment.

We are leaders in infrastructure, Blockchain, and cryptography because of our expertise in:

- **Effective code analysis -** We find the bugs that other firms miss. In parallel, we assess code architecture with an iterative process that allows us to make holistic recommendations for eliminating entire classes of bugs.
- **Formal verification of code correctness -** When needed, we go a step further and confirm that your code behaves as intended, and only as intended.
- **Tool development -** We dig deeper than any other company to fix problems at the core, and we've built some of the best tools in the industry that address low-level vulnerabilities. We're proud of the quality of our tools and open-source many of them. You're invited to assess their quality yourself, or even use them to confirm audit results.
- **Ongoing support -** Past the formal end date of our projects, we provide best-effort support and guidance. You'll receive the tools we use in our assessments so you can continue to use them to mitigate issues. When we update those tools, you will receive the updates too.

What to expect during a Trail of Bits security review

Our expert staff applies decades of security knowledge in reverse engineering, cryptography, virtualization, and software exploits to deliver a detailed definition of your code's security and the difficulty of compromise from an external attacker's point of view.

The following is a list of what to expect from an audit:

- **Day 0** - To make the most of our engagement, we recommend that all customers read our blog post "How to prepare for a security review." Based on pre-assessment discussions, our experts diagnose and prioritize your concerns, determine how to make the greatest impact, and develop a plan that best fits your exact needs.
- **Day 1** - We identify known bugs and run safety checks extracted from previous assessments done to date. Within the first day, we find as many bugs and conduct as many safety checks as other firms do in weeks.
- **Daily** - We encode your requirements into our tools. Then, we programmatically verify that your code meets your goals. In parallel we review your code's architecture and design for evidence of best practices. When needed, we build application-specific tools to keep your codebase secure.
- **Weekly reports** - At the end of every week during our engagements, we provide our most-recent findings and recommendations so you can begin remediation immediately. We will educate your team so you can avoid discovered and known vulnerability categories in your code, prevent future implementation flaws, and refine your testing techniques.
- **End of Audit** - Trail of Bits delivers a final report suitable for publication. The final report provides context that should allow a technically knowledgeable reader to gain an accurate understanding of the security posture and risk landscape of your system.
- **After the Audit** - If needed, we schedule an abridged retest and deliver an updated report to confirm that all critical issues have been addressed.

Project Outcomes

Project deliverables are custom to each audit and include:

- A list of discovered issues with detailed explanations;
- Attack and exploit scenarios that illustrate real-world impact;
- Clear short- and long-term recommendations for remediation;
- Tools customized to your codebase to ensure lasting improvements; and
- Reference material used to support findings.

Upon request, we can:

- Write public reports for C-level readers that summarize the technical issues and business impacts necessary to make smarter decisions. For practitioners, our deliverables are customized to provide the most value to each client's technology.
- Provide customized versions of our tools and the training to leverage them.
- Help prepare blog posts to describe our findings to your customers.
- Deliver supplementary material to maintain your code's security: additional unit tests, custom testing harnesses to use with our tools, etc.

Success Stories

- Kubernetes - a container orchestration system written in Go, reviewed broadly to discover dozens of issues, produce a threat model and a whitepaper.
- Western Digital - reviewed an encrypted hard drive firmware for cryptographic flaws.
- RandomX - reviewed an ASIC-resistant Proof-of-Work algorithm.
- Compound - a distributed exchange written in Solidity that runs atop Ethereum, reviewed from architectural, oracular, and on-chain perspectives.
- Paxos Standard - Ethereum smart contracts, reviewed for low-level security risks and compliance with NYS DFS NYCRR500 regulations.
- Cosmos - a decentralized network of independent blockchains powered by Tendermint.
- Loom - a Layer-2 scaling (or side-chain) solution for Ethereum.
- Centrifuge - a decentralized platform to connect the global financial supply chain.
- Pantheon - an Ethereum client written in Java.

Additional companies that allowed us to speak about our work with them can be found on our "publications" repository on GitHub.

Areas of Expertise

- **Cryptography:** Our engineers have extensive experience crafting and reviewing cutting edge and widely used cryptographic libraries. We have worked with developers on a spectrum of tasks ranging from finding bugs in existing code to building entirely new libraries that can be integrated into a codebase. We know where to look for bugs and how to fix them.
- **High-assurance software:** We are no strangers to high-assurance work. With a staff of expert security engineers responsible for shipping code in complex systems on a daily basis, our engineers work to make products markedly more secure. We build secure software updaters, low-level software libraries, and high-assurance operating system components to harden existing infrastructure with a realistic, threat-focused approach.
- **Smart Contracts, Blockchain, and Application Security:** Our expert staff brings decades of security knowledge to the field of smart contracts and blockchain implementations, and keeps informed about the latest developments in security. Applied in combination with our unique expertise with static analysis, fuzzing and concolic testing, we dig deeper into the design of smart contracts, consensus algorithms, network protocols, and other related components than any other team, to identify design-level risks and implementation vulnerabilities. We provide recommendations on best practices, and educate teams on common and novel security flaws and testing techniques.
- **Threat Modeling:** We provided threat modeling exercises in multiple styles, such as NIST 800-154 ("Guide to Data-Centric System Threat Modeling") and Adam Shostack's "Threat Modeling: Designing for Security." Focusing on capturing, organizing, and analyzing application development and security controls, we provide informed recommendations about security risk at technological, procedural, and design levels.
- **Manual and Automated Code Verification:** Code verification gives the highest degree of trust possible, and we use a combined approach to identify a system's security risk. In contrast to a purely manual approach, our assessments take advantage of our automated analysis tools to verify and cover all the behaviors of the code. As opposed to a purely formal verification approach, our review benefits from our manual expertise and automated testing tools to explore threats that are out-of-scope of formal verification.

From Our Clients

- Loom: “We want to thank @trailofbits for doing an amazing job helping us audit #PlasmaChain security.”
- Pegasys: “Trail of Bits's engineers, who bring deep backgrounds in security and Java, discovered some obscure vulnerabilities and bugs.”
- MakerDAO: “Trail of Bits, who is a world leader in the information security industry, particularly around bytecode analysis of compiled software.”

Want to know more?

Visit our Blog or drop in on our blockchain office hours	Check out our open source tools like Manticore and Crytic	Join us at Empire Hacking	Follow us on Twitter

Let us help with your most difficult security challenges! Visit our Contact Us page to get started.

Frequently Asked Questions

How is the level of effort (LOE) determined for my project?
Depending on your goals and expectations, we offer fixed-fee security reviews in different buckets of effort:

Tiny: Anywhere from 1 day to two engineer-weeks of effort
- Scoped to fit tight timelines or budgets
- A best effort spot check of the codebase to quickly identify low hanging fruit

Small: 2 calendar weeks x 2 engineers = 4 engineer weeks
- A focused due diligence review of the codebase

Medium: 3 - 4 calendar weeks x 2 engineers = 6 - 8 engineer weeks
- A detailed, in depth review of the codebase

Large: 5 - 6 calendar weeks x 2 engineers = 10 - 12 engineer weeks
- A deep dive into the more strategic issues within the codebase as well as custom tooling and verification

Retainer Services: Monthly fixed-fee
- Monthly help with security concerns that come up e.g., off-chain questions about authentication and authorization, key storage, cryptography, etc.

How is the cost determined for a security review?
We charge a standard rate per engineer per week for each review. Projects are typically done by pairs of engineers, therefore the number of engineer-weeks incurred will be completed in half the number of calendar-weeks.

Are fixed fee projects the only agreements Trail of Bits offers?
No. We offer Time & Materials “bucket of hours/weeks” agreements used until all service hours are completed. Time and materials are billed monthly for hours worked.

I have a tight budget, but security is a priority to me. How can Trail of Bits help?
Since it is our job to help keep you safe, first and foremost, we make recommendations for level of effort by prioritizing security and the overall outcome. However, we recognize that's not always how things work for our customers and time and budget constraints may necessitate a shorter project. If that's the case, we are able to dial our efforts closer to your expectations to ensure you are doing your due diligence.

What are some ways to reduce the LOE associated with my project?
In place of a final report, we can share a private GitHub repository with project deliverables:

- Identified security issues will be filed as issues in the repository
- Analyses and security tool integrations will be checked into the source repository

This saves more time for code review by eliminating time spent writing a PDF document.

As always, we will provide a final discussion of the findings lasting one hour with one or more technical representatives from the Customer team. This meeting will cover flaws identified during the assessment in depth and offer guidance on structuring remediation efforts and more effective security testing.

How are projects staffed?
Projects are collaborative and are typically done by pairs of engineers. We have a deep bench of experts in many different disciplines and technology areas, and will staff the project to target the help you need most.

What if I need a retest?
Our statements of work include an optional retest usually lasting to 1-3 days. If a retest can be completed in less than 2 hours, we will be happy to review the fixes at no charge. If the fix review requires more than 4 hours of effort, we will invoice for 1-3 days of effort depending on hours worked.