Trail of Bits Citation Guidelines

These guidelines explain how our clients may use Trail of Bits assessment work products in their sales, marketing, and/or promotional materials.

Trail of Bits has created these guidelines to help parties understand how their company can use the results of a Trail of Bits security review in a fair and objective fashion to communicate the strengths of their service or product. Trail of Bits strives to create guidelines that uphold a mutually respectful environment that is fair to all parties and reinforce Trail of Bits' value as an objective and independent security provider.

In addition to publishing audit work products, Trail of Bits may selectively engage in co-marketing activities with clients. These activities could include joint social media posts, co-authored blogs, case studies, or live streams. If you're interested in exploring co-marketing opportunities, please contact your Trail of Bits Project Manager for more information. Detailed guidelines for co-marketing initiatives can be found in Appendix A.

Trail of Bits Security Review Methodology

Our evaluations allow our clients to make informed decisions about risks to their systems and the security-relevant modifications that may be necessary for a secure deployment. Using our custom tools and unique expertise with static analysis, fuzzing, and concolic testing, we serve as a knowledgeable, dedicated adversary to identify vulnerabilities that otherwise go undetected.

Our assessments estimate the overall security posture and the difficulty of compromise from an external attacker. We identify design-level risks and implementation flaws that illustrate systemic risks. At the conclusion of every assessment, we provide recommendations on best practices to improve resistance to attacks and educate in-house security teams on common and novel security flaws and testing techniques.

At the end of every assessment, Trail of Bits provides a final work product analyzing the system's overall security risk based on the findings. We encourage our clients to publicly share assessment results, and we often assist in reviewing blog posts or white papers for publication. We have developed guidelines for citing the company in published work to protect the message delivered with the Trail of Bits name attached to it.

Note: These guidelines do not override any obligations under the MSA or constitute our consent to disclose Trail of Bits confidential information or to use Trail of Bits' name or trademarks.

Trail of Bits Work Product Publication Guidelines

All parties, whether clients or third parties, must follow these guidelines when sharing or referring to Trail of Bits or a Trail of Bits work product.

All Trail of Bits work products will include either a “PUBLIC“ or “CONFIDENTIAL“ designation in the bottom right corner to clearly identify the distribution status.

Publication Process

1. The client informs Trail of Bits of their intention to publish the work product(s).
2. Trail of Bits copyedits the work product and finalizes it for publication. The work product will include a “PUBLIC” disclaimer in the bottom right corner.
3. Trail of Bits publishes the work product on its GitHub Publications page the same day as the client’s announcement.
4. The client links to the published work product on Trail of Bits’ GitHub Publications page in their announcement.
5. Clients who wish to publicly share a previously confidential work product must first contact Trail of Bits to request appropriate modifications suitable for public release. Only after Trail of Bits approval and modification may the work product be made publicly available through the official Trail of Bits publication channel.
6. The client provides Trail of Bits with an opportunity to review/suggest messaging in prewritten content, such as but not limited to the following, before publicly sharing it:
    a. Blog posts
    b. Social media posts
    c. Press releases
    d. Quotes or comments given to the press

Work Product Publication Guidelines

Work Product Hosting and Distribution

- **No modifications permitted**: All parties may not create copies, excerpts, or derivative versions of, or make any modifications to, Trail of Bits work products, letters of attestation, or other work products. All content must remain in its original, unaltered form.
- **Official sources required**: All parties making public references to Trail of Bits work products or letters of attestation must direct users to the official Trail of Bits publication to ensure document integrity and accuracy.

- **External confidential sharing**: Clients may share confidential work products with external parties such as investors, partners, or vendors. Clients must distribute materials only in their original, unmodified form. Clients are prohibited from making any alterations to content, format, or structure when sharing externally.
- **Distribution categories**: Trail of Bits work products are either confidential or public. Confidential work products may be shared internally within the client organization or externally with specific third parties under confidentiality or business relationships. Public work products are available for open, unrestricted sharing. “Public“ refers to open, unrestricted sharing accessible to anyone (websites, social media, press releases).
- **Work products defined**: “Work products“ include any materials Trail of Bits produces and shares with clients under the agreements, including work products, letters of attestation, rapid reviews, and any other work products.

Coordination and Approval

- Clients must coordinate with Trail of Bits to approve language for any announcements, publications, or descriptions of work.
- Approval is required for tagging Trail of Bits’ social media handles.
- Approval is required for using the Trail of Bits logo.
- Approval is required for mentioning Trail of Bits on any website page.
- Clients should not announce their intention to work with Trail of Bits before an assessment is complete.

Language and Terminology

- Prohibited terms:
    - Clients must not refer to Trail of Bits as a “partner.“ Trail of Bits is solely contracting with clients as a vendor.
    - The full name “Trail of Bits“ must be used; shortening the name to TB, Trail of B, or any other variation is prohibited.
    - Clients must not use the term “critical” to refer to vulnerabilities; Trail of Bits work products use high, medium, low, informational, and undetermined severity levels.
- Avoiding absolute statements:
    - Clients must avoid using absolute phrases like “Our company passed the Trail of Bits audit.“

- Accurate representation of audit scope:
    - Clients must avoid language implying comprehensive security based solely on the audit.
    - Clients should accurately specify the scope of the assessment, acknowledging that the audit covers only specific aspects or components of their product or system.
    - Trail of Bits' assessments are not checkboxes or graded work products, but assessments with recommendations for improvements.
- Avoiding implied endorsement:
    - Clients must refrain from using the name "Trail of Bits" in assertive phrases that imply endorsement.
    - Phrases suggesting perfect or complete security post-audit must be avoided.

Logo and Brand Usage Guidelines

- Do not use Trail of Bits Brand Assets as part of any of your own trademarks, logos, company names, icons, product or feature names, domain names, social media handles, or avatars.
- Do not modify Trail of Bits Brand Assets in any way, including changing colors, dimensions, obstructing or printing over any part of the asset, or adding your own design elements.
- Do not imitate the distinctive look and feel of Trail of Bits' website, apps, logos, trade dress, slogans, taglines, color scheme, icons, or marketing materials.
- Do not register or use a domain name that incorporates "Trail of Bits" or any confusingly similar term.
- Explicit permission from Trail of Bits is required before using its logo on any social media platforms, websites, blogs, press releases, or other forms of media.
- Full details on logo and brand usage are available in the Trail of Bits Brand & Style Guide.
- Approved clients may find copies of the logo on the Trail of Bits website.

Social Media Guidelines

- After approval, tag Trail of Bits using the following social media accounts:
    - X: @trailofbits

    - LinkedIn: https://www.linkedin.com/company/trail-of-bits
    - Mastodon: https://mastodon.social/@trailofbits@infosec.exchange
- For blockchain publications only:
    - If Trail of Bits agrees to reshare a client's blockchain-related post, these handles will be used:
        - X: @trailofblocks
        - Warpcast: @trail-of-blocks
    - Note: Trail of Bits does not guarantee retweets or additional posts from its main account.

Citation Examples

Proper and improper examples of mentioning and citing Trail of Bits are provided to guide clients in their publications. More examples can be found on our GitHub Publications page.

Proper Examples

- "Our Product's GitHub repository includes documentation, a comprehensive test suite, and an independent third-party audit by the security research firm Trail of Bits."
- "We also have a new audit available, thanks to the Trail of Bits team. We engaged Trail of Bits to undertake an audit of all three libraries mentioned above, with the RZL MPC paper and MPC wiki as documentation/guidelines for expected behavior."
- "Sweet B is designed to provide a new level of safety and assurance in open-source elliptic curve cryptography and its GitHub repository includes documentation, a comprehensive test suite, and an independent third-party audit by the security research firm Trail of Bits."
- "We are proud to announce that the etcd team has completed a 3rd party security audit for the etcd latest major release 3.4. The third party security audit was done for etcd v3.4.3 by Trail of Bits. A work product from the security audit is available in the etcd community repo."

Improper Examples

- ❌"We have partnered with Trail of Bits for an upcoming security review of our new product, stay tuned for the results!"
    - Issue: Clients must not refer to Trail of Bits as a "Partner."
- ❌"Trail of Bits confirmed that our smart contracts are secure" or "We passed a Trail of Bits audit"
    - Issue: Clients must avoid using absolute phrases.
    - Issue: Clients must not use phrases that can be interpreted as their project or product being completely secure now that a Trail of Bits audit is complete.

Enforcement of Guidelines

Trail of Bits requires explicit permission for the use of our name, logo, social media handles, and any of our work in public domains. If a client or any third party uses these assets without prior authorization, we will take the following actions:

1. **Immediate request for compliance:** Trail of Bits will promptly reach out to the involved party to request edits or removal of the unauthorized content.
2. **Legal enforcement measures:** If the requested action is not taken in a timely manner, Trail of Bits will file a Digital Millennium Copyright Act (DMCA) violation against the offending party.

These steps ensure that our brand integrity and intellectual property rights are protected, maintaining the accuracy and integrity of information associated with Trail of Bits.

Appendix A: Co-Marketing Guidelines

This appendix provides detailed guidelines for co-marketing initiatives with Trail of Bits.

Engagement Policy

- Trail of Bits engages in co-marketing activities selectively, based on the specifics of each case.

Types of Co-Marketing

We have successfully collaborated on various co-marketing initiatives, such as the following:

- **Social media posts:** Jointly branded posts to promote collaborative efforts.
- **Blogs:** Co-authored articles or guest posts highlighting mutual work.
- **Case studies:** In-depth analysis and documentation of joint projects.
- **Live streams/webinars:** Real-time, co-hosted events discussing industry topics or showcasing collaborative projects.

Process for Co-Marketing

1. Contact your Trail of Bits Project Manager to discuss the co-marketing opportunity.
2. If the project is deemed suitable, you will be connected with our Marketing Manager for further steps.
3. Any co-marketing content must be reviewed and approved by Trail of Bits before publication to ensure alignment with our brand guidelines and messaging.

Flexibility and Adaptability

Each co-marketing initiative is tailored to fit the unique requirements of the collaboration, ensuring that both parties benefit and the integrity of the Trail of Bits brand is maintained.