ROAR Third-Party Vendor Assessment Report

Vendor: Sentry
Assessor: Adam Richie-Halford, ROAR Information Security Officer

Overview

Sentry is a popular application monitoring platform used to track and resolve software issues. This assessment evaluates Sentry's compliance with recognized standards and verifies its suitability for integrating with ROAR's monitoring needs.

Certifications and Compliance

- **SOC 2 Type II**: Sentry has achieved SOC 2 Type II certification, indicating that it meets high standards for security and confidentiality in data management. This certification ensures that Sentry's internal controls protect customer data against unauthorized access.
- **ISO 27001**: Sentry is certified under ISO 27001, an international standard for information security management systems (ISMS). This certification demonstrates GitHub's commitment to systematically managing and protecting sensitive information.

Sentry's SOC 2 report and ISO 27001 certificate are available via our Sentry account or upon request. Further details are on Sentry's Security and Compliance page.

Security Practices

- **Data Encryption**: Sentry encrypts data at rest using AES-256 and uses TLS to secure data in transit, maintaining strong protection for sensitive information.
- **Access Management**: Sentry employs role-based access control and supports multi-factor authentication (MFA) to limit access to authorized personnel.
- **Incident Response**: Sentry has a structured incident response plan in place, with real-time monitoring and protocols for responding to security incidents.

Conclusion

Sentry's compliance with SOC 2 Type II and ISO 27001 certification, along with its strong security practices, make it a suitable choice for integrating monitoring and error tracking with ROAR.