PocketSOC™

Security & Trust Overview

Version: 1.0 | Last Updated: February 2026

Security is foundational to PocketSOC. The platform is designed and operated using secure engineering practices intended to protect customer data, preserve system integrity, and meet modern enterprise security expectations.

This document provides a high-level overview of the security practices, development approach, and operational safeguards used for PocketSOC. It is intended for pre-sales review and customer trust discussions and avoids sensitive implementation details.

Product Overview

PocketSOC is a mobile incident response application that helps security teams monitor alerts and take response actions from supported security platforms. The product includes a cloud-hosted backend used for account management, configuration, and notification workflows.

- Deployment model: Mobile iOS application with a cloud-hosted backend service.
- Primary use case: Security operations visibility and response workflows across connected integrations.
- Customer credentials remain under customer ownership and administrative control.

Secure Development Lifecycle (SDLC)

PocketSOC follows a lightweight but structured secure development lifecycle appropriate for an early-stage security product.

- Security considerations are incorporated during design and feature planning.
- Code changes are validated through automated checks and build verification.
- Static analysis and secure coding practices are applied as part of ongoing development.
- Testing includes functional validation and user acceptance testing with test users.
- Continuous improvement informed by testing feedback and operational experience.

Security Testing & Validation

Security testing is performed at a high level to reduce common software risks and improve overall code quality.

- Static application security testing (SAST) is used to identify common coding risks.

- Build and dependency validation are performed during development cycles.
- Findings are reviewed at a high level and remediated based on severity and context.
- Detailed vulnerability findings are not publicly disclosed.

Authentication & Access Control

PocketSOC uses authentication and access controls designed to limit unauthorized access and protect customer data.

- User authentication and account management are handled through the cloud-hosted backend.
- Role and access configuration is managed through the administrative portal.
- Sensitive integration credentials are stored securely and scoped to customer profiles.

Data Handling & Encryption

PocketSOC is designed to minimize data retention and exposure while supporting security operations workflows.

- Data transmitted between app, backend, and integrations is protected using industry-standard encryption (TLS).
- Sensitive values are handled with secure storage mechanisms appropriate to the platform.
- Data access is limited to what is required for product functionality.

Infrastructure & Hosting

PocketSOC uses a cloud-hosted architecture built on established cloud infrastructure providers.

- Hosting model: Cloud-hosted backend services.
- Infrastructure providers maintain independent third-party security certifications (e.g., SOC 2).
- Infrastructure components are configured following security best practices and reviewed periodically.

Third-Party Integrations

PocketSOC integrates with third-party security platforms to retrieve alerts and perform response actions.

- Integrations operate using customer-provided credentials or authorization flows.
- Actions taken within the app are executed via vendor APIs with customer-granted permissions.
- Integration behavior and capabilities may vary based on vendor APIs and customer configuration.

Responsible Disclosure

Security issues can be reported through designated support or security contact channels. Reported issues are reviewed and prioritized based on severity and impact.

Continuous Improvement

PocketSOC evolves continuously, and security practices are reviewed and refined as the product grows. Improvements are driven by development learnings, testing outcomes, and customer feedback.

Security Commitment

PocketSOC is committed to maintaining a strong security posture as the platform evolves. Security considerations are integrated into product design, infrastructure management, and operational processes to support customer trust.