eventus™

eventussecurity.com

SOFTWARE SECURITY

Managed Application Security Services

Minimize the risk of a breach by identifying and exploiting business critical vulnerabilities with Eventus's Managed Software Security expertise

WHAT EVENTUS OFFERS

Our assessors have the experience and expertise to deliver high-value test results, as we conduct around 250 managed application security tests a month.

We follow a top-down approach in order to ensure that your business needs take precedence and are executed with adequate safeguards so as to prevent and mitigate the risks of cyber incidents. We work with several industry defined enterprise security frameworks like **SABSA, TOGAF, COBIT, NIST, ITIL, and ISO and OWASP and SANS** application security guidelines to model software security that support your critical business initiatives.

Our review framework is flexible, scalable, and applicable to any industry sector. And the outcome of the review process is a detailed report that identifies opportunities for improvement and provide detailed guidance so as to reinforce the strength and agility to adapt to an ever-changing threat landscape.

Key elements of Eventus's Security Architecture Review and Threat Modelling process includes:

- **Authentication & Authorization Review:** Ensures that only verified users have access to sensitive data.
- **Data Encryption Assessment:** Evaluates encryption mechanisms for data in transit and at rest.
- **Secure Code Review:** Identifies vulnerabilities like SQL injection and cross-site scripting (XSS) in the codebase.
- **Security Testing:** Includes penetration testing, vulnerability scanning, and static/dynamic analysis.
- **Access Control Assessment:** Reviews role-based access control (RBAC) and the principle of least privilege implementation.
- **Third-Party Security Compliance Review:** Ensures adherence to compliance standards such as ISO 27001, SOC 2, GDPR, and HIPAA.

Key Benefits

- **Proactive Security:** Our approach helps identifies potential vulnerabilities early in the development lifecycle.
- **Risk Assessment:** Enable our customers with informed decision-making by understanding the likelihood and impact of threats.
- **Targeted Mitigation:** Expert personnel and AI mechanisms, help prioritize security controls based on the most critical risks.
- **Improved Communication:** Provides a clear document for stakeholders to understand the system's security posture.

MITIGATION STRATEGIES:

- **Security Controls:** Specific security measures to address identified threats (e.g., encryption, access controls, input validation, network segmentation).
- **Implementation Details:** How the security controls will be implemented and monitored.
- **Residual Risk:** Remaining threat level after applying mitigation strategies

© 2025 Eventus Security Private Limited. All Rights Reserved.

REVIEW AND VALIDATION:

- **Stakeholder Feedback:** Input from relevant stakeholders regarding the identified threats and proposed mitigations.
- **Prioritization:** Ranking of threats based on their likelihood and impact to guide mitigation efforts.
- **Re-evaluation Plan:** Process for periodically reviewing and updating the threat model as the system evolves

Choose the type of assessment and depth of test to best match the risk profile of each application in your portfolio. Our Managed Software Security combines multiple testing tools, automated scans, and in-depth manual tests to give you the most comprehensive application security evaluation.

Contact us at

sales@eventussecurity.com

www.eventussecurity.com

©2025 Eventus Security Private Limited. All Rights Reserved.