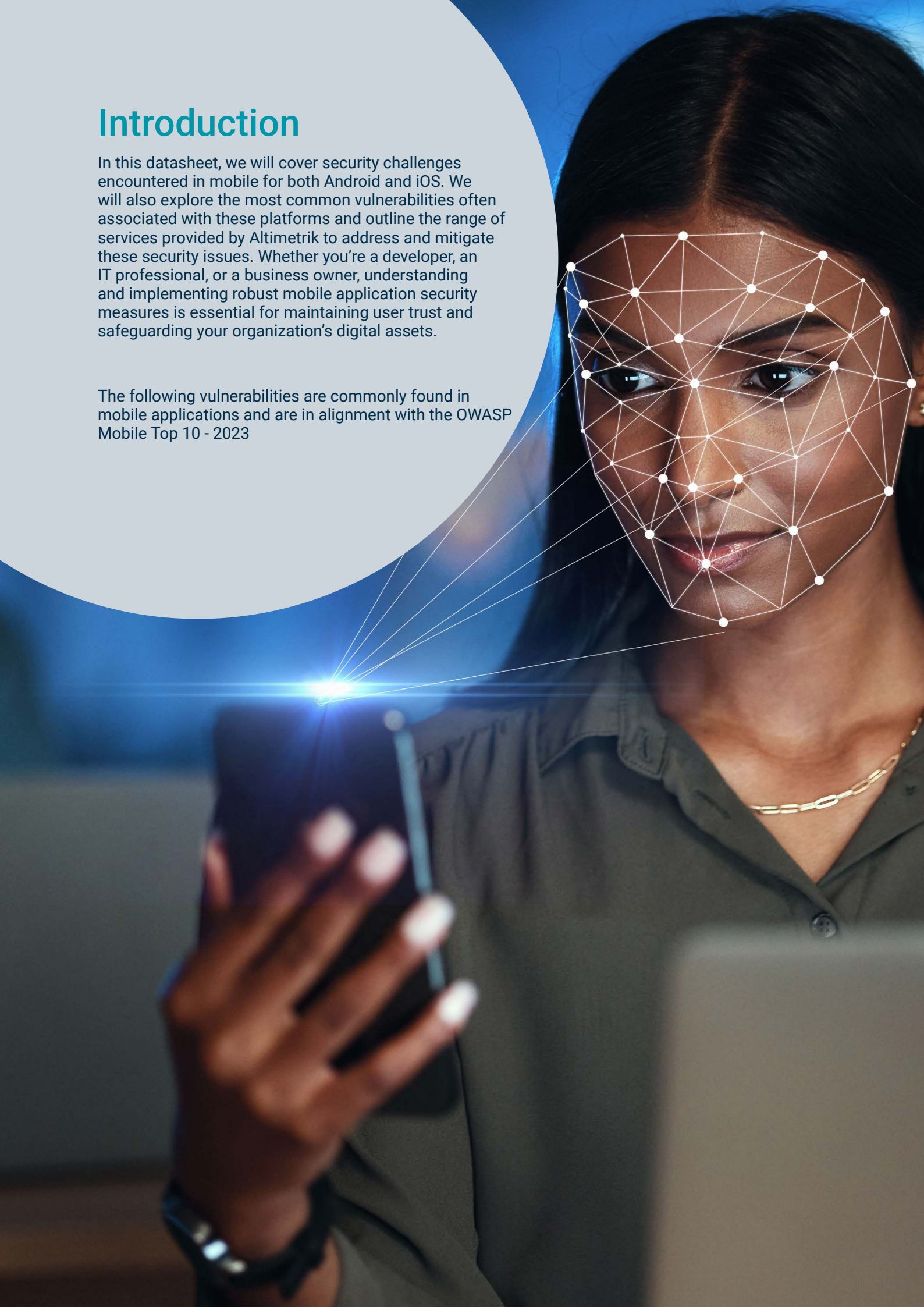
ALTIMETRIK

Mobile Application Security Services Datasheet

Introduction

In this datasheet, we will cover security challenges encountered in mobile for both Android and iOS. We will also explore the most common vulnerabilities often associated with these platforms and outline the range of services provided by Altimetrik to address and mitigate these security issues. Whether you're a developer, an IT professional, or a business owner, understanding and implementing robust mobile application security measures is essential for maintaining user trust and safeguarding your organization's digital assets.

The following vulnerabilities are commonly found in mobile applications and are in alignment with the OWASP Mobile Top 10 - 2023



OWASP Mobile Top 10 - 2023

1. **Improper Credential Usage:** This vulnerability refers to the improper handling of credentials, including the use of hardcoded credentials within the application's source code or configuration files. To prevent this vulnerability, developers should avoid using hardcoded credentials and ensure that user credentials are handled securely, including encryption during transmission and avoiding storing them on the device.

2. **Inadequate Supply Chain Security:** Potential exploitation of vulnerabilities within the development and distribution process of the app is evidence of a supply chain security issue. Attackers can manipulate the app's functionality by inserting malicious code or exploiting weaknesses in third-party components. An attacker can insert malicious code into the mobile app's codebase or modify the code during the build process to introduce backdoors, spyware, or other malicious code.

3. **Insecure Authentication/Authorization:** This vulnerability references the potential exploitation of weaknesses in the processes that verify and grant access to users. Attackers, typically using automated tools, can exploit these vulnerabilities in two main ways. They can either fake or bypass authentication directly with the backend server, or they can log in as a legitimate user and then access vulnerable parts of the application.

4. **Insufficient Input/Output Validation:** Mobile applications that fail to properly validate and sanitize data are at risk of being exploited through attacks specific to mobile environments, including SQL injection, Command Injection, and cross-site scripting (XSS) attacks.

5. **Insecure Communication:** Most modern mobile applications exchange data with one or more remote servers. When the data transmission takes place, it typically goes through the mobile device's carrier network and the internet, a threat agent listening on the wire can intercept and modify the data if it transmitted in plaintext or using a deprecated encryption protocol.

6. **Inadequate Privacy Controls:** Mishandling of personally identifiable information (PII) within mobile applications constitutes vulnerabilities in inadequate privacy controls. PII includes sensitive data like names, addresses, and financial information. If not properly protected, attackers may exploit this information for fraudulent activities, blackmail, or other harmful actions.

7. **Insufficient Binary Protections:** This refers to a vulnerability where mobile app binaries, which contain valuable information or critical code, are not adequately safeguarded. Attackers can exploit this by reverse engineering the binary to extract sensitive data or by tampering with the code to bypass security checks.

8. **Security Misconfiguration:** Improper setup of security settings, permissions, and controls, can lead to vulnerabilities and unauthorized access. This vulnerability allows attackers, including those with physical access to the device or malicious applications, to exploit weak configurations, potentially accessing sensitive data or executing unauthorized actions within the app.

9. **Insecure Data Storage:** This refers to the improper handling of sensitive information, making it vulnerable to unauthorized access. Threat agents like skilled adversaries, malicious insiders, cybercriminals, and others can exploit weaknesses like weak encryption and improper data protection. Common manifestations include storing passwords in plain text, inadequate encryption, and insecure data caching, emphasizing the need for robust encryption and secure storage practices.

10. **Insufficient Cryptography:** In mobile applications this refers to the improper use or implementation of cryptographic techniques, which can lead to compromised confidentiality, integrity, and authenticity of sensitive information. Common manifestations include weak encryption algorithms, inadequate key lengths, and flawed encryption implementation, highlighting the importance of using strong encryption methods.

Mobile Application Security Methodologies

To effectively identify and mitigate these issues, the following testing methodologies and approaches can be used in design, development and production. This section will cover the following:

1. Mobile Architecture Risk Analysis
2. Cloud Application Security Assessment for Mobile
3. Manual Mobile Application Security Assessment
4. API Security Assessment
5. Static Application Security Testing (SAST)
6. Dynamic Application Security Testing (DAST)
7. Mobile Application Vulnerability Management

Mobile Architecture Risk Analysis

Understanding the architecture of a mobile application is a fundamental step in conducting a thorough security assessment. Gaining insights into its internal structure, design, processes, and involved stakeholders lays the groundwork for a successful evaluation. This allows security assessors to pinpoint critical areas within the application's infrastructure that might be most vulnerable or pose significant risks to the business. This involves an in-depth review of existing architecture diagrams, dataflow, and design, along with an evaluation of the mobile application services, frameworks and protocols. Next, organizations need to develop a threat model through collaborative workshops with the IT and operations/engineering teams. Visual representations of potential control system attacks using the NIST Cybersecurity Framework must be created. This approach helps prioritize security control implementations by identifying the most critical attack vectors, thereby reducing your mobile application's risk and exposure

Cloud Application Security Assessment for Mobile

The Cloud Application Security Assessment (CASA) adopts the OWASP Application Security Verification Standard (ASVS) to thoroughly evaluate application security, particularly when integrating third-party APIs into mobile applications. Google, among other companies, mandates CASA to ensure the stringent security standards necessary for utilizing their APIs, especially those handling Google user data. This assessment verifies that your application is fortified against vulnerabilities and adheres to robust security measures, providing assurance of data protection and meeting the prerequisites for API usage and access to sensitive user information.

Manual Mobile Application Security Assessment

Manual mobile application security assessments involve conducting a simulated attack on a mobile application to uncover potential security weaknesses and vulnerabilities. This rigorous testing methodology helps to identify and exploit security flaws within the app, its infrastructure, APIs, backend systems, and the overall mobile environment. By mimicking real-world attack scenarios, assessments can test an application's resilience against various cyber threats and to provide actionable insights to enhance its security posture.

The benefits of mobile application security assessments are substantial. It allows organizations to proactively identify and rectify vulnerabilities before malicious actors exploit them, thus mitigating the risk of data breaches, unauthorized access, and other security incidents.

API Security Assessment

APIs serve as a vital foundation for mobile applications, seamlessly integrating various microservices to offer essential functionalities to users. While these integrations significantly enhance an application's capabilities, understanding and securing APIs are crucial. They expand the potential attack surface, especially when integrating third-party API services that may introduce unforeseen risks to the environment. This is why it's imperative to thoroughly comprehend and secure these integrations to safeguard against potential vulnerabilities that could compromise the application's integrity and user data through an API security assessment. API security assessments uncover potential weaknesses or vulnerabilities within APIs, ensuring that potential entry points for attackers are addressed proactively. Assessments help ensure compliance with security standards and best practices, mitigating risks associated with data breaches or non-compliance.

Static Application Security Testing (SAST)

In SAST, the analysis is performed at an early stage of the software development life cycle (SDLC). It examines the application's source code, byte code, or binary code to identify potential security vulnerabilities, coding errors, and weaknesses that could be exploited by attackers.

SAST tools scan the codebase for known patterns or signatures that indicate common security issues such as SQL injection, cross-site scripting (XSS), buffer overflows, insecure coding practices, and more. It helps developers identify and fix security flaws before the application is deployed, reducing the risk of potential security breaches.

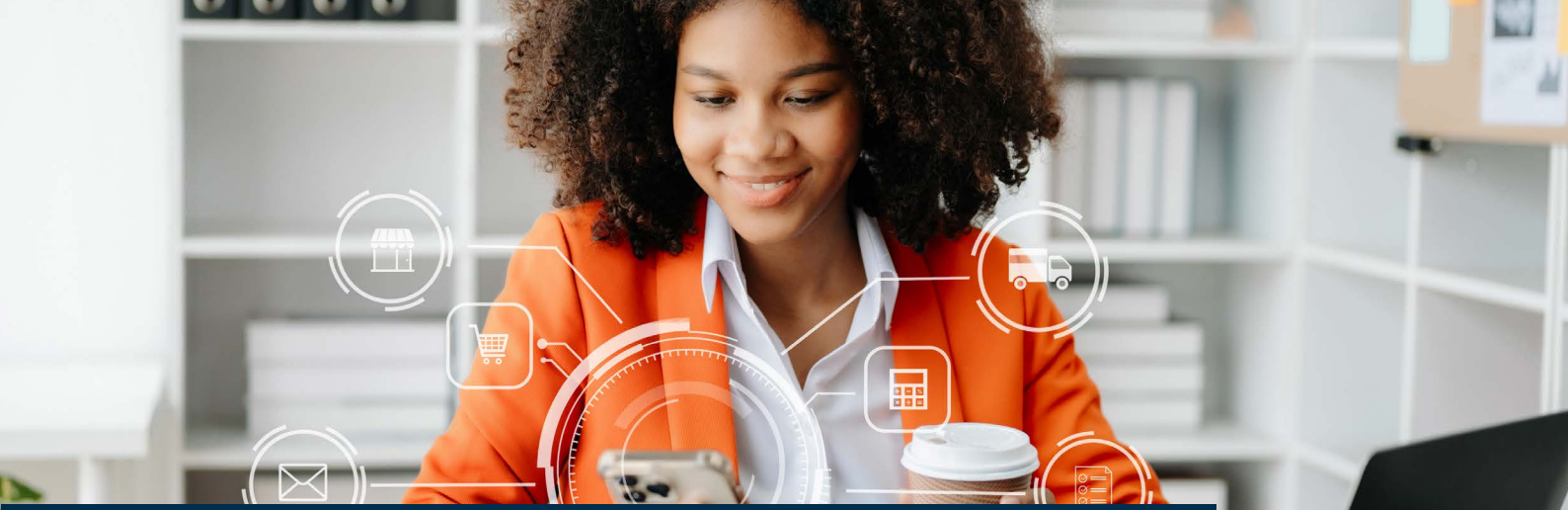
Dynamic Application Security Testing(DAST)

DAST tools simulate real-world attacks by sending various inputs to the application, observing its responses, and identifying vulnerabilities that could be exploited by attackers. It examines the application from the outside, testing it in its complete, deployed state, including its interfaces with other systems and dependencies.

This testing method identifies vulnerabilities such as input validation errors, session management issues, authentication flaws, and other security weaknesses that may not be detected by static analysis alone. DAST helps organizations understand their security posture in real-time and provides insights into how an attacker might exploit vulnerabilities in a live environment.

Mobile Application Vulnerability Management

Mobile Application Vulnerability Management involves the proactive identification, analysis, and mitigation of security vulnerabilities present within mobile applications. This process encompasses comprehensive assessments and continuous monitoring to detect potential weaknesses in the application's code, logic, or design. Addressing these vulnerabilities and remediating them through patching, code remediation, or adopting secure coding practices ensures the application's resilience against potential threats and fortifies its overall security posture.



Altimetrik Mobile Security Services

1. Mobile Architecture Risk Analysis

We identify and prioritize potential threats and vulnerabilities unique to your mobile application, tailoring our approach to address your specific security challenges. Beyond risk identification, we conduct a thorough assessment of the potential consequences of security breaches, providing you with a clear understanding of the potential impact on your application and business. Experts evaluate your front-end and back-end components as well as commonly used mobile database storage i.e. SQLite and Firebase for security measures, ensuring robust protection of your sensitive data. Our security team provides you with robust risk mitigation strategies and reporting, empowering you to proactively tackle security concerns and minimize the likelihood of breaches.

2. Cloud Application Security Assessment (CASA) Services

Altimetrik performs Cloud Application Security Assessments in alignment with the App Defense Alliance(ADA) to ensure that your mobile application is robust and meets all OWASP security standards. Our application security team delivers reporting on project milestones, vulnerability findings, and remediations aligned with OWASP ASVS. We work with stakeholders to track any vulnerabilities from discovery to remediation.

3. Mobile Application Security Assesment Services

Our Mobile Application Security Assessments simulate real-world attacks, identifying vulnerabilities and weaknesses in your mobile applications before malicious actors can exploit them. Our team of security testers employ the MITRE ATT&CK methodology to comprehensively test your mobile applications, ensuring they stand up to the most sophisticated threats. With our in-depth testing and thorough reporting, you gain valuable insights into potential security risks and receive actionable recommendations for remediation. Our team will work closely with stakeholders to track issues to remediation and also educate them to prevent any future threats.

4. API Security Assessment Services

At Altimetrik, we recognize that APIs are the lifeblood of modern mobile applications, but they can also be a significant security risk if not properly protected. Mobile security experts evaluate common API endpoints (REST, SOAP, GraphQL) and perform API Security Assessment services tailored to help you secure your APIs and third party API Integrations against unauthorized access, data breaches, and misuse. We conduct a comprehensive evaluation of your APIs, identifying potential vulnerabilities, weak authentication mechanisms, and data exposure risks. We also help you implement rate limiting and input validation strategies to prevent common attacks, such as DDoS attacks and injection attacks. By partnering with Altimetrik for API security assessments, you can enhance the reliability and integrity of your APIs, protect sensitive data, and maintain the trust of your users and partners.

5. Code Review, Static Application Security Testing (SAST)

Altimetrik offers Code Reviews, Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) services delivered by our team of experts. We review code from all popular frameworks such as React Native, Flutter and Xamarin. Our SAST services involve a thorough examination of your source code and application binaries, meticulously scanning for potential vulnerabilities and security weaknesses within the application's codebase. Using OWASP Mobile Security Best Practices, our team of experts conducts in-depth code reviews, code obfuscation to deter reverse engineering attempts, and utilizes industry-leading tools and methodologies to ensure your application's code is robust and resilient against potential threats.

6. Dynamic Application Security Testing (DAST)

Simultaneously, our professionals conduct DAST evaluations, employing dynamic testing techniques that simulate real-world attacks on live applications to identify vulnerabilities at runtime. With our expertise in these testing methodologies, we provide comprehensive and robust security assessments, ensuring that your mobile applications are rigorously tested for vulnerabilities, threats, and weaknesses.

7. Configuration Management and Vulnerability Management Services

Altimetrik will create an interface for the purposes of cybersecurity incident response. We identify and track software defects found in operations monitoring and feed them back to development for fixing. We track and fix software bugs found in operations to enhance the SSDLC and prevent future software bugs and track remdiation to completion using popular bug tracking platforms such as JIRA, Bugzilla and Trello. We automate verification of operational infrastructure security and publish risk data for deployable artifacts.

8. Security, Governance, Risk and Compliance Services

Altimetrik will unify regulatory pressures, identify privacy obligations and assist your organization with creating policy. Our GRC experts implement and track controls for compliance as well as include software security SLAs in all vendor contracts as well as ensure compatible vendor policies. We ensure executive awareness of compliance and privacy obligations and drive feedback from software lifecycle data back to policy.

9. Mobile Application Security Training

Our experts conduct software security awareness training as well as deliver on-demand individual training to better enhance security in all phases of the SSDLC. We will create and use material specific to company history and deliver role-specific advanced curriculum. We also provide annual refresher training, training for vendors and outsourced workers as well as provide our expertise via open collaboration

Benefits

Enhanced Cybersecurity Posture: Clients will benefit from a significantly improved cybersecurity posture for their mobile applications on Android and iOS. This enhanced security will safeguard critical assets, reduce vulnerabilities, and protect against a wide range of cyber threats.

Data Protection: Safeguard sensitive user data, ensuring privacy and compliance. Data breaches can have devastating consequences for both users and businesses. With Altimetrik's mobile application security services, you can be confident that sensitive user data is handled with the utmost care. We employ industry-leading encryption protocols, secure authentication mechanisms, and best practices in data handling to ensure that personal and confidential information remains protected. By prioritizing data privacy and security, you demonstrate a commitment to user trust and regulatory compliance.

Regulatory Compliance: Our services ensure that clients meet various regulatory requirements and standards such as GDPR, HIPAA and PCI DSS. Compliance with these standards not only avoids legal penalties but also demonstrates a commitment to data privacy and security.

Reduced Risk and Cost Savings: By identifying vulnerabilities and implementing robust security controls, Altimetrik security services help clients mitigate risks associated with cyberattacks, operational disruptions, and data breaches. This risk reduction minimizes potential financial losses and reputational damage.

Resilience and Continuity: Altimetrik helps clients build resilience in their mobile application environments. This resilience ensures continuity of operations even in the face of cyber threats, enhancing overall business continuity and minimizing downtime.

Conclusion

As technology advances so do the threats to mobile applications and their critical infrastructure. We are committed to empowering organizations with tailored solutions that enhance your mobile application security posture and reduce vulnerabilities. With our comprehensive suite of services, spanning from architecture risk analysis, SAST and DAST testing, SSDLC, API security assessments, code review, threat hunting and security audits, configuration and vulnerability management, SGRC services and mobile application security training, we provide the expertise and support needed to safeguard operations, protect assets, and maintain the resilience of business critical services.

Contact

For more information, please visit us at:

www.altimetrik.com

About Altimetrik

Altimetrik is a data and digital engineering services company focused on delivering business outcomes with an agile, product-oriented approach. Our digital business methodology provides a blueprint to develop, scale, and launch new products to market faster. Our team of 5,500+ practitioners with software, data, cloud engineering skills help create a culture of innovation and agility that optimizes team performance, modernizes technology, and builds new business models. As a strategic partner and catalyst, Altimetrik quickly delivers results without disruption to the business.