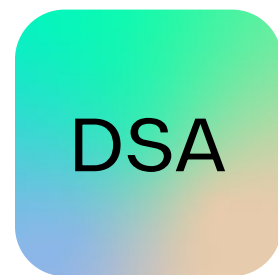


mobisec

**Enhance
your
Security**



mobisec

Metti in sicurezza le tue applicazioni mobile

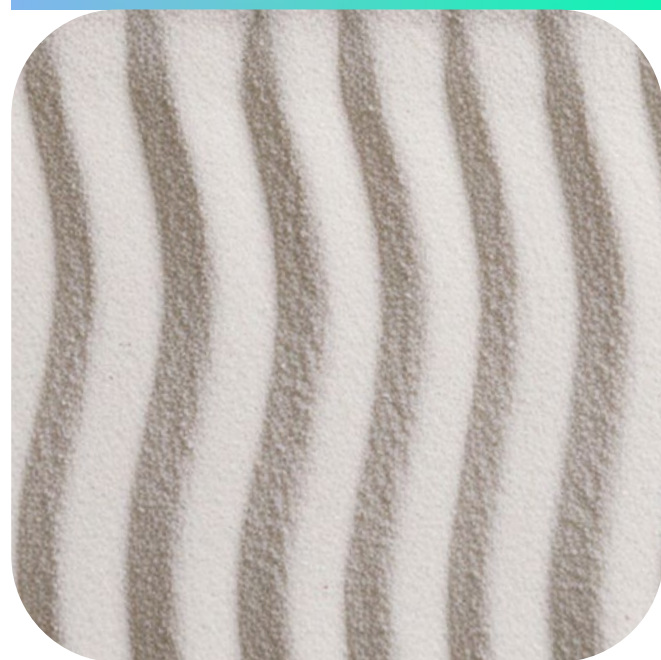
DSA

Dynamic
Security
Analysis

La piattaforma di vulnerability assessment e penetration test creata da Mobisec per garantire la sicurezza delle applicazioni mobile.

Progettata per ridurre le preoccupazioni sulla security e permettere alla tua azienda di concentrarsi sul business.

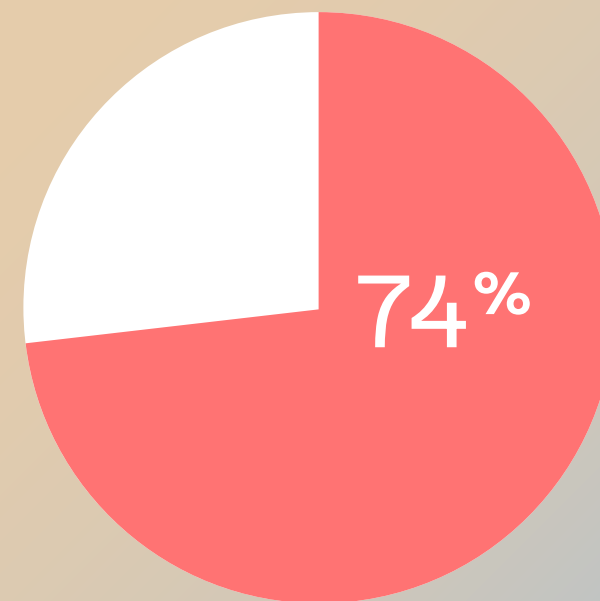
Perché la Mobile Security è Business Critical



Preoccuparsi della sicurezza delle proprie App è strategico.

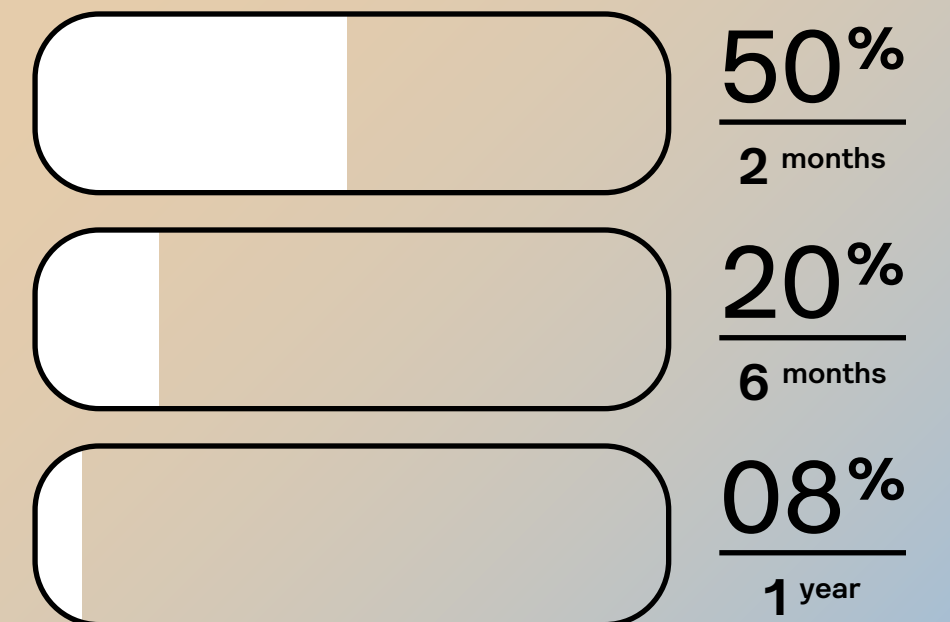
Proteggi i tuoi utenti e il tuo business dai rischi di un data breach capendo, dando priorità e rimediando le vulnerabilità della tua applicazione.

Gli attacchi, grazie anche al fatto che la liability relativa alla sicurezza è sempre più a carico dei Service Provider, si stanno spostando sempre più dalle infrastrutture alle applicazioni, in particolare quelle mobili. Le App diventano dei veri e propri cavalli di Troia, mettendo a rischio l'azienda e i suoi clienti, con gravi conseguenze per il business e la reputazione.



Attacchi dovuti a disattenzione umana

Verizon, 2024. Data Breach Investigations Report



Vulnerabilità non rimatee entro...

Dati Mobisec 2024.

+68%

Attacchi derivati da vulnerabilità applicative (VS anno precedente)

Identity Theft Resource Center, Data Breach Analysis Q3 – 2023

2016 58%
2023 88%

La cybersecurity riconosciuta come problema di business

Gartner, 2024 Gartner Board of Directors Survey “La cybersecurity è un problema tecnologico o di business?”

STRESSA LA TUA APP NON IL TUO BUSINESS

01

Vulnerability Assessment

Eseguiamo inizialmente una valutazione delle vulnerabilità dell'applicazione utilizzando la nostra piattaforma che unisce automatismi, talento umano e intelligenza artificiale. Lo facciamo in modalità black box, senza che il nostro cliente debba dare accesso al codice, né scaricare alcun software.

02

Penetration Test

Successivamente, il nostro team di ethical hacker simula il comportamento di un vero attacco per verificare la robustezza dell'applicazione. La nostra piattaforma monitora, registra e analizza tramite Artificial Intelligence tutti i processi per individuare le possibili situazioni di criticità.

03

Detailed Reporting

Al termine del nostro lavoro, generiamo e presentiamo un report chiaro, dettagliato e senza falsi positivi. Un documento comprensibile ai vari livelli di management, che includerà la classificazione delle vulnerabilità per gravità e le indicazioni necessarie e precise per la remediation.

Perché DSA

1/3

Il nostro approccio è unico

Rispetto alle principali soluzioni sul mercato, Mobisec DSA è l'unica che integra tutte le seguenti caratteristiche



Una sola piattaforma

VA e PT nello stesso strumento, per garantire la copertura di tutto il ciclo di sviluppo del software.



Sforzo minimo per il cliente

Non c'è bisogno di imparare a usare la nostra piattaforma o di condividere il tuo codice; svolgiamo noi il lavoro, senza il tuo intervento.



Test su Api Gateway

VA e PT nello stesso strumento, per garantire la copertura di tutto il ciclo di sviluppo del software.



Hacker point of view

Il nostro approccio è Gray o Black box, per riflettere la prospettiva di chi attacca.



Integrazione fluida

Siamo perfettamente integrabili con i principali tool di gestione dei processi come Jira, Jenkins e Redmine, per favorire la fluidità dei tuoi flussi di lavoro in un'ottica DevSecOps.

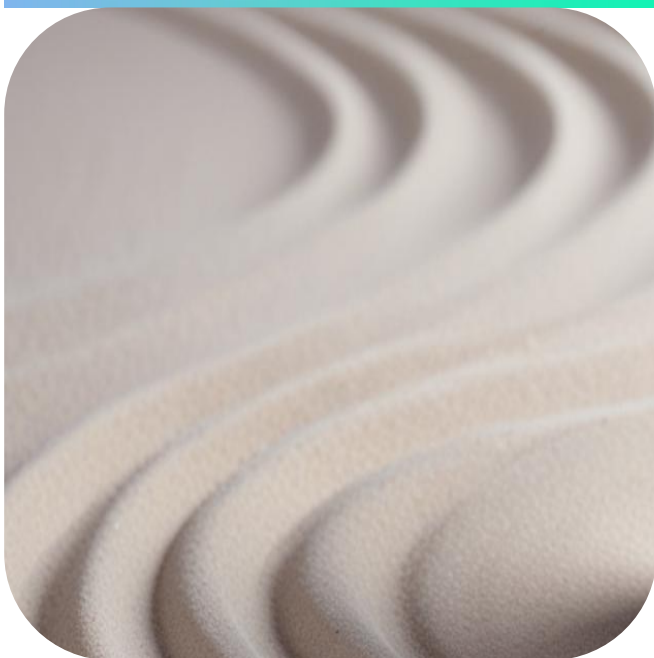


Standard internazionali

Full compliant con gli standard OWASP e contributori della Linux Foundation App Defense Alliance (ADA), per garantire la qualità degli output indipendentemente dall'operatore che esegue i test.

Perché DSA

2/3



Certificazione ISO 27001

Ci muoviamo nell'ambito della certificazione ISO 27001, per garantire che le nostre e le tue informazioni siano gestite secondo le best pratiche più severe.



No falsi positivi

Forniamo risultati completi in due giorni e con la verifica dei nostri operatori eliminiamo i falsi positivi, così che tu possa concentrarti solo sulle criticità reali, risparmiando il tempo dei dev.



Score personalizzato

Lo scoring viene personalizzato dal nostro team per essere coerente con il tuo business e prioritizzare correttamente le remediation.



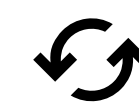
Linguaggio comprensibile

Le risultanze sono descritte utilizzando un linguaggio comprensibile a diversi livelli, con approfondimenti legati al business, per permettere una condivisione interna più facile e diretta.



KPI finale

Grazie al nostro punteggio sintetico, sarà più facile monitorare e illustrare il miglioramento nel tempo delle tue app.



Sicurezza proattiva

Svolgiamo re-test automatici, senza input da parte tua, se emergono variazioni nei Sistemi Operativi o se vengono scoperte nuove vulnerabilità che possono interferire con la tua app.



Supporto continuativo

Il nostro contributo non si esaurisce con il report: diamo supporto e consulenza in fase di presentazione del report e siamo con te per i successivi follow up.

Perché DSA

3/3

la nostra proposta è
una soluzione semplice per una scelta difficile

Semplificare la vita dei decision-maker

Offriamo una soluzione che include tutte e solo le funzionalità critiche quando si parla di Application Security, evitando i rischi e le problematiche delle alternative presenti ad oggi sul mercato.

Affiancamento costante e completo

Offriamo un supporto all-inclusive che non vincola ad un numero massimo di report e re-check. Coniugando i vantaggi degli automatismi con i benefici della human intelligence.

La Continuous Security è fondamentale

Con Mobisec DSA sei certo che le tue app siano al sicuro in ogni momento del ciclo di sviluppo e che il processo di remediation si svolga in maniera rapida ed estremamente efficace.

Le principali alternative sul mercato
hanno almeno una lacuna

Soluzioni handmade non standardizzate

L'approccio "handmade" artigianale ha solitamente tempistiche molto lunghe e non sempre garantisce il necessario standard qualitativo dell'output, che invece potrebbe variare notevolmente a seconda dell'operatore che esegue i test.

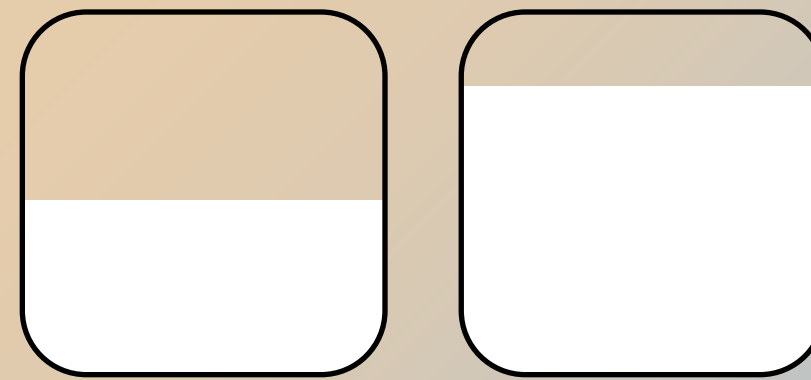
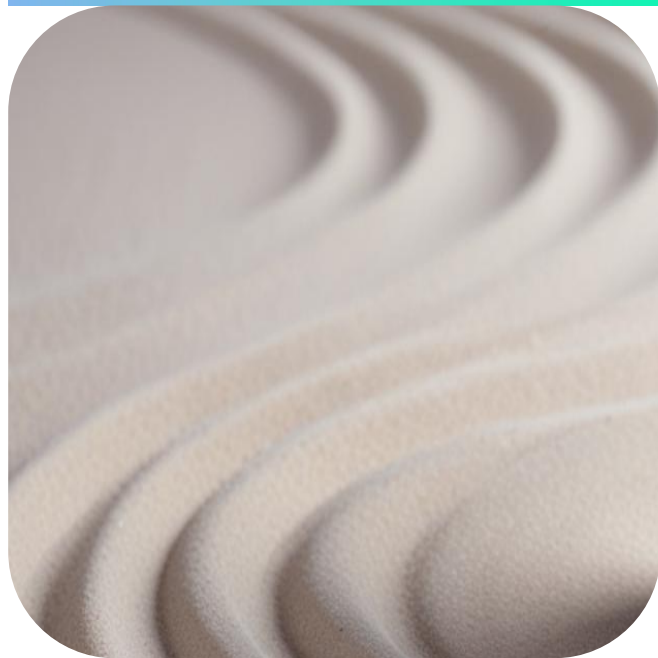
Soluzioni automatiche superficiali

I report mancano di analisi approfondita e presentano molti falsi positivi. Lo scoring delle vulnerabilità è generico e non adattato alle esigenze specifiche del tuo business. Servono risorse e competenze interne per utilizzarli.

Soluzioni Pay per Use limitate

Non tengono conto del processo di continuo sviluppo e rilascio delle app e degli aggiornamenti per ciascun OS. Obbligano a un nuovo processo di acquisto ogni volta che si vogliano mantenere sicure le proprie app.

DSA in numeri



Primo Pentest

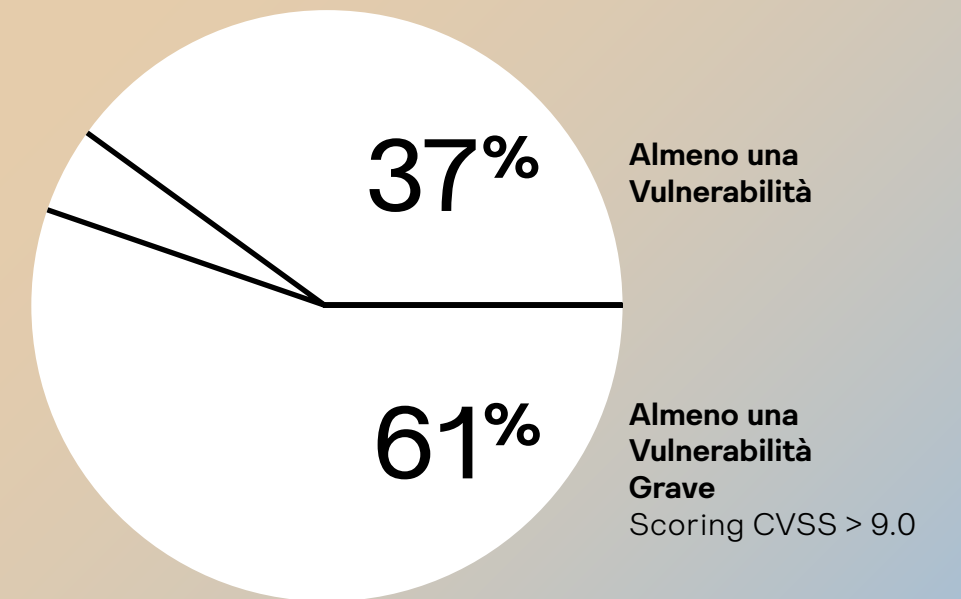
48%

Ultimo Pentest

85%

Scoring KPI medio
delle app testate

Dati Mobisec 2024.



Vulnerabilità
nelle app testate

Dati Mobisec 2024.

2 days

Il tempo medio per
l'invio di un report
dopo la prima run

Il primo test richiede
in media 5 giorni

+25 Mln

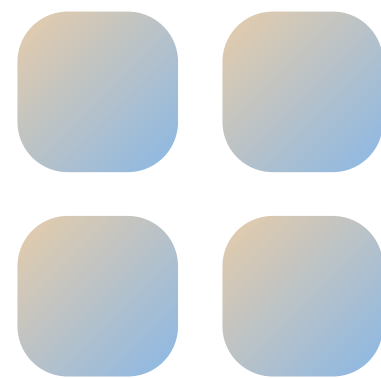
Il numero di utenti finali
che usano app testate
da Mobisec

LE FASI DI ANALISI



DSA Agent

Sui device è installato il nostro agent, insieme all'app da testare. Questo ci permette di avere sotto controllo non solo l'app, ma anche le interazioni con gli altri elementi del device stesso.



Data Collection

Raccogliamo i dati e le informazioni sugli eventi generati dall'utilizzo dell'app. Migliaia di informazioni, relative ad ogni singola azione e ad ogni evento che l'utilizzo dell'app produce, sono trasmesse alla nostra piattaforma.



Matching Engine

L'AI esamina i dati per verificare l'assenza di (vulnerabilità note) CVE e pattern critici. Infine testa strategie: combinazioni di condizioni che, singolarmente innocue, potrebbero causare problemi di sicurezza se fatte collidere.



Final Report

Generato in automatico, dopo che il nostro team ha ripulito i risultati dei falsi positivi, assegnato lo scoring CVSS più appropriato, integrandolo con annotazioni e approfondimenti per renderlo di facile comprensione ai diversi stakeholder.

Hanno scelto Mobisec



Insights sul mondo trasporti

Un attacco riuscito a un'azienda di trasporti può causare interruzioni delle attività core business e ritardi nell'erogazione dei servizi. Queste interruzioni possano rappresentare una minaccia critica o addirittura diventare un evento non tollerabile per un'organizzazione.

Ad esempio, un attacco riuscito che metta fuori uso l'applicazione di un vettore comporta l'impossibilità per i passeggeri di acquistare i biglietti o controllare gli orari.

top 10

I trasporti sono stati uno dei 10 settori più bersagliati nel 2023

20%

Un attacco su cinque al settore dei trasporti ha sfruttato una vulnerabilità applicativa

7/10

Incidenti cyber nel settore dei trasporti hanno causato interruzioni dell'attività core business

+36%

Incremento anno su anno degli attacchi andati a buon fine a livello mondiale nel settore dei trasporti

Insights sul mondo bancario

Il numero di cyberattacchi nel settore bancario cresce di anno in anno. Nel terzo trimestre del 2023, il numero di attacchi cyber è raddoppiato rispetto allo stesso periodo dell'anno precedente.

Ciò indica la maggiore attenzione dei criminali verso questo settore. Gli attaccanti compromettono le organizzazioni finanziarie non solo con mezzi tradizionali (es: tramite sms phishing) ma anche sfruttando attivamente le vulnerabilità delle applicazioni.

2°

Il settore finanziario è al secondo posto nelle statistiche globali sugli attacchi cyber dopo il settore sanitario

IBM Cost of a Data Breach Report

32%

Degli attacchi al settore bancario hanno sfruttato una vulnerabilità applicativa

73%

Dei Chief Risk Officer (CRO) globali considera la cybersecurity come il principale rischio per il 2024, accentuato dalle tensioni geopolitiche

3 Mrd \$

Le perdite causate da attacchi cyber al settore bancario dal 2004 ad oggi

Insights sul mondo assicurativo

Secondo il rapporto “Insurance Banana Skins 2023”, il cyber crime è la maggiore minaccia che il settore assicurativo globale dovrà affrontare nei prossimi 2-3 anni.

Gli attacchi informatici nel settore assicurativo stanno crescendo in modo esponenziale. Offrendo nuovi prodotti tra i quali portali per le agenzie, le app per le polizze online e le applicazioni basate su web e dispositivi mobili, aumentano le possibilità di generare vulnerabilità che potrebbero essere sfruttate dagli aggressori.

Un attacco riuscito potrebbe compromettere la continuità aziendale e il furto di dati sensibili, con conseguenze disastrose in termini di reputazione per le singole aziende e per l'intero settore.

1°

Le compagnie assicurative mettono al primo posto di importanza la cybersecurity, per le richieste di risarcimento e per le vulnerabilità dei sistemi interni

87%

Dei manager dichiara che la propria azienda non è adeguatamente protetta contro i rischi informatici

4/5

Il voto medio del livello di preoccupazione in merito ai rischi di cybersecurity nell'ambito assicurativo

+200%

Incremento anno su anno degli attacchi indirizzati alle aziende del settore assicurativo

COSA FACCIAMO

M

Mobile Security

DSA

Dynamic Security Analysis è la nostra piattaforma di vulnerability assessment e penetration test per la sicurezza delle applicazioni mobili.

W

Web Security

WAPT

Così come per le app mobile, effettuiamo test di penetrazione delle applicazioni Web e API Gateway.

D

Data Intelligence

HiWave

La nostra piattaforma di Data Intelligence, costruita per essere adattata in modo flessibile in funzione del caso d'uso.

A

Security Assessment

Consulting

MDM, Security by Design, Enterprise Security e consulenza speciale per dare supporto e servizi professionali ai nostri clienti.

Votati alla Security

La nostra mission è ridurre i rischi e le preoccupazioni dei clienti con un approccio innovativo alla sicurezza mobile.

Fondata nel 2015, Mobisec si è focalizzata fin dall'inizio sulla cybersecurity applicativa, quando tutti erano concentrati sulla sicurezza infrastrutturale, sulla digitalizzazione dell'azienda e sullo spostamento della gestione aziendale sul cloud

Proprio con l'aumento dell'uso del cloud, lasciando esposti i sistemi logico-applicativi, la responsabilità della sicurezza infrastrutturale è sempre più nelle mani degli hyperscaler. Così abbiamo risposto a questa esigenza sviluppando competenze in ethical hacking e innovazione, offrendo soluzioni su misura per la sicurezza di applicativi, dispositivi mobili e IoT.

mobisec

**Keep
in touch!**

sales@mobisec.com
mobisec.com
follow us on LinkedIn

ITA
Viale della Repubblica
22/III Villorba (TV)

USA
4010 Moorpark Avenue
San Jose, CA 95117