appdome

THREAT-EVENTS™

Choose the DevOps way to build, test, release and monitor threat-intelligence in Android and iOS apps and save time, money and achive your goals.

THREAT-EVENTS™, FAST & EASY IN-APP MOBILE THREAT INTELLIGENCE & CONTROL

Threat-Events™ offers mobile developers in-app mobile threat intelligence and control to deliver on-brand mobile app experiences to mobile customers when attacks and threats occur. In Android & iOS apps, mobile developers register, consume, and use real-time attack intelligence inside the app, including attack type, source and other attack details and make data-based decisions on what, when, and how to defend mobile apps and users. With Threat-Events, you get:

IN-APP THREAT INTELLIGENCE & CONTROL

Threat-Events™ is a comprehensive in-app mobile threat and attack intelligence framework for Android and iOS apps. Threat-Events are designed to make mobile app experiences threat-aware and integrate security at every level of the mobile end user experience. Using Threat-Events is easy. Built around standard and secure methods to consume and use data passed between frameworks, the mobile developer's code has total awareness and control if, and when any of 12,000+ mobile app security, RASP, mobile fraud, MiTM attack, jailbreak, rooting, modding, instrumentation, patching, hooking, mobile malware, mobile cheat and other attacks occur.

FULL THREAT AWARENESS & VALIDATION

Threat-Events can be configured in multiple ways. Using In-App Detection, Appdome detects the attack or threat, and passes the event to the developer's code for processing, including in-app enforcement and the end-user experience. Using In-App Defense, Appdome detects the attack or threat, defends the mobile app, handles the mobile user notification, and passes the event to the developer's code for data-capture, allowing the developer to design second step mobile end-user workflows. All Threat-Events are fully integrated with Certified Secure™ and ThreatScope™, Appdome's Mobile Threat Intelligence and Security Operations Center (SOC), for lifecycle validation.

THREAT-CODES™ - ATTACK IDENTIFICATION

Threat-Codes™ are unique identifiers for specific on-device attacks and threats occurring within each threat category. Threat-Codes provide a quick and easy identification of specific malware packages, malware interactions, exploit attempts, attack patterns, and more. Threat-Codes can be used to aggregate and analyze broad or release-specific threat patterns and can be used to provide user-facing resolution paths for L1 support teams.

HIGH FIDELITY THREAT SIGNAL INSIDE APPS

Threat-Events make the entire spectrum of attack and threat detail available to the mobile developer without the need for external servers, services, or attestation services. This has three main benefits: (1) faster performance between detecting and passing events between the security framework and the developer's code, (2) no risk of in-transit exploit, signal spoofing, hijacking or other attacks that can compromise the integrity of the threat signal, and (3) hardened binding between the developer's code and Appdome's detection methods, eliminating the risk of an attacker disabling the Threat-Events signals.

RICH ATTACK & THREAT META DATA

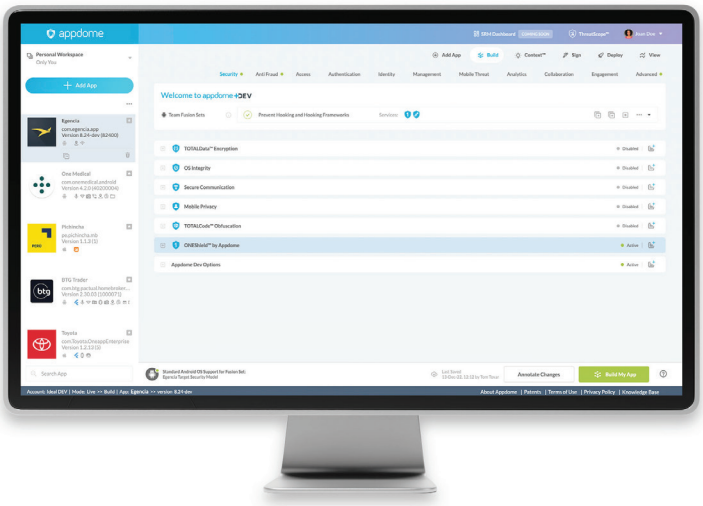
Each Threat-Event can be configured to provide detailed meta-data about the specific mobile attack or threat on each end-user device. Meta-data elements include device type, device model, device manufacturer, device ID, OS, OS version, geo-location, timestamp, network, attack description and more. This data can be integrated with other mobile threat feeds, SIEM or analytics systems. The data can also be used as attestation data against Credential Stuffing, network-based attacks or fraud and incident response programs.

THREAT-SCORES™ - BETTER THREAT HANDLING

Threat-Scores™ are numerical values (1-1000), set by the mobile developer or cyber team, for each mobile app security, RASP, anti-fraud, anti-malware, anti-cheat and other detection and protection added to the mobile app via Appdome's DevSecOps build system. Using Threat-Scores, developers can create advanced attack and threat handling in Android & iOS apps. In each Threat-Event, a Threat-Score for the specific event is passed as well as the aggregate Threat-Score for the end-user device. A Threat-Score for a lower ranked attack may not require any action. However, if multiple attacks or threats occur, the combined Threat-Score may be used to trigger immediate escalation to the support or incident response teams. Threat-Scores can be used as attestation data against

ONE SOLUTION IS ALL MOBILE DEVSECOPS NEEDS.

Appdome delivers mobile app protection, certification, XDR, and cyber release management in one unified, fully integrated platform.



THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for in-production Android & iOS mobile apps. ThreatScope Moible XDR gives mobile brands a consolidated view and real-time visibility into the entire range of threats and attacks impacting the mobile brand, apps and users, including full visibility into 1000s of threat streams covering mobile app security, mobile fraud, malware, cheat and bot attacks. As an XDR, ThreatScope also provides the configuration as code power to remediate attacks instantly build-by-build, and release-by-release. With ThreatScope, organizations can (1) see and analyze the top mobile app threats and attacks impacting the native mobile channel, (2) prove the value of protections deployed in mobile apps by version, OS, device or other parameters (3) make data-based decisions of what protections to deploy in each release, and (4) create customized views and comparisons that track the most relevant threats and attacks impacting the mobile business. Stay one step ahead of attackers, fraudsters and hackers with ThreatScope!

MOBILE CYBER DEFENSE AUTOMATION

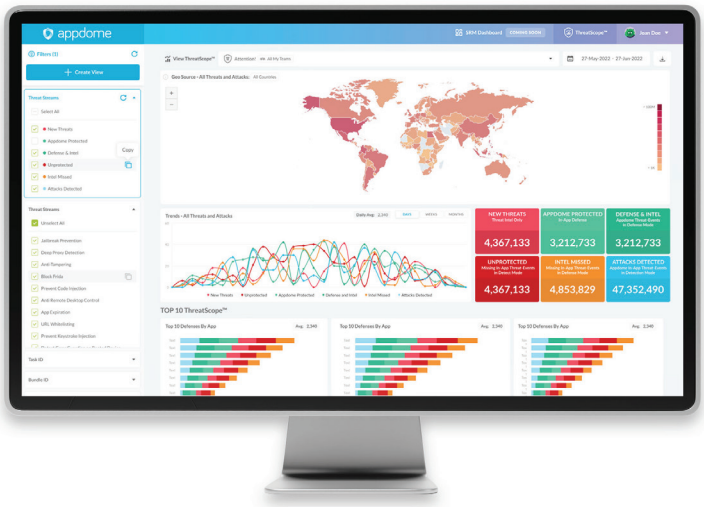
Appdome pioneered the no-code mobile app security market with its one-of-a-kind Mobile Cyber Defense Automation platform. This flagship product provides mobile developers, cyber security and fraud teams a centralized system and configuration as code ease to build, test, release and monitor mobile app security, anti-fraud, anti-malware, anti-cheat and anti-bot features in Android or iOS apps. Patented cyber release management, event logging, build tracking, version control, code freeze, security templating, role-based access and CI/CD DEV APIs allow instant DevOps readiness for any mobile app.

THREAT-EVENTS™ THREAT AWARE UI/UX CONTROL

All runtime and dynamic protections come enabled with Threat-Events™, Appdome's in-app attack intelligence and UI/UX control framework. Threat-Events empower developers to read/write from the Appdome Security Framework™, gather data on each attack inside the app and use the detection and defense data to create and control beautiful user experiences when attacks occurs.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Each protected build generated on Appdome comes with a Certified Secure™ certificate that guarantees the mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot and threat intelligence features protecting the mobile app. Moible Dev Teams use Certified Secure™ as the DevSecOps artifact to clear apps for release and save money and time vs. using code scans and penetration tests in



ABOUT APPDOME

Appdome's mission is to protect the mobile economy and the people who use mobile apps in their lives and at work. Appdome's industry defining Mobile Cyber Defense Automation Platform simplifies and accelerates mobile app protection, delivering rapid, no-code, no-SDK implementation and configuration as code ease, Threat-Events™ in-app threat intelligence and UI/UX control, and ThreatScope™ Mobile XDR all to detect, control and defend mobile apps when security, fraud, malware, cheat or bot attacks occur. As a platform, Appdome also serves as the centralized system of management, visibility and compliance control for all mobile app security, anti-fraud, anti-malware, anti-cheat and anti-bot initiatives, providing full release orchestration, user-build-event logging and guaranteeing Certified Secure™ mobile apps in the CI/CD pipeline. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to protect apps, users and data, preempt fraud, and consistently deliver richer and safer mobile experiences to hundreds of millions of mobile end users globally. Learn more at www.appdome.com. Open a free account at fusion.appdome.com and start securing your apps!