ZIMPERIUM

Zimperium Remote Security Diagnostics

Overview & Problem Statement

The challenge of effectively managing mobile threats is often hindered by the inability to access diagnostic logs from end-user devices. When issues arise, security teams face significant friction:

- **Technical Literacy:** End users often lack the technical expertise to locate, collect, and transmit diagnostic logs from their mobile devices.
- **Operational Inefficiency:** Security teams cannot rely on manual collection methods, which require physical access to the device. This is particularly prohibitive for remote workforces or devices located off-site, leading to significant delays of weeks or more for investigation and incident response.

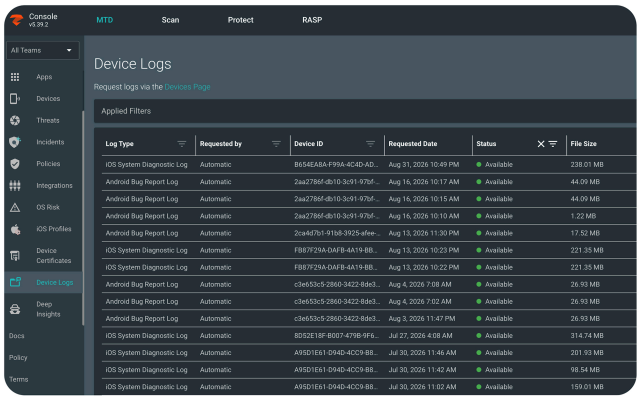
Solution Description

Zimperium Remote Security Diagnostics streamlines the troubleshooting process by enabling administrators to extract logs directly from devices, reducing or eliminating the need for end-user intervention or physical access to the device. The solution encompasses both essential MTD app log collection (included with MTD) and advanced, premium forensic device log capabilities and can shrink investigation timelines from weeks to days, or even hours.

Zimperium Remote Security Diagnostics provides a unified approach to mobile log collection, ensuring security teams have the forensic data they need to investigate incidents promptly.

Base MTD App Log Collection Functionality (Feature included in Base MTD license)

This free feature allows console administrators to remotely request Zimperium MTD app logs from the device. By eliminating the need for users to manually share logs via email, it streamlines basic troubleshooting and support workflows.



Premium Forensic Features (requires purchase of Remote Security Diagnostics)

Zimperium Remote Security Diagnostics extends log collection beyond the MTD app logs to include device logs.

- **Android Security Log Collection:** This feature automatically collects and shares security logs with the Zimperium MTD console every 24 hours with no intervention required from the end user or administrator. The Android OS Security Log is designed to capture high-signal security events for post-incident auditing, threat detection, and compliance, focusing specifically on administrative actions, authentication attempts, app execution, and integrity checks.
- **Android Bug Report Log Collection:** Enables the MTD app to request a system-generated bug report. An Android bug report captures deep-system telemetry inaccessible to standard apps, including system-wide application execution logs, kernel event buffers, active network socket states, and cross-process runtime traces. Users are guided through an on-demand process to generate and securely share the report for advanced analysis.
- **iOS System Diagnostic Log Collection:** Enables the collection of iOS system diagnostic files. In-app tutorials guide the end user to initiate the collection and share the file directly with the MTD console. Unlike a simple text log, the iOS system diagnostic contains system traces, database dumps, raw process activity, and crash reports used to troubleshoot performance, network, hardware, and OS-level issues.

Key Benefits & Value

- **For SOC Analysts:** Significantly reduces investigation time by ensuring critical diagnostic data is available faster, allowing for rapid response to security incidents.
- **For Administrators:** Eliminates the logistical challenges of manual log collection. Administrators save valuable time and resources while gaining direct visibility into device behavior.

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including mishing, malware, and zero-day attacks.

ZIMPERIUM®

Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244