ZIMPERIUM®

Zimperium Premium Threat Intelligence

Accelerate Incident Response with Deep Attribution and Unified Mobile Forensics

Executive Summary

As cybercriminals adopt a sophisticated, mobile-first attack strategy, mobile devices and applications have become an organization's most vulnerable attack surface. Security operations center (SOC) teams are increasingly flooded with alerts but lack the specialized context needed to quickly remediate mobile-specific threats.

Zimperium Premium Threat Intelligence is a premium feature sold as an add-on to Zimperium Mobile Threat Defense (MTD) designed to eliminate security blind spots. By embedding deep, actionable context, relational mapping, and adversary attribution directly into the management console, it empowers security teams to instantly understand the *who, what, and why* behind an attack—slashing Mean Time to Resolution (MTTR) from days to minutes.

The "Visibility Gap" in Mobile SecOps

Traditional security infrastructure frequently falls short when handling mobile threats, leading to severe operational friction for overworked SOC teams. Analysts typically face three core challenges:

- **The "Swivel-Chair" Core Loop:** When a mobile threat occurs, analysts are forced to manually bounce between separate security consoles and external threat feeds to investigate malicious files or URLs.
- **Lack of Specialized Expertise:** Most corporate analysts are extensively trained in traditional desktop, server, and network environments. They lack the specialized, mobile-specific threat expertise needed to rapidly deconstruct advanced mobile malware or mishing (mobile phishing) threats.
- **Attacks at the Speed of AI:** Threat actors are leveraging advanced AI to rapidly stand up unique phishing sites and deploy specialized mobile vectors. Without real-time contextual data, security teams remain purely reactive, investigating alerts after the damage is already done.

The Solution

Zimperium Premium Threat Intelligence seamlessly bridges this visibility gap by integrating a dedicated intelligence ecosystem directly within the MTD platform. Instead of treating mobile alerts as isolated telemetry points, this premium capability provides full relational clarity and attribution without the need for manual, external lookup tools.

Core Capabilities

- **Unified Threat Intelligence Hub:** Offers a fully integrated threat analysis center inside the console, purpose-built for dissecting mobile-specific malware strains and targeted malicious URL architectures.
- **Direct Adversary Attribution:** Instantly links detected mobile threats or active campaigns to known advanced cybercriminal groups and state-sponsored threat actors, giving analysts immediate context into the attacker's intent.
- **Dynamic Relational Indicator Mapping:** Visually and programmatically correlates critical threat indicators—mapping the relationships between malicious files, compromised IPs, rogue host domains, and underlying infrastructure associated with an attack.
- **MITRE ATT&CK Alignment:** Integrates seamlessly alongside Zimperium's native mapping to ensure all mobile-specific indicators are explicitly tied to documented adversary tactics.

Key Business Values & Outcomes

Accelerate MTTR

Eliminate manual external lookups. By putting unified mobile forensics at an analyst's fingertips, security teams reduce threat investigation and resolution timelines from hours or days to mere minutes.

- **Empower Overworked SOC Teams:** Acts as a technical force multiplier by embedding both Zimperium zLabs' elite mobile threat expertise and external threat intelligence straight into day-to-day triage workflows.
- **Proactive Attack Surface Hardening:** Delivers the comprehensive intelligence required to not only respond to an active exploit but to actively block associated downstream infrastructure (IPs, domains) across the entire enterprise.
- **Maintain Strict Privacy Compliance:** Operates entirely within Zimperium's secure, privacy-by-design architecture, ensuring advanced threat hunting data is enriched without exposing personal end-user data or communication content.

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.

To see a live demonstration of Zimperium Premium Threat Intelligence, visit www.zimperium.com.

ZIMPERIUM®

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