ZIMPERIUM

Zimperium Mobile App Response Agent

A Force Multiplier for Every SOC and Fraud Analyst Facing Mobile Threats.

The Challenge: The Mobile Security Gap in the SOC

As cybercriminals adopt a **mobile-first attack strategy**, mobile apps have become one of the largest and most vulnerable attack surfaces for enterprises. Despite this shift, most Security Operations Center (SOC) teams and Fraud analysts struggle to defend the mobile frontier effectively.

Analysts are often challenged by:

- **A New Threat Surface to Master:** Deep expertise in endpoints and networks but mobile device and app-level attacks generate different signals, require different investigation workflows, and demand a new approach most SOC teams weren't trained for.
- **Volume of Mobile Investigations:** Many teams are overwhelmed by the sheer volume of alerts requiring their attention. With mobile apps becoming a primary attack surface, these teams need a way to prioritize and automate the most critical investigations.
- **Two Languages, No Translator:** Fraud signals live in one tool. Mobile app security threats live in another. Fraud Analysts are left connecting the dots manually across systems that were never designed to talk to each other.

The Solution: Zimperium Mobile App Response Agent

The **Zimperium Mobile App Response Agent** is a premium AI-empowered solution that supplements the Mobile App Protection Suite (MAPS) and functions as a force multiplier for your security operations and fraud teams. Analysts trigger on-demand investigations on any device, and within minutes the agent determines whether an incident has occurred, prioritizes confirmed incidents, and delivers a clear attack narrative with response guidance enabling analysts to respond with speed and precision.

Key Capabilities

- **Incident Discovery:** Automatically determines if a series of events comprise a mobile security incident and provides a confidence score to reduce false positives.
- **Event Correlation:** Clusters related mobile telemetry events—including device, app, network, and web signals—into a single, cohesive incident.
- **Attack Context:** Creates clear incident narratives and timelines in plain language, allowing SOC teams to quickly communicate findings to leadership.
- **Fraud Signal Correlation:** Translates mobile security telemetry into clear fraud context, helping fraud teams understand what happened on the device and act on it.
- **Remediation Guidance:** Maps threats to **MITRE ATT&CK** tactics and provides step-by-step remediation guidance and recommended actions.

Customer Value: Why Choose the Mobile App Response Agent?

Feature	Benefit
Increased SOC Capacity	Automatically investigates and correlates every critical mobile threat alert, reducing alert fatigue and making analysts more effective and efficient when managing mobile threats.
Built-In Mobile Expertise	The Mobile App Response Agent includes Zimperium's industry leading mobile security experience, based on mobile-dedicated threat intelligence across 500M+ devices and 1,000+ apps under protection globally, empowering your SOC and Fraud analysts with expert-level precision.
Faster Incident Response	Cuts the time from alert-to-containment by delivering an instant verdict, attack narrative, and step-by-step response guidance so threats like malware and overlay attacks are stopped before they result in fraud.

How It Works: The AI-Empowered Workflow

1. **Trigger:** An analyst triggers an investigation on demand on any device.
2. **Analyze:** The Mobile App Response agent analyzes the selected event and prior telemetry on the device to identify related activity.
3. **Correlate:** Related events are grouped into an incident, assigned a confidence rating and enriched with key forensics and MITRE tactics.
4. **Resolve:** The analyst receives an executive-ready summary with clear attack context and follows guided steps to remediate.

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.

Ready to empower your AppSec and fraud teams?

ZIMPERIUM®

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