ZIMPERIUM

Zimperium MTD Mobile SOC Agent

A Force Multiplier for Every SOC Analyst Facing Mobile Threats.

The Challenge: The Mobile Security Gap in the SOC

As cybercriminals adopt a mobile-first attack strategy, employee mobile devices and apps have become your largest and most vulnerable attack surface. Despite this shift, most Security Operations Center (SOC) teams 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 SOC teams are overwhelmed by the sheer volume of alerts requiring their attention. With mobile devices becoming the primary attack surface, SOC teams need a way to prioritize and automate the most critical investigations.
- **Attacks at the speed of AI:** Attackers are using AI to increase both the speed and scale of attacks on your mobile fleet. SOC teams have to respond much faster, which requires the ability to correlate and prioritize in a much shorter time window than in the past.

The Solution: Zimperium Mobile SOC Agent

The **Zimperium Mobile SOC Agent** is a premium AI-empowered solution that supplements Zimperium Mobile Threat Defense (MTD) and functions as a force multiplier for your security operations team. The agent automatically investigates critical threat alerts from MTD, 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.
- **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 SOC 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	Mobile SOC 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 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 mishing attacks are stopped before they become breaches.

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 SOC?

ZIMPERIUM®

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