

Zimperium Deep Insights

Forensic Mobile Threat investigation within the Zimperium MTD Console

Executive Summary

Zimperium Deep Insights is a premium feature available to Zimperium MTD customers that empowers SOC analysts and Incident Responders to perform detailed forensic analysis of events that have occurred on iOS-based employee mobile devices.



The Challenge: Forensic Analysis for Mobile Devices

Weaponized AI is here and is silently wreaking havoc on the enterprise's most vulnerable attack surface: mobile. This AI powered risk landscape raises the urgency to monitor and analyze mobile devices for security risk and incidents for security conscious organizations.

Employees that travel internationally are at particular risk to complex attacks such as spyware infections that occur due to connections they make to risky wifi networks exposing them to MITM attacks, rogue access points and more. This risk means that security teams need to increase their forensic analysis scope to include mobile devices and do it quickly. But these already overstretched teams are faced with challenges:

- **Device Availability:** Thorough investigations often require employees to ship a device to the IR team for analysis, causing days of delay as well as inconvenience for the end user that is without their device.
- **Insufficient investigation staffing level:** Security teams often lack the resources necessary to expand investigations across the entire mobile device fleet, forcing them to limit analysis to critical cases such as C-suite employees, raising risk of missing another compromised device.
- **Explosion of evidence:** Root cause analysis (RCA) time takes too long and the compromise continues until the RCA is complete.
- **Lack of complete context** for mobile threats to understand the correlated attack chain of events.



The Solution to Mobile Forensics: Zimperium Deep Insights

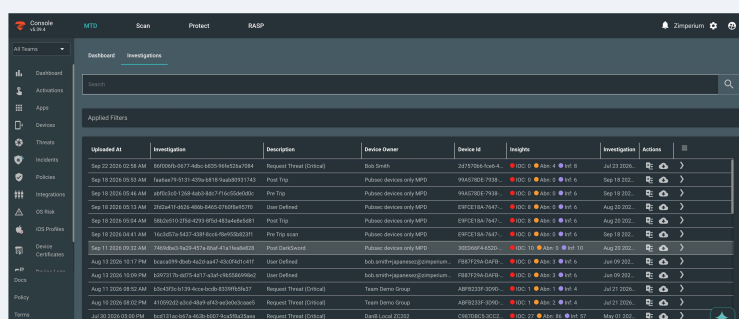
Zimperium's Deep Insights is a premium advanced mobile forensic and context analysis solution integrated into the MTD platform that extends beyond real-time threat detection to reconstruct the full story of a device's activity, assisting the SOC and IR teams by:

- **Reducing** investigation time from days to hours.
- **Speeding up** root cause determination for mobile security incidents.
- **Enabling SOC teams to operationalize threat hunting** by comparing “before and after travel” device configurations and translating complex file mutations into an intuitive, chronological chain of attack timeline.
- **Reducing investigation costs by automating** threat investigations and reducing false positives before escalation to the IR team.

Through an intuitive console experience, Deep Insights transforms complex forensic data into actionable insights, enabling security analysts to understand attack context, validate compromise, and respond faster without immediately relying on specialized forensic teams.

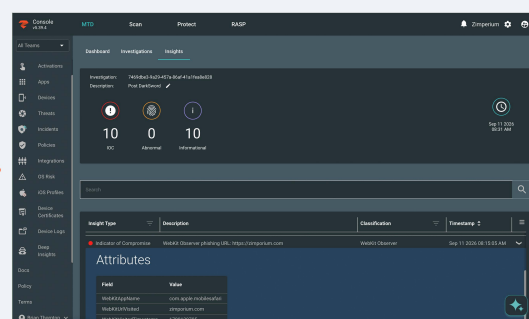
By embedding this capability directly into the existing security workflow, Deep Insights reduces investigation time from days to hours, lowers operational costs, and provides a scalable path from high-level threat detection to deep forensic analysis—supporting both incident response and proactive hygiene use cases such as pre/post travel validation and device posture assessment.

Deep Insights Determination of Mobile Device Compromised by DarkSword



Updated At	Investigation	Description	Device Owner	Device ID	Insights	Investigation	Actions
Sep 22 2020 02:58 AM	8050965-2677-480c-6820-565425a7324	Request Threat (Critical)	Bob Smith	26777656-8a6d-4	IOC: 0 ● Alert: 4 ● Inf: 0	Jul 23 2020	Reinvestigate
Sep 18 2020 03:53 AM	8a6a791-5737-429a-8f18-8a6a79371743	Post Trip	Public devices only MTD	99A570EE-7938	IOC: 0 ● Alert: 0 ● Inf: 0	Sep 18 2020	Reinvestigate
Sep 18 2020 03:46 AM	a8f83d9-1368-6a60-8a67-f1c556a090	Pre Trip	Public devices only MTD	99A570EE-7938	IOC: 0 ● Alert: 0 ● Inf: 0	Sep 18 2020	Reinvestigate
Sep 18 2020 02:51 AM	202a9f1-6205-480a-8062-2156a05070	User Defined	Public devices only MTD	49FCE15A-7647	IOC: 0 ● Alert: 0 ● Inf: 0	Aug 20 2020	Reinvestigate
Sep 18 2020 03:53 AM	086a091-076a-4291-8945-8a6a79371743	Post Trip	Public devices only MTD	49FCE15A-7647	IOC: 0 ● Alert: 0 ● Inf: 0	Aug 20 2020	Reinvestigate
Sep 18 2020 04:41 AM	15a0d76a-5837-438f-8c6a-08a0506231	Pre Trip scan	Public devices only MTD	49FCE15A-7647	IOC: 0 ● Alert: 0 ● Inf: 0	Sep 18 2020	Reinvestigate
Sep 17 2020 09:32 AM	786a0d6-8a2b-4f7a-80af-4111a0a028	Post Checkpoint	Public devices only MTD	30255094-6303	IOC: 10 ● Alert: 0 ● Inf: 10	Aug 20 2020	Reinvestigate
Aug 13 2020 10:17 PM	8a0a9f9f-d842-4a20-a247-43a0f4014817	User Defined	Public devices only MTD	F8B717DA-0A79	IOC: 0 ● Alert: 0 ● Inf: 0	Jun 09 2020	Reinvestigate
Aug 13 2020 10:00 PM	8a0a9f9f-d842-4a20-a247-43a0f4014817	User Defined	Public devices only MTD	F8B717DA-0A79	IOC: 0 ● Alert: 0 ● Inf: 0	Jun 09 2020	Reinvestigate
Aug 13 2020 08:52 AM	53a493fa-1d38-4a4a-ba6b-833010104817	Request Threat (Critical)	Team Device Group	AFB8333F-3000	IOC: 1 ● Alert: 1 ● Inf: 4	Jul 21 2020	Reinvestigate
Aug 13 2020 08:19 PM	49f8022-6205-480a-8062-2156a05070	Request Threat (Critical)	Team Device Group	AFB8333F-3000	IOC: 1 ● Alert: 1 ● Inf: 4	Jul 21 2020	Reinvestigate
Aug 13 2020 05:00 PM	8a0a9f9f-d842-4a20-a247-43a0f4014817	Request Threat (Critical)	Team Device Group	AFB8333F-3000	IOC: 1 ● Alert: 1 ● Inf: 4	Jul 21 2020	Reinvestigate
Aug 13 2020 05:00 PM	8a0a9f9f-d842-4a20-a247-43a0f4014817	Request Threat (Critical)	Team Device Group	AFB8333F-3000	IOC: 1 ● Alert: 1 ● Inf: 4	Jul 21 2020	Reinvestigate

Drill down for Deep Insights into one of the IOCs



Investigation Type	Description	Classification	Timeline
Indicator of Compromise	Mobile Device phishing URL: https://imperium.com	Medium	Sep 11 2020 08:18:53 AM

Attribute	Value
Mobile Device	Team Device Group
Mobile Device ID	AFB8333F-3000
Mobile Device Name	Team Device Group
Mobile Device OS	Android
Mobile Device Version	8.0.0

Zimperium Deep Insights is part the Zimperium Mobile Forensic Feature Set

Solution	License	Use Case Examples	Data Source	Security Team involved	Value
Runtime Protection	Core MTD	- Abnormal traffic analysis - Phishing detection - System tampering	Device run time info	End user and security admin	Run Time Threat Alerting on Mishing, System Tampering; no user action required to run
Deep Scan	Core MTD	- Device Rebooting - System Tampering Trigger	Device System Log	End user and security admin	Log Level Threat Visibility
Deep Insight	Premium	- Pre-post trip comparison - Application and device context and timeline	Runtime + System log + backup	End User, Security Admin and Forensics Team	- Turns forensic data into actionable insights. - Reduces Investigation Time and accelerates MTTR

Ready to empower your SOC and Forensic Teams to quickly identify and respond to AI Attacks? [Contact Us](#) now for a demo and needs assessment.

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.



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

© 2026 Zimperium, Inc. All rights reserved.