Lookout Digital Forensics and Incident Response (DFIR) Services

Mission

Lookout Digital Forensic and Incident Response (DFIR) Services provide unmatched forensic analysis into mobile threats for organizations that have experienced a cybersecurity incident. The service was formed in response to the increasing frequency of significant cybersecurity attacks that leverage, exploit, and compromise mobile devices. Advancements in nation-state mobile malware capabilities, record numbers of iOS zero-day vulnerabilities, and a heavy reliance on mobile-focused social engineering are three signs that we've entered an era where mobile devices must be included in the scope of incident response engagements.

The team supporting DFIR Services is composed of industry veterans and experts with extensive experience in mobile device and mobile application analysis and is supported by a world-class mobile threat research team.

The Problem

Lookout DFIR Services fill a common gap across many existing incident response organizations that may not currently include mobile devices as part of the scope in their investigations. While there may be a number of reasons for this, our conversations with various incident response firms show that they acknowledge their lack in expertise on mobile devices, lack of proper tooling or mature analysis processes, or inability to retrieve the physical device because their client allows for BYOD without an ability to requisition the devices.

Incident Response firms that do investigate mobile threats typically leverage commercial tooling for data acquisition and lean on automated analysis results. Alone, these tools focus on gathering criminal evidence about the device's user, not declaring the health state of the device itself and providing the data required for proper forensic investigation.

The Lookout Advantage

Whether by partnering with your existing incident response vendor and ensuring inclusivity of mobile devices as part of your investigation or working independently from that partner to investigate your mobile devices, the Lookout DFIR Services team provides an unmatched range of mobile-specific expertise. This enables investigation into many mobile incident categories such as:

- Malware and Application Infections
- Device Compromises
- Unauthorized Access and Identity Based Attacks
- Insider Threats

Nobody knows mobile like Lookout. With a powerful combination of automated analysis tooling, hands-on investigation, the industry's largest AI-driven mobile security dataset, and unmatched domain expertise, the Lookout DFIR Services team is uniquely positioned to help your team understand the extent to which mobile devices are involved in a cybersecurity incident. In addition, Lookout Threat Intelligence researchers are pulled in to corroborate information from external incident response partners and identify novel indicators of compromise (IOCs).

Organizations can submit evidence digitally or physically by sending devices and evidence to the forensics lab in our Boston office. If our team is given the ability to review your third-party investigative reports, we will look at the incident holistically and provide our own incident advisory recommendations as part of our incident report.

To work with the Lookout DFIR team, please contact us at mobile-dfir@lookout.com