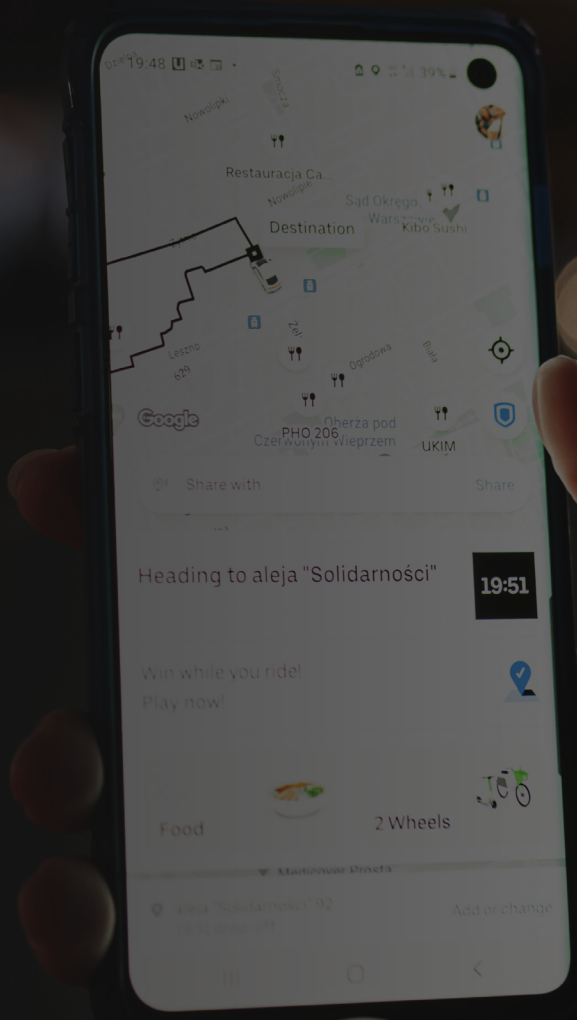
INDIUM

Safeguarding Digital Identities: How Indium Combated Account Takeover for a Global Ride-Hailing Giant

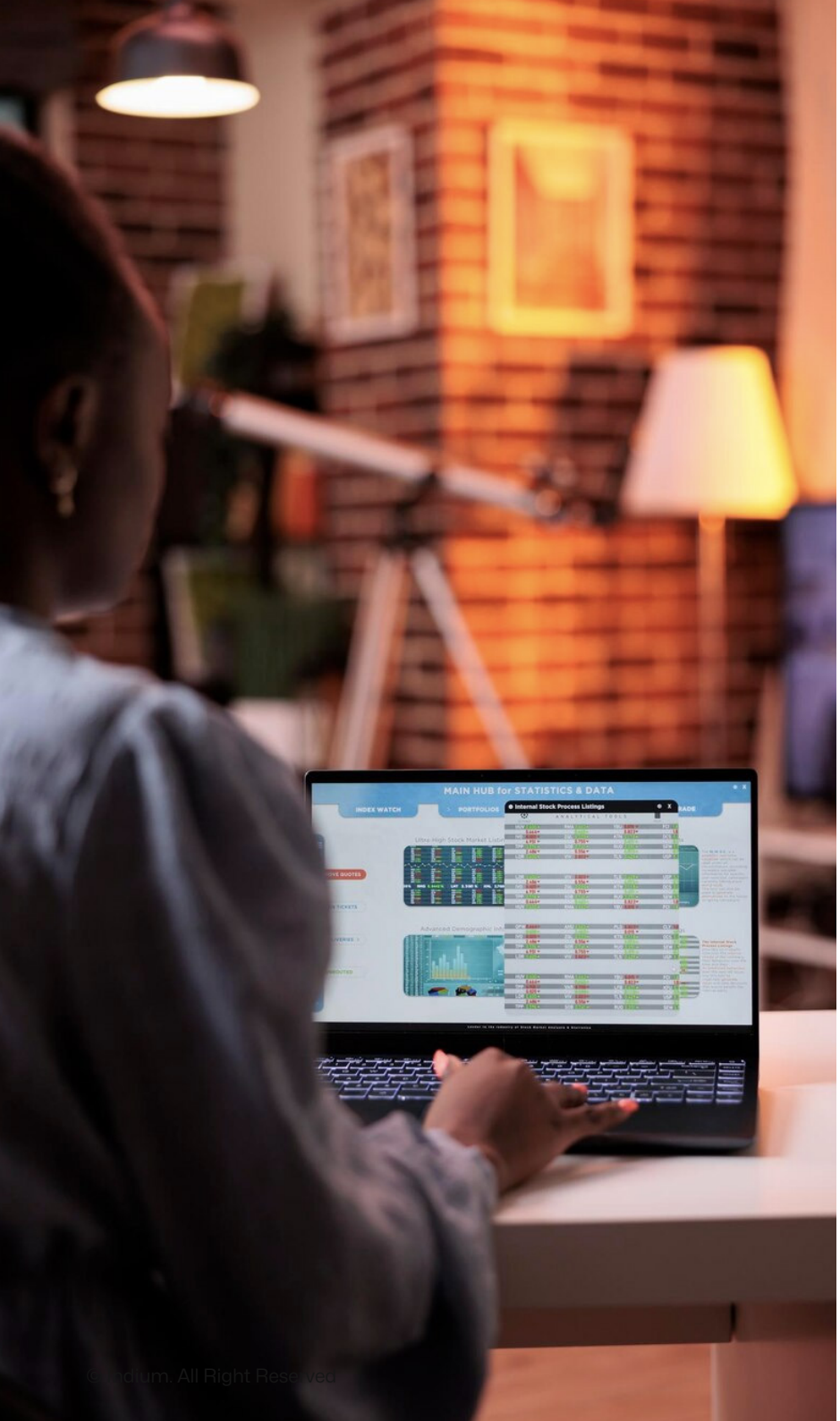


SUCCESS STORY

Securing user accounts is a top priority, especially for companies operating on a global scale. A leading ride-hailing and transportation network company with over 900 metropolitan areas worldwide faced a serious threat–Account Takeover (ATO). ATO incidents led to unauthorized access, financial losses, and significant reputational damage. This is where Indium stepped in, offering a perfect solution to detect and mitigate these security breaches.

The Challenge: Rising Account Takeover Threats

The client was grappling with an escalating number of ATO incidents. Unauthorized users were gaining access to customer accounts, altering payment details, and causing substantial financial damage. The breaches posed a direct financial threat and risked eroding customer trust, leading to legal repercussions and operational disruptions. The client needed an immediate and effective solution to identify vulnerabilities, detect ongoing breaches, and prevent future incidents.



Indium's Strategic Approach: Detecting, Monitoring, and Analyzing

We developed a multi-faceted approach to tackle the ATO challenges. Our strategy was built on four key pillars:

- **Detecting Suspicious Users:** Indium used SQL and Python to analyze historical data and identify high-risk users who modified payment details shortly after being added. By flagging these suspicious accounts, Indium prevented potential security threats. Google Sheets and GDS were used for data simulation and visualization.

- **Monitoring Banned Devices:** The team tracked accounts created using devices banned due to suspicious activity. These accounts were flagged and closely monitored to prevent any further unauthorized transactions.

- **Analyzing User Behavior**: Indium's solution monitored user interactions, particularly those focused on high-risk areas like the banking page. We scrutinized users for unauthorized activity and secured their accounts from potential ATO attempts.

- **Flagging Non-Client Locations**: Accounts created from locations outside the client's typical operating regions were identified and flagged. This proactive measure helped prevent fraudulent activities before they escalated.

Implementation: Protecting Customer Trust and Ensuring Business Continuity

Indium's approach delivered significant results:

- **Proactive Threat Detection:** Indium effectively curtailed about 15K ATO incidents by identifying and isolating suspicious users and devices. This proactive stance allowed the client to prevent substantial financial losses and maintain customer trust.
- **Enhanced Security Measures:** Implementing behavior analysis and location-based monitoring added layers of security, making it increasingly difficult for unauthorized users to exploit vulnerabilities.
- **Operational Efficiency:** By implementing a streamlined process for identifying and addressing potential threats, the client could focus resources on growth and service improvement rather than damage control.
- **Increased Client Trust:** By swiftly addressing the ATO challenges, Indium helped restore and reinforce customer confidence in the client's platform, ensuring sustained user engagement and loyalty.

Business Impact

Indium's solutions were a game-changer for the client. Our approach resolved the immediate ATO threats and fortified the client's overall security posture. Indium's expertise in digital security can protect global enterprises from sophisticated cyber threats, ensuring business continuity and customer satisfaction.