From Big Tech To Your Tech

Unleashing Elite Threat Intelligence & Incident Response Strategies

enprivacy


facebook

enprivacy


The Tipsy Owl


B Capital
Founders Circle
with Eduardo Saverin

The Post-Cambridge Analytica Era:

Post-Cambridge Analytica Shift:

Big Tech prioritized privacy by design, with stricter data collection, transparency, and user consent mechanisms in response to heightened scrutiny and regulatory changes (e.g GDPR).

Proactive Threat Intelligence:

Companies implemented AI-driven real-time threat detection, established elite incident response teams (e.g., Google's Project Zero), and fostered cross-industry collaboration (Meta's ThreatExchange).

Zero Trust Security Models:

Adoption of Zero Trust architectures, assuming continuous threats and requiring strict access verification for all systems, internal or external.

User Empowerment and Default Security:

Enhanced user privacy controls, end-to-end encryption, and proactive auditing with bug bounty programs to discover vulnerabilities before they are exploited.

Inside Meta - A Deepdive Into Proactive Defence

Overview of the Breach

In April 2021, a dataset containing personal information, including the phone numbers of 533 million Facebook users, was found on a public forum. The data, which also included names, locations, and email addresses, was scraped from Facebook due to vulnerabilities in its system.

Root Cause

The 2021 Meta Phone Number Breach was a result of data scraping that exploited a vulnerability in Facebook's Contact Importer tool. This tool allowed users to upload their contact lists to find friends on the platform. Attackers exploited a flaw in this feature to associate phone numbers with Facebook IDs, enabling them to scrape personal data. The compromised data included phone numbers, names, locations, email addresses, and other personal details of 533 million users.

The 360 Defence

Strengthening Meta's Defense Against Data Scraping

- **Vulnerability Fixed:** Meta patched the Contact Importer tool flaw in 2019.
- **Improved Scraper Detection**: Meta's EDM team used AI to better identify unauthorized scraping.
- **Rate Limits:** Meta applied rate limits to reduce large-scale scraping attempts.

Legal and Enforcement Actions

- **Legal Action:** Meta took legal measures against entities involved in data scraping.
- **Cease-and-Desist:** Meta issued cease-and-desist letters to those engaged in scraping.
- **Law Enforcement Collaboration:** Meta worked with authorities and hosting providers to remove scraped data and track down offenders.
- **GDPR Fine:** Meta was fined €265 million by the Irish DPC in 2022 for GDPR non-compliance.

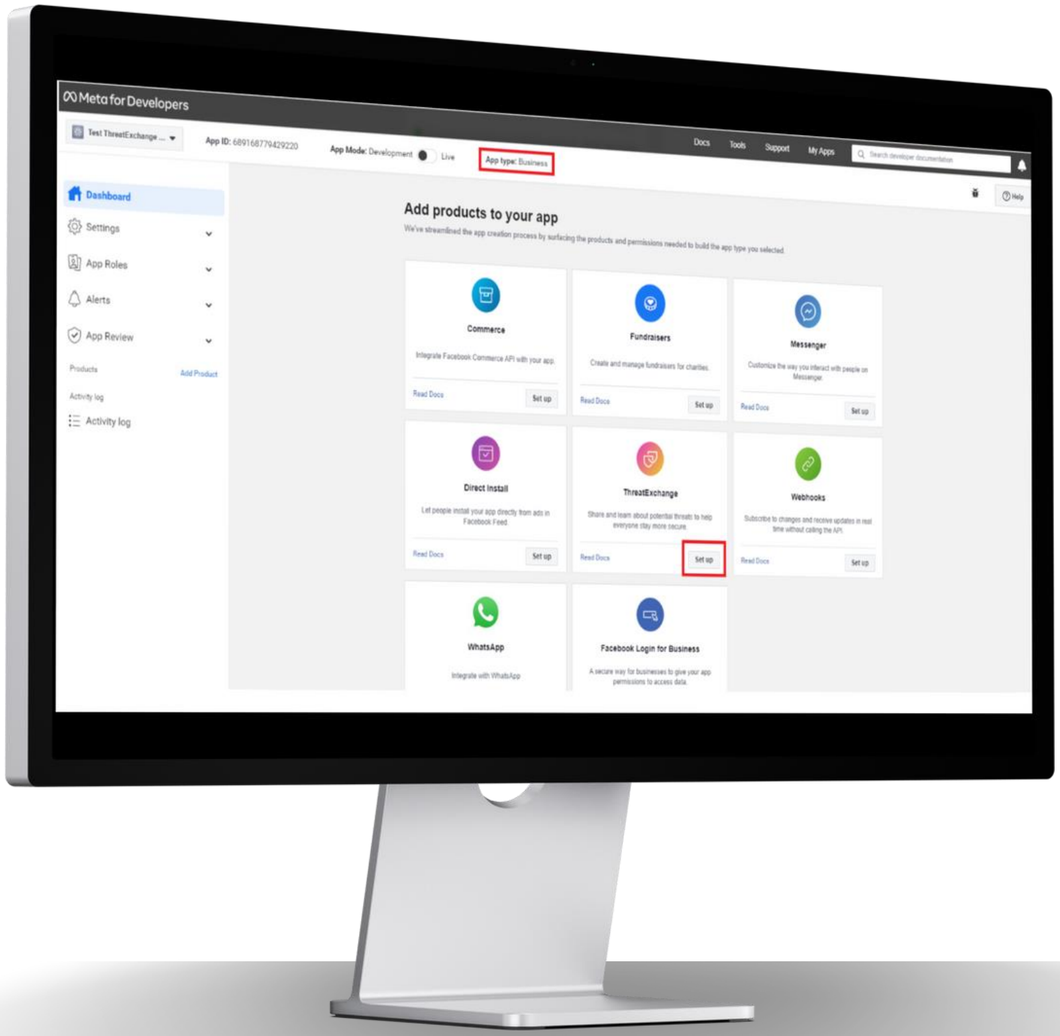
System Enhancements Post-Breach

- **Stricter API Controls:** Meta tightened access to its APIs, limiting third-party apps from retrieving excessive user data.
- **Enhanced Real-Time Scraping Detection:** Meta improved its ability to detect and block scraping attempts proactively.
- **Proactive Data Protection:** Meta strengthened its security measures to better safeguard user data against future threats.

Long-Term User Protection Initiatives

User Empowerment: Meta updated its Privacy Checkup tool, giving users greater control over their data and visibility through enhanced privacy settings.

Meta’s ThreatExchange Program



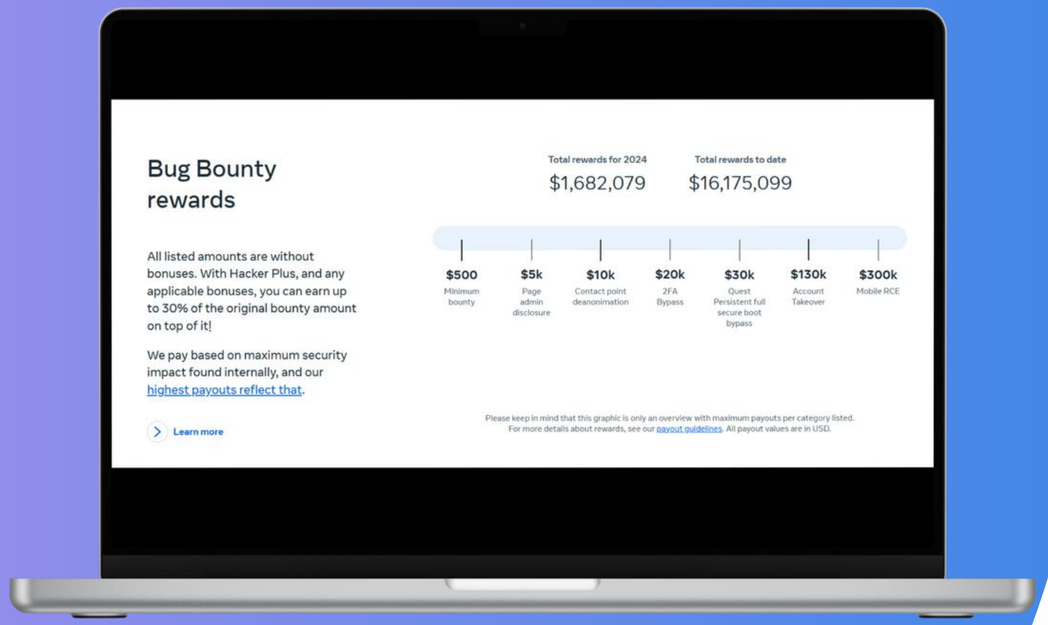
Collaborative Threat Sharing: Meta's ThreatExchange allows real-time sharing of cyber threat intelligence across industries.

Real-Time Detection: Access to real-time threat data enables quicker detection and response.

Automated & Customizable: APIs automate data sharing with customizable privacy controls for participants.

Cross-Industry Participation: Involves major companies like Microsoft and Dropbox for diverse threat insights.

Meta’s Data Abuse Bounty Program



01

Targets Third-Party Data Misuse:
Rewards researchers for uncovering third-party misuse of user data, like unauthorized collection or sharing.

02

Incentivizes Reporting:
Offers financial rewards for identifying serious data abuses, focusing on external app violations.

03

Enforces Legal Action:
Leads to proactive steps, like disabling apps, issuing cease-and-desist orders, and pursuing legal cases.

04

Strengthens Data Protection:
Insights from the program enhance Meta’s internal policies and enforcement against data misuse.

Big Tech Collaboration

Big Tech’s Playbook: Proactive Security In Action

Clear Reporting Channels

Establish anonymous and non-anonymous systems for reporting data misuse, similar to Meta’s Data Abuse Bounty Program.

Cross-Functional Teams

Create teams across HR, legal, and IT to handle reports, ensuring shared responsibility, like Meta’s EDM team.

Privacy-First Culture

Make data privacy a core value, as Apple and Google do by integrating security into product development.

Incentivize Reporting

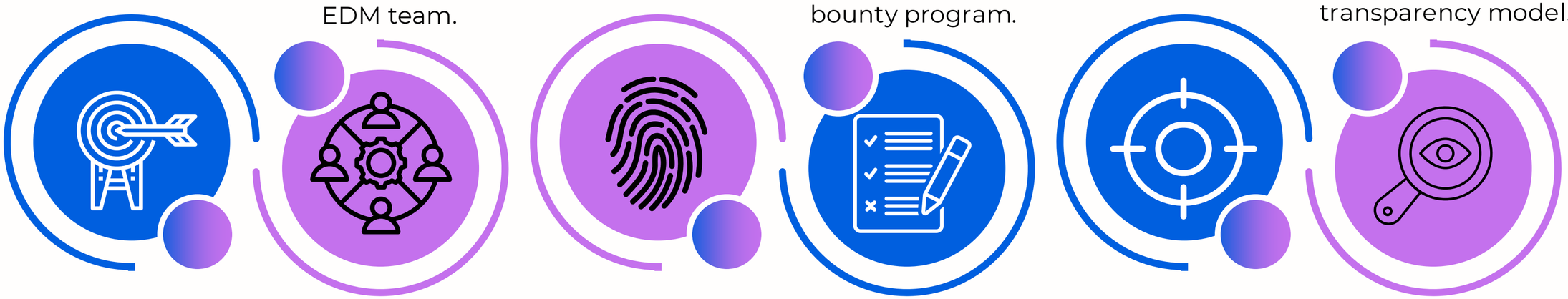
Reward and recognize data misuse reports, similar to Meta’s bug bounty program.

Automated Threat Detection

Use automated tools for monitoring misuse, like Amazon’s GuardDuty.

Transparency

Publish regular reports on misuse cases, following Google's transparency model.



Ranuk Mendis

Founder+CEO @ enprivacy (Ex Meta)

enprivacy