

Utilizing Your Red Team For Privacy



David Renardy

Privacy Engineer - Red Team



01

What's Privacy red teaming?

Red teaming in security

“I’m confident we are compliant with standards and regulations but how well do our defences stand up to malicious actors?”

“We have a blue team in place to detect and respond to attacks, but we aren’t sure how effective their processes/technology are - how can we pressure test them?”



Meta's Privacy Red Team Mission

“To continuously strengthen Meta’s privacy posture through proactive testing of people, processes and technology from an adversarial perspective.”









What data do you have and who wants it?

Industry/company

This varies by type and volume

-  Health
-  Financial
-  Social media
-  Defense
-  Government

Potential adversaries

-  Data brokers
-  Nation state actors
(espionage)
-  Private investigation
firms
-  Stalkers
-  Advertising agencies
-  Political campaign firms

Who are your privacy adversaries?

- **Privacy Adversarial Framework (PAF):** Applied to cases and adversarial examples discovered by the red team or encountered by the blue team.
 - TTP taxonomy finds choke points for fingerprinting or remediating adversary behavior

https://github.com/facebookresearch/privacy_adversarial_framework
- **Meta Weakness Enumeration (MWE):** Applied to privacy, security and integrity events to measure commonalities in attack surface across products and features. Helps drive blue team resource allocation / planning / training as well as driving red team focus.

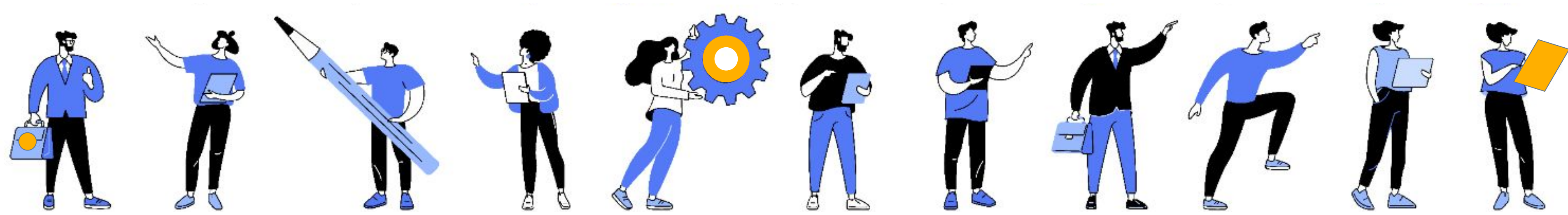


02 How do you plan and run a privacy-focused, red team operation?

How do you plan and run a privacy-focused red team operation?

Who is your blue team?

- Purely external engagements can be challenging in Privacy
- Having trusted agents with awareness of the product space is important for operation success and remediation of operation findings
- Internal tooling often acts as a force multiplier for demonstrating attacks.



What are the privacy goals for the operation?

Privacy Adversary Emulation

Objective-based, campaign style operations.

Scope: Spans products, services, and features.

Goal: Test defenses against real adversary activity.

- Like traditional red team operations

Product Compromise Test

Compromising a thing (feature, API, etc.) from a privacy perspective.

Scope: to a specific product, service, or feature.

Goal: Enumerate privacy weaknesses

- Like finding all the vulnerabilities

Goal: Gain access to all the data

- Like getting root

How do you plan and run a privacy-focused red team operation?

What do you need to do to prepare?

In security operations, you usually stop when encountering potential data. That's not an option for us!

Work with legal partners to structure safe and compliant operation procedures:

- Global regulations
- Minimize risks
- Build in mitigations

Some standard operating procedures:

Tracking of operational assets

Data handling / analysis policies

Scraping policy including standard traffic tagging

Fake / test account creation guidance

OpSec guidance

Deletion scheduling for operational assets

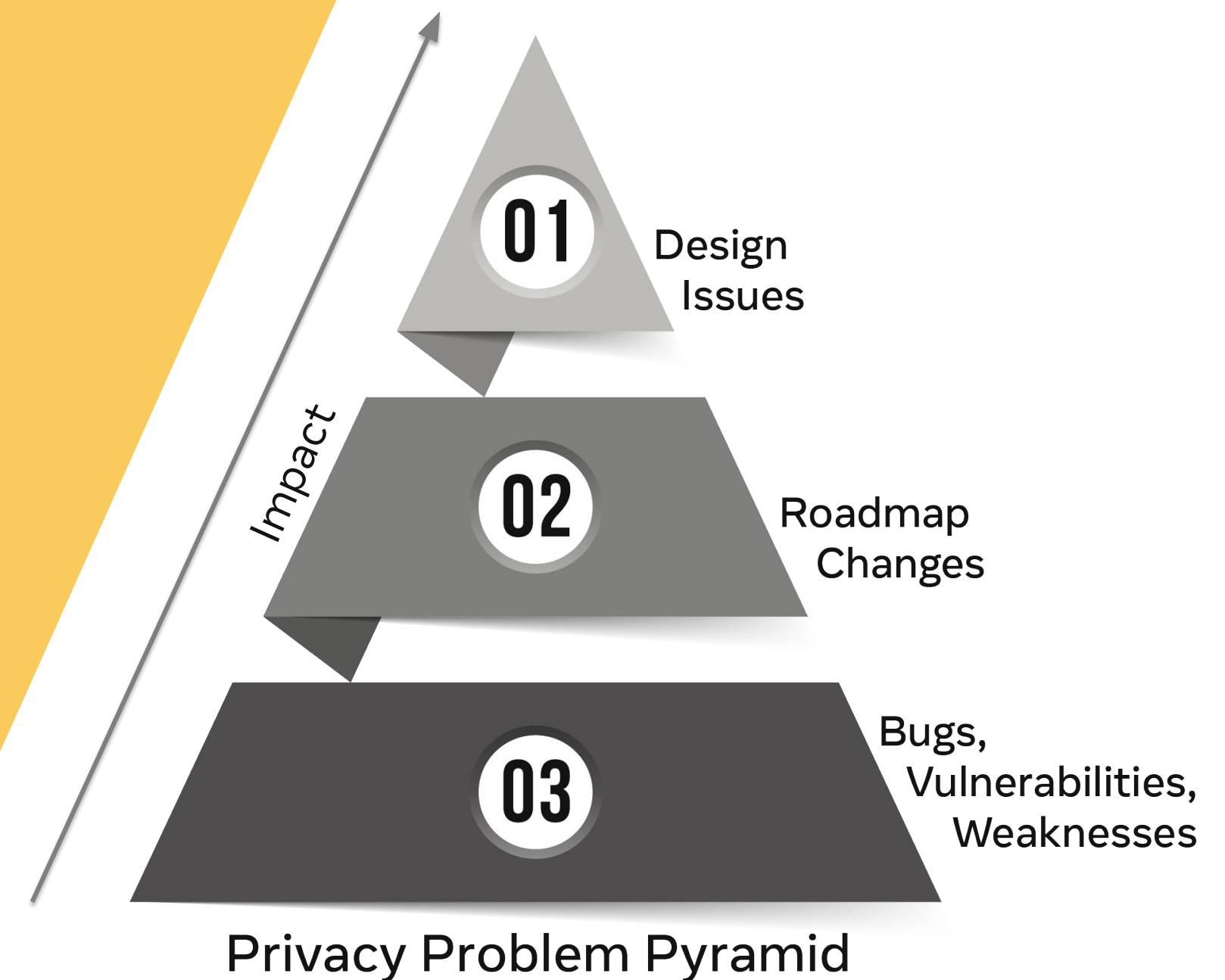
03 How can the findings of a privacy red team operation strengthen your privacy posture?

What kinds of findings are there?

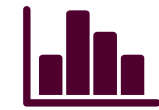
Goal: Drive fundamental change in your privacy posture.

Desired outcomes:

- Expanding understanding of privacy weaknesses
- Expanding understanding of privacy adversaries
- Measure how we're doing
 - Defenses validated
 - Gaps identified
 - Quantify risk



What additional considerations might be required for privacy findings?



1. How does abuse scale?



2. Does this finding have regulatory reporting requirements?



3. Is the product behavior consistent with customer expectations?



4. What kind of detections could be used to identify past or future abuse?

Strengthen your privacy posture through offensive privacy



- What types of data do you hold and how sensitive is it?



- Who wants it, who are your adversaries?



- Who are your blue teams?



- When will your red team start hunting for privacy weaknesses?





drenardy@meta.com