
# Better Privacy Through Offense: How To Build a Privacy Red Team

Scott Tenaglia

Engineering Manager, Privacy Red Team, Meta

# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

03 Meta’s Privacy Red Team

04 Operations Ideas

05 Final Thoughts

# This talk is...

- The start of a conversation about offensive privacy.
- Potentially a blueprint for how your company could create a similar team or offering.
- To help you understand how privacy red teaming fits into a holistic privacy program.

# This talk is not...

- A product or service pitch.
- A conversation about any other aspect of Meta beyond privacy red teaming.
- About absolutes.
- The final word on this topic.

# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

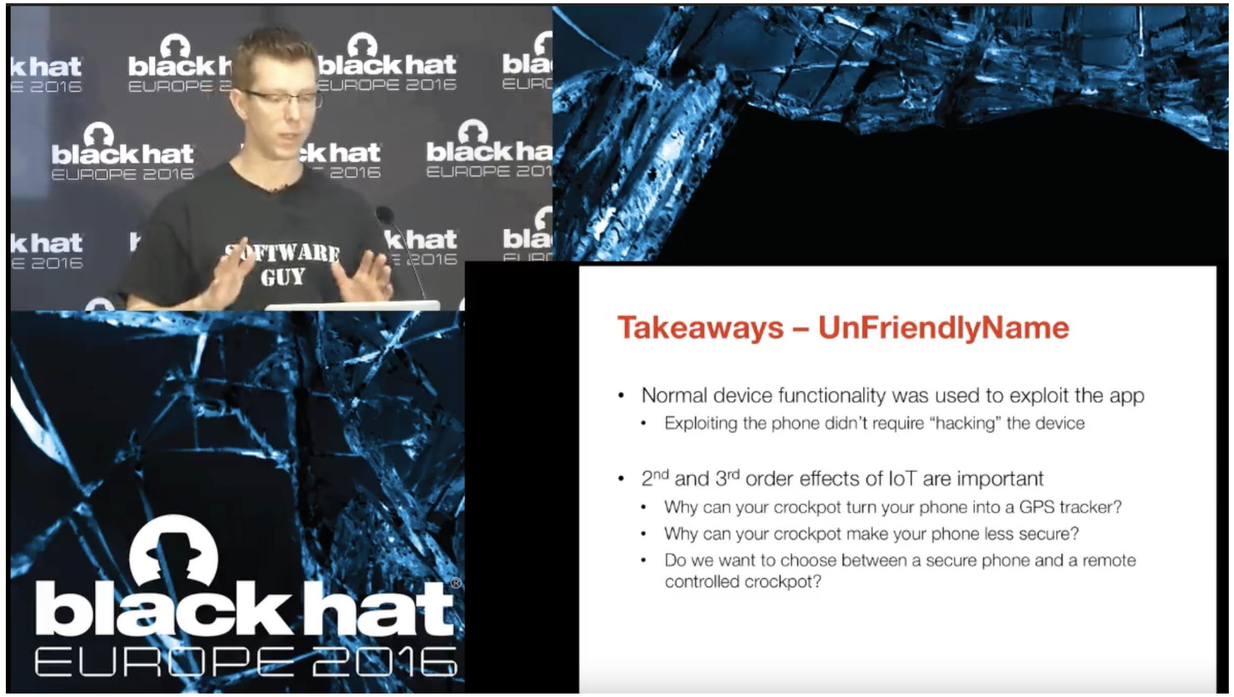
03 Meta's Privacy Red Team

04 Operations Ideas

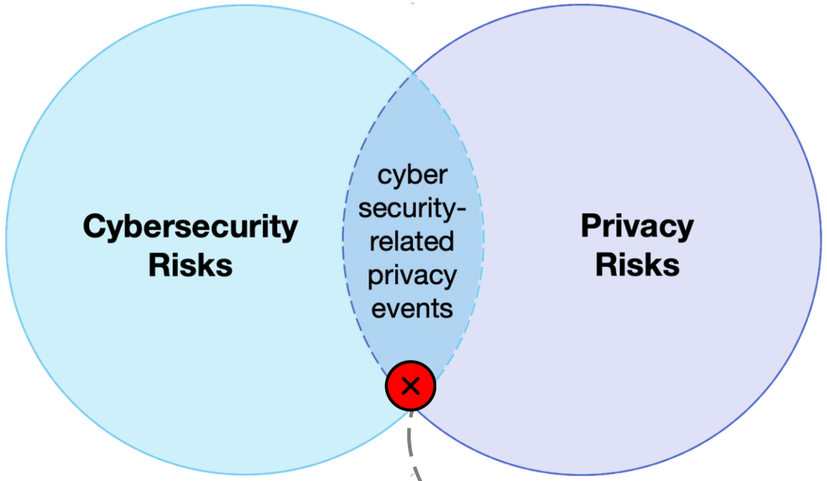
05 Final Thoughts

# Have you ever...

- Been on an op, come across some PII, but don't know what to do about it?
- Been asked to start recording access to user data as a finding?
- Been asked to perform a more privacy-focused assessment?
- Had a finding but no one cared because it have enough "security" impact?

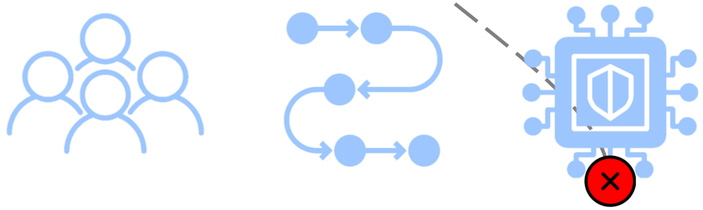


## Perceived Risk




Security and Privacy programs help mitigate risk.

## Mitigations



Mitigations are a combination of people, process, and technology (i.e., a blue team).

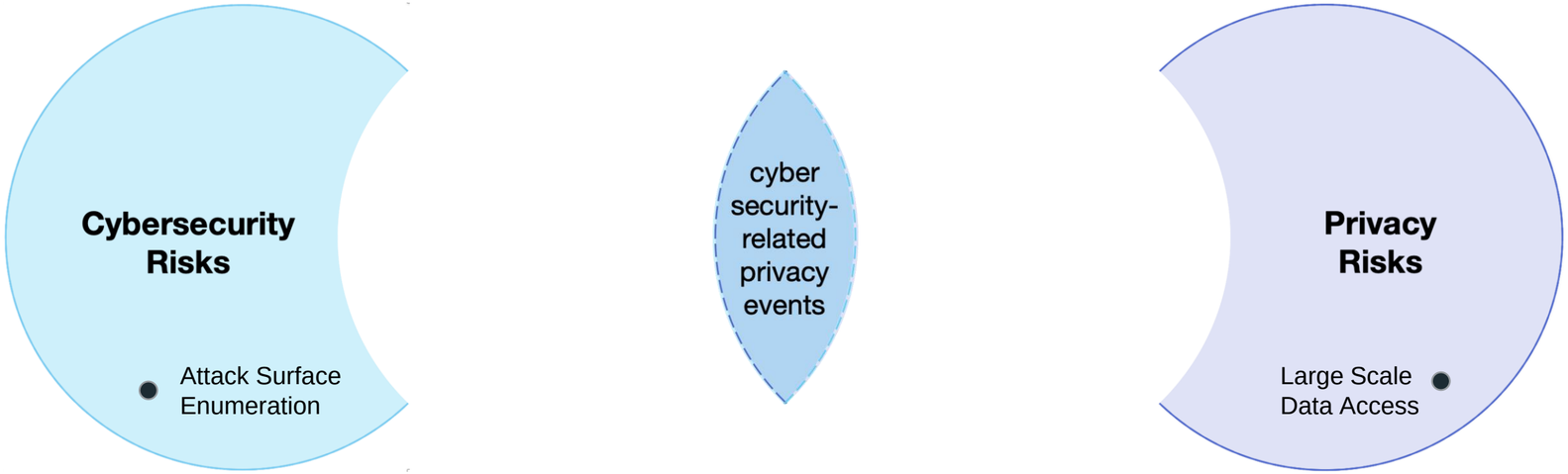
## Red Team

Red teams identify actual risk by testing mitigations from an adversarial perspective.



*Image courtesy of the NIST Privacy Framework https://www.nist.gov/privacy-framework/privacy-framework

## Perceived Risk




## Mitigations

## Red Team

Identify the actual risk to systems and networks.


Identify the actual risk to the user's privacy and their data.




*Image courtesy of the NIST Privacy Framework https://www.nist.gov/privacy-framework/privacy-framework

# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

03 Meta's Privacy Red Team

04 Operations Ideas

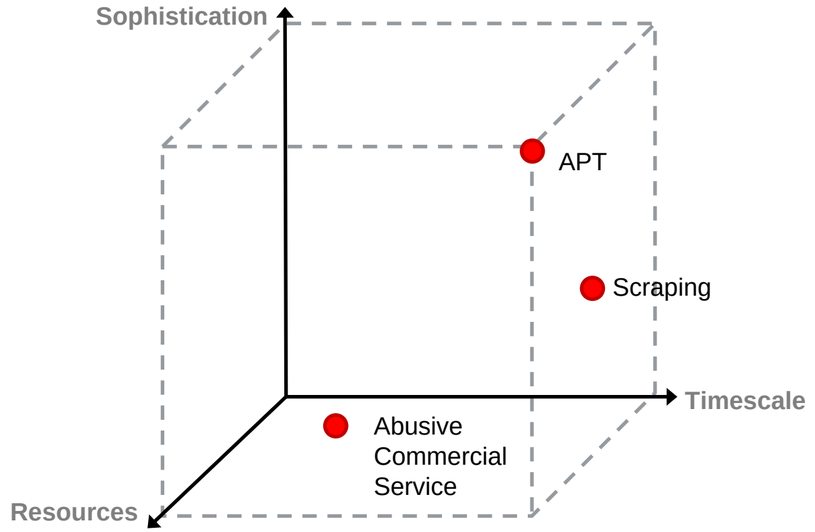
05 Final Thoughts

# Accessing Data

- Security red teams may avoid accessing user data because of the regulatory and legal implications.
- Privacy red teams focus on finding access to user data.
- This is a key differentiator in privacy red team operations.
- Partner with your legal team early and often to mitigate any legal and compliance consequences.

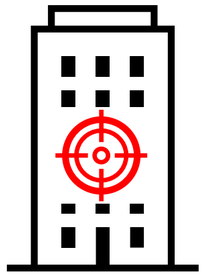
# Adversaries

- Much of the adversarial conversation in security is dominated by APTs and cyber criminal groups.
- Privacy adversaries differ in 3 ways:
  - Timescale
  - Resources
  - Technical sophistication



# Targets

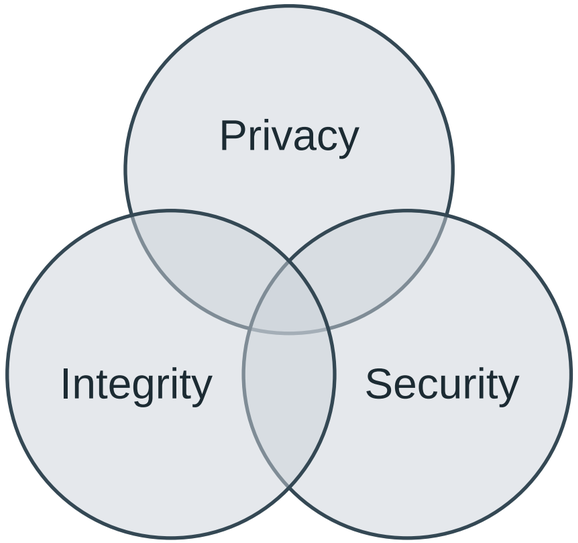
- Security operations compromise systems and networks to *indirectly* access data.
- Privacy operations *directly* access data through products and services, because this is where many privacy controls are implemented.



*“Security targets the company, while privacy targets user data.”*

# Blue Teams

- At Meta we hired people, created processes, and developed technologies to mitigate privacy risks. This could be considered a privacy “blue team.”
- But adversaries have different motives and use various methods to take data.
- Privacy red team operations often test multiple blue teams.



# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

03 Meta’s Privacy Red Team

04 Operations Ideas

05 Final Thoughts

# Meta's Privacy Red Team

## Mission

**Proactively** test people, processes, and technology from an **adversarial** perspective to identify the actual risks to protecting users' data and their privacy.

## Functions

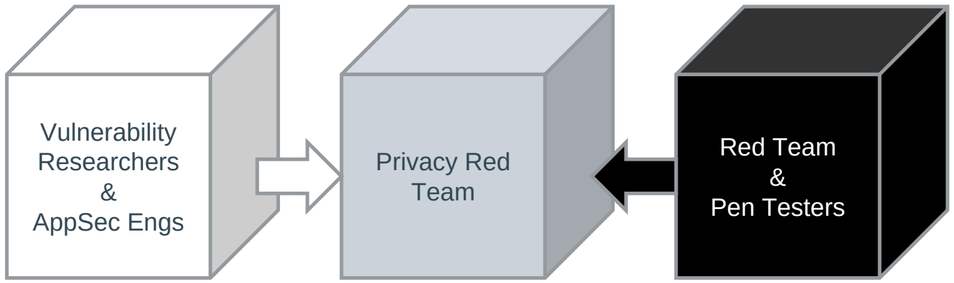
- Privacy Adversary Modeling
- Technical Assessments
- Privacy Weaknesses Cataloging
- Educate & Inform

## Key Products/Services

- ❑ Privacy ATT&CK Framework
- ❑ Privacy Weaknesses Taxonomy
- ❑ Privacy threat modeling
- ❑ Tabletop exercises
- ❑ Adversary emulation
- ❑ Privacy purple team
- ❑ Product compromise test
- ❑ Risk management feedback
- ❑ Incident response support
- ❑ Engineering support
- ❑ Privacy education and training

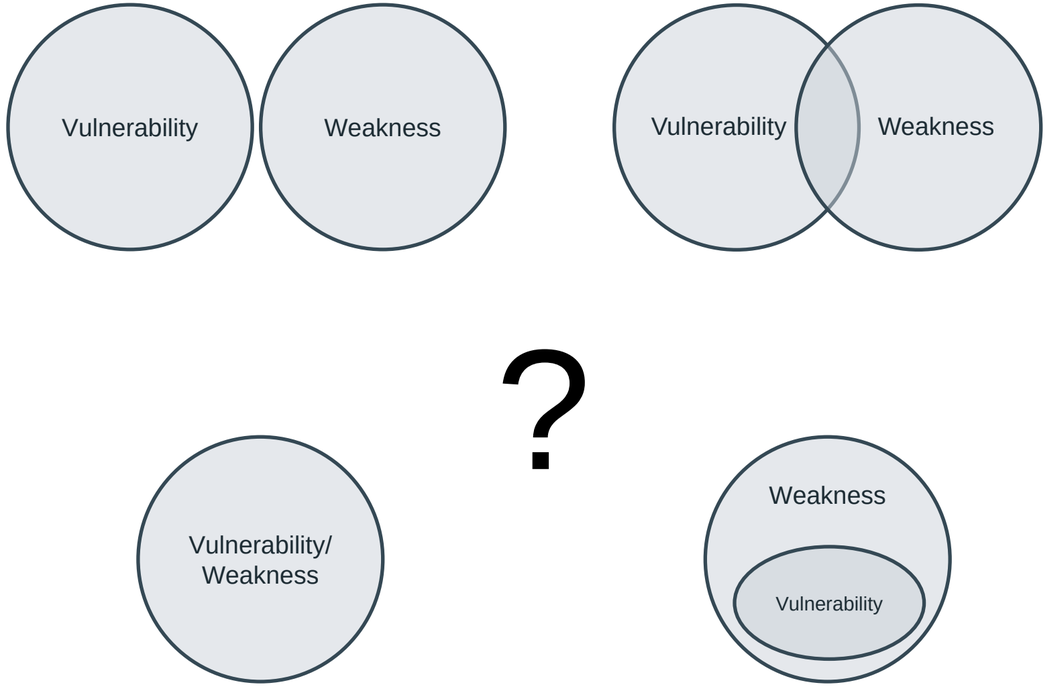
# Team Composition

- An Engineering-First Discipline.
  - We do technical assessments, not risk assessments.
- Looking for people with
  - ✓ Adversarial mindset
  - ✓ Offensive security skillset
  - ✓ Privacy instincts
- We recruit from 4 disciplines: Red Teamers, Pen Testers, Vulnerability/Security Researchers, AppSec Engineers.
- Legal, risk, and policy are important partners, but not team members.
  - Meta is setup to facilitate these partnerships.



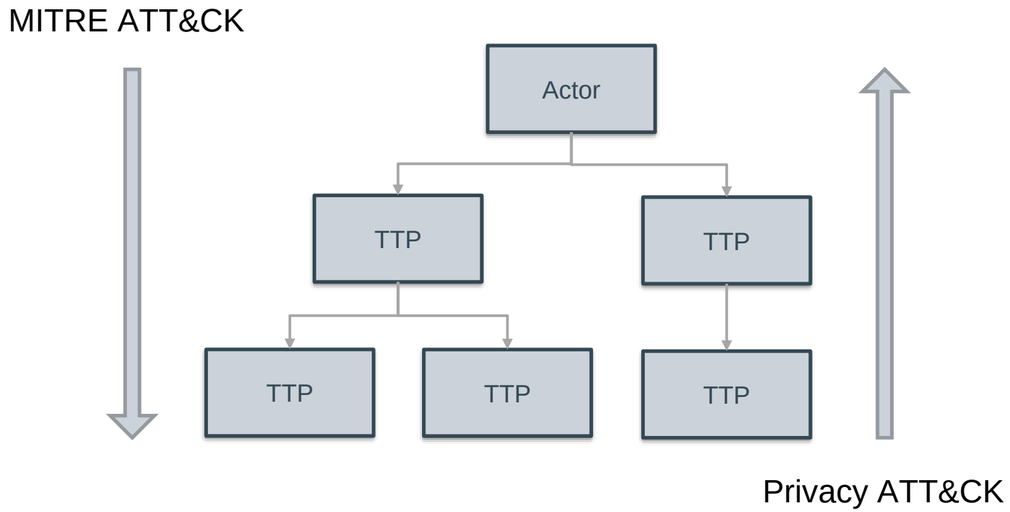
# Privacy Weakness Taxonomy

- A compendium of weaknesses, faults, flaws, and bad practices that are the root cause of privacy issues, as well as a taxonomy for categorizing them.
- Goals:
  - Provide a centralized and authoritative source of knowledge about privacy weaknesses.
  - Provide a common language to discuss privacy weaknesses.
  - Define a new metric for measuring privacy risk.
  - Understand the difference between security vulnerabilities and privacy weaknesses.



# Privacy ATT&CK Framework

- Effort to accurately capture privacy-focused adversarial Tactics, Techniques and Common Knowledge.
- The types of adversaries that we focus on in privacy may not be a one-to-one match to those seen in cyber security and their TTPs and objectives also differ.
- Goals:
  1. To improve the detection, measurement, and hence mitigation of threats.
  2. To ensure that Red Teams can accurately emulate real world adversaries.



# Technical Assessments

## 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

## Privacy Purple Operations

Working with a blue team to improve defenses using specific TTPs.

**Scope:** A specific privacy control or safeguard.

**Goal:** Test a particular defense's resilience to specific TTPs.

- How easy is it to bypass?
- What are the corner cases?

## 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

# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

03 Meta's Privacy Red Team

04 Operations Ideas

05 Final Thoughts

# Account Attribution

**Type of Operation:** Adversary emulation

**Adversarial Profile:**

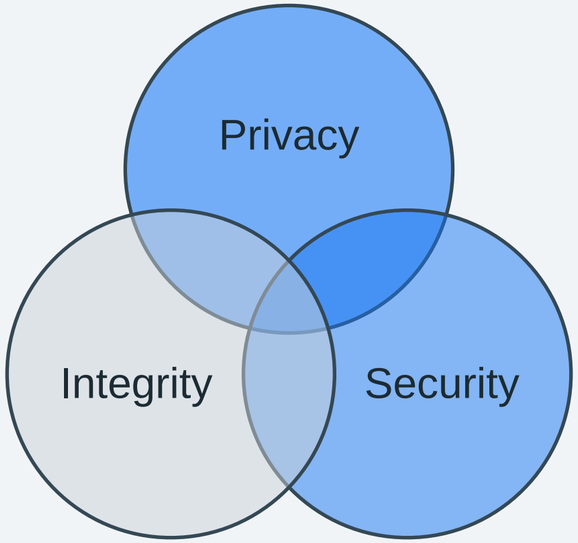
- A political campaign's digital PR agency have a data dump of voter contact details.
- An internet troll trying to dox a bunch of people.

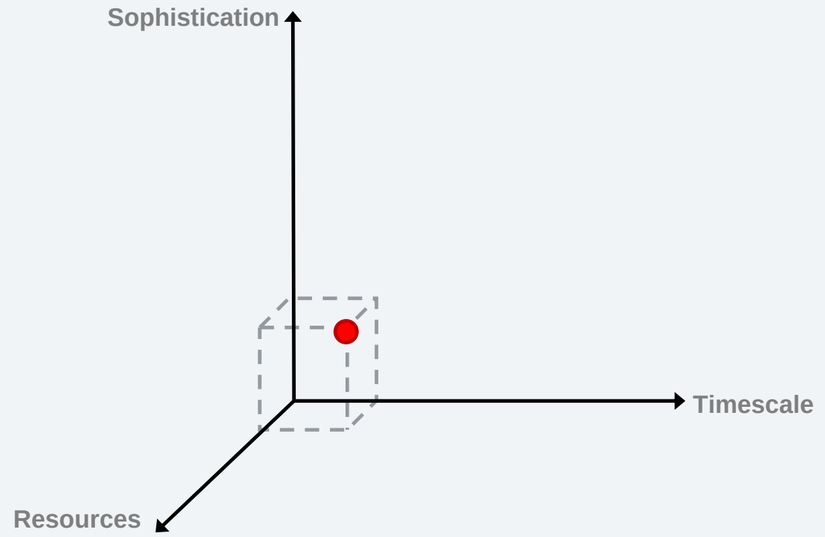
**Objective(s):**

- Identify the risk of account enumeration and UII scraping associated from contact information (i.e., phone numbers and email addresses) and measure opportunity for scale.
- Identify for a given list of user accounts what associated contact point data can be obtained (reverse of point 1) and measure opportunity for scale.

**Methodology:** Focus on combining functionality

- Authentication systems
- Account recovery workflow
- Contact importer
- Developer APIs



# Sensitive Data Leak

**Type of Operation:** Privacy purple operation

**Adversarial Profile:**

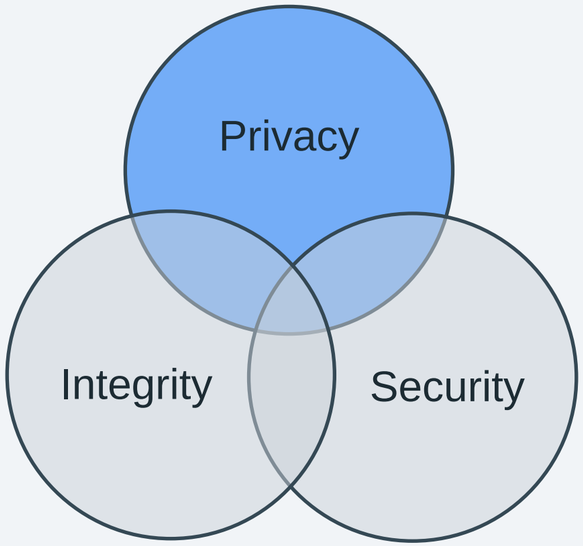
- Absent minded developer
- Insider threat
- External actor with access to our internal network

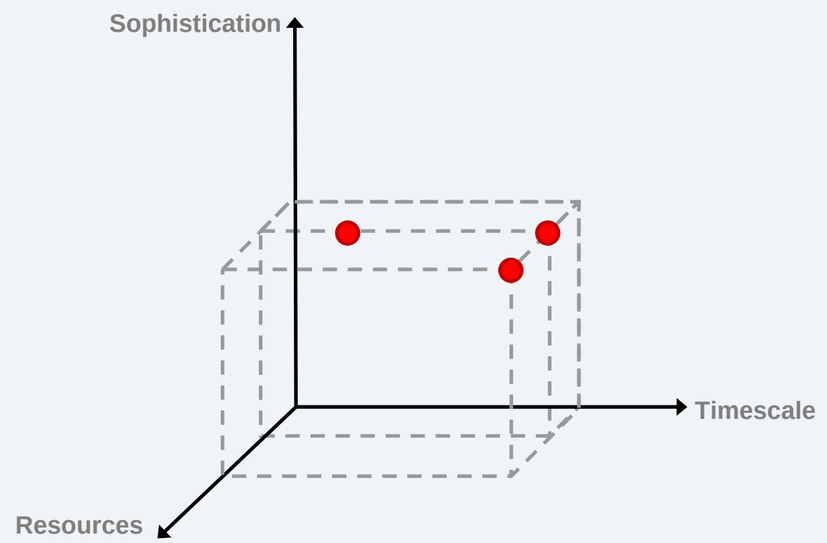
**Objective(s):**

- Test effectiveness of detection mechanisms in identifying new streams with sensitive data exiting infrastructure.
- Test ability to track detected streams to owners.

**Methodology:** 2-week sprint model

1. Develop and release new data streams based on TTPs
2. Blue team hunts for the new data streams
3. Both teams identify data streams that avoided detection



# Data Type Focused

**Type of Operation:** Adversarial emulation

## Adversarial Profile:

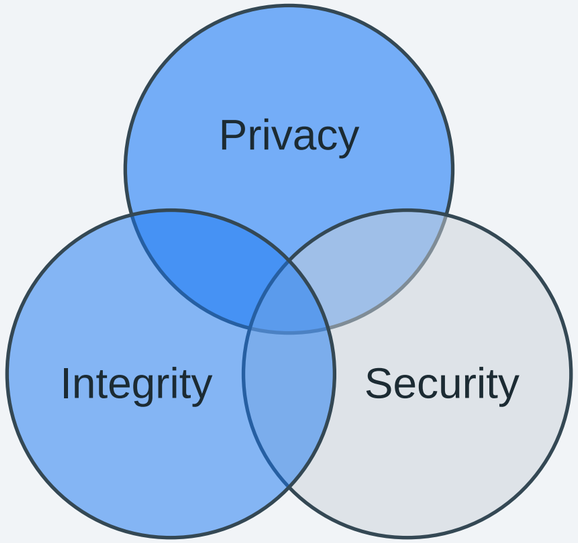
- **Low-capability adversary**: Abusive commercial services with access to off-the-shelf, open source and inexpensive commercial tools.
- **High-capability (nation state) adversary**: Has access to custom tooling, on-platform assets, insider information, 0-day or n-day exploits, and skilled teams.

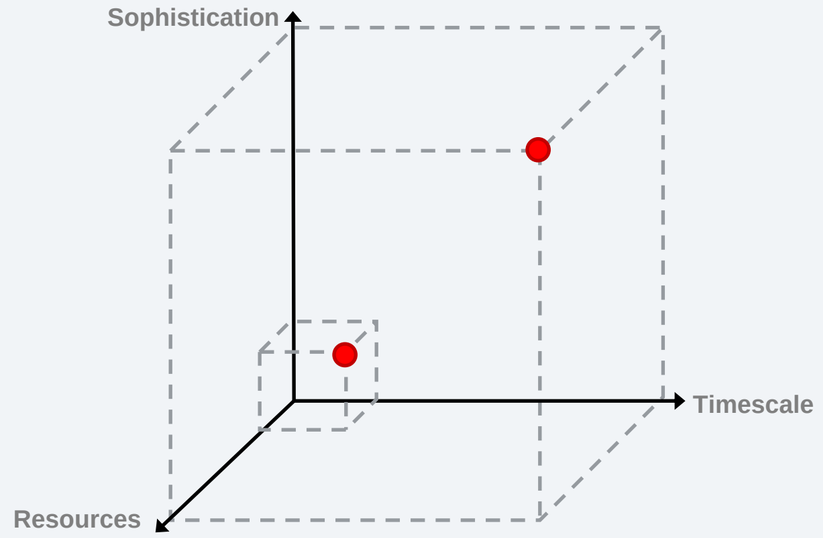
## Objective(s):

- Proactively identify how an adversary would access/use/modify a type of data.
- Improve detection and and prevention of that activity.

## Methodology:

- Identify data types you have that are valuable to the adversary.
- Enumerate TTPs to obtain data about high value targets and their immediate contacts.
- Test TTPs and existing on-platform defenses and detections.



# Findings

- Security findings can be more **objective.**
  - The impact of security vulnerabilities (e.g., XSS or code injection) is well known.
  - There are industry best practices for mitigation (e.g., input validation and data encoding).
- Privacy findings can be more **subjective.**
  - Legal and regulatory environments help determine what is a finding.
  - The organization's own statements about user/data privacy may make something a finding.
  - Often, we must take the users expectation of privacy into account.
- As privacy matures, we hope that findings become more objective.
  - We understand privacy weaknesses better
  - We understand privacy by design better

# Agenda

01 The Case for Offensive Privacy

02 Security and Privacy

03 Meta's Privacy Red Team

04 Operations Ideas

05 Final Thoughts

# Metrics

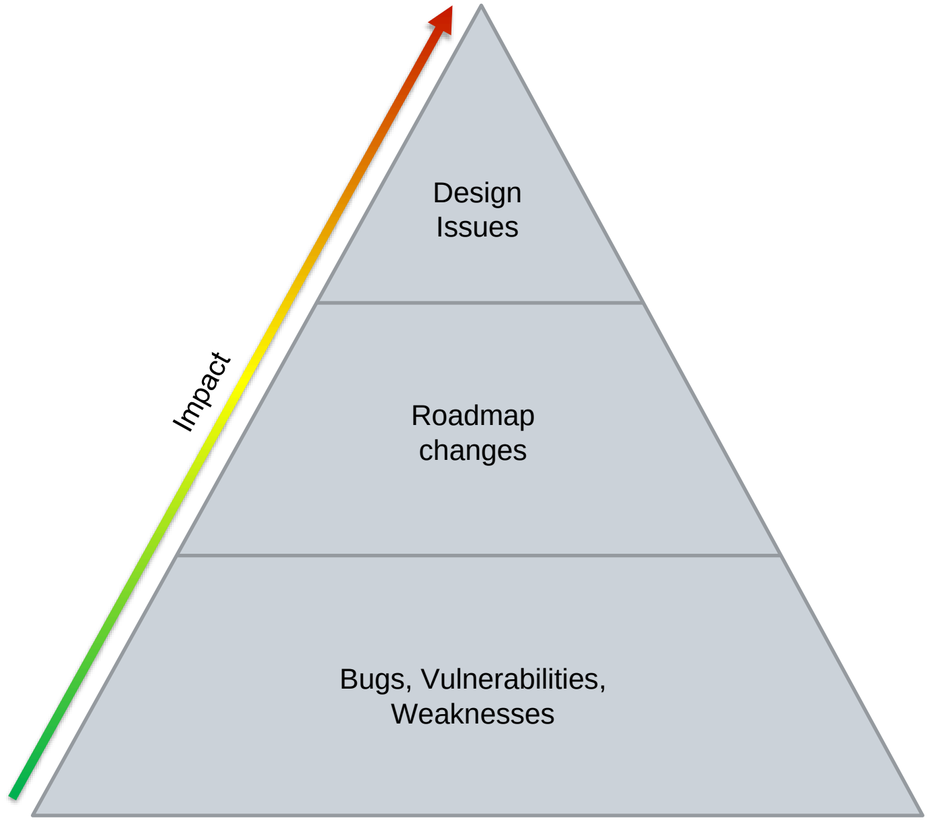
**Problem:** Traditional red team metrics don't necessarily apply

- Time to compromise or time to detection don't make sense

**Goal:** Drive fundamental change in our privacy posture.

**Things to measure:**

- Understanding the space
  - New weaknesses
  - New TTPs
- How we're doing
  - Defenses validated
  - Gaps identified
- The team's impact
  - Problems found




Privacy Problem Pyramid

# Lessons Learned

## Compliance vs. Assurance

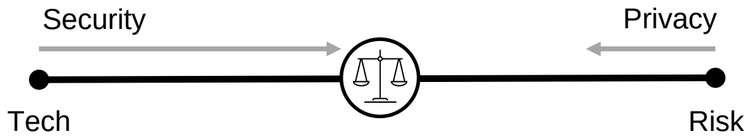
- Compliance is ensuring that you are meeting some requirement (e.g., policy, law, regulation, etc.)
- You can be compliant but still vulnerable to adversary behavior.
- Assurance goes beyond compliance to provide additional confidence.

## Legal risks may be different than for a security red team

- You're may be accessing, collecting, storing, and using data in a different way.
- Global regulations may require different mitigations to the risks of doing so.

## We're in the early stages of

- Privacy as a technical discipline, separate from but linked to, legal and policy.
- Offensive privacy as a fundamental component of a holistic privacy program.



# Let’s Keep Talking

tenaglia@fb.com

@scotttenaglia