Threat Model Exercise

A worksheet to help you and your team develop, iterate, and implement your threat model.

https://hackablebook.com

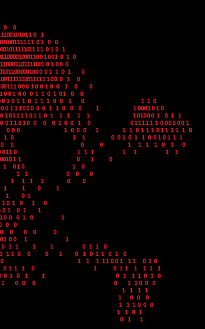
PURPOSE

The purpose of this document is to help you establish (if you don't have one yet) or update (if you already have one) the threat model for your company. Once complete, you'll have a well-thought out draft to bring back to your organization and drive the conversation around how to implement safeguards against the issues outlined in here.

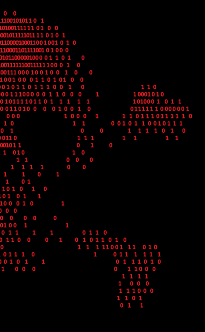
As always, if ever need help, I'm only an email away (ted@tedharrington.com).

Good luck!

Ted

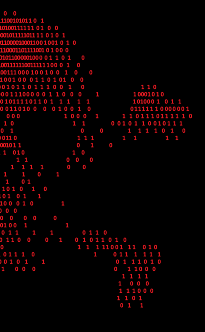


THREAT MODEL OVERVIEW

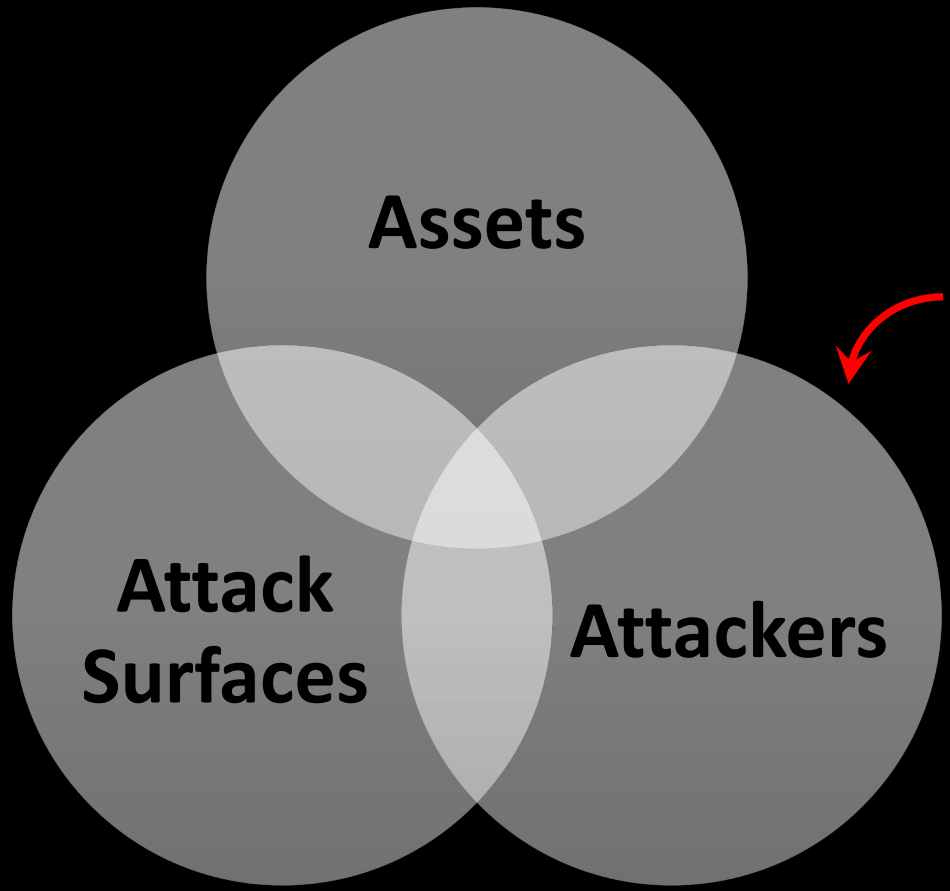


THREAT MODEL OVERVIEW

- Threat modeling is an adversary-centric exercise that answers five crucial questions:
  - What do you want to protect?
  - Whom do you want to defend against?
  - Where will you be attacked?
  - What possible exploit scenarios should you consider?
  - What should you do to defend?
- Your threat model is the foundation of your entire security plan. It helps you determine:
  - How much to invest
  - Where to invest it
  - How to measure success

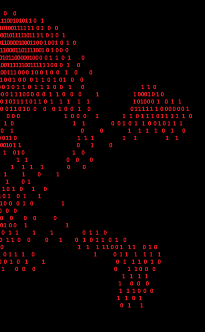


THREAT MODEL COMPONENTS



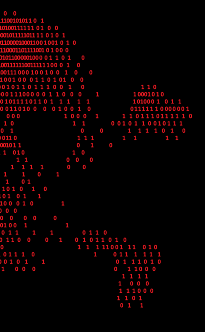
Also known as "Threats," hence "Threat Modeling"

STEP 1: ASSETS



ASSETS

- Assets are the things you want to protect.
- They come in two forms:
  - Tangible: material things that can be compromised, such as data or money.
  - Intangible: conditions that can be undermined, such as brand reputation or system availability.
- Companies often fail to consider *all* of the assets that they care about. Be exhaustive when listing every single thing your company cares about.



THE TWO TYPES OF ASSETS

TANGIBLE

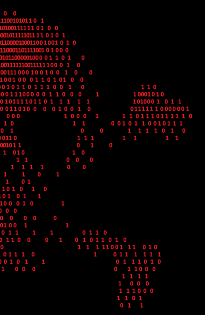
e.g. data, money

What most people focus on

INTANGIBLE

e.g. reputation, trust

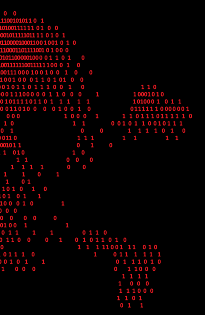
But don't forget about these!



Exercise: Identify Your Tangible Assets

The question this portion answers: “What do you want to protect?”

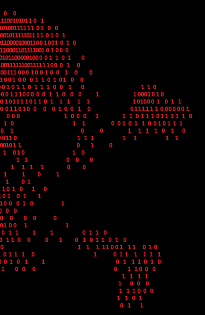
- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}



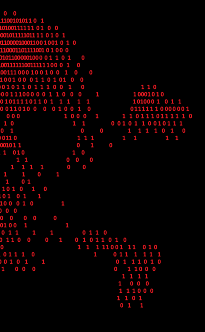
Exercise: Identify Your Intangible Assets

The question this portion answers: “What do you want to protect?”

- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}

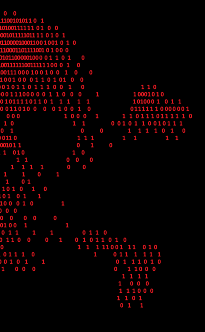


STEP 2: ATTACKERS

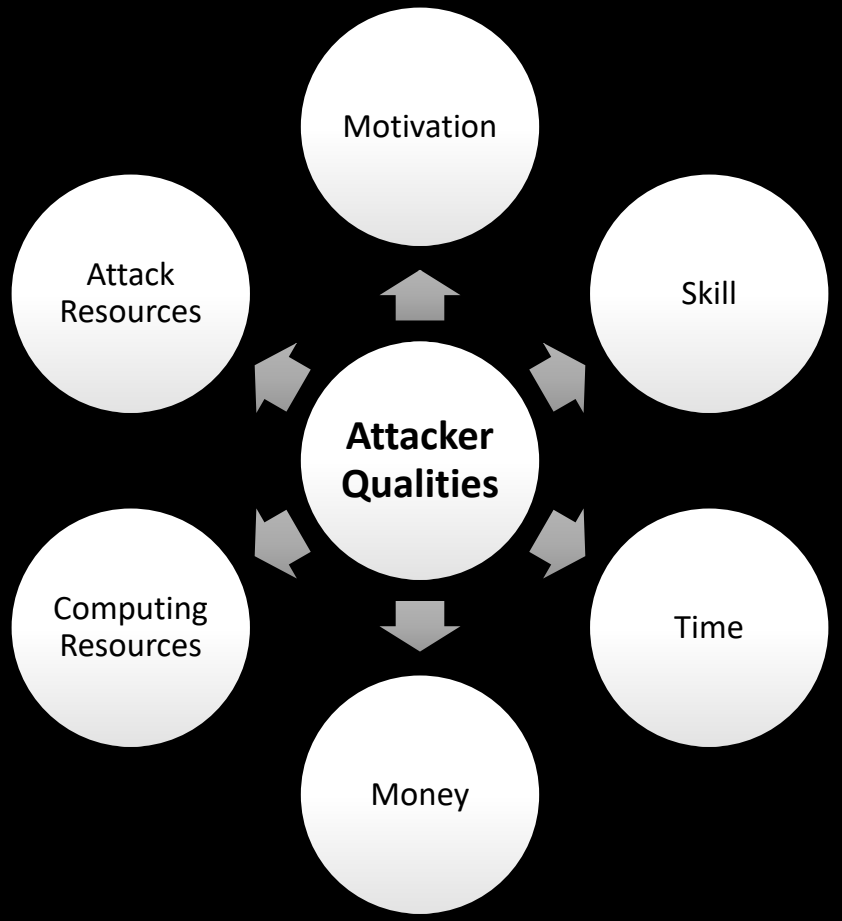


ATTACKERS

- Different adversaries attack for different reasons.
- They all have different levels of skill and access to resources.
- They come as both external attackers and the insider threat (with the difference being that insiders have elevated trust and access).



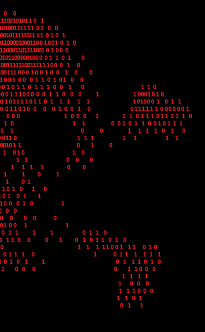
ATTACKER QUALITIES



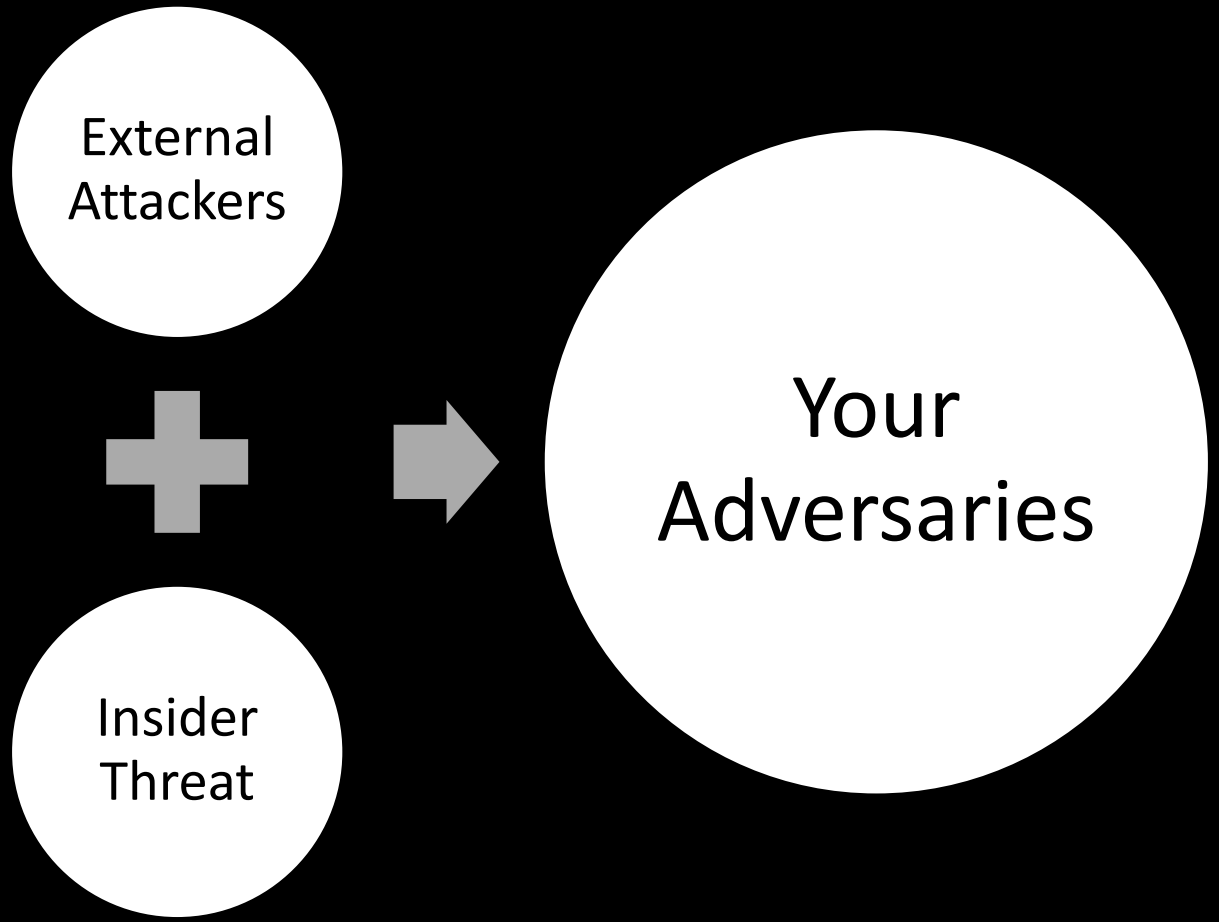
ATTACKER MOTIVATIONS

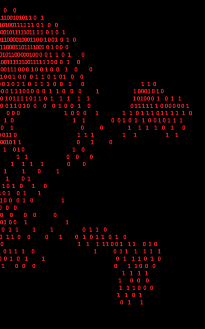
Common attacker motivations include:

- **Profit**: they want to make money
- **Notoriety**: they want to make a name for themselves
- **Challenge**: they want to prove they can do it
- **Geopolitical Gain**: they want to advance their nation's agenda
- **Advocacy**: they want to highlight a cause
- **Competitive Advantage**: they want to get an edge over a rival
- **Revenge**: they want to retaliate for a real or perceived injustice
- **Terrorism**: they want to instill fear
- **Espionage**: they want to obtain secrets
- **Economic Warfare**: they want to advance their own financial position and weaken a rival's financial position



THE TWO CATEGORIES OF ATTACKERS

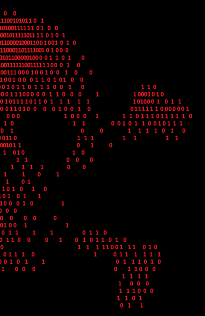




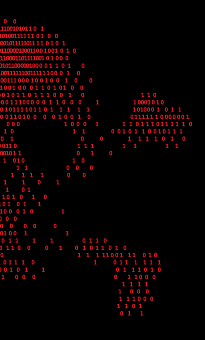
Exercise: Identify Your Attackers

The question this portion answers: “Whom do you want to defend against?”

- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}



STEP 3: ATTACK SURFACES

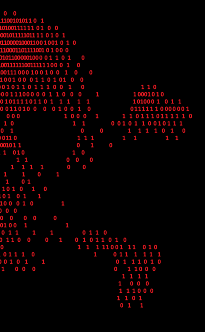


ATTACK SURFACES

The technical definition of an attack surface is anywhere that data ingresses, egresses, or is accessed. However, the easier way to think about it is simply wherever you could be attacked.

Examples of your application's attack surfaces include:

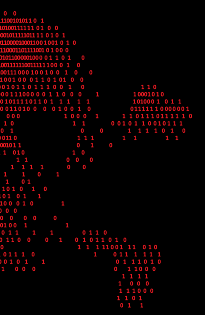
- **Input fields:** login pages, web forms, contact fields.
- **Interfaces**: APIs, admin interfaces, transactional interfaces, libraries.
- **Integrations**: third-party systems, cloud deployments, integrations with your other systems.
- **Storage**: databases, file systems, local storage.
- **Security functionality**: authentication, authorization, cryptography, session management.
- *And more...*



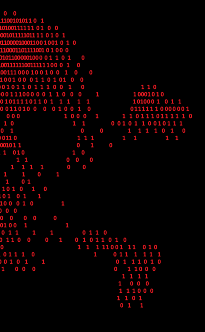
Exercise: Identify Your Attack Surfaces

The question this portion answers: “Where will you be attacked?”

- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}

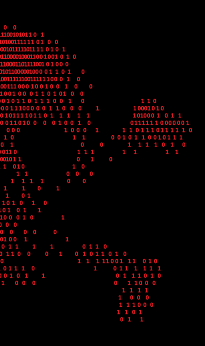


STEP 4: MISUSE & ABUSE CASES

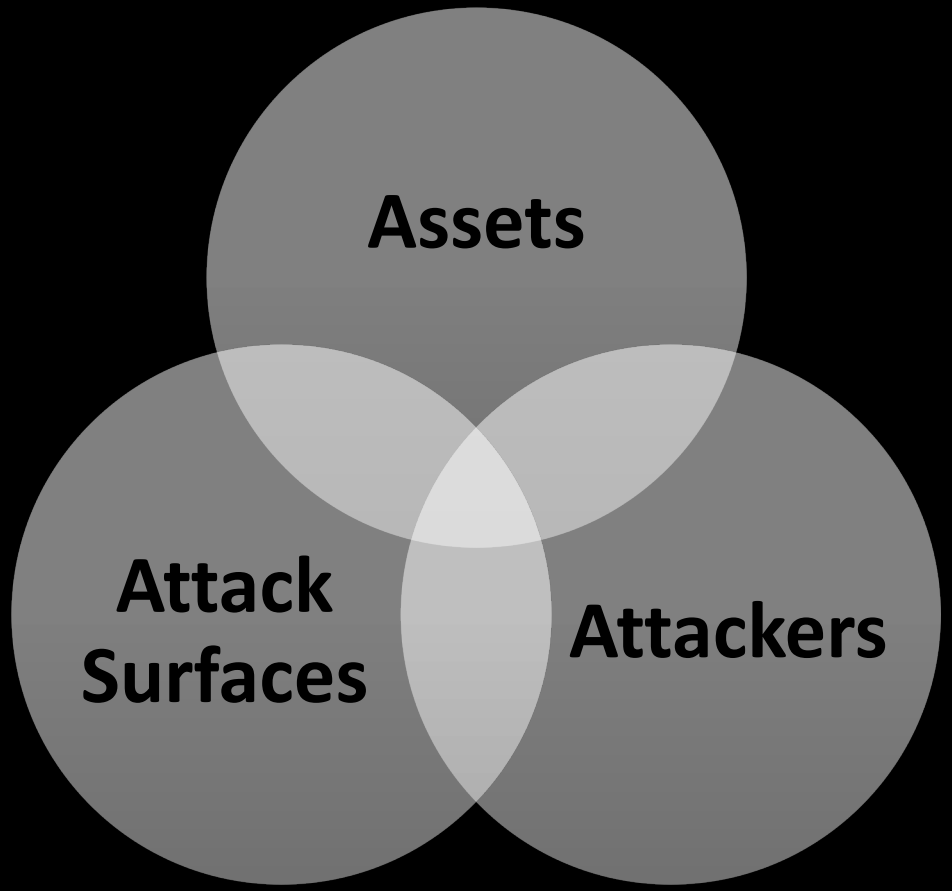


MISUSE & ABUSE CASES

- Now for the fun part: time to think like a hacker!
- Considering everything you've identified so far, now you want to consider how adversaries would attack your system, why they'd do it, what assets they'd compromise, and the outcomes that would deliver (both in terms of downside for you, and upside for them).
- Get creative, and be exhaustive! For purposes of this exercise, no scenario is too far-fetched. In fact, the more extreme, the better. That will stretch your thinking to reveal the unexpected issues you *do* want to take action on.



MISUSE & ABUSE CASES

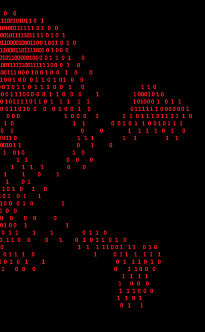


EXPLOIT

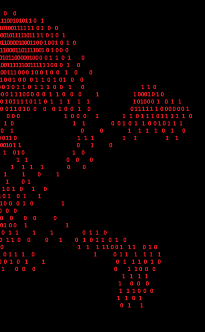
Exercise: Identify Your Abuse Cases

The question this portion answers: “What possible scenarios should you consider?”

- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}



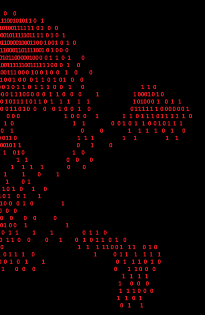
STEP 5: DEFENSE PLAN



https://hackablebook.com

DEFENSE PLAN

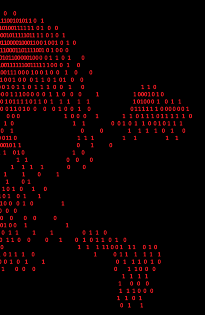
- Now that you've identified what to defend, whom to defend against, where you'll be attacked, and the possible exploit scenarios, you need to translate it all into action.
- Given the exploit scenarios identified, consider:
  - Where do you need to prioritize investments of time, effort, and money?
  - What have you not been focusing on yet that you now realize you need to?



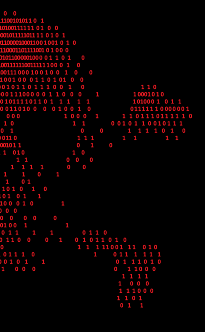
Exercise: Identify Action

The question this portion answers: “What should I do to defend?”

- {Write these down somewhere! If you need a template, there’s a simplified form at the end of this document}



PRINTER-FRIENDLY WORKSHEET



THREAT MODELING STEP 1: Identify Your Assets.

"What do you want to protect?"

Tangible Assets (e.g. data, money)

Intangible Assets (e.g. reputation, system availability)

THREAT MODELING STEP 2: Identify Your Attackers.

"Whom do you need to defend against?"

External Attackers

Insider Threat

THREAT MODELING STEP 3: Identify Your Attack Surfaces.

"Where will you be attacked?"

Input Fields

Interfaces

Integrations

Storage

Security Functionality

Other

THREAT MODELING STEP 4: Identify Your Misuse & Abuse Cases.

"What possible exploit scenarios should you consider?"

Obvious

Far-fetched

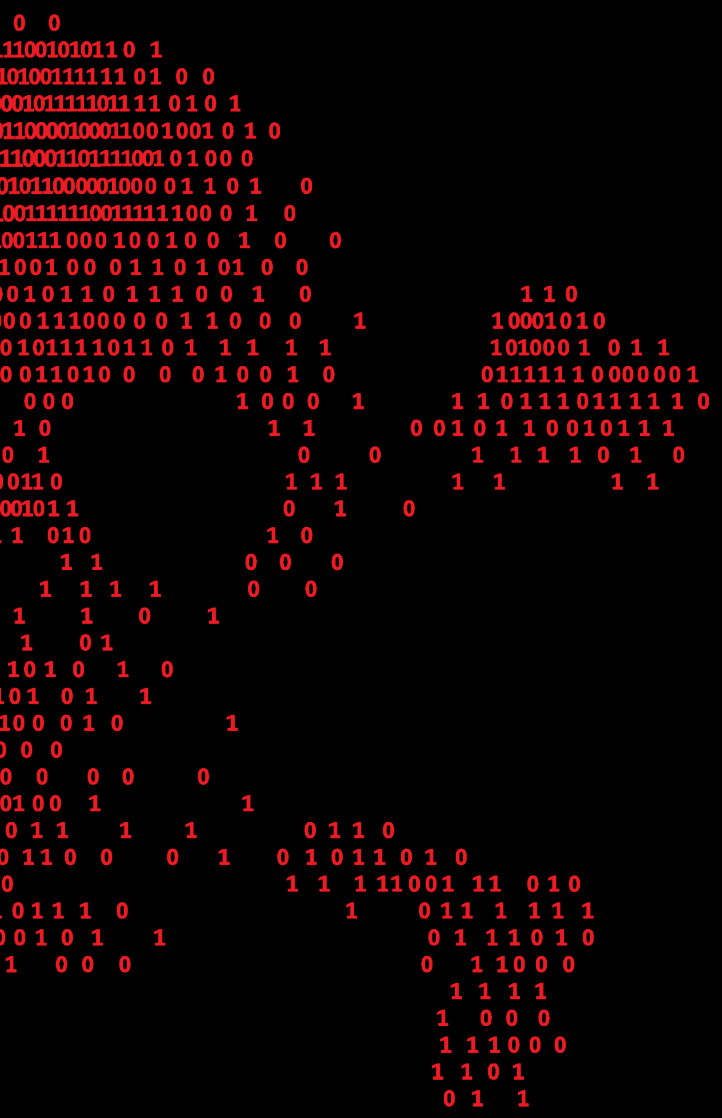
Impossible.... Right?

THREAT MODELING STEP 5: Identify Your Defense Plan.

"What should I do to defend?"

Places to invest time, effort, and money

Places you haven't been focusing on, but need to



HAVE FUN!

PS – Do you need security consulting, security testing, penetration testing, or a keynote speaker?

If so, contact me at ted@tedharrington.com