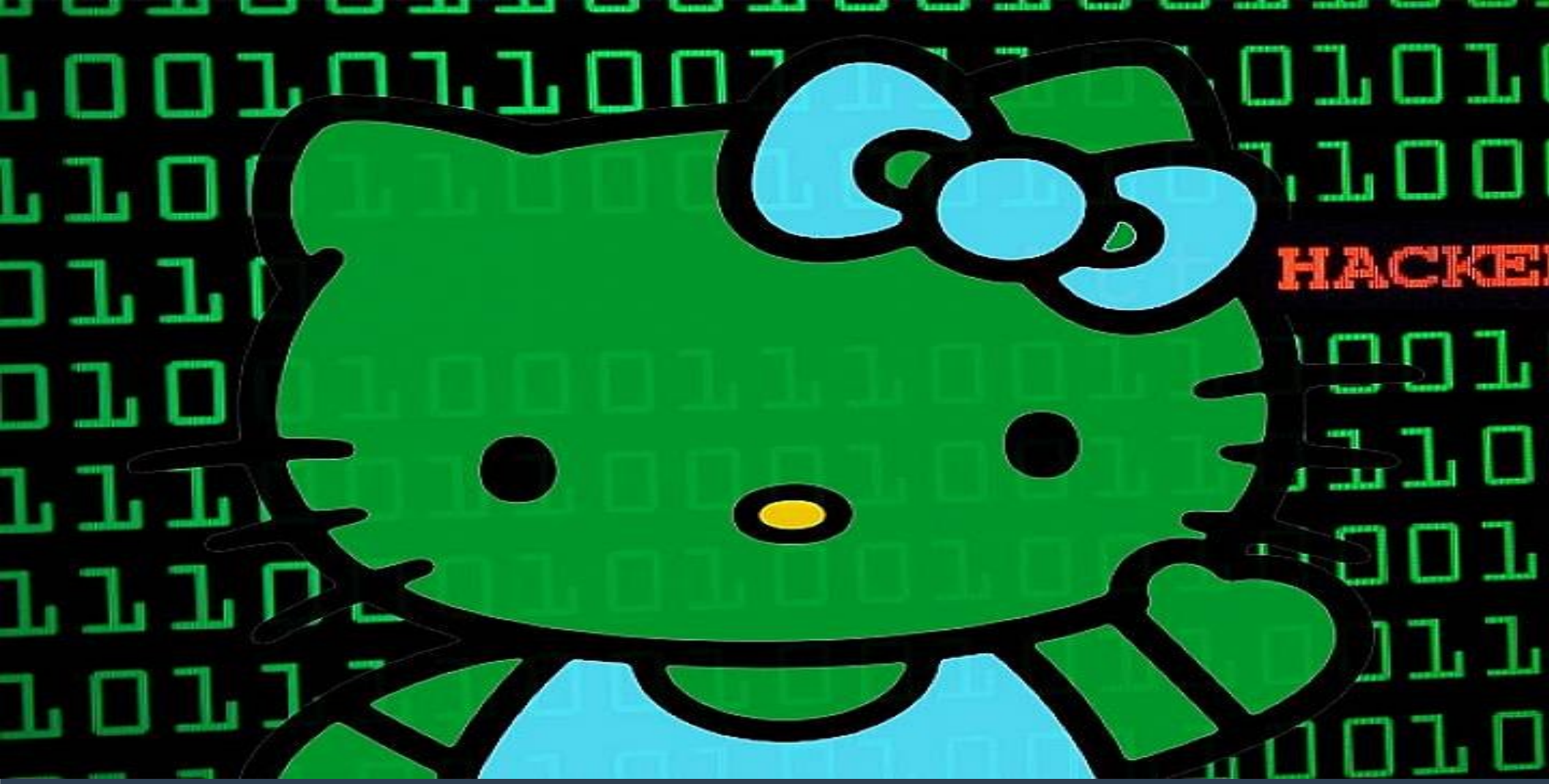


Safe and Sound: Threat Modeling & Holistic Security

CyPurr Collective

Who are we? Who are you?

- We are the…
  - The Cypurr Collective: A group of folks that organize cybersecurity workshops and socials, looking to spread knowledge and talk about privacy rights!
- ...and you are?
  - Name
  - Pronouns (i.e. he/him, she/her, they/them, ze/zer, etc)
  - In a few words, what brings you here today?

A few rules for this workshop …

- Share the space!
  - Step Up Step Back: Ask a question, give a comment, leave room for others to speak
- Stack!
  - Raise your hand and we will put you on the speaking queue
- Saf(er) Space
  - We DO NOT tolerate language or behavior purposefully meant to demean or harm folks based on their identities
  - No one should be forced to discuss their own

Overview

- Threat Modeling?
- *Holistic Security* – Tactical Tech Collective

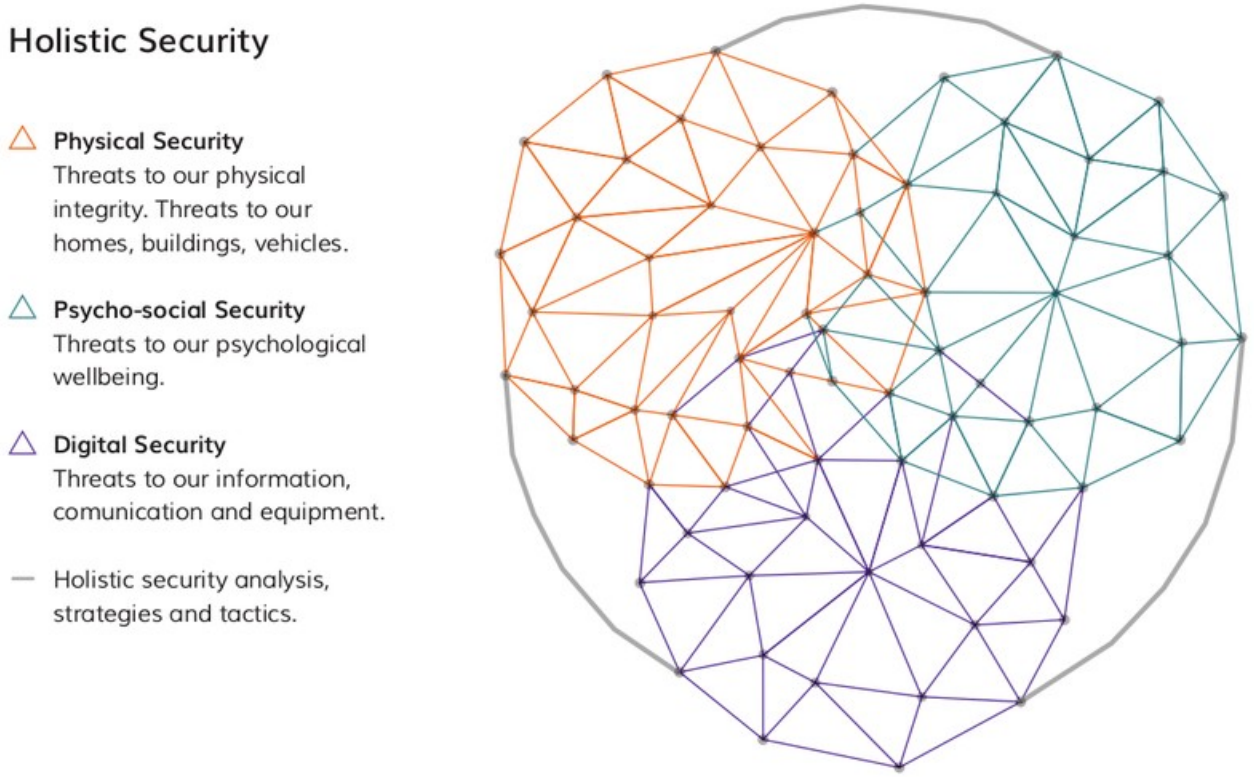


Image from *Holistic Security* by Tactical Tech Collective

Part I: Threat Is Valid

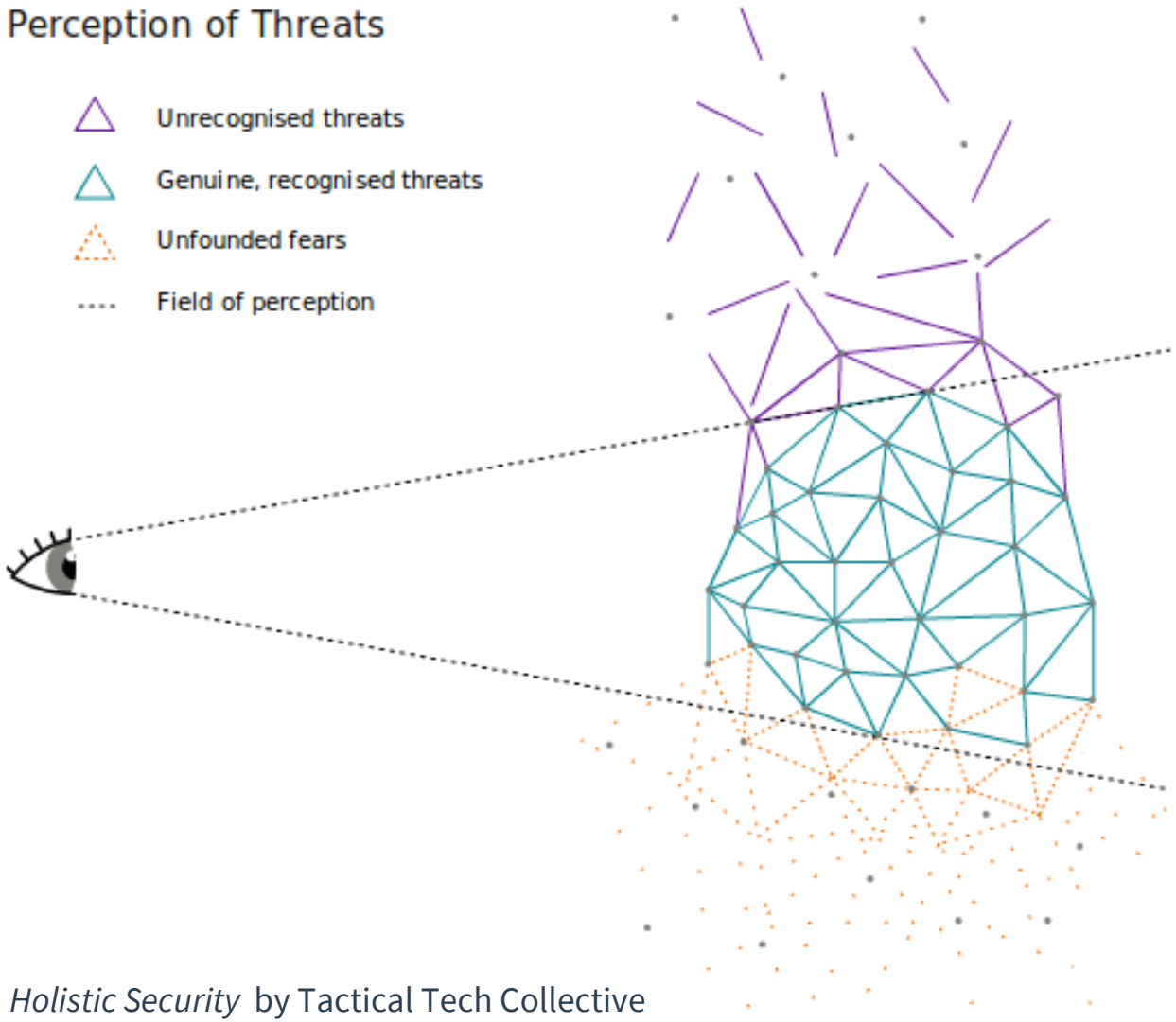


Image from *Holistic Security* by Tactical Tech Collective

Part I: Threat Is Valid

Individual Response

- Freeze
- Fight
- Flight
- Comply
- Tend
- Befriend
- Posture

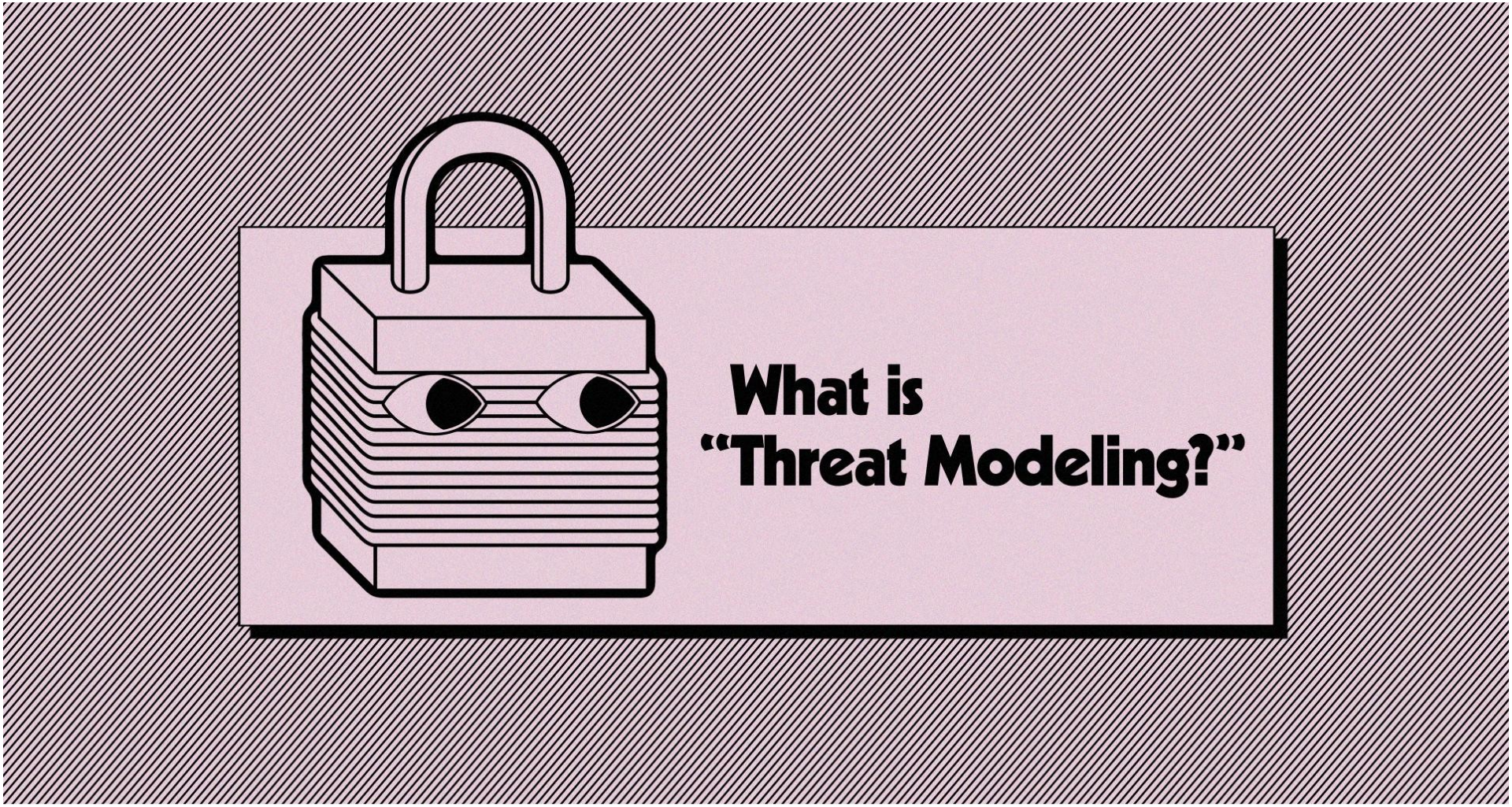
Group Response

- Harder Group Boundaries
- Authoritarianism
- Fixed Patterns

	Indicators (How do you recognise that you are at this stress level? What makes this phase qualitatively different from the previous level?)	**What can you do to reduce the level of stress, or increase your ability to cope?**	**Resources needed**
Green			
Yellow			
Red			

Image from *Holistic Security* by Tactical Tech Collective

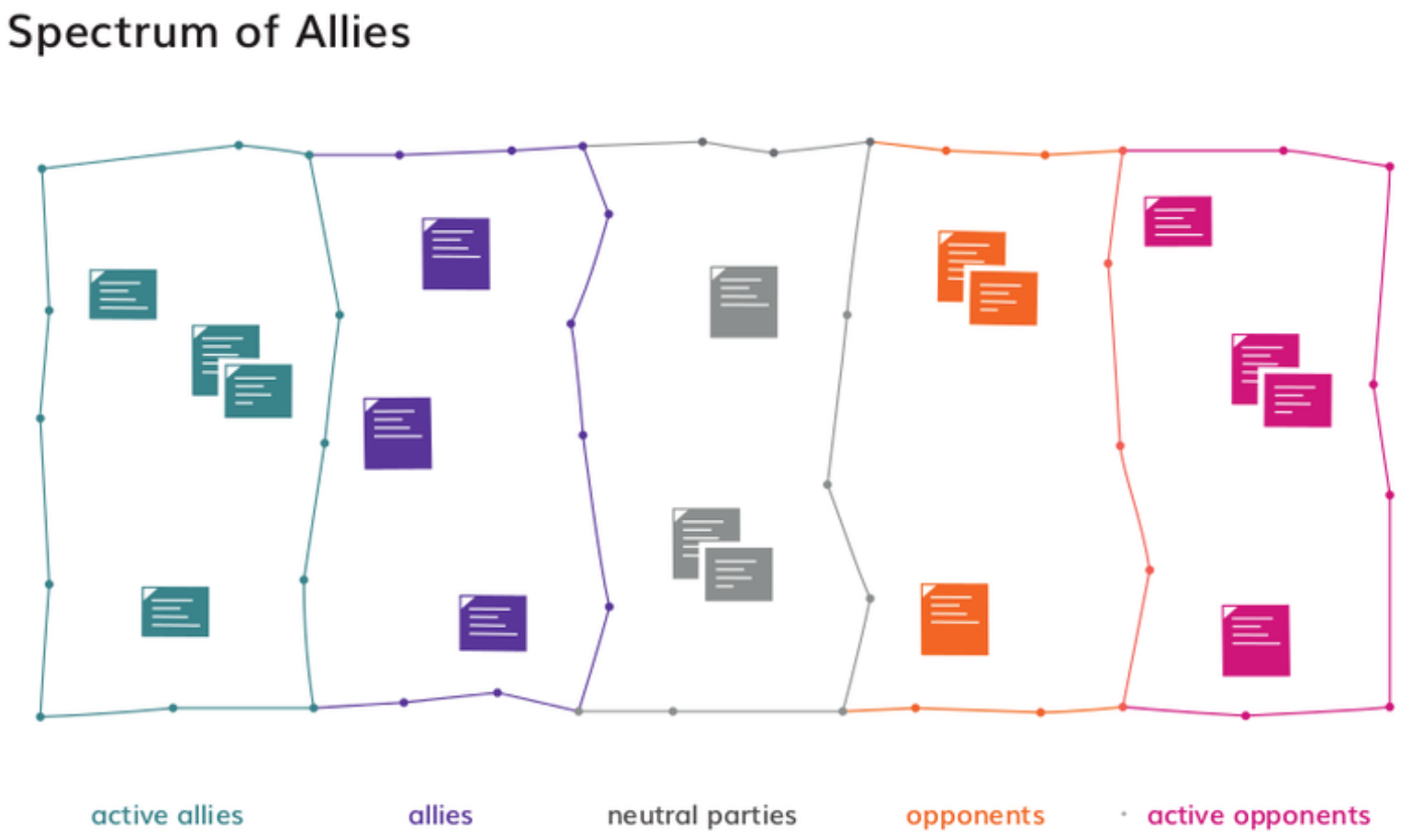
Part II: Threat Analysis



Step 1: Situational Analysis & Vision

- PESTLE
  - Political
  - Economic
  - Scientific
  - Technological
  - Legal
  - Environmental
- Vision
  - What do I want to change?
  - How do I want to change it?

Step 2: Actor & Information Mapping



Information at rest				
What (examples)	Attributes			
	Where does it reside?	Who can/does access it?	How sensitive is it?	How should it be protected?
Financial documents in electronic form	Secure shared folder–file server	Executive team	Secret	Saved in hidden encrypted partition. Backed up daily to encrypted hard-drive
Program reports for the censorship campaign	Documents folder–file server	Team members, program director	Confidential	Saved in encrypted partition
Adobe InDesign for the web developer	Web content manager's laptop	Web content manager	Confidential	Licensed, password-protected

Image from *Holistic Security* by Tactical Tech Collective

Data in Motion

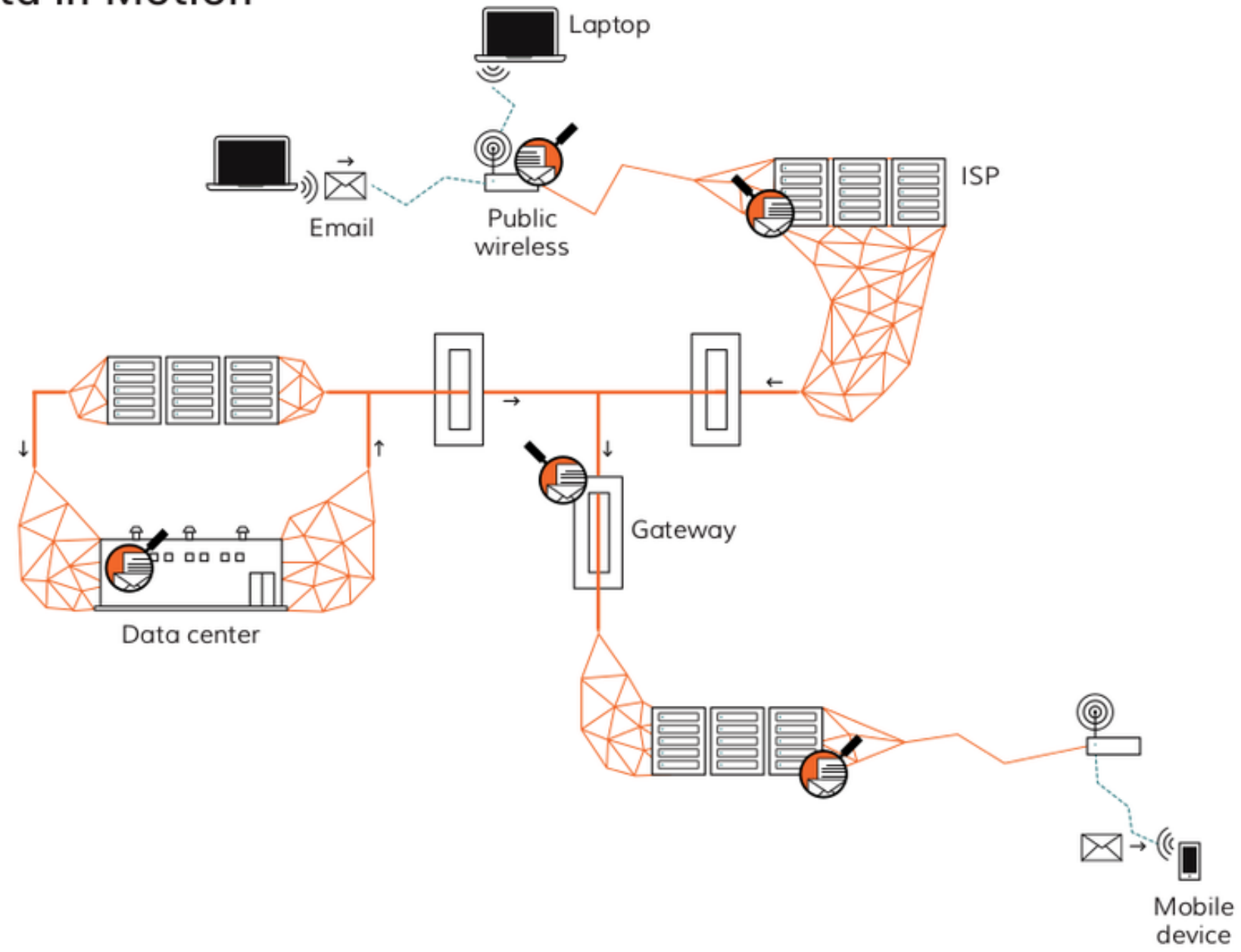


Image from *Holistic Security* by Tactical Tech Collective

Information in motion					
What (examples)	**Attributes**				
	What method of transfer are you using?	**Who has (or wants) access to it?**	**What physical or virtual routes does it take (origin, path, destination)?**	**How sensitive is it?**	**How should it be protected?**
General emails among team members	Email (Gmail)	Team members, email provider	**Origin:** staff computers **Path:** internet (via Google servers **Destination:** staff computers	Confidential	GPG encryption
Check-ins during missions	Text messages (SMS)	Team members, telecom company	**Origin:** mobile phone **Path:** mobile network **Destination:** mobile phone	Secret	Code words

Image from *Holistic Security* by Tactical Tech Collective

Step 3: Security Indicators

- Security indicator vs. Threat
  - Indicator is the instance
  - Threat is the feeling that an instance will bring harm, or that a series of instances will bring harm
- Something out-of-the-ordinary?
  - Negative: I’m being followed by a van
  - Positive: a strong ally just gave us some funds!!!!!!!!
- Making space to share
- Keeping track

Step 3: Security Indicators

1. **What happened?**
2. **When did it happen?**
3. **Where did it happen?**
4. **Who was affected?**
5. **Was gender-based violence involved?** This is especially important in the case of concrete incidents involving third parties. Consider physical and psychological factors.
6. **In the case of aggressions – who was responsible?**
7. **Why do we feel this happened?** Try to avoid being accusatory here but rather establish the facts of the incident.
8. **What was its origin?** Was this related to common delinquency, environmental factors or our work and activism?

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	**Target**	**Adversary**	**How**	**Where**
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Image from *Holistic Security* by Tactical Tech Collective

Step 4: Threat Analysis

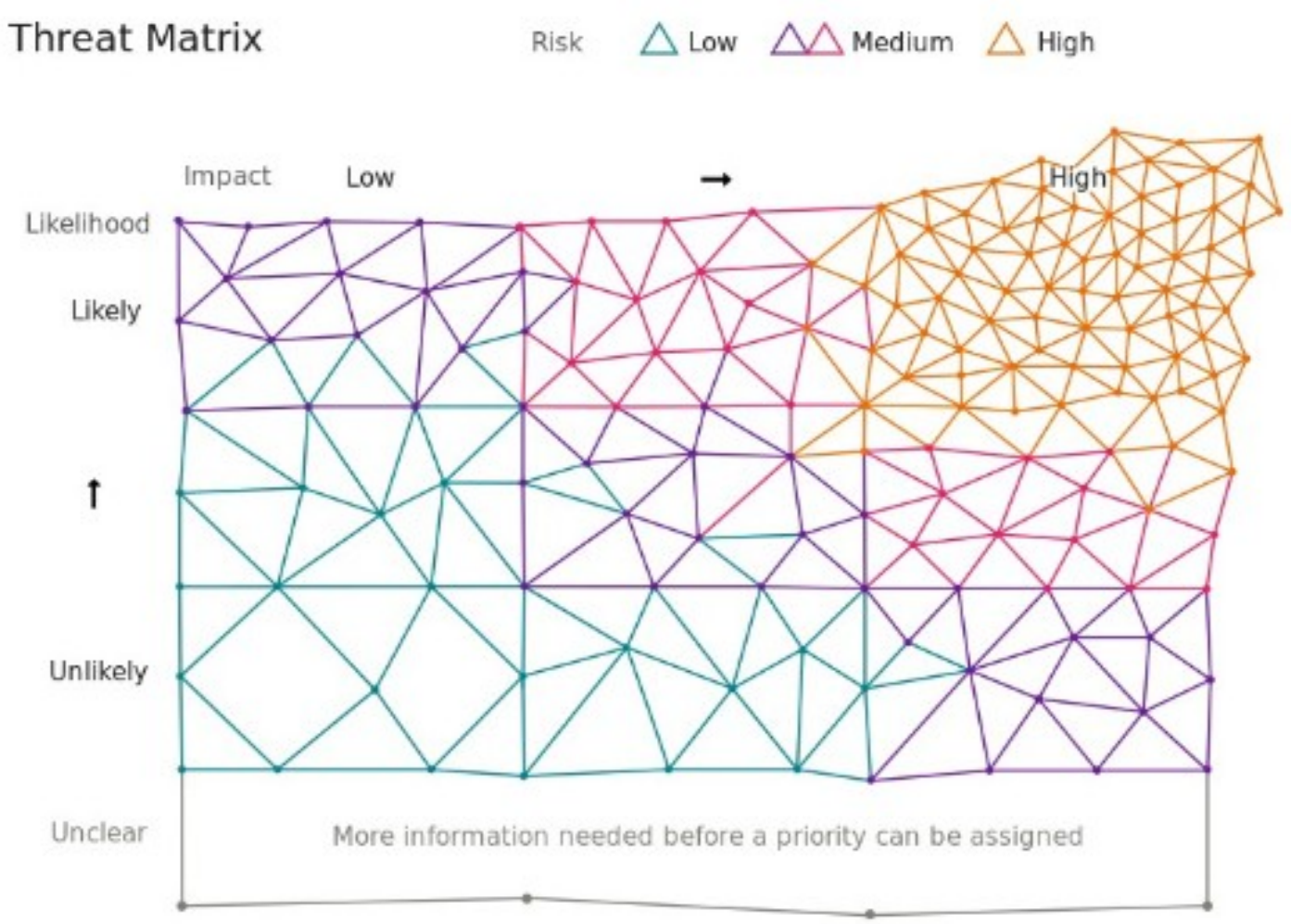


Image from *Holistic Security* by Tactical Tech Collective

Step 5: Security Planning

- What to include in security plan
  - Objective of activity
  - Threat identified
  - Preventative actions/resources
  - Response to emergency situation (how you define emergency)
  - Communication and devices
  - Self-care and well-being

Step 5: Security Planning

- What's working already? (Existing Capacities)
- What needs work? Gaps? (Vulnerabilities)
- Strategies
  - Acceptance-raising support
  - Deterrence-raising cost of attack
  - Protection-building strength to make attack harder

Summary

- Main Themes
  - Prioritize Security in planning convos
  - Create Safe Space for folks to discuss security
  - Talk often!

- Security isn’t antithetical to…
  - Action
  - Risk
  - Progress
  - Success

Further Resources

- Holistic Security – Tactical Tech Collective
- An Introduction to Threat Modeling – SSD by EFF
- CyberSecurity Training
  - Online
    - http://cutealism.com/fight/
    - Privacytools.io
  - In-Person
    - CyPurr Collective (on Facebook)
    - CryptoParty.in

Further Resources

- Self-Defense/Fitness
  - Pop Gym (@popgymbk Twitter, Facebook, Instagram)
  - Trans Boxing (on Facebook)
  - Spectrum Wrestling (on Facebook)
  - Masterskya
  - Traditional Okinawan Karate School
  - Rev Fitness
  - Physical Culture Collective