



# WHAT BASE JUMPING TAUGHT ME ABOUT RISK

BRUCON 2015

# ABOUT ME

Former hacker - Head of Security - Skydiver - BASE Jumper



**Shyama Rose**

## BIO

Shyama Rose is an accomplished Information Security visionary strategist with a 15-year track record for assessing risks and building ground-up security initiatives for Fortune 100 companies.

She is known within the industry as a business security leader with a unique blend of technical and business acumen. As a leader she implements and matures Information Security and Compliance programs. Using her penetration testing roots she designs holistic security solutions, builds world class teams and mitigation controls for enterprise infrastructures and applications.

Shyama is a regular keynote and industry speaker and the author of several Center for Internet Security benchmarks. She has lectured in New York University's "Application Security" course.



@pencilsareneat



[shyama@gmail.com](mailto:shyama@gmail.com)

# Embracing Risk

01

What is BASE jumping and why is it risky?

02

Risk in security.

03

What should we do with this risk stuff?





BASE

**BUILDING**



6%

**ANTENNA**



12%

**SPAN**



10%

**EARTH**



71.5%



# THE MOST DANGEROUS SPORT

Recorded Deaths

270

Fatality Rate

1 in 2,000 jumps, 1 in 60 jumpers

Risk

100x more dangerous than skydiving

Friends Dead in 2015

5

JOSH SHEPPARD

1984 - 2015

# WHY I BASE JUMP

Worth the risk, or not?

1

## Understand Fear

- ✓ Real vs. Fake Fear
- ✓ Master to adrenaline management

2

## Community

- ✓ Have good times with friends
- ✓ Super secret sneaky activity

3

## Understand Risk

- ✓ Learn systematic risk reduction
- ✓ Pair risk vs. threats
- ✓ Get a reality check

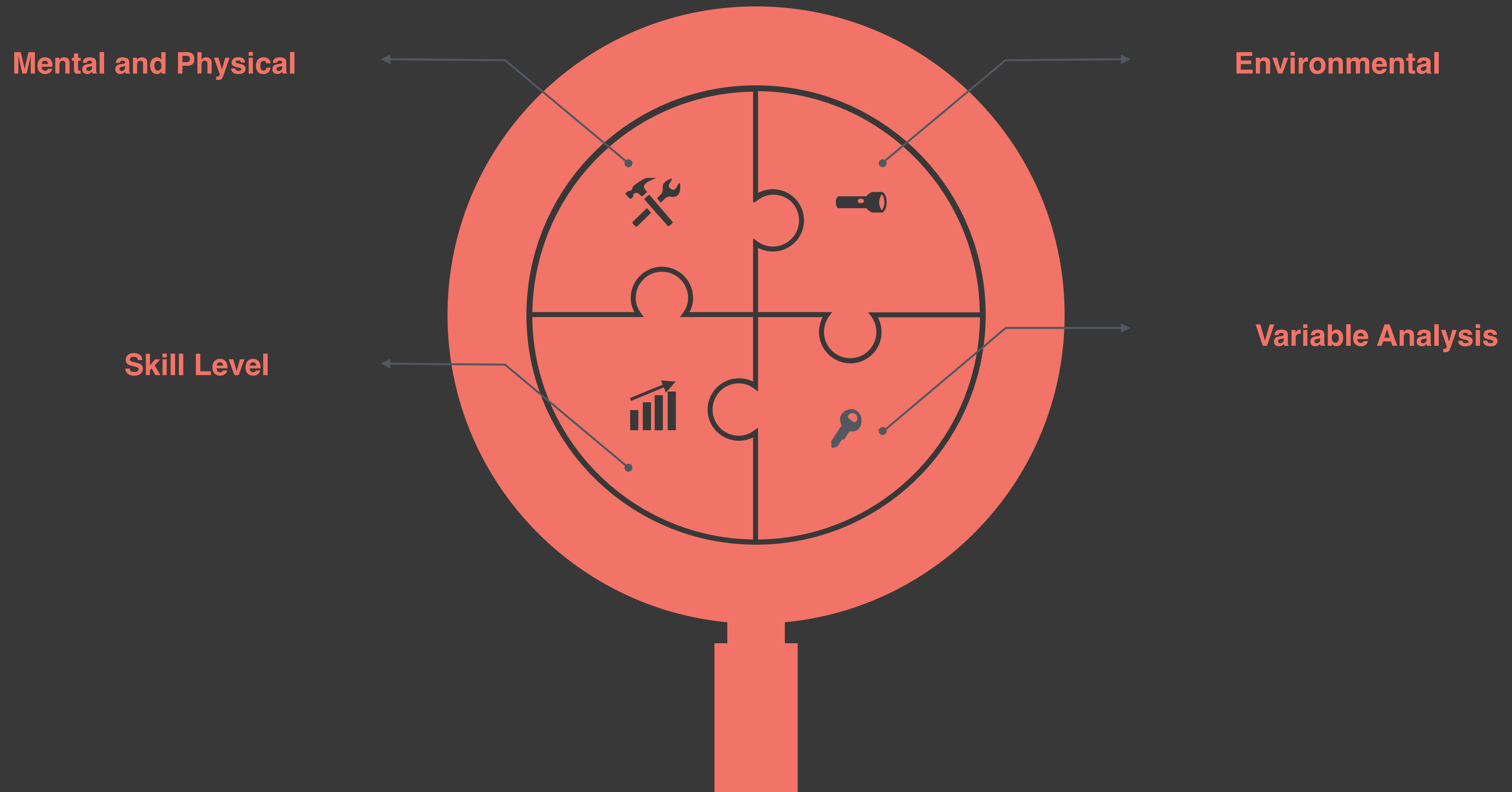
4


## Feel Good

- ✓ That dopamine rush, tho
- ✓ Be active

# HOW BASE JUMPERS ASSESS RISK

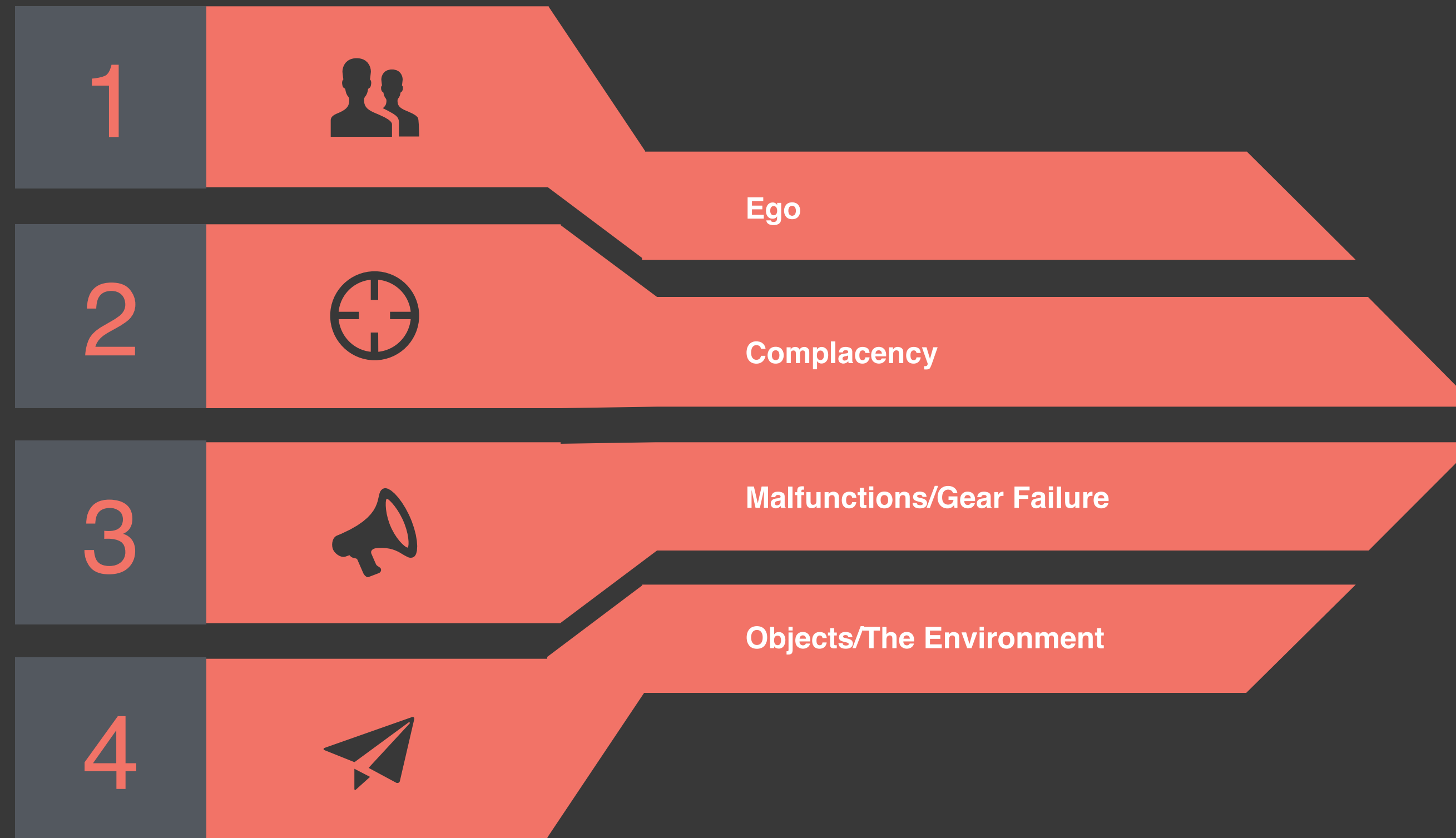
Safety Third!



A person in a blue wingsuit is captured mid-jump, silhouetted against a vast, mountainous landscape. The jumper is positioned on the edge of a rocky cliff, with their wings spread wide. Below them, a deep valley unfolds, filled with green fields and winding paths. In the distance, more mountains rise, partially shrouded in soft, white clouds. The sky is filled with large, billowing clouds, creating a dramatic and awe-inspiring scene. The overall atmosphere is one of adventure and the thrill of the unknown.

BASE jumping is one of the only activities that as you get safer, the odds of death increase.  
The best of the best die.

# What Actually Kills BASE jumpers?



# Why talk about BASE at a security con?

## Similar Sports

- Fun
- Sexy
- Cool
- Mental
- Community building
- Slightly out of touch
- Sensational
- Niche
- Expert

## Risky

- Nefarious
- Edgy
- Forbidden
- Boundary pushing
- Dopamine inducing

## Stark Realities

- Safety
- Security
- Reputation impacting
- Life/Death
- Risky if done wrong

A woman with blonde hair, wearing a black wetsuit, goggles, and a swim cap, is climbing a metal railing on a rooftop terrace. She is smiling and looking down at the railing. The railing is made of dark metal with a brick-like pattern. In the background, there is a brick building with large windows and a sign that reads "TWIN FALLS AREA CHAMBER OF COMMERCE SOUTHERN IDAHO TOURISM". The building has a modern design with a mix of brick and dark panels. The sky is clear and blue.

# Risk in Security

# The Business of Risk



Takes What's In Use

Prioritizes What To Do

Holds People Accountable

Computes Cyber Posture Score

Company Determines/Prioritizes Protective Suite (CSF Profile):

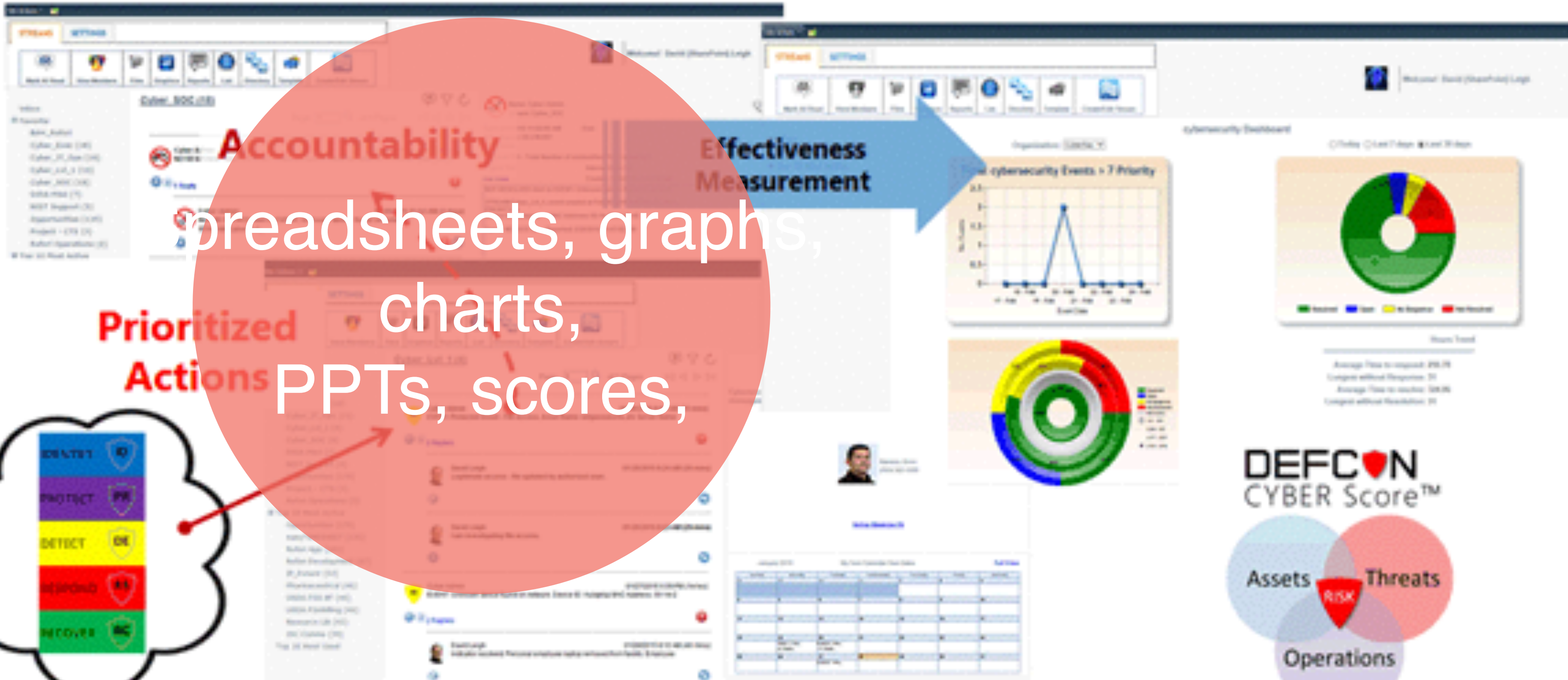
- Intrusion Detection
- Anti Malware
- Vulnerability Management
- Log Management
- Anomalous activity detection

Example Cybersecurity Protection Products

Your Protection Suite

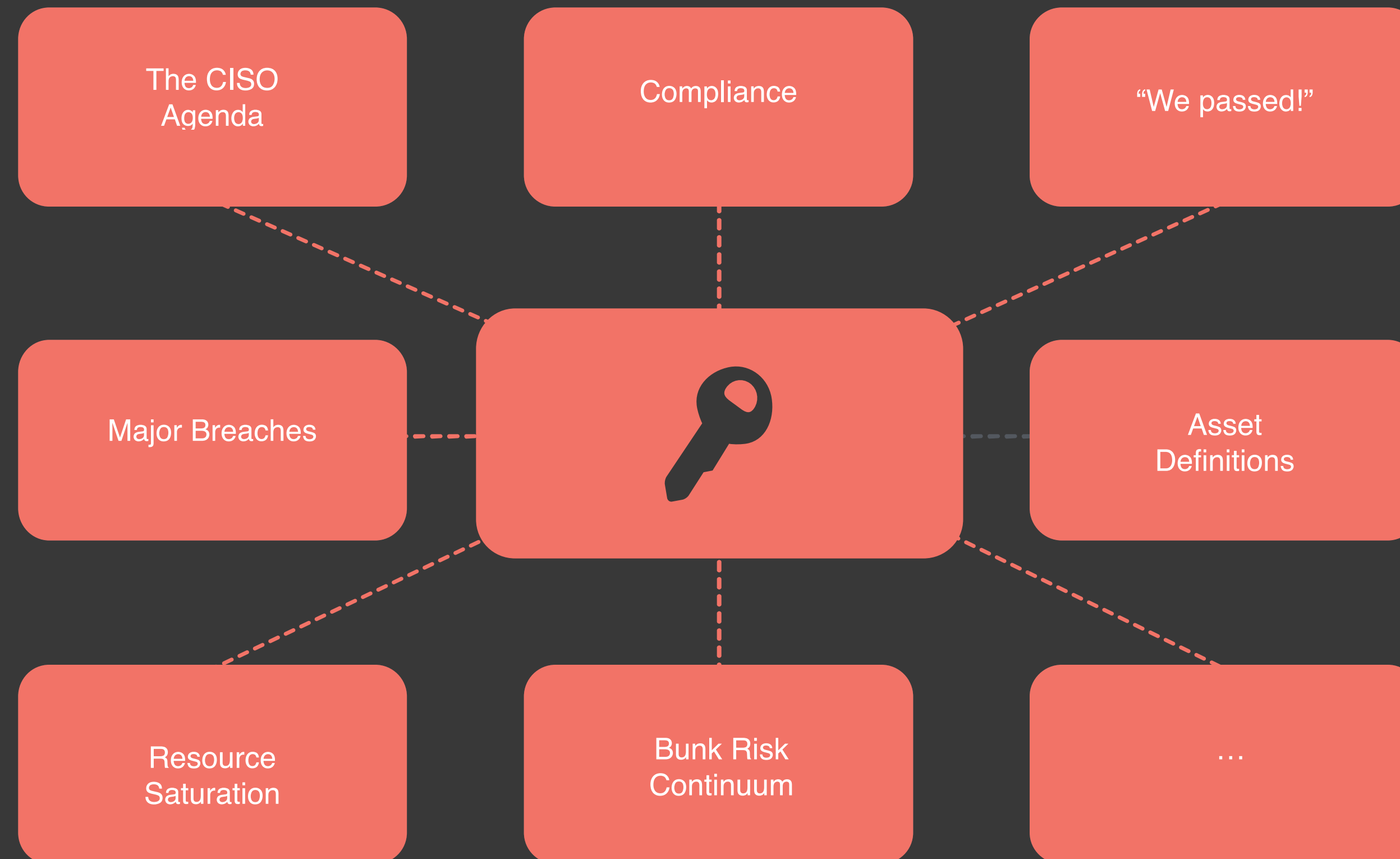


NIST Framework  
Makes Indicators  
Actionable



# Misaligned Risk

Stories from the Trenches





- > Solving the world's problems one spreadsheet at a time.
- > Hey, it's either suits like me or the government.

- Mr. Robot

#	Section	T
1	Risk Management	5
2	Security Policy	9
3	Organization Security	9
4	Asset Management	9
5	Physical and Environmental	1
6	Communications and Connectivity	3
7	Change Control	1
8	Operations	6
9	Logical Access Control	1
10	Data Integrity	4
11	Encryption	7
12	Website	1
13	System Development	1
14	Incident Response	7
15	Business Continuity and Disaster Recovery	1
16	Endpoint Protection and Patching	1
17	Backup and Offsite Storage	9
18	Media and Vital Records	7
19	Third Party Relationship	9
20	Standard Builds	1

> Solving the world's problems one spreadsheet at a time.

> Hey, it's either suits like me or the government.

- Mr. Robot

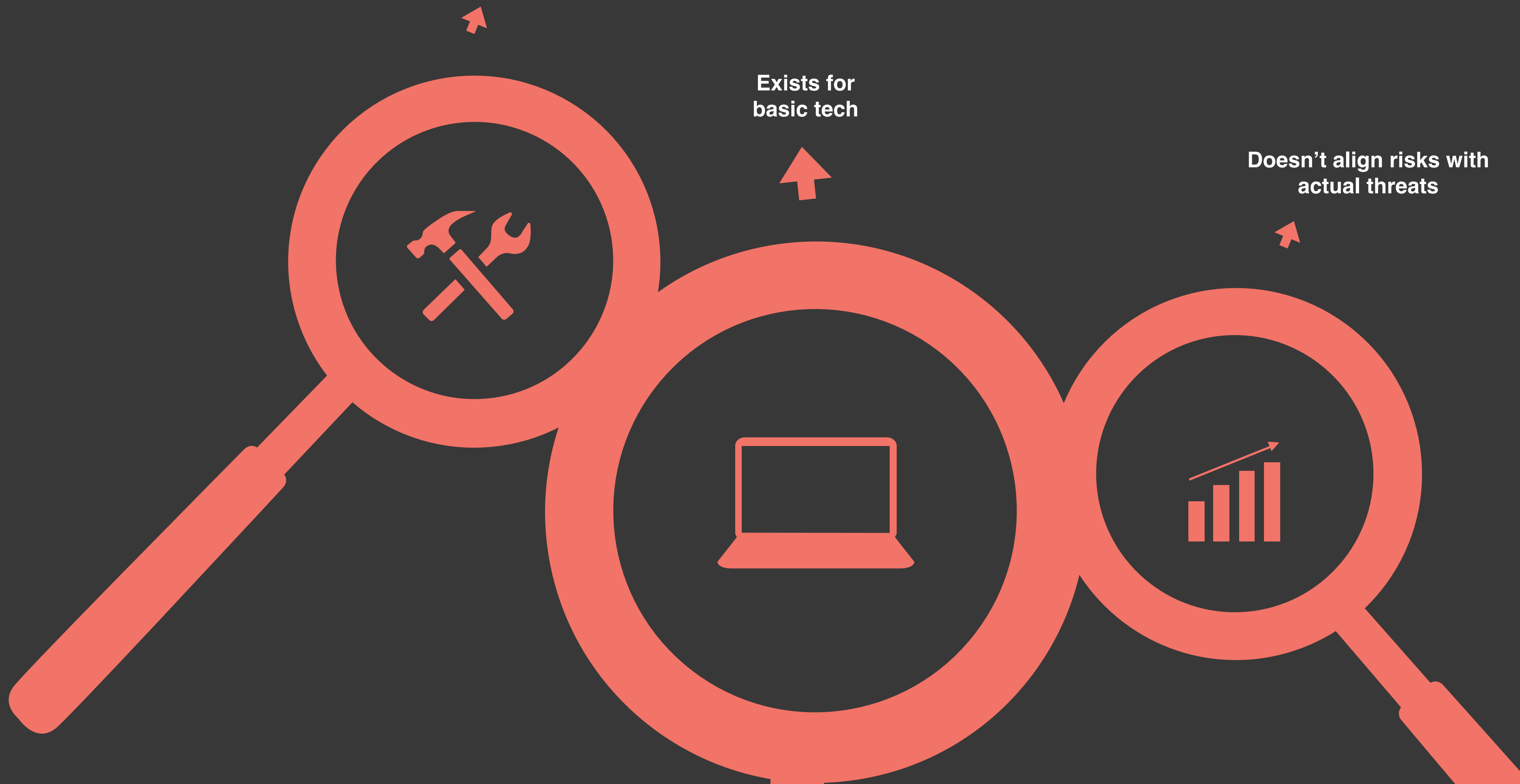
# THE RISK CONTINUUM

It is Lacking

Fluctuating asset and  
definitions

Exists for  
basic tech

Doesn't align risks with  
actual threats

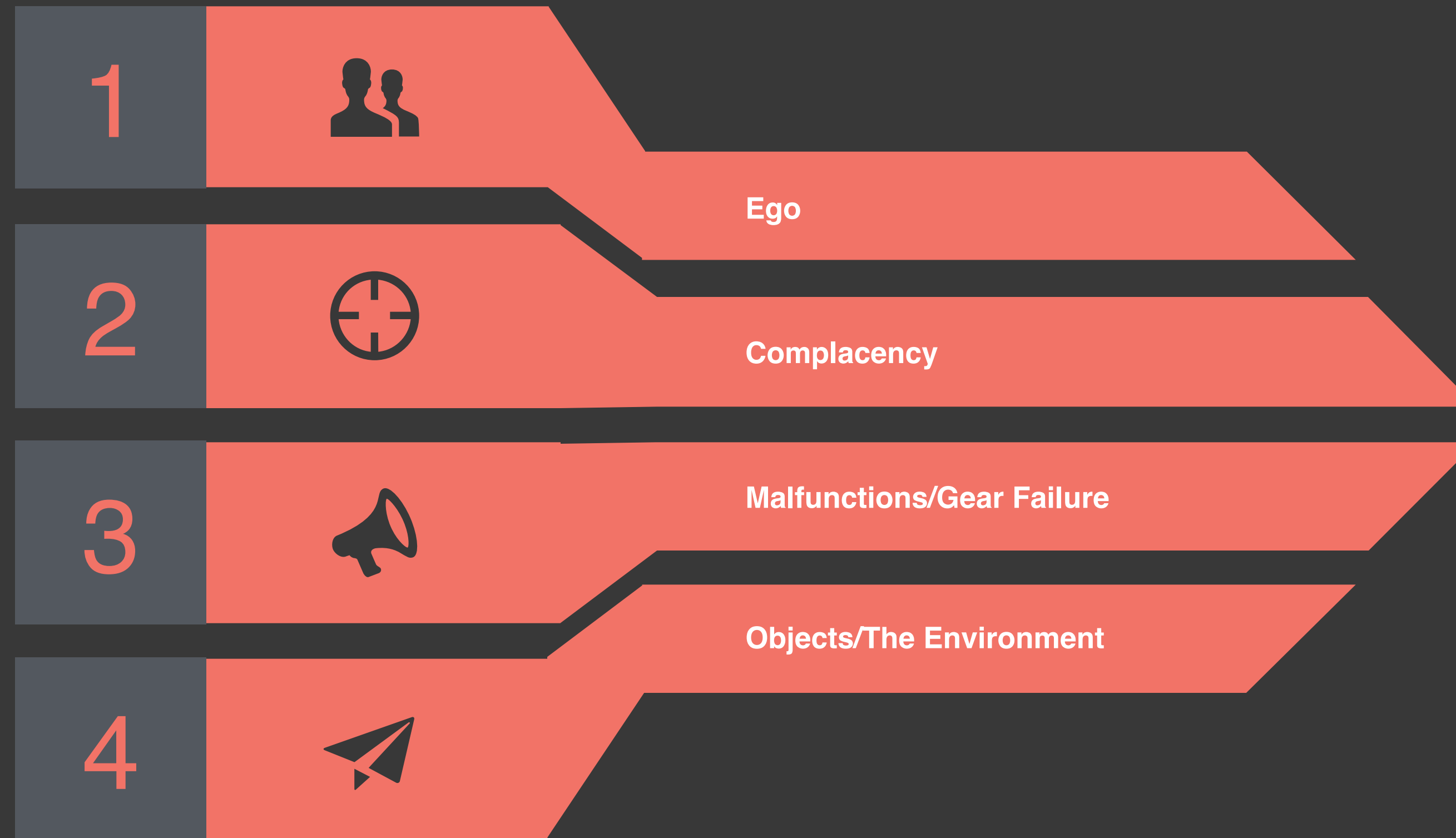




What should  
we do  
differently?

# What Actually Gets Us Breached?

Remember this visual? It's the same for security.



# BROADEN THE RISK CONTINUUM



# SYSTEMATIC RISK REDUCTION



Engineering



Execution



Trust



Innovation

# BRING ON THE RISK

Today's msg: don't jailbreak because of some risk. We should say: Cool, a risk! Let's work to reduce risk and be free to jailbreak!

- Adam Ely

# RESPONSE

Improving CERT



- ✓ Reaction Time
- ✓ Resource coordination and communication
- ✓ Technology Insight



Q&A