Humans Are Awesome
(at Risk Management)

Andy Ellis

How To CISO

Andy Ellis

Andy Ellis

www.csoandy.com

@csoandy

Quick CV

- **Principal** *Duha*
- **Author** *1% Leadership*
- **2021 inductee** *CSO Hall of Fame*
- **Podcast Co-host** *CISO Series*
- **Author** *How To CISO*
- **Partner** *YL Ventures*
- **Advisory CISO** *Orca Security*
- **CSO** *Akamai*
- **Officer** *US Air Force*
- **6-3, minor in 18** *MIT*

How To CISO

Humans Are Awesome
(at Risk Management)

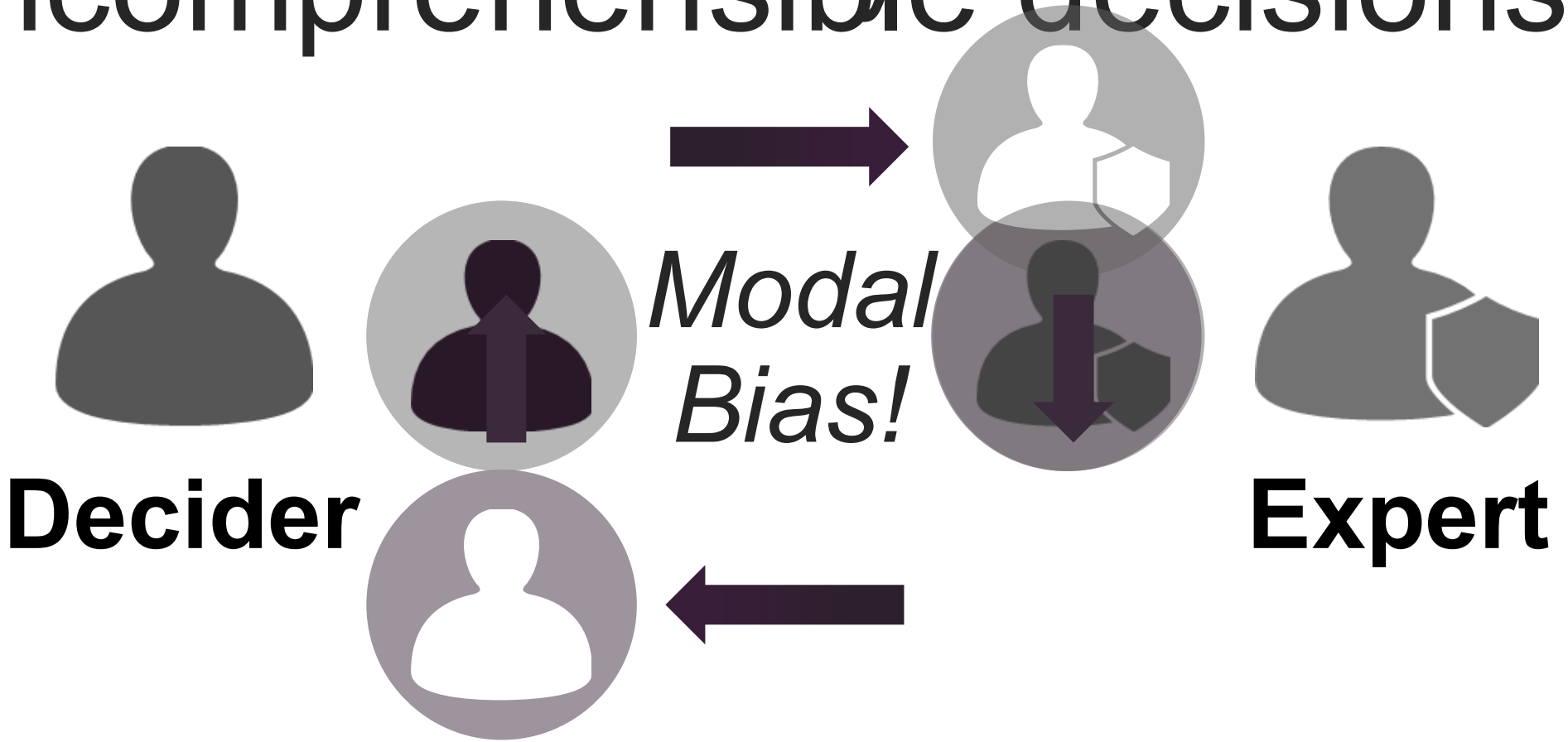
Andy Ellis

How To CISO

Why do people make ~~"bad" or "stupid"~~ *"impossible"* decisions?

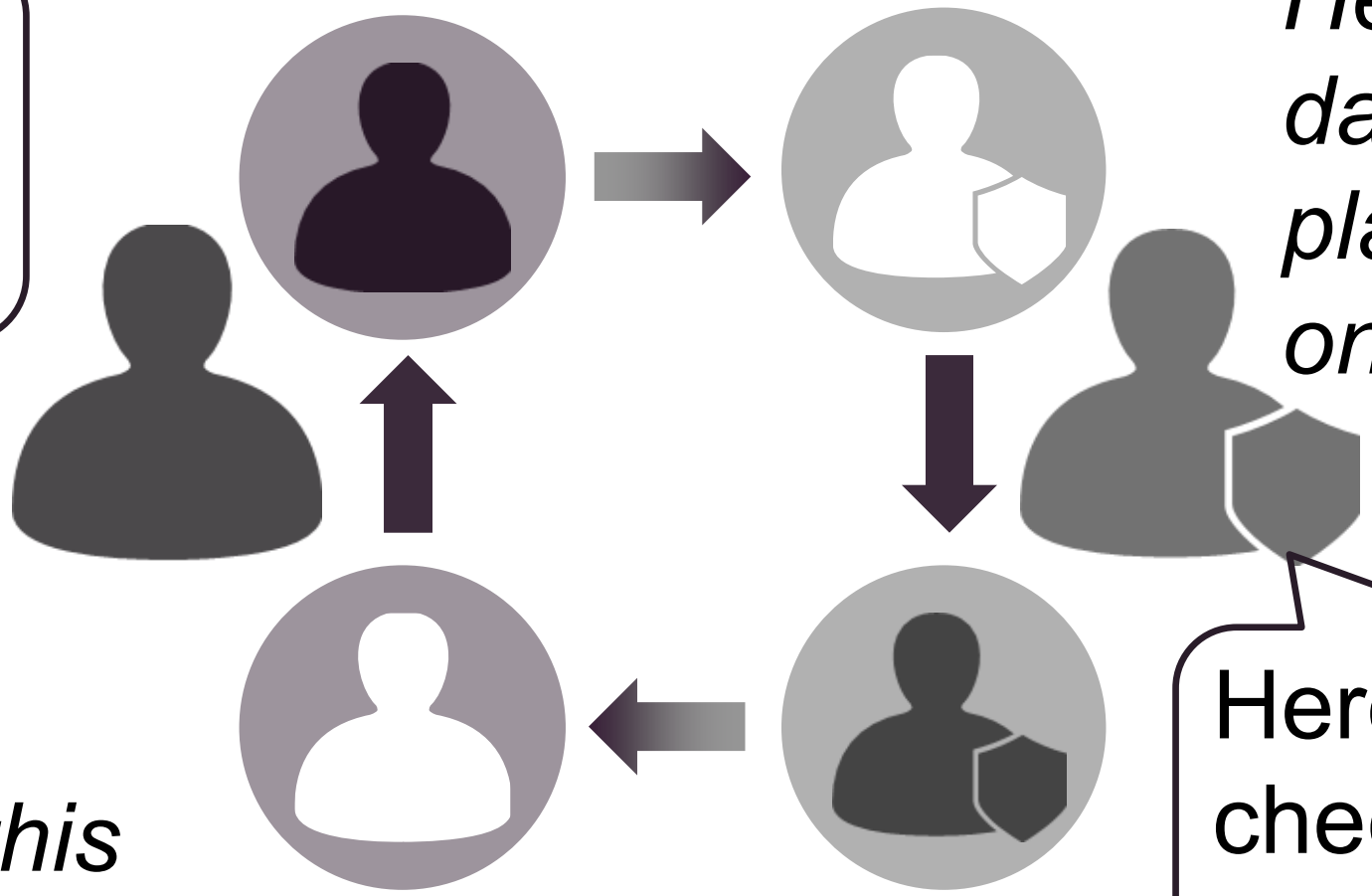
Anyone can be a villain in someone's story

Why do people make incomprehensible decisions?



A business conversation?

Here is my project. Is it safe?



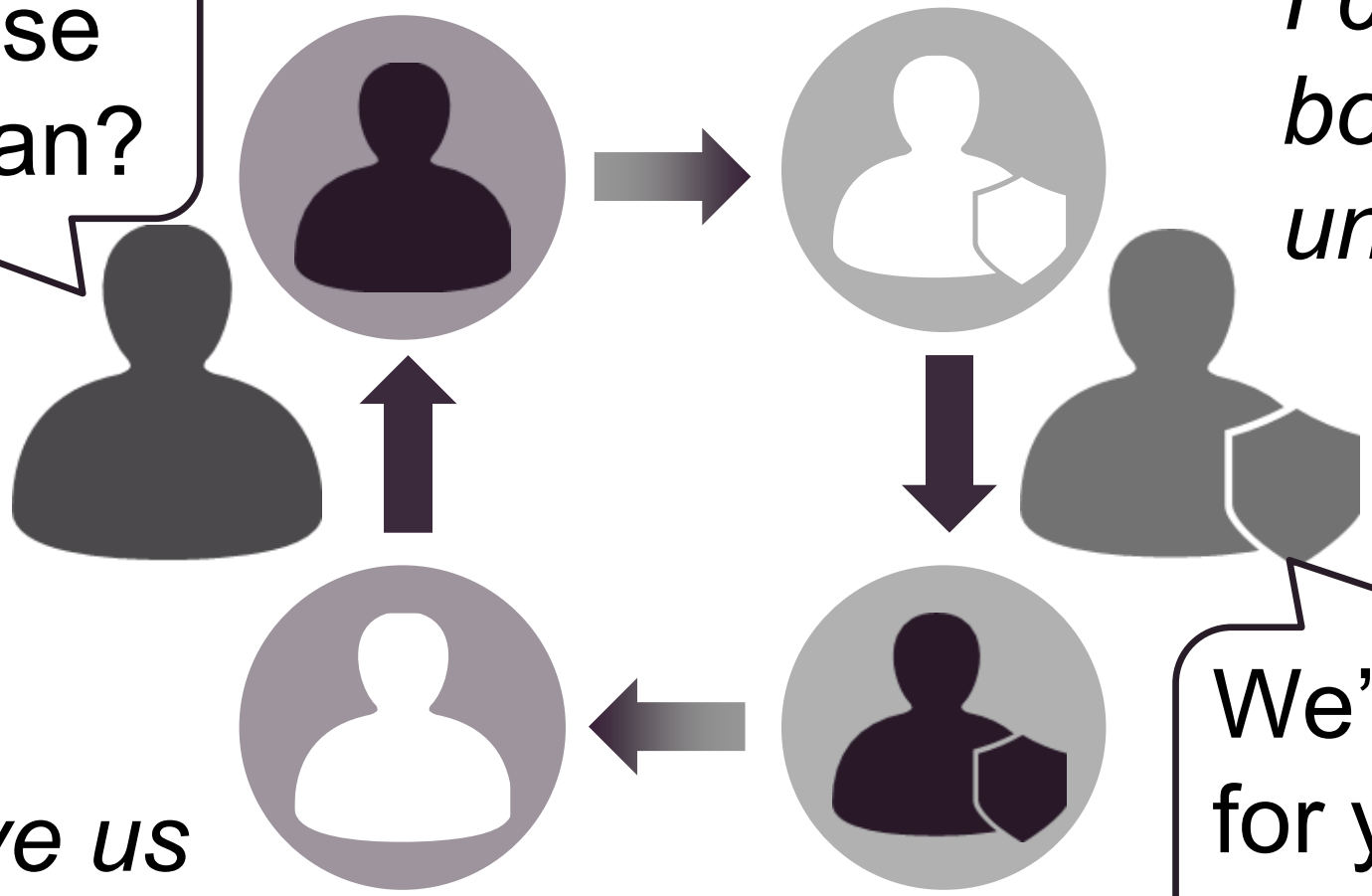
Here is my dangerous plan! Sign off on it!

Here's a checklist! Fill it out!

Justify our budget with this makework!

A business conversation?

What do these phrases mean?



I can't be bothered to understand this.

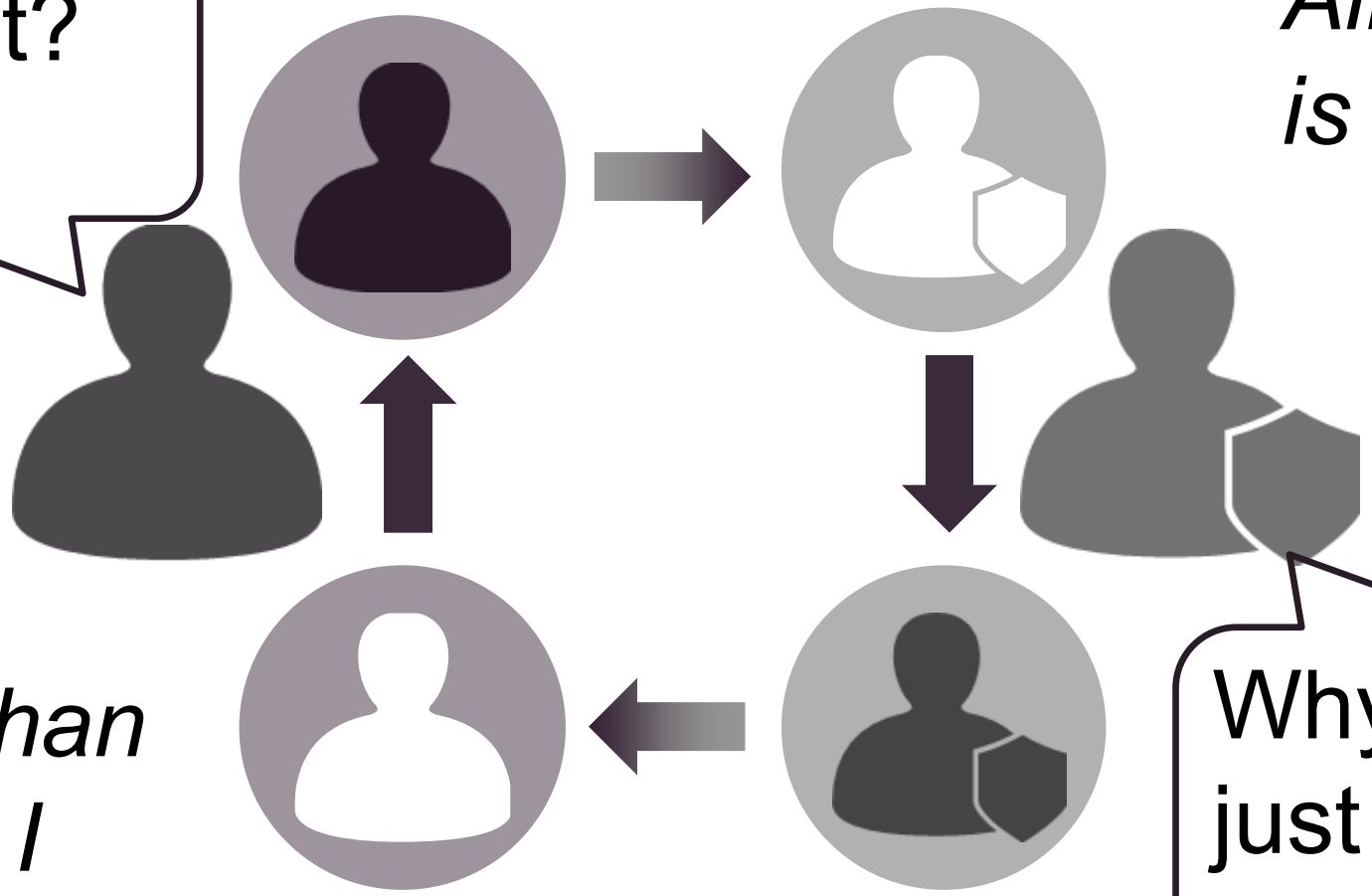
We'll fill it out for you.

We'll do the work, just give us more budget!

A business conversation?

Is it done yet?

All I care about is my schedule.



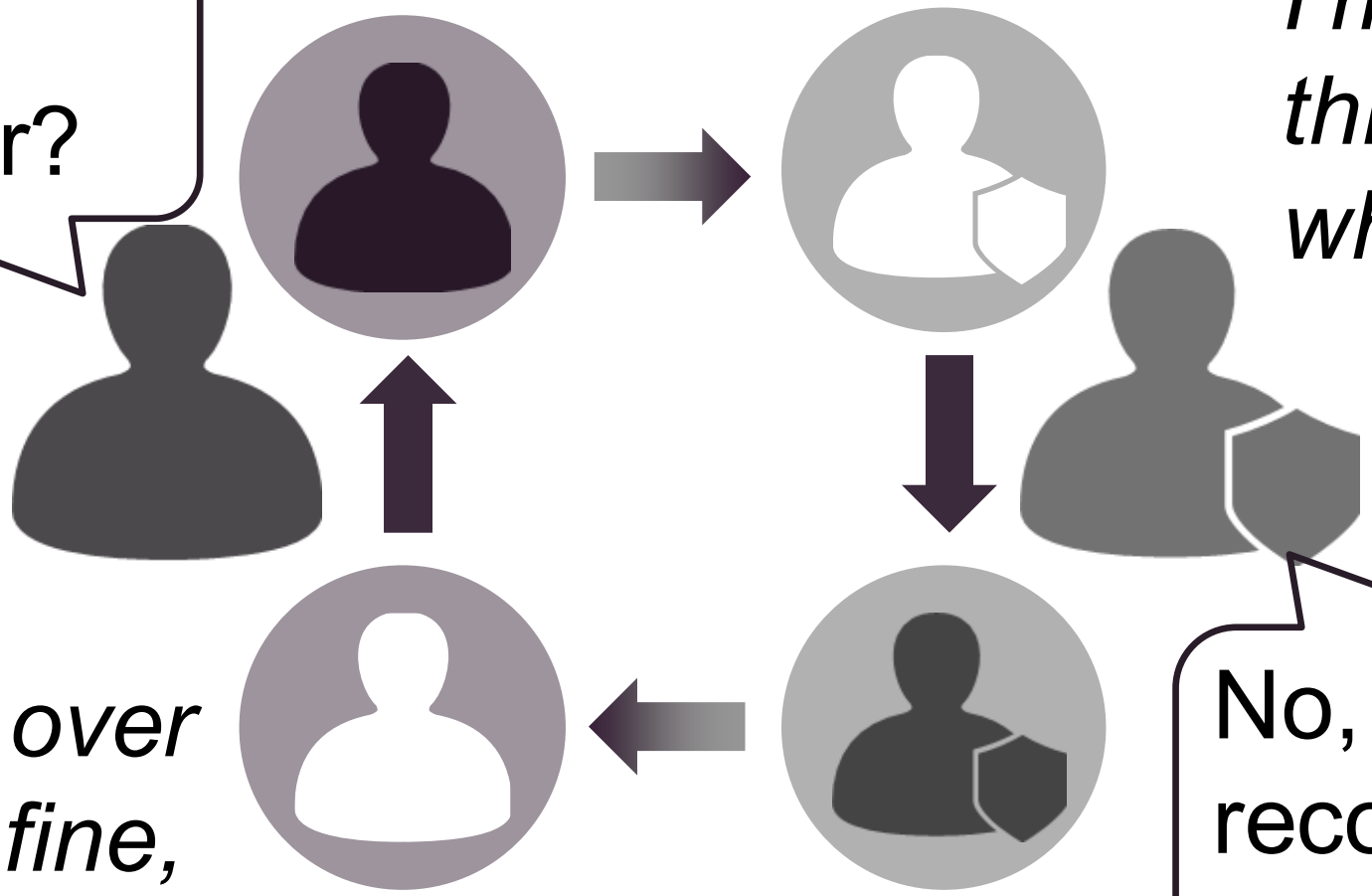
I'm smarter than you are, and I know big words.

Why didn't you just <♑□♌♌●♏♎♋♑□□&>?

A business conversation?

Is that a showstopper?

I'm going to do this no matter what….



No, but we don't recommend you do this.

I'm just CYA over here. You're fine, but I won't admit it.

Humans are

at risk management.

Humans are
awesome
at risk management.

Cybersecurity

What is it?

Cybersecurity

What is it?

Enabling and facilitating organizations to make *wiser* risk decisions

Cybersecurity

What is it?

Enabling and facilitating organizations to make *wiser* risk decisions

Decision Making

Humans make decisions.

Or do they?

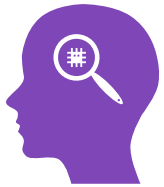
Cognitive Party Tricks

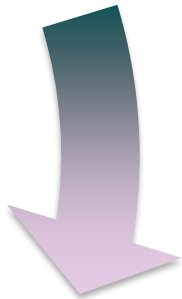
Audience Participation

How To CISO

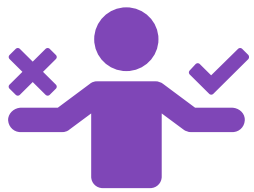
OBSERVE

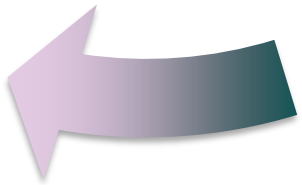
ORIENT



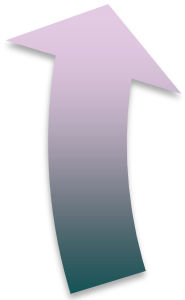


DECIDE





ACT



ACT

ACT Gordon's Stages of Learning

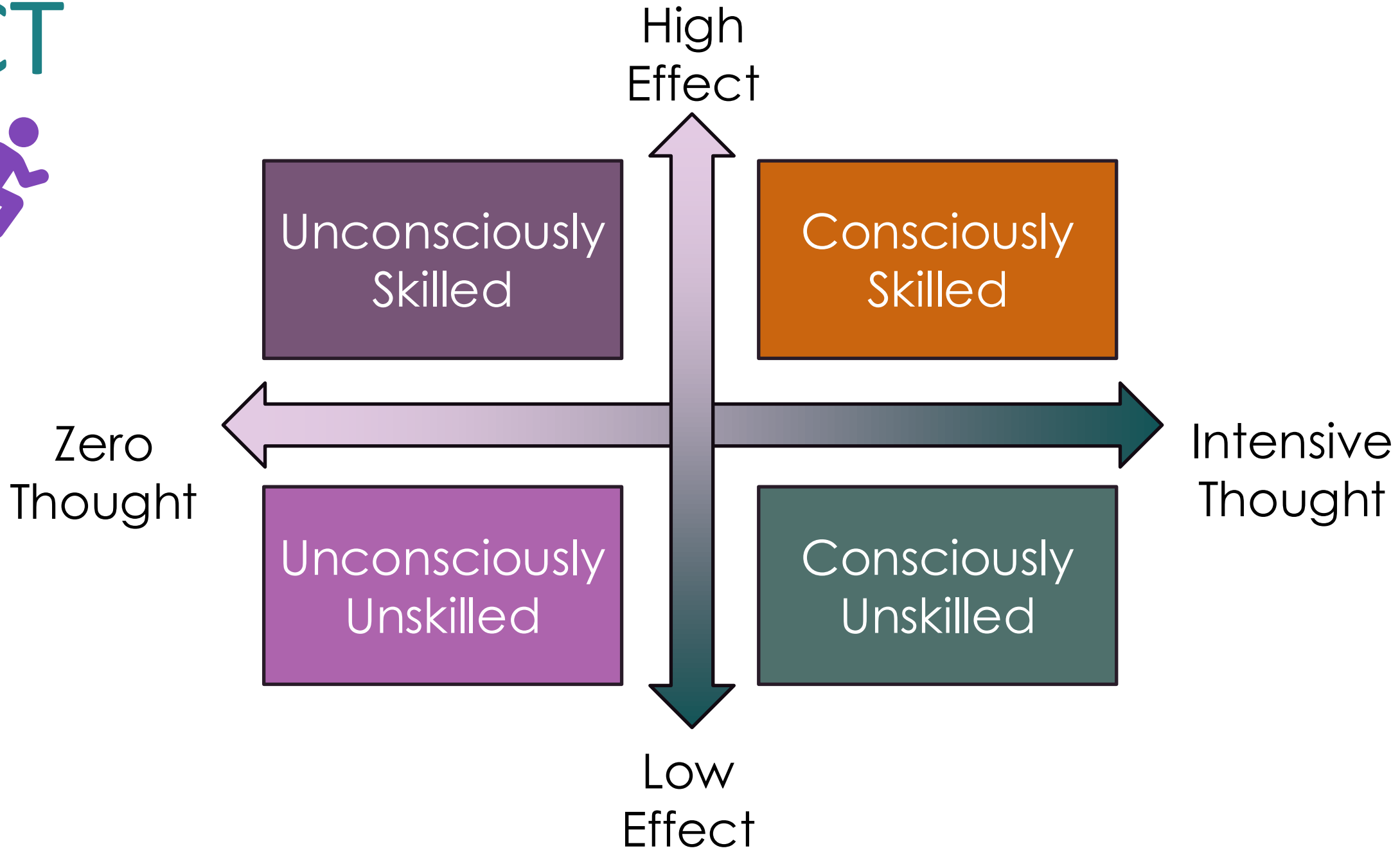
Unconsciously Skilled

Consciously Skilled

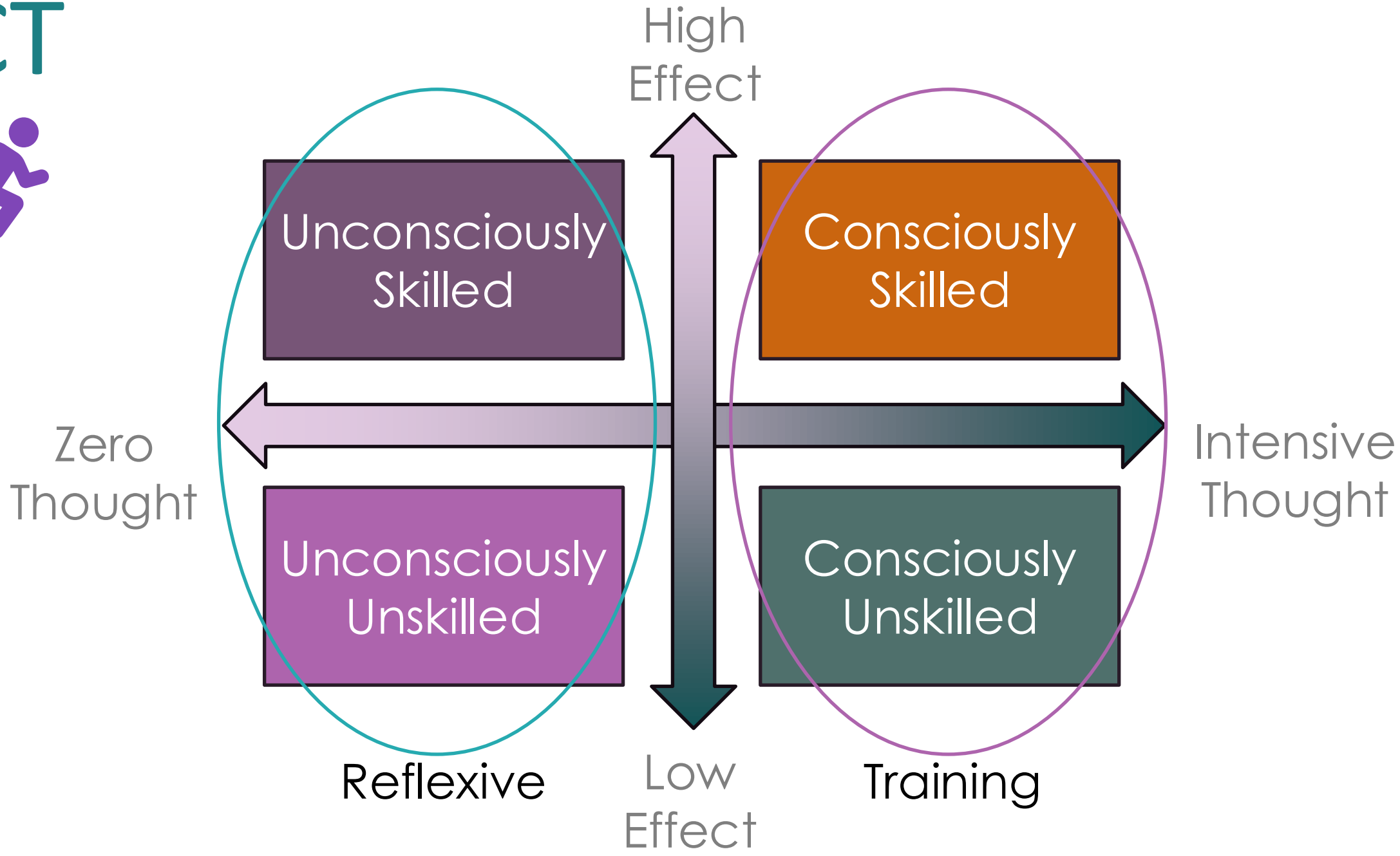
Consciously Unskilled

Unconsciously Unskilled

ACT

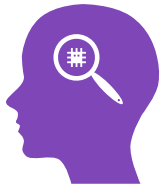


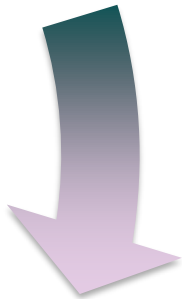
ACT



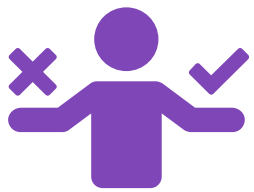
OBSERVE

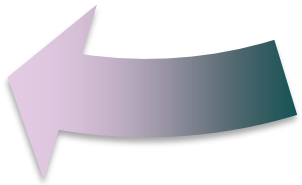
ORIENT



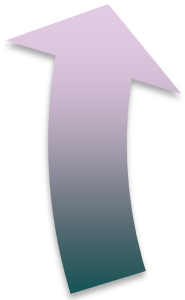


DECIDE

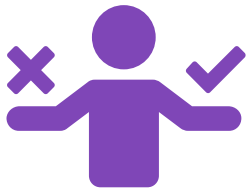




ACT



DECIDE



DECIDE Risk management ought to be easy

Loss	$5M	
Probability	10% / year	
ALE	$500K	

Price of buying	$50K	
Maintenance	$14K	
Reduction in events	10%	

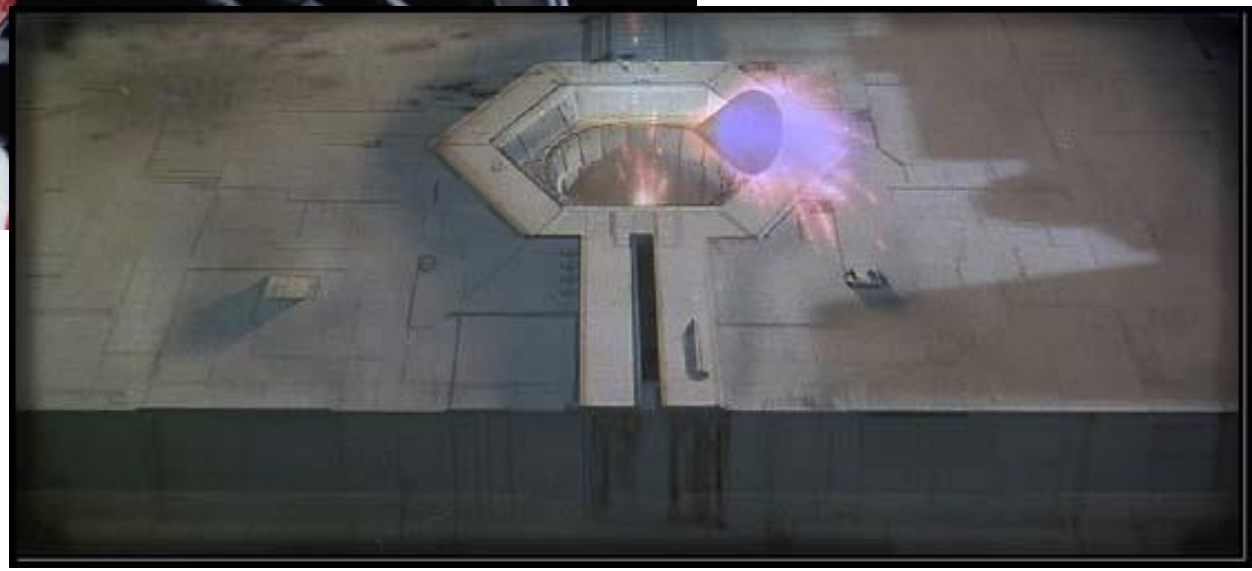
Cost	$26K / year	
Risk Reduction	$50K / year	
Savings	$24K / year	

DECIDE

Actuarial risk measurement is *expected* loss measurement

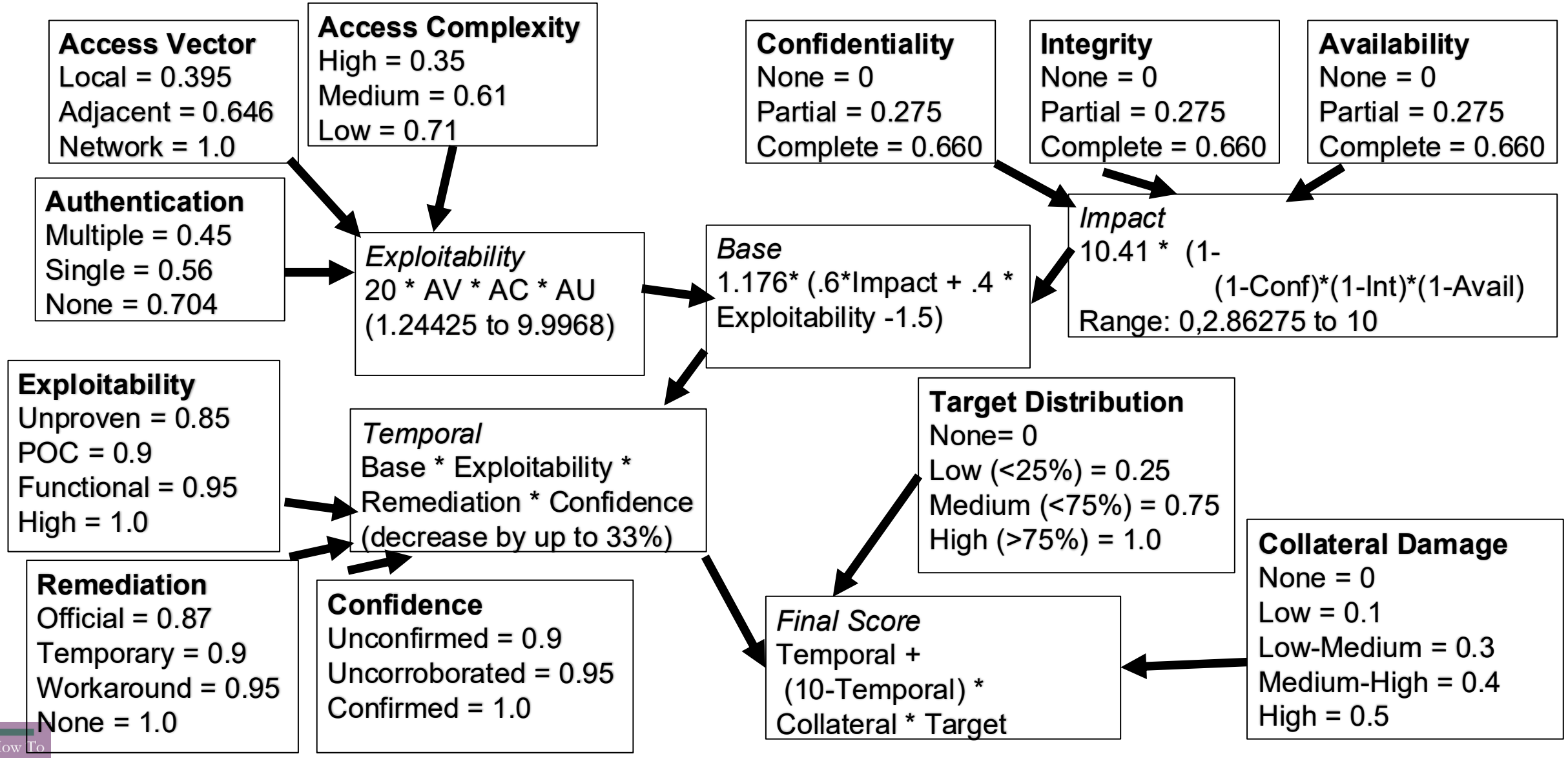
DECIDE

Unique Events are Hard



DECIDE

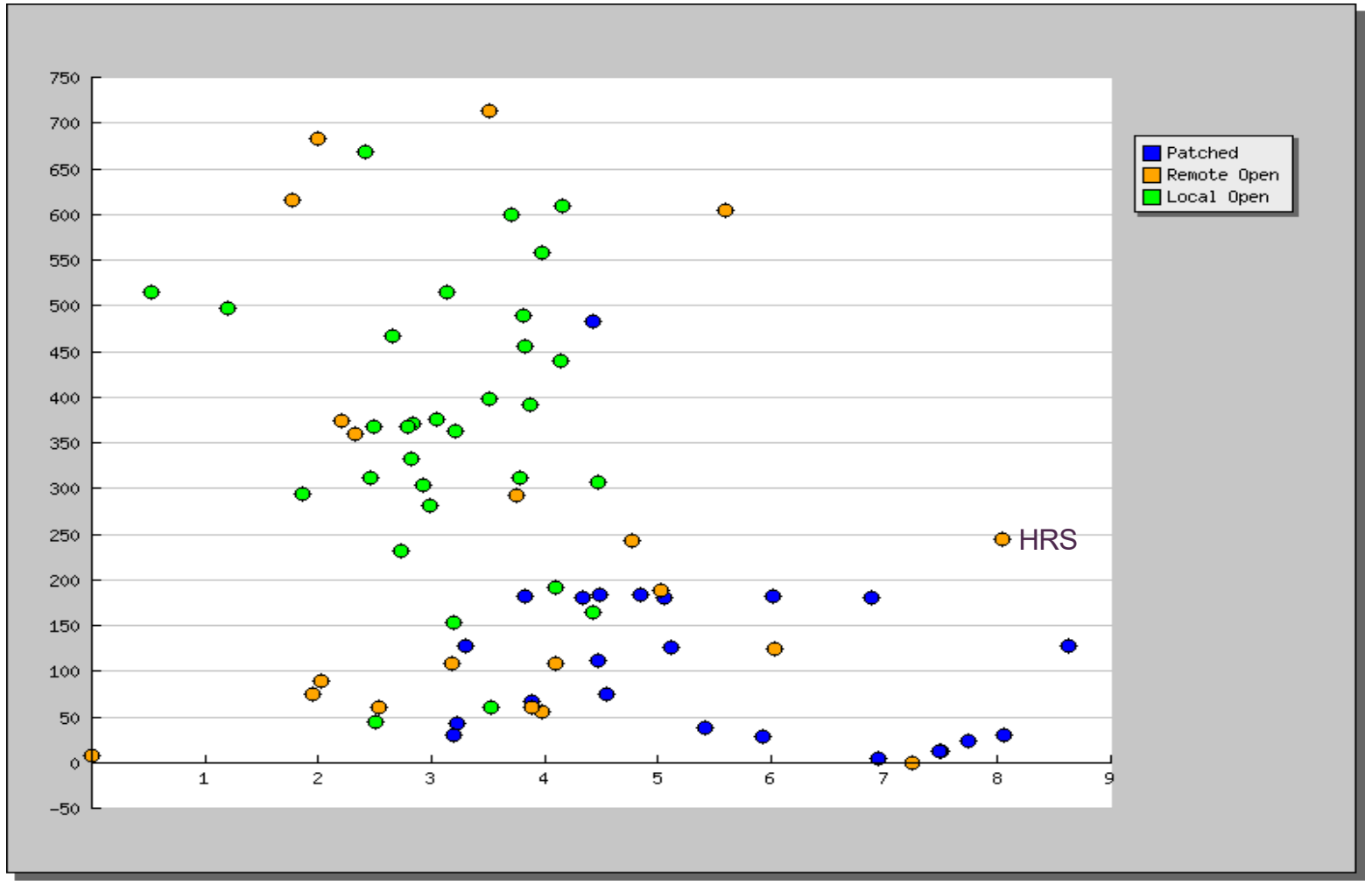
CVSS 2.0



DECIDE 700K possibilities! (45M with customization)

DECIDE

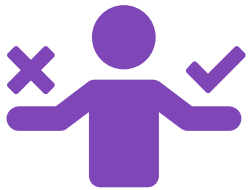
Or maybe about 30....



CVSS

DECIDE

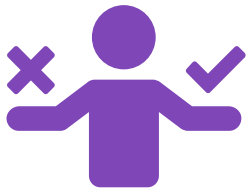
SCENARIO



DECIDE

SCENARIO

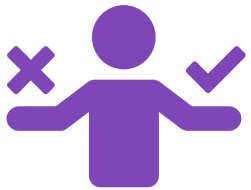
Reflexive



DECIDE

SCENARIO

Reflexive



Training

DECIDE

Cost Context Matters

- You are given one opportunity to play a game.
- A fair, 20-sided die will be rolled.
- You bet X; if your number is rolled, you keep your bet, and get back 20X; otherwise, you lose your bet.
- Your expected payout is thus 1.05.

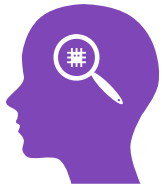
- **Would you bet $1?**
- **Would you bet $10?**
- **Would you bet $100?**
- **Would you bet $1,000?**
- **Would you bet $10,000?**
- **Would you bet $100,000?**
- **Would you bet $1,000,000?**

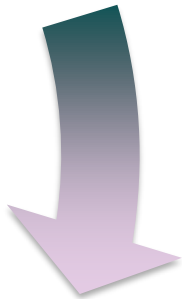
How To CISO

Audience Participation

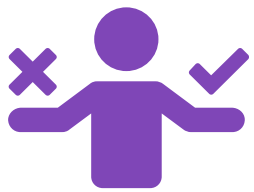
OBSERVE

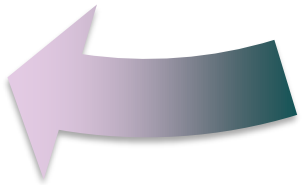
ORIENT



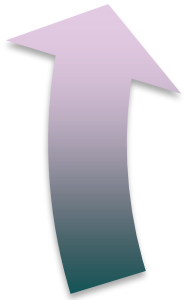


DECIDE



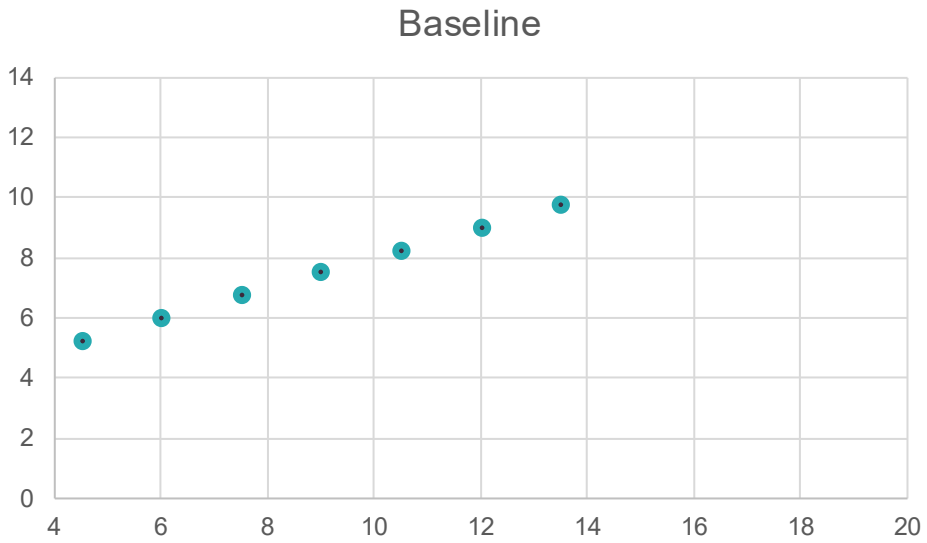


ACT

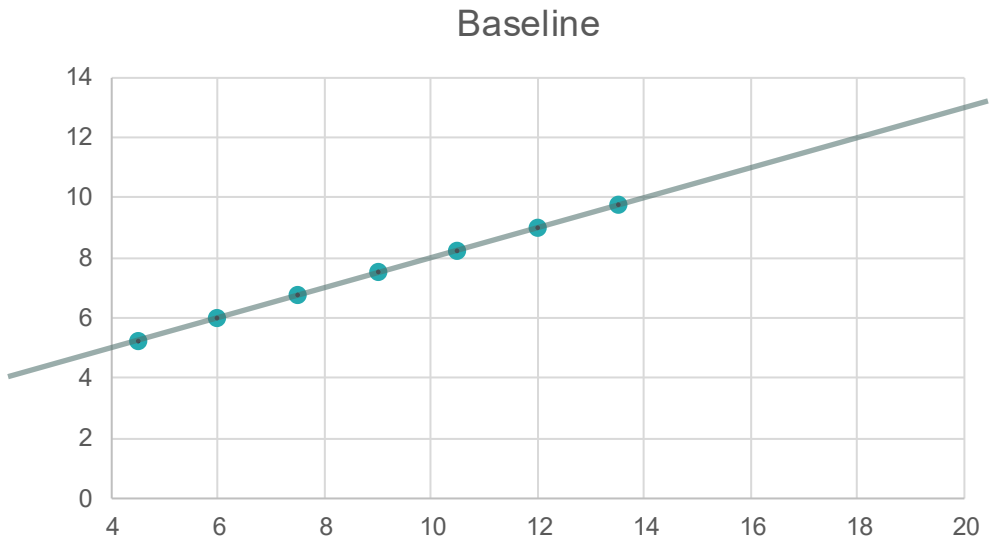


ORIENT

ORIENT



ORIENT



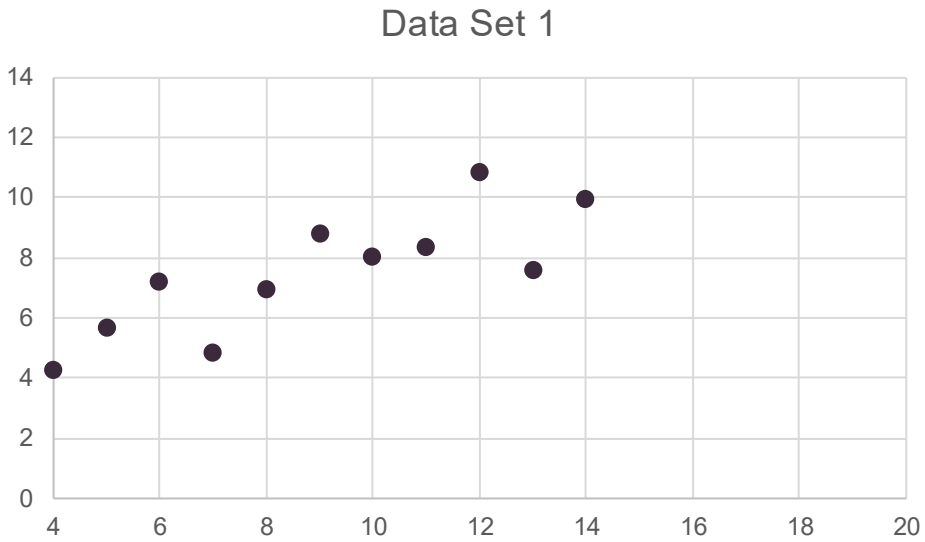
X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	1.000

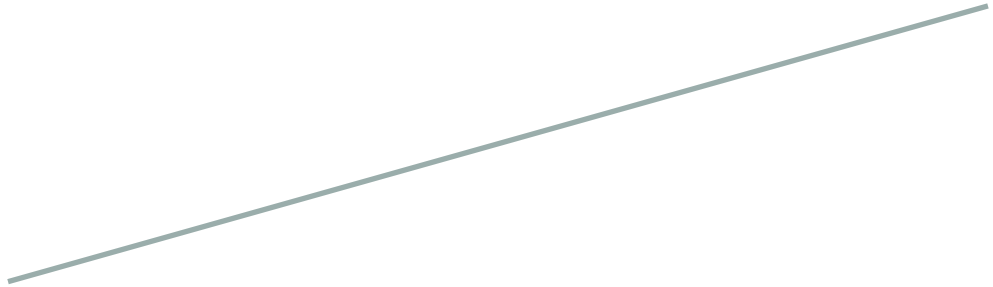
How To CISO

ORIENT

X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	1.000

ORIENT

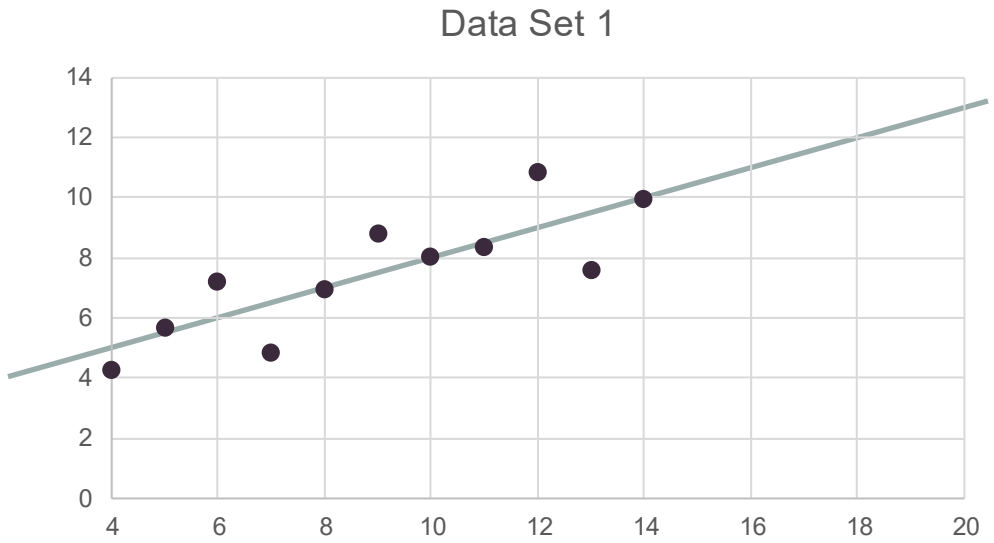




X-average: 9
Y-average: 7.5
Slope: 0.5
Y-Intercept: 3
Correlation:

How To CISO

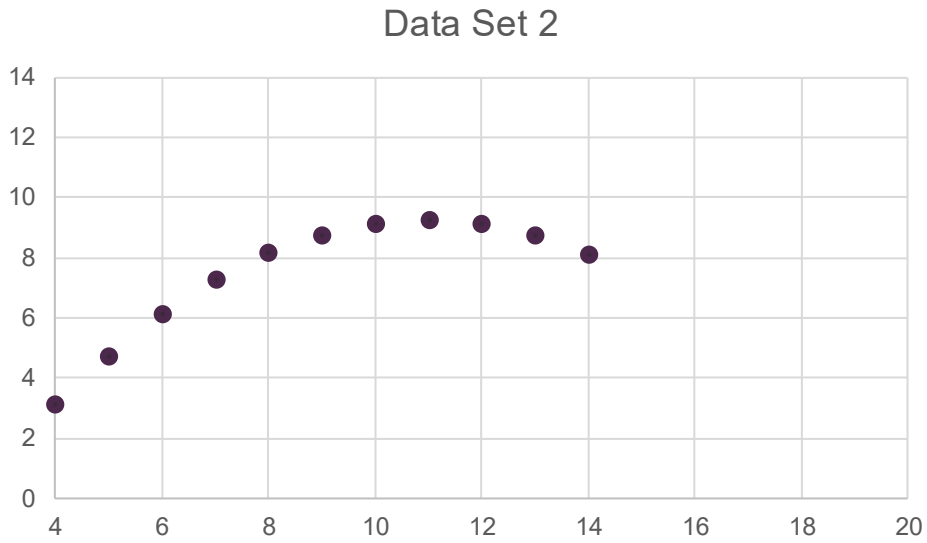
ORIENT

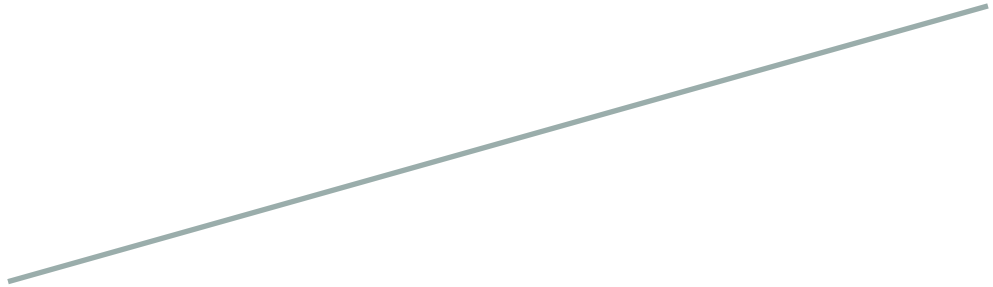


X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	0.816

How To CISO

ORIENT

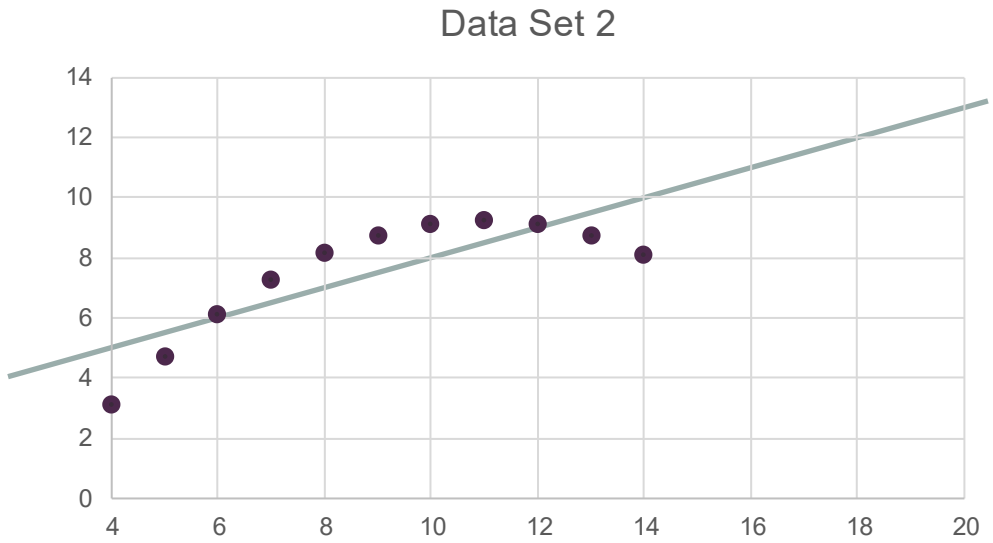




X-average: 9
Y-average: 7.5
Slope: 0.5
Y-Intercept: 3
Correlation: 0.816

How To CISO

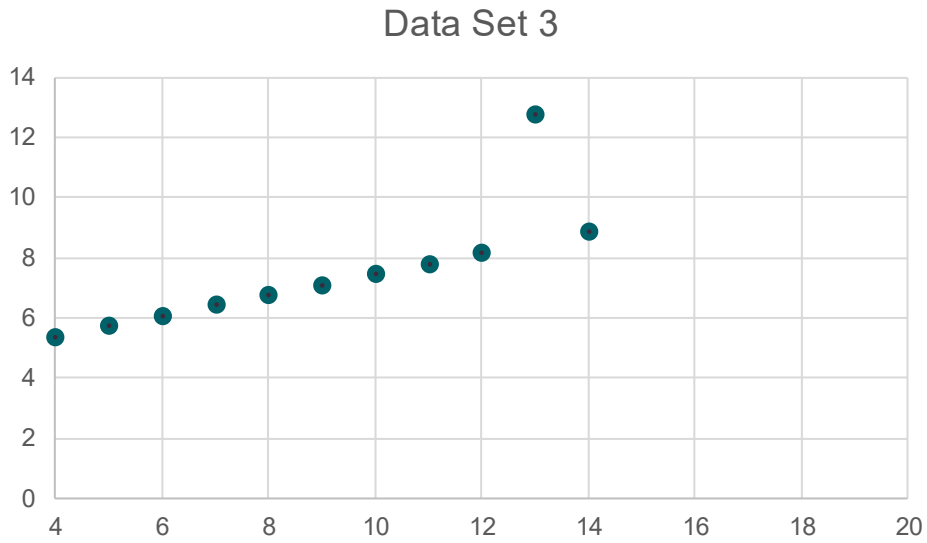
ORIENT

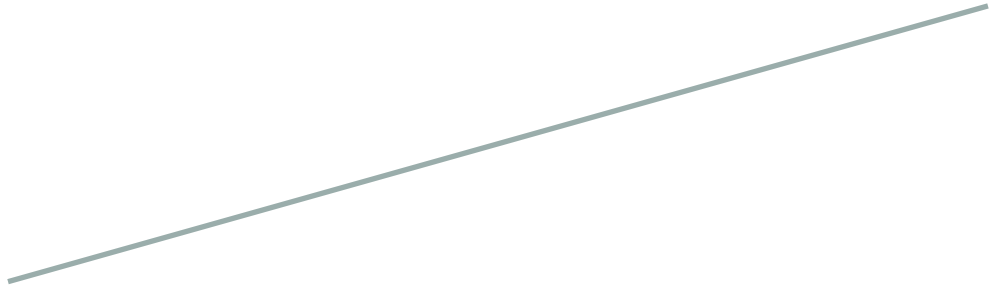


X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	0.816

How To CISO

ORIENT

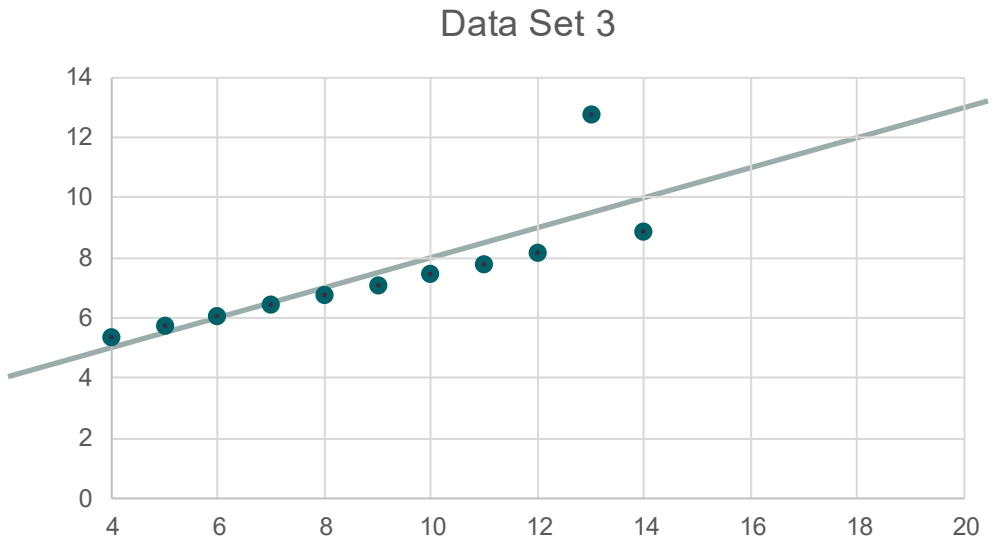




X-average: 9
Y-average: 7.5
Slope: 0.5
Y-Intercept: 3
Correlation: 0.816

How To CISO

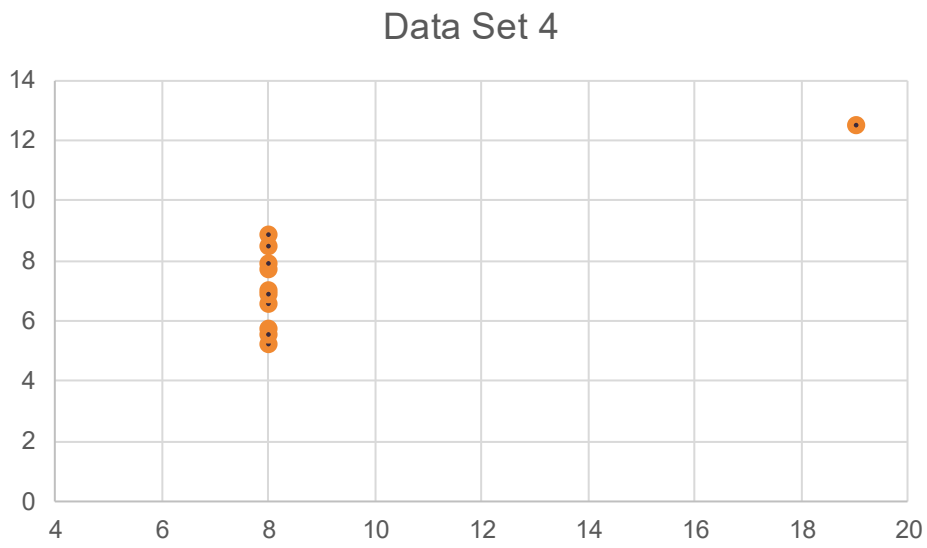
ORIENT

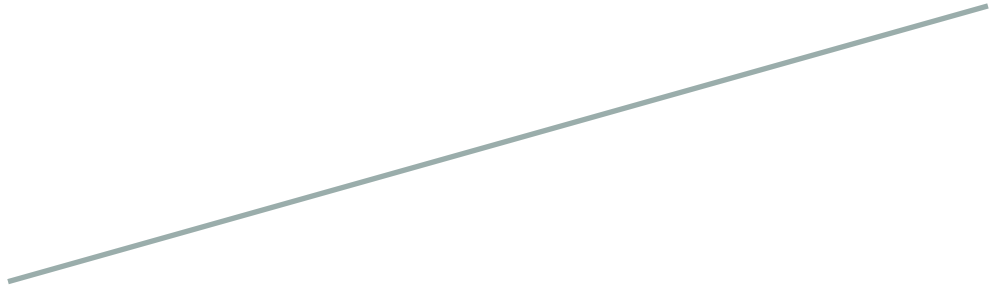


X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	0.816

How To CISO

ORIENT

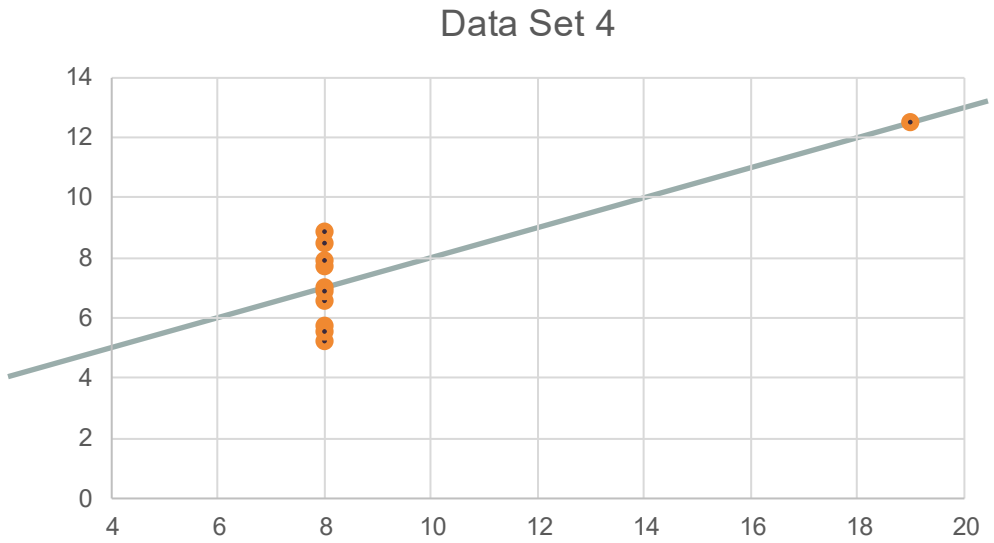




X-average: 9
Y-average: 7.5
Slope: 0.5
Y-Intercept: 3
Correlation: 0.816

How To CISO

ORIENT

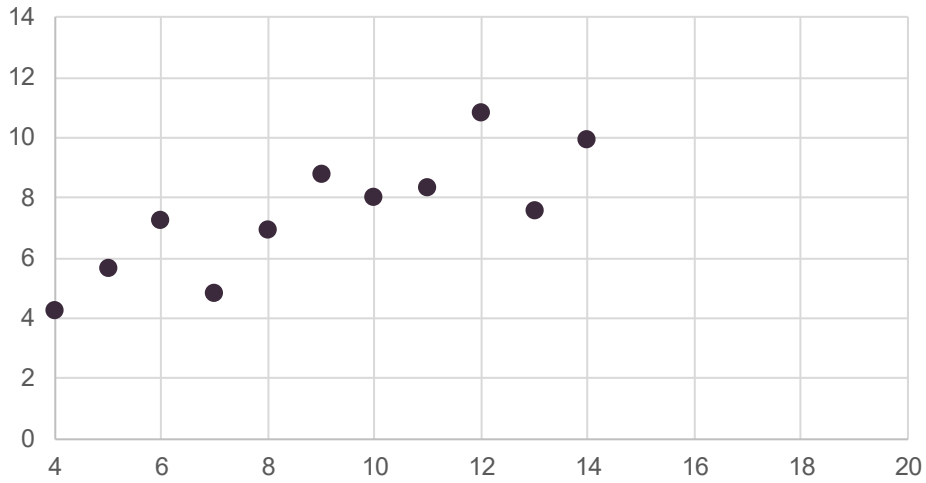


X-average:	9
Y-average:	7.5
Slope:	0.5
Y-Intercept:	3
Correlation:	0.816

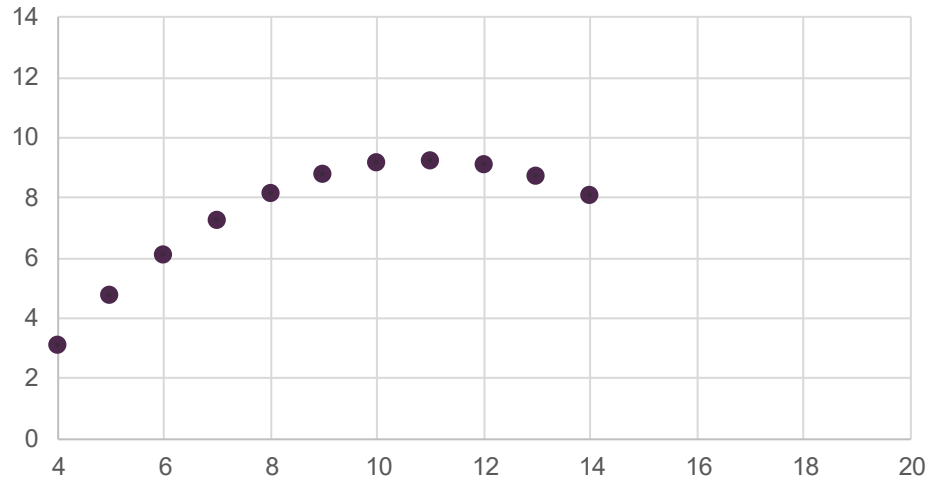
How To CISO

ORIENT

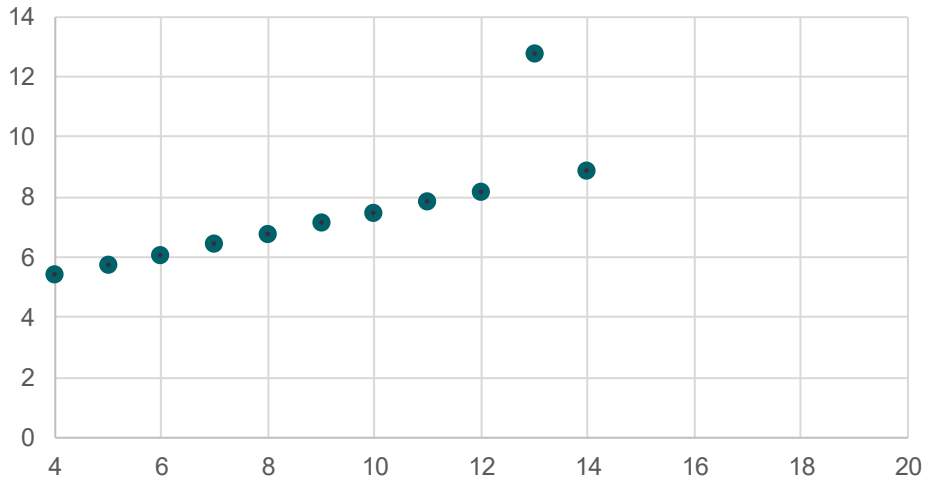
Data Set 1



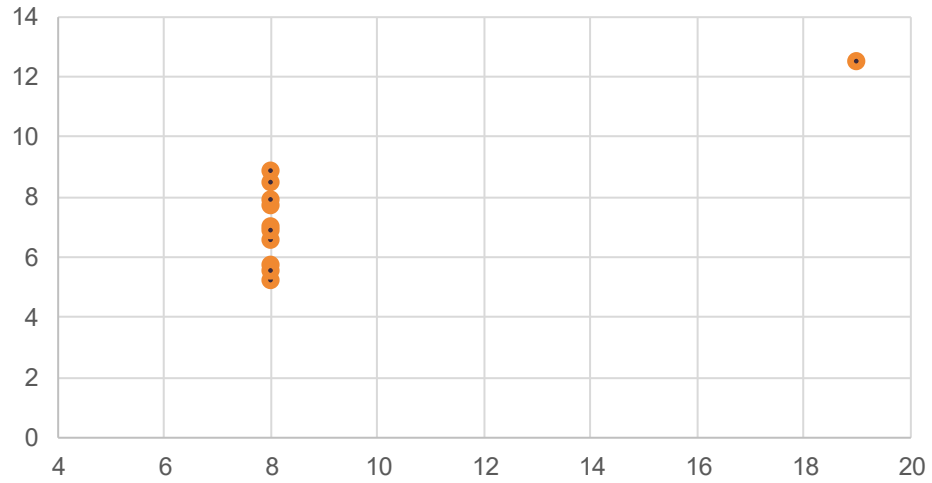
Data Set 2



Data Set 3



Data Set 4



How To CISO

ORIENT

ORIENT

Nine-Box

Likelihood	Impact: High	Impact: Medium	Impact: Low
High			
Medium			
Low			

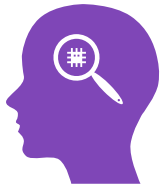
ORIENT

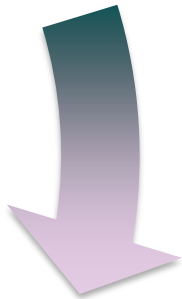
Four-Box

Likelihood	Impact: High	Impact: Medium	Impact: Low
High	Incidents		Hygiene
Medium			
Low	Programs		Litter

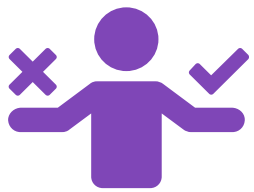
OBSERVE

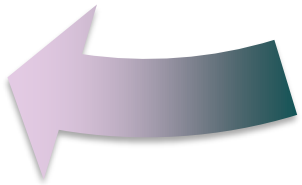
ORIENT



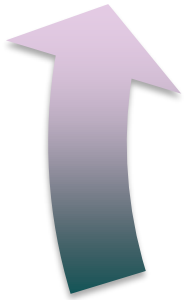


DECIDE





ACT



OBSERVE

OBSERVE

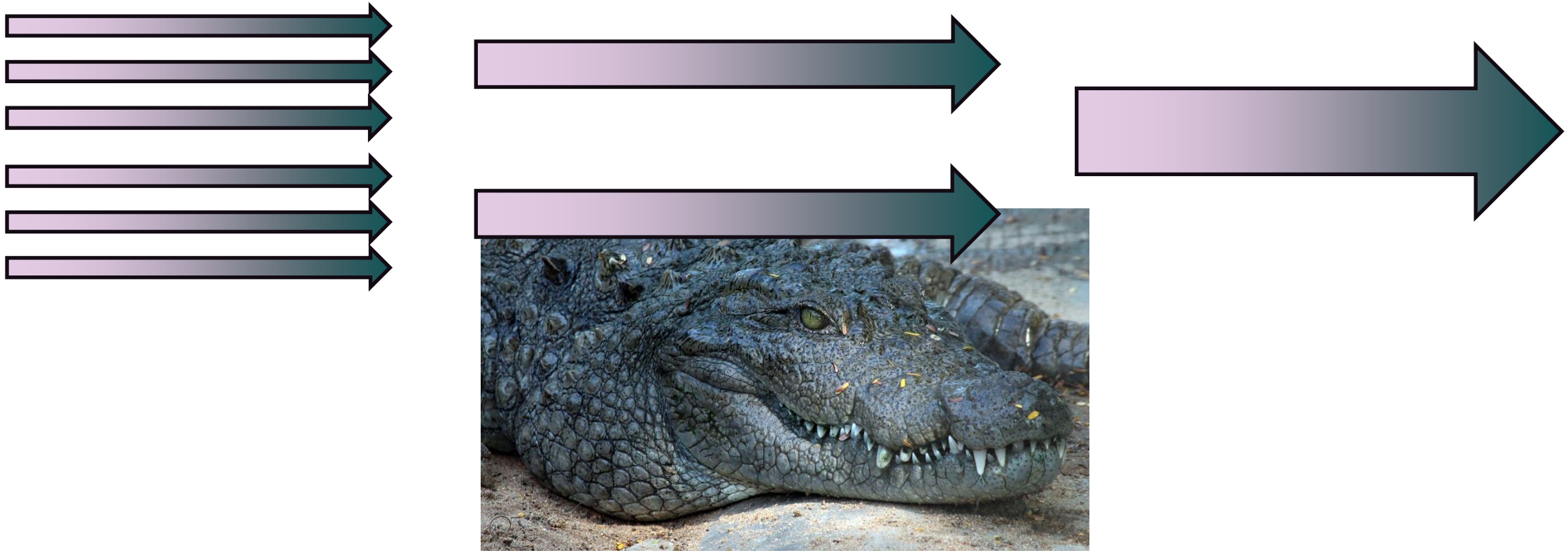
How To CISO

OBSERVE

OBSERVE

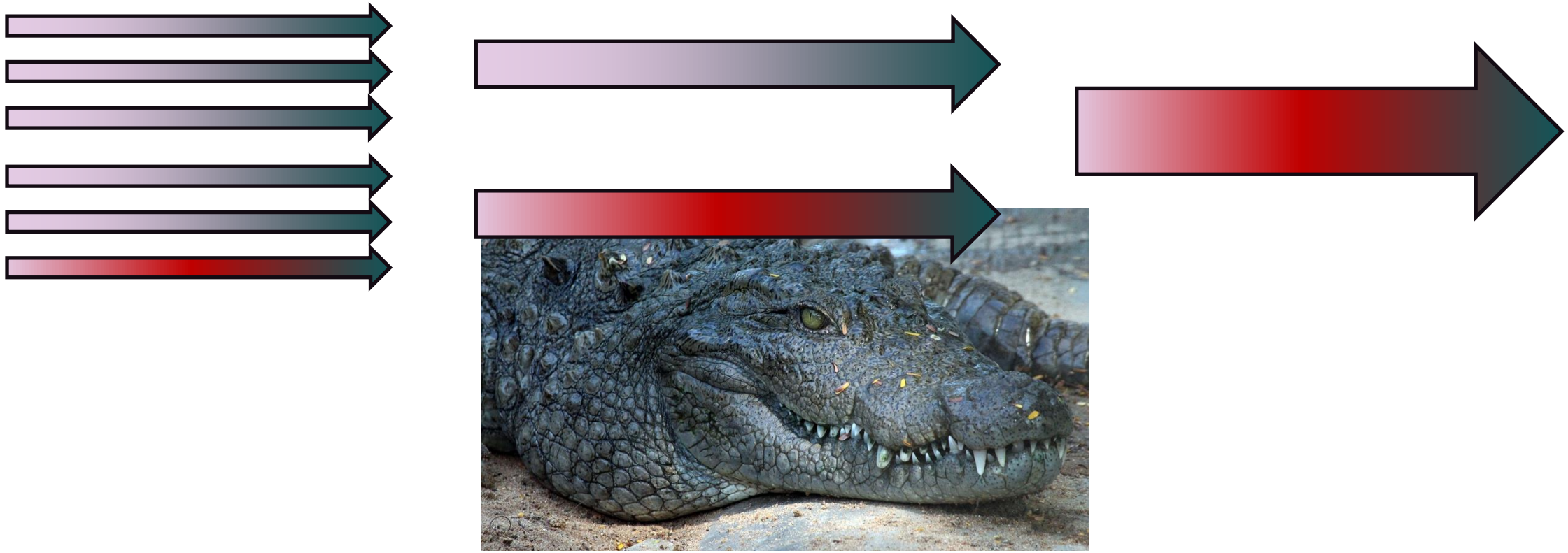
How To CISO

OBSERVE



How To CISO

OBSERVE



How To CISO

OBSERVE

How To CISO

OBSERVE

10,000,000

40

How To CISO

OBSERVE

How To CISO

OBSERVE

ORIENT

ACT

DECIDE

OBSERVE

Optimized to filter out the unnecessary

ORIENT

Frames tend to be *sticky*

ACT

Learn by doing uncomfortable things

DECIDE

Preference reflexive actions

OBSERVE	ORIENT	DECIDE	ACT
 Optimized to filter out the unnecessary	Frames tend to be *sticky*	Preference reflexive actions	Learn by doing uncomfortable things

Humans are

awesome

at risk management.

Humans Are Awesome
(at Risk Management)

Andy Ellis

How To CISO