TIDAL

THREAT-INFORMED DEFENSE

Balancing the Scale of Just-Good-Enough

The Techniques vs. Procedures Debate

Why not both?

Ian Davila
Frank Duff

Who We Are

Frank Duff

CHIEF INNOVATION OFFICER, TIDAL CYBER

Before that…

18 years at MITRE (Signal Processing, Detection Engineering, Lead ATT&CK Evals)

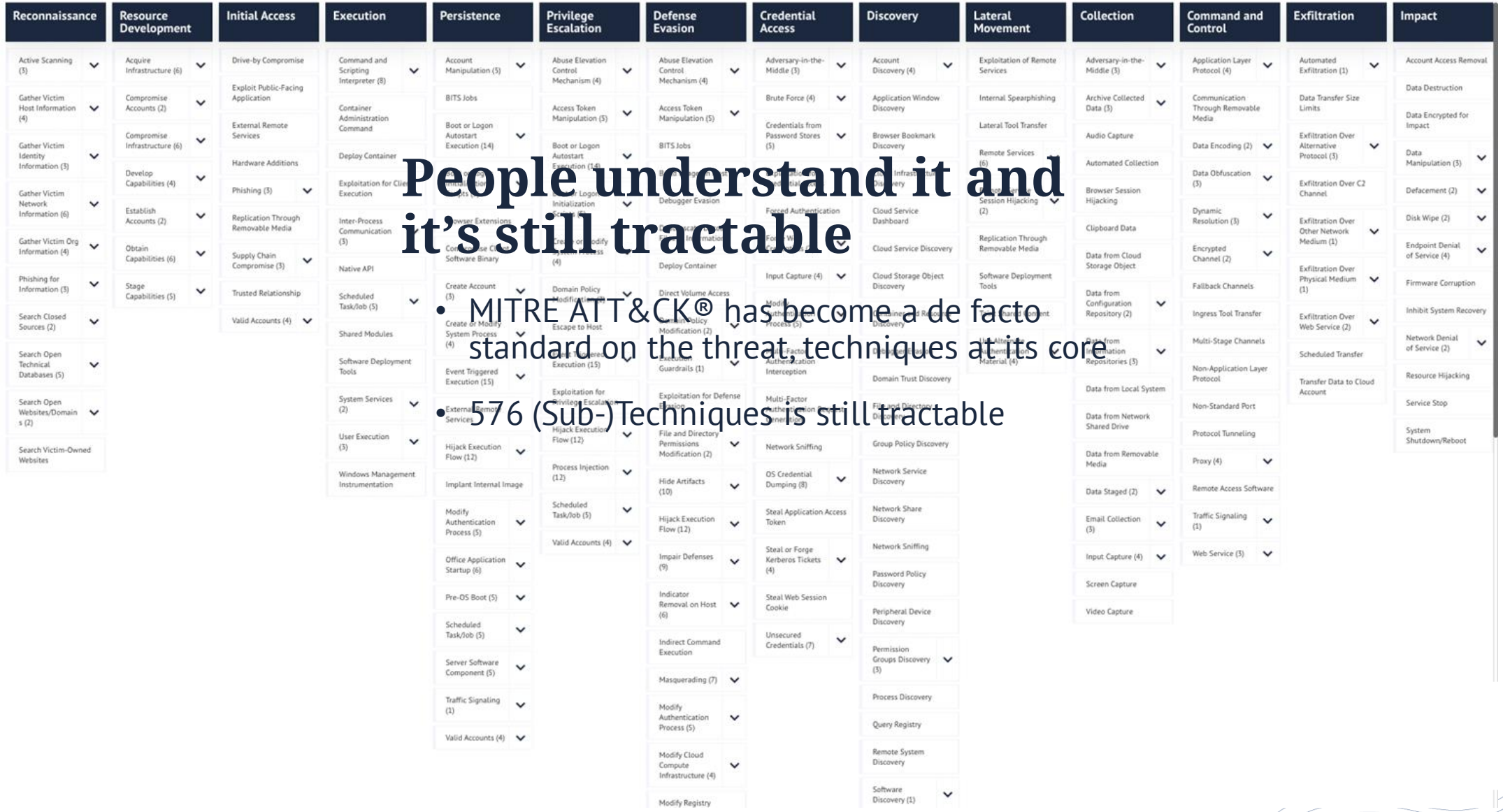
Ian Davila

LEAD ADVERSARY EMULATOR, TIDAL CYBER

Before that…

Computer Scientist, MITRE ATT&CK, ATT&CK Evals

Techniques



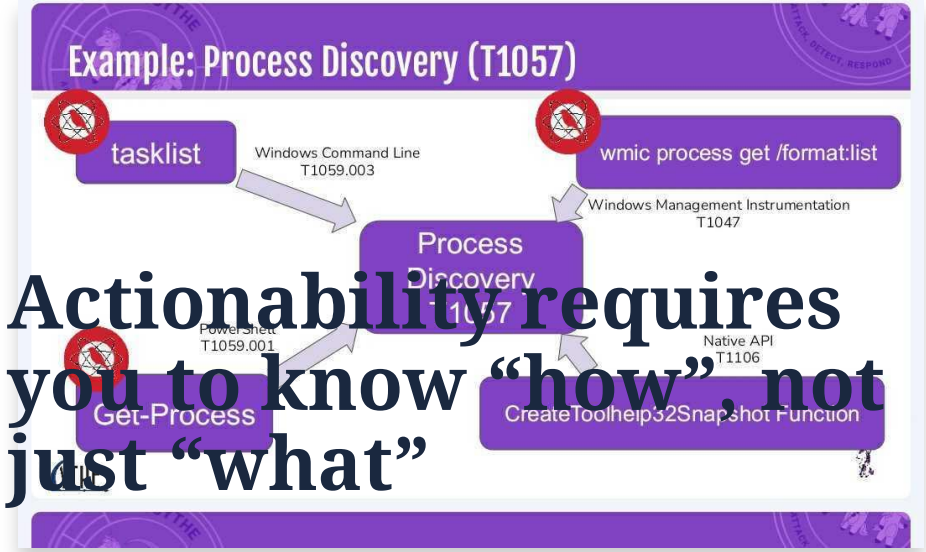
People understand it and it's still tractable

- MITRE ATT&CK® has become a de facto standard on the threat, techniques at its core
- 576 (Sub-)Techniques is still tractable

Procedures

Credit: Jamie Williams, MITRE

[Dissecting a Detection: An Analysis of ATT&CK Evaluations Data (Sources) Part 1 of 2]

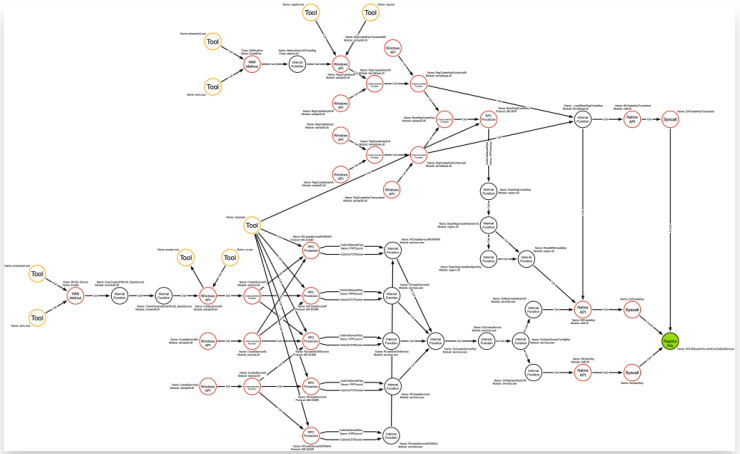


Actionability requires you to know "how", not just "what"

- Procedures give you the how to drive red and blue

Credit: Tim Schulz, Scythe

[Devil in the Details: Why Legacy Breach and Attack Simulation (BAS) Falls Short, SecureWorld]



Credit: Jared Atkinson

[https://twitter.com/jaredcatkinson/status/1512067698863198215]

Techniques? Procedures?

TECHNIQUES???

PROCEDURES???

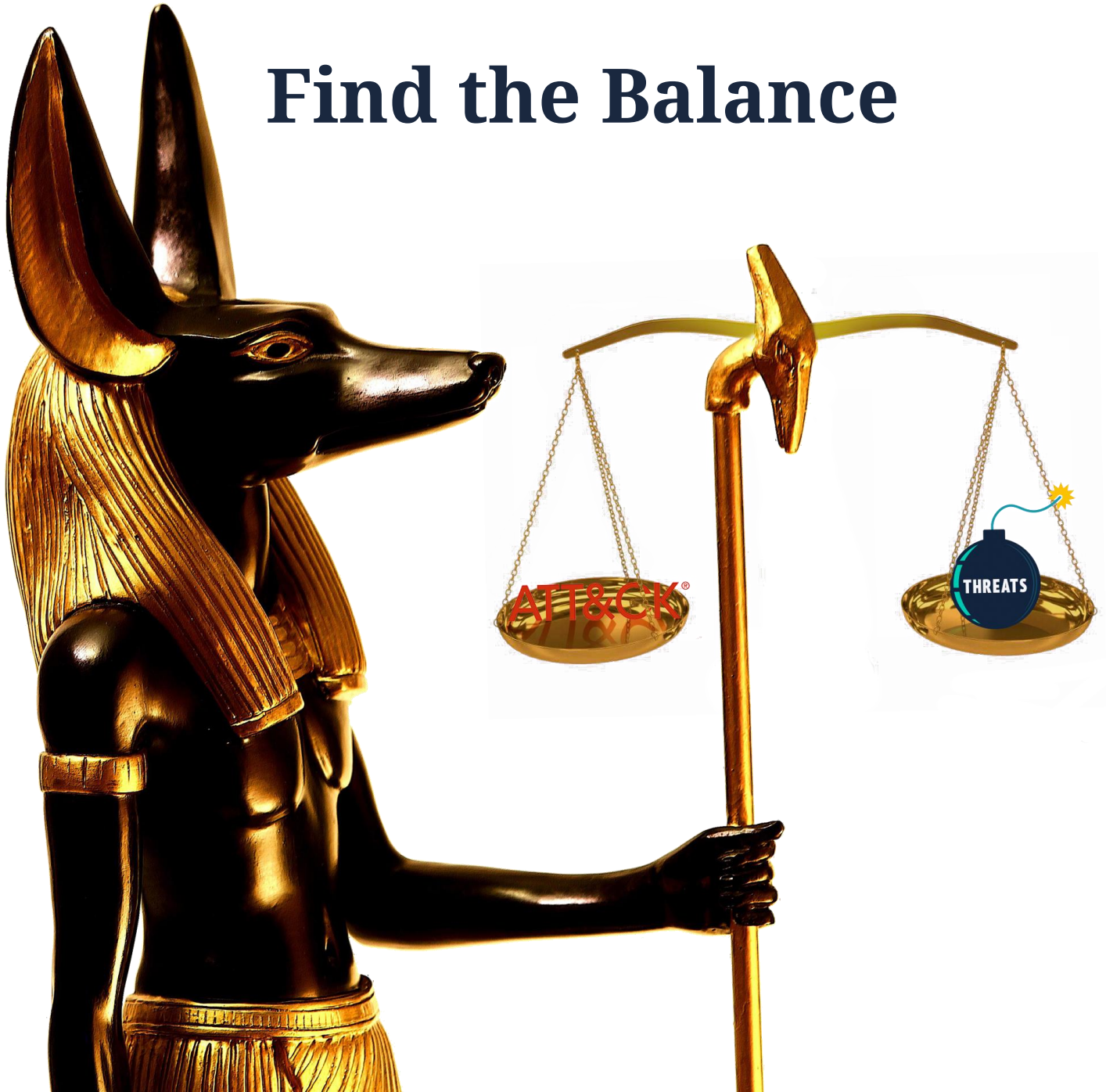
Technique “coverage” is an overgeneralization

What it takes to cover a technique is misunderstood or abused, leading to misplaces confidence

Procedure “coverage” drives complexity and costs up

Procedure variance requires you to develop and run multiple test scenarios. Skills, money, time all become an issue.

Find the Balance



Techniques are the heart

ATT&CK enhances understandability

Procedures are the feather of truth

Procedures enhance confidence

How do we balance the scales?

- CTI, Offensive, Defensive considerations
- Easier to build technique flow than procedure flow, start there
- Sub-techniques are more specific than techniques
- For each (sub-)technique… many procedures
- Do we have all the necessary information to emulate procedures?

CTI Considerations

Closing Gaps

Goal is to be as close as possible to real threat

Sometimes you must be an artist

* shoutout to Cat Self

Close gaps in procedures

- Lack of intel
- Inferred intel
    - Not enough information but can infer from known

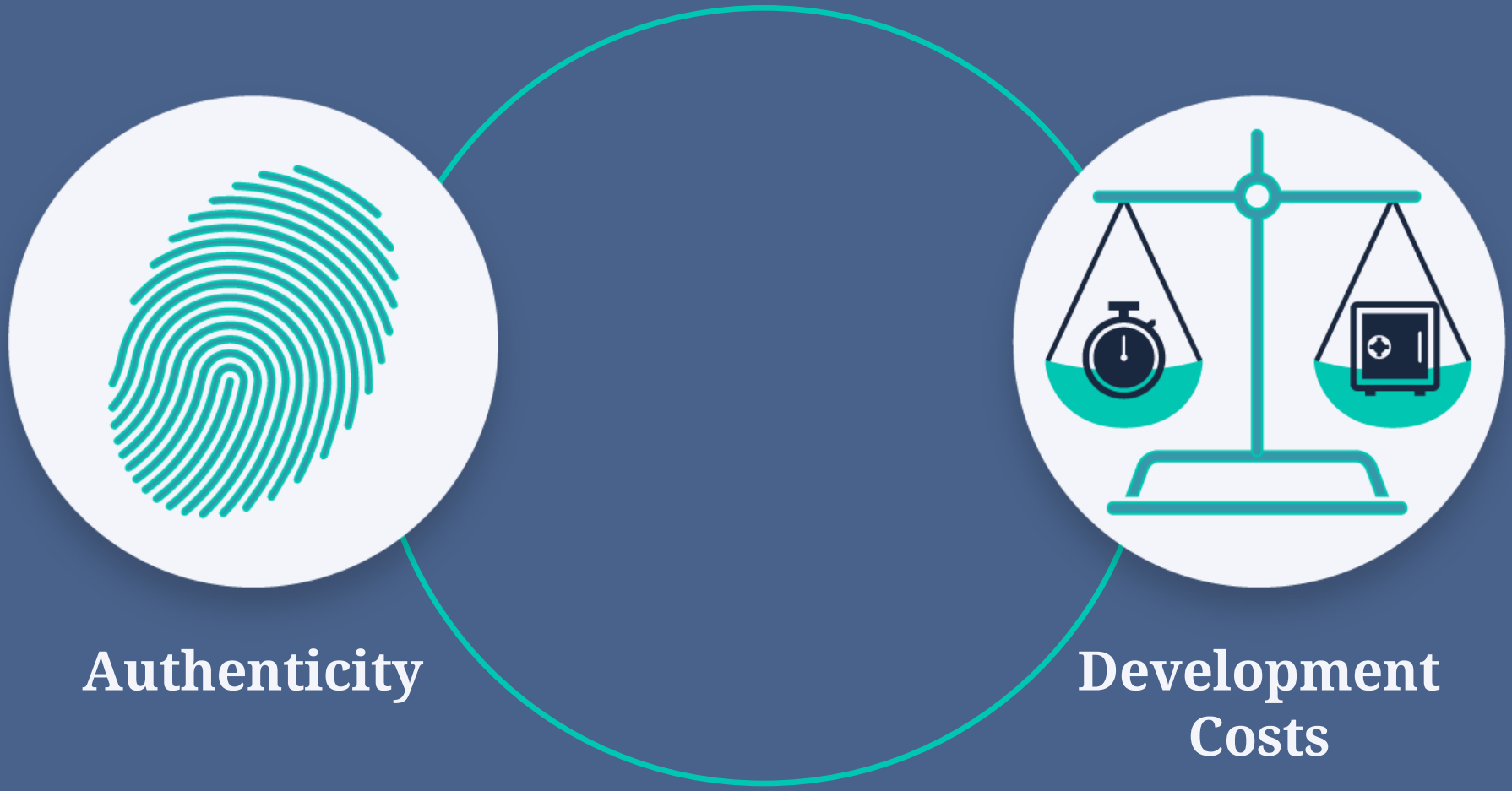
Offensive Considerations

Testing

Development Costs

Offensive Considerations

Testing

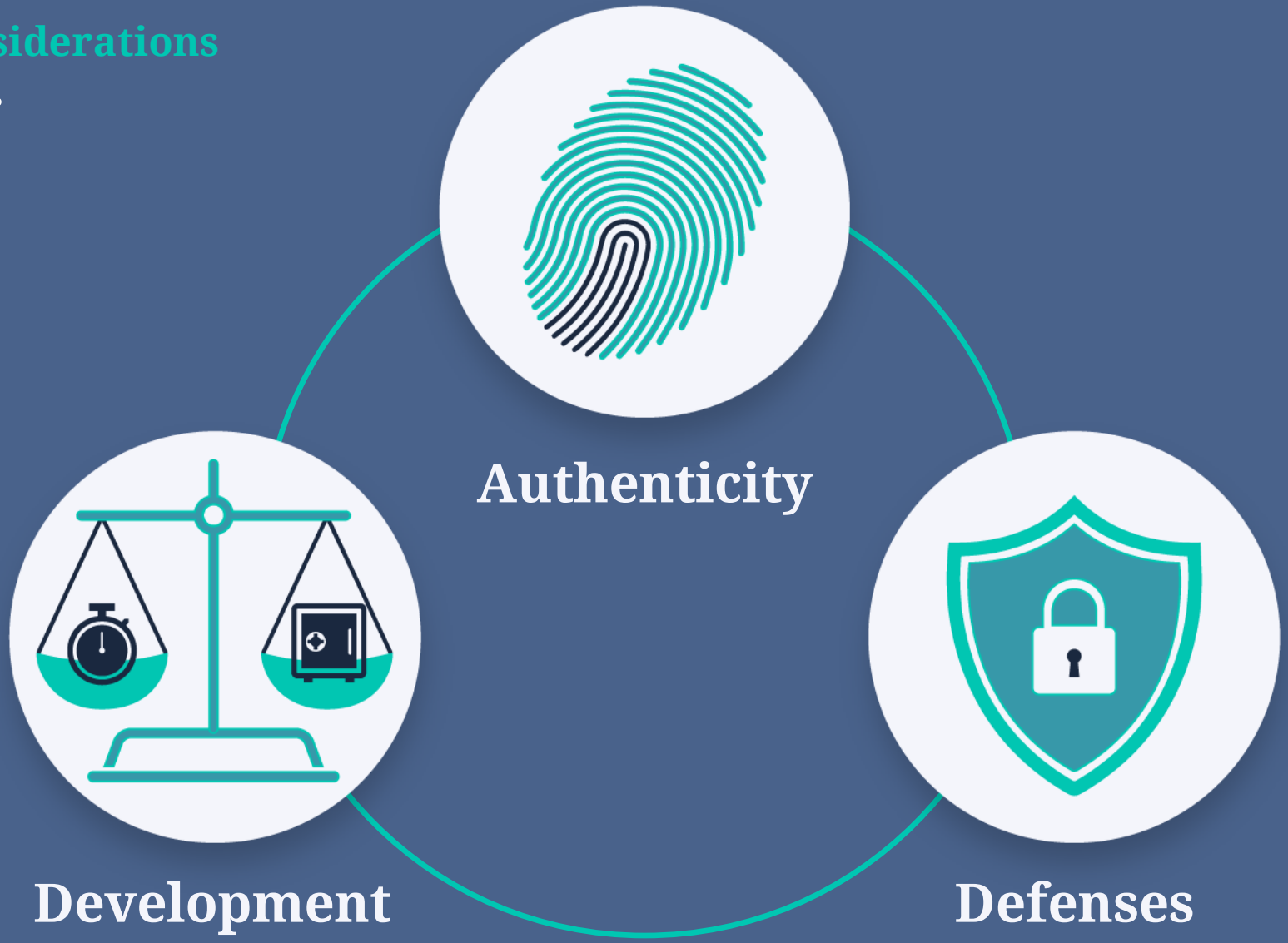


Authenticity

Development Costs

Offensive Considerations

Testing



Defensive Considerations

Not all detections are created equal

Graph based detections

- Hard
- Expensive
- Data Sources/Components
- More than one procedure

It is easier to detect at the procedure level

- Process creates + arguments

Chained detections

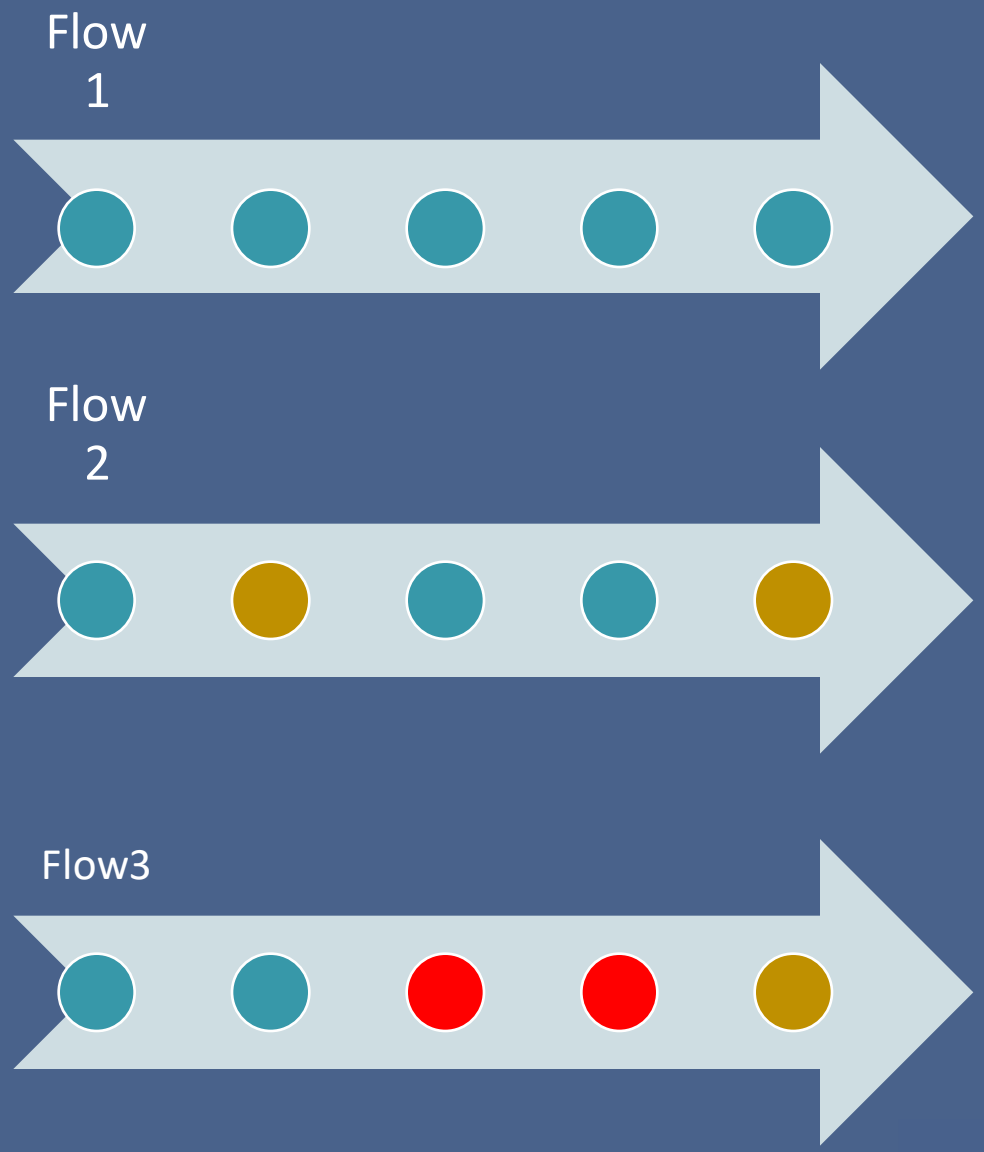
Our Approach

Flows that align to specific threats we care about

- Potential targeting of user
- User says they care about them
- Bang for the buck

We want procedural variance to test defenses

Execute flows – chained detections



Final Statements

- 1 test or 1 detection isn't "Coverage"
- Look at procedure coverage through the lens of technique coverage
- Understand what you detect and what you test (and why!)
- Don't let perfect be the enemy of the good

Thank you!

Frank.duff@tidalcyber.com
Ian.Davila@tidalcyber.com