Attacking ATT&CK

A Practical Guide for Elevating your Threat-Informed Defense Strategy

January 25, 2024

Frank Duff, Co-Founder and Chief Innovation Officer

TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Introduction

Chief Innovation Officer @ **Tidal Cyber**

ex-MITRE, ATT&CK Evals creator, detection engineer at heart, all things ATT&CK

Threat-Informed Defense: *Systematic application & deep understanding of adversary tradecraft and technology to assess, organize, and optimize your defenses*

Get in touch:

- **LinkedIn:** Tidal Cyber / Frank Duff
- **Twitter/X:** @TidalCyber / @frankduff
- **Email:** contact@tidalcyber.com

TIDAL CYBER

THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

The State of Threat-Informed Defense

TIDAL CYBER

THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Implementing Threat-Informed Defense

More threats are identified each year

More “threat-informed” resources are being published (good news!)

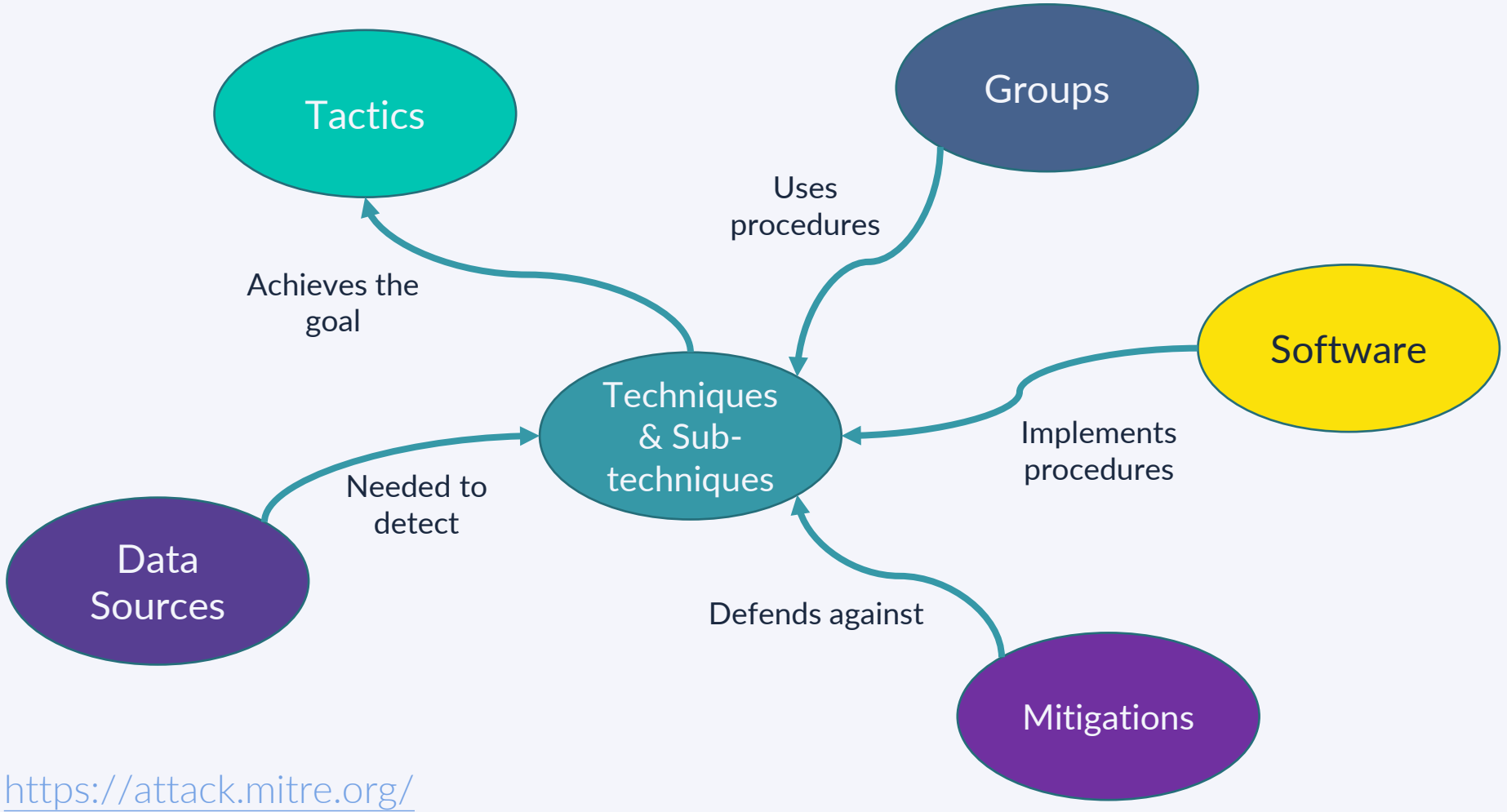
More awareness is needed on how to systematically apply the growing catalog of TID-related content (**cue today’s session**)

TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Reintroducing ATT&CK: Connecting the Dots

ATT&CK Knowledge Base elements



https://attack.mitre.org/

TIDAL CYBER
THREAT-INFORMED DEFENSE

The ATT&CK Way Back Machine

ATT&CK was built out of necessity to solve a specific problem:

Enable cross-team communication from CTI to Blue to Red to Leadership

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Implementing Threat-Informed Defense

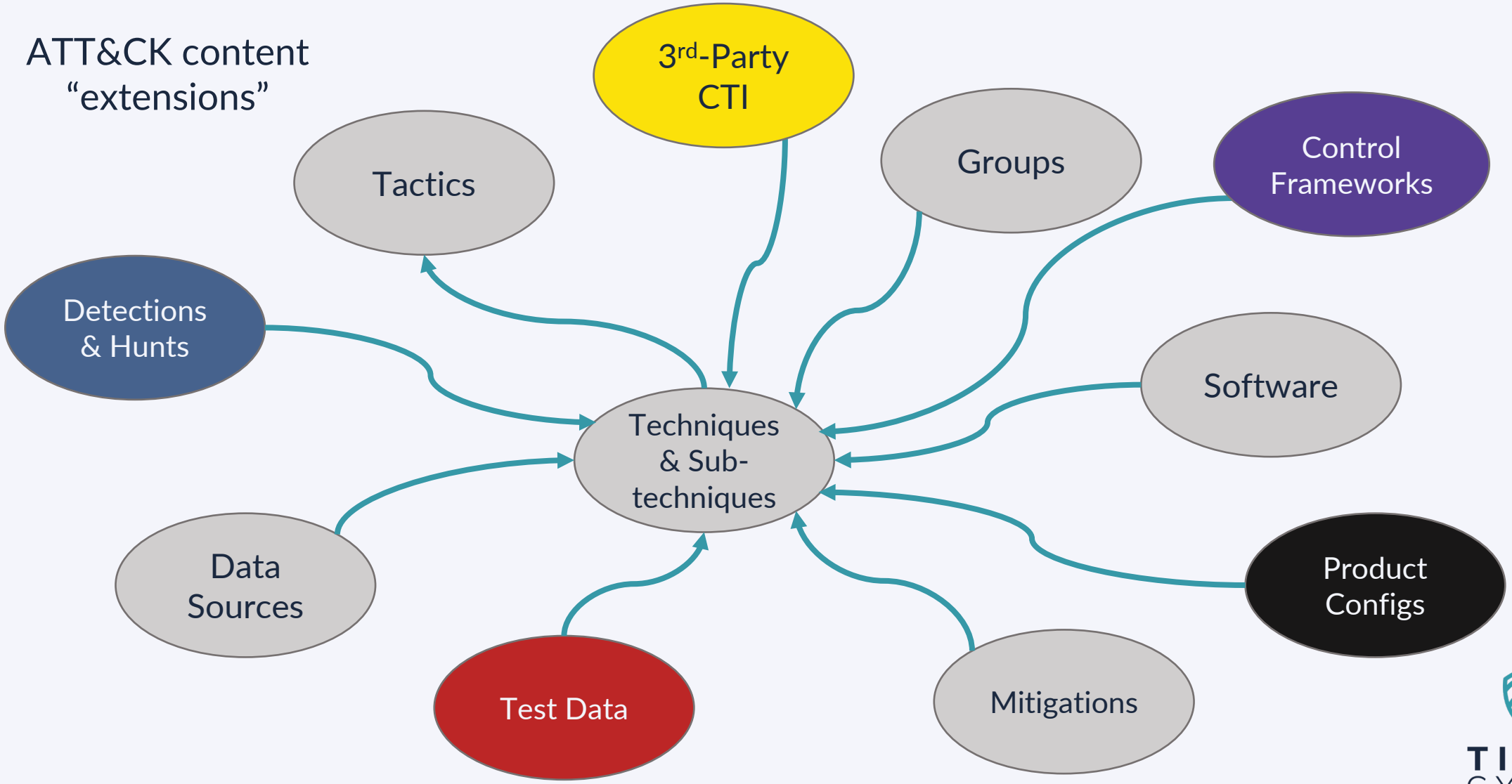
Common misconceptions:

- ATT&CK is a comprehensive, always up-to-date CTI source
- Adversary behaviors never change
- Detection-in-Depth = Defense-in-Depth

TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Reintroducing ATT&CK: Connecting the Dots



TIDAL CYBER
THREAT-INFORMED DEFENSE

Threat-Informed Defense: Making Sense of the Dots

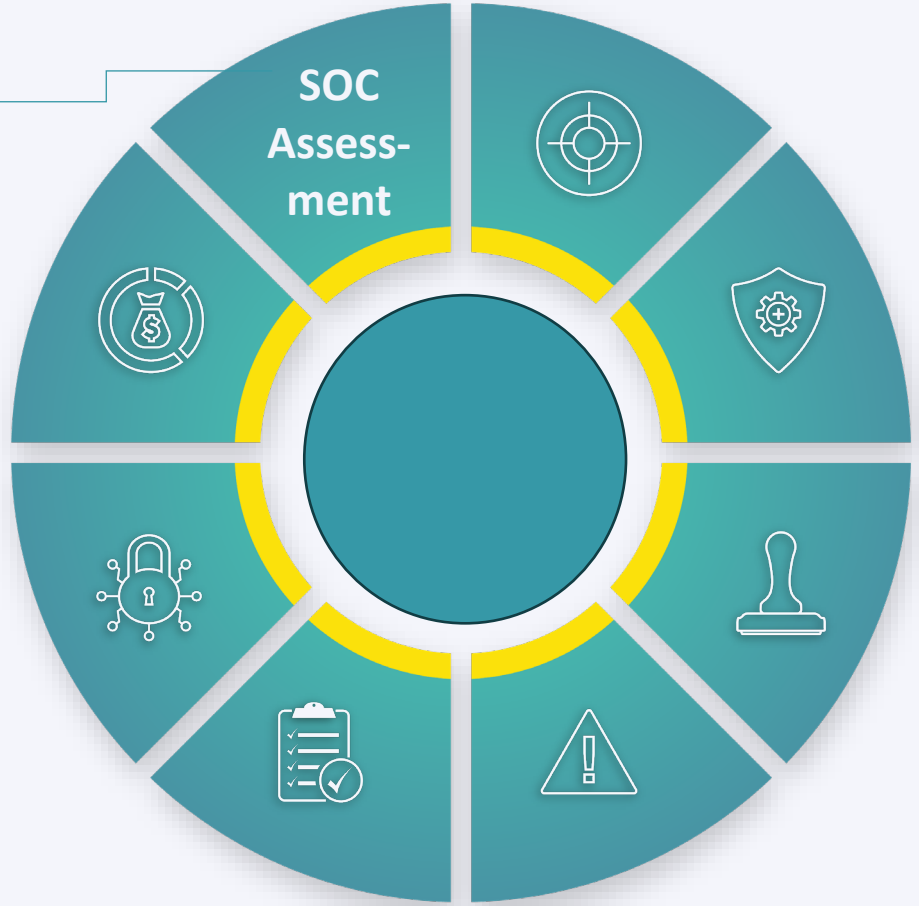
- SOC/Security Assessments
- Stack Optimization
- Threat Analysis
- GRC
- Vuln Management / Prioritization
- Testing
- Detection Engineering
- Threat Hunting

And so many more…

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

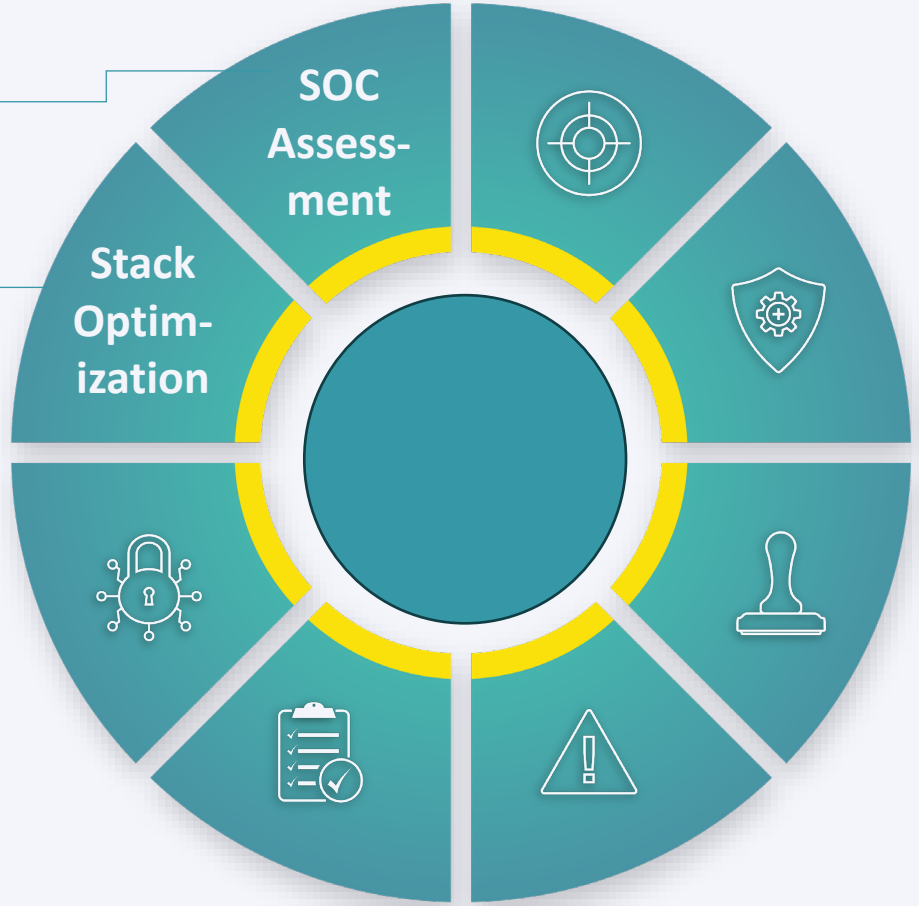


© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.



© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

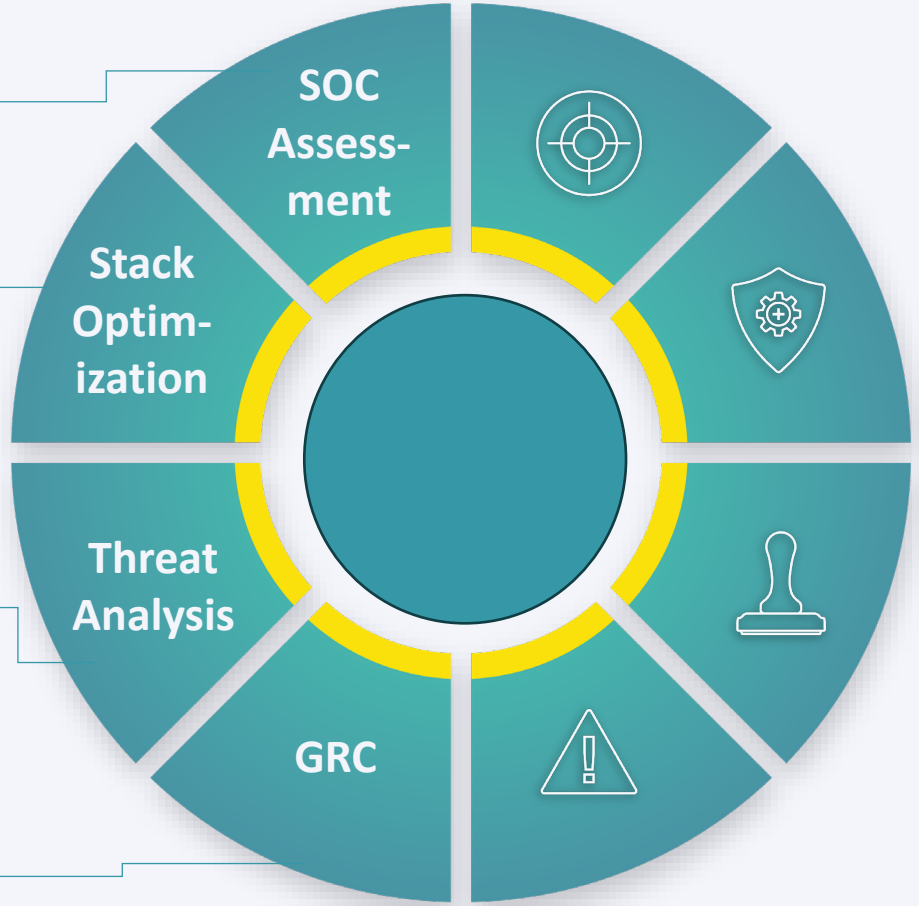
Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

Calculates the security benefit of control standards. Makes value-at-risk finally practical.



© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

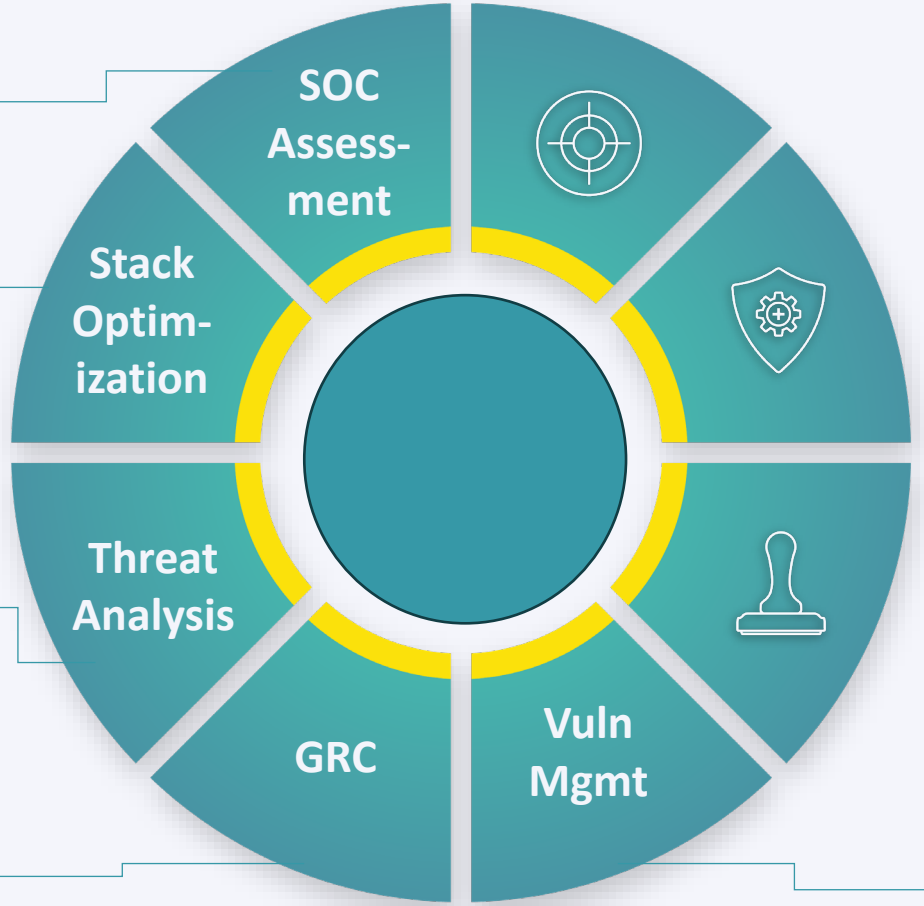
Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

Calculates the security benefit of control standards. Makes value-at-risk finally practical.



Calculates exploitability post-initial access. Eliminates overemphasis on patching.

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

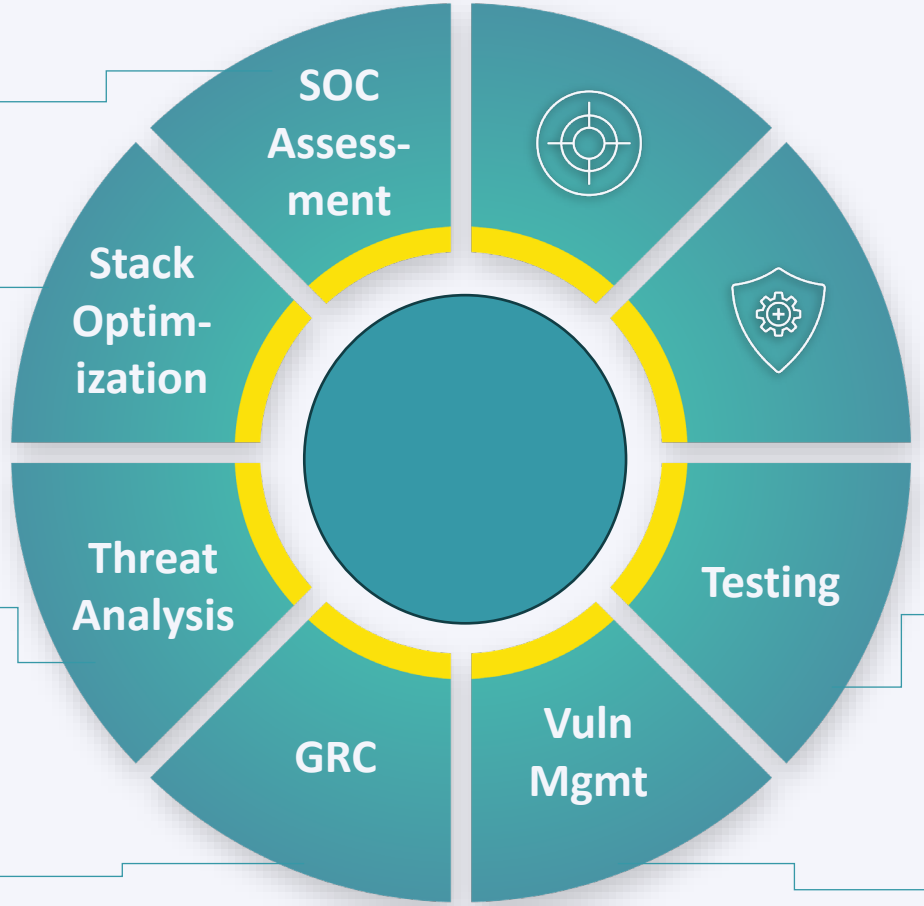
Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

Calculates the security benefit of control standards. Makes value-at-risk finally practical.



Prioritizes testing based on residual risk. Integrates empirical data into efficacy assumptions.

Calculates exploitability post-initial access. Eliminates overemphasis on patching.

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

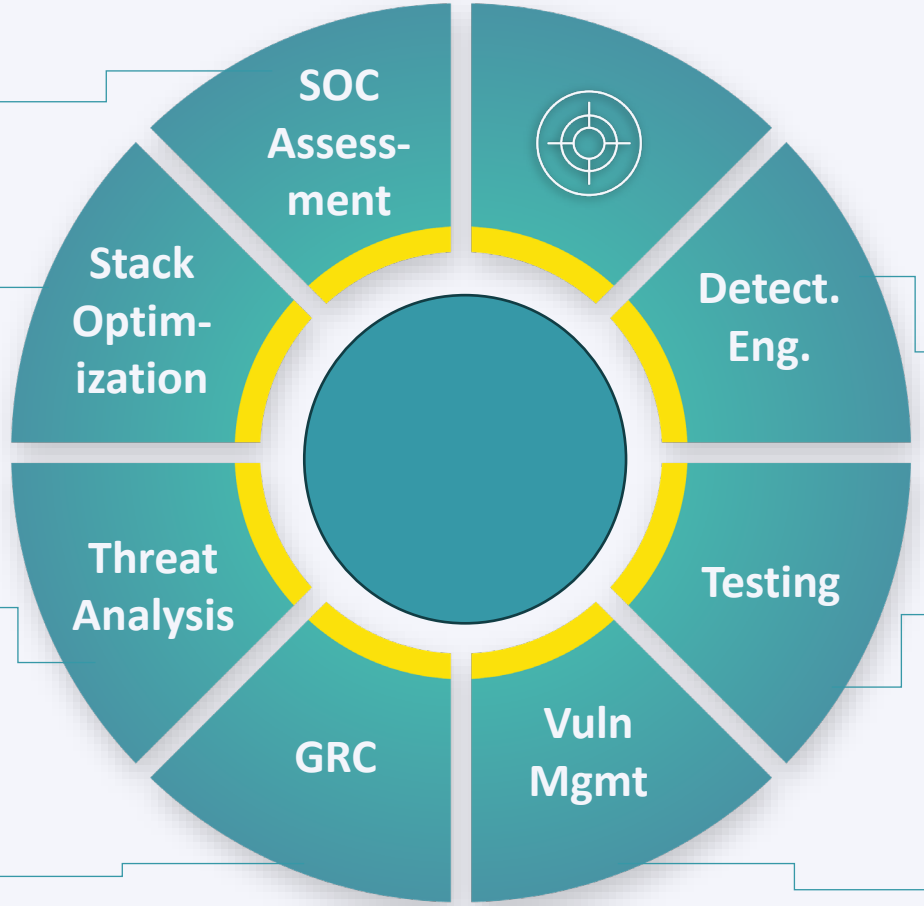
Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

Calculates the security benefit of control standards. Makes value-at-risk finally practical.



Focuses expensive detection engineering resources on most risky threats.

Prioritizes testing based on residual risk. Integrates empirical data into efficacy assumptions.

Calculates exploitability post-initial access. Eliminates overemphasis on patching.

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

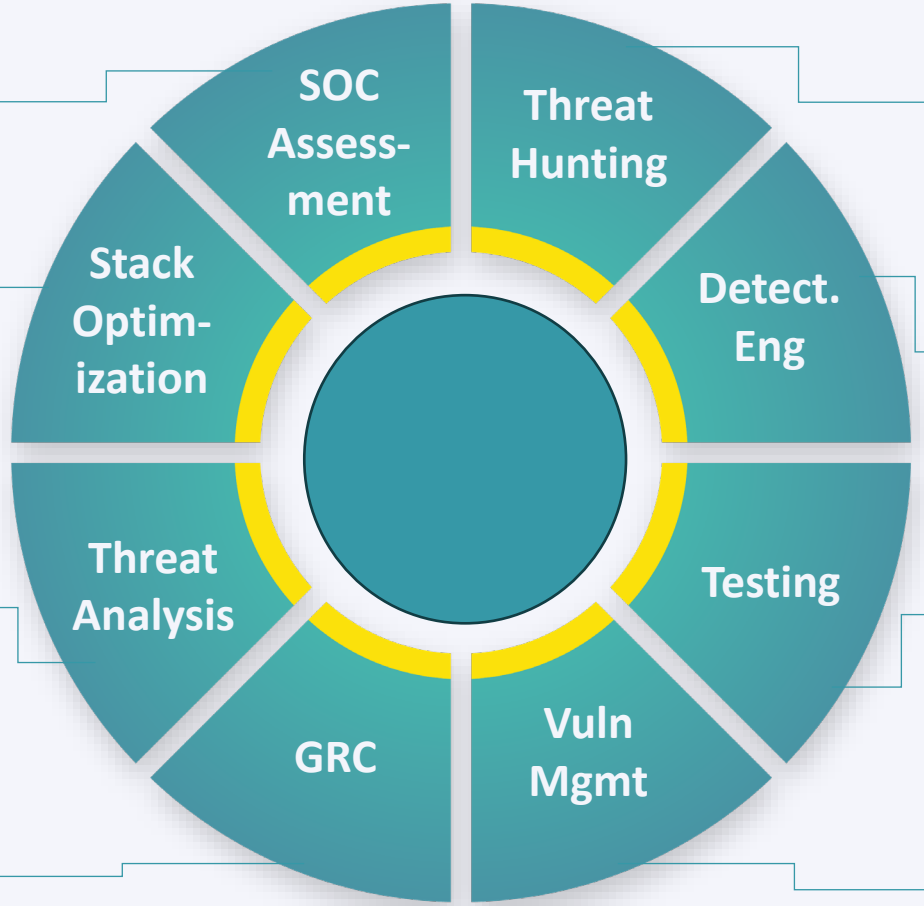
Threat-Informed Defense: Making Sense of the Dots

Eliminates significant expense of coverage analysis.

Identifies unnecessary redundancies and opportunities for savings.

Eliminates expensive grunt work and provides actionable behavioral context

Calculates the security benefit of control standards. Makes value-at-risk finally practical.



Prioritizes hunts toward behaviors that represent greatest risk.

Focuses expensive detection engineering resources on most risky threats.

Prioritizes testing based on residual risk. Integrates empirical data into efficacy assumptions.

Calculates exploitability post-initial access. Eliminates overemphasis on patching.

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Maturing a Threat-Informed Defense Program

TIDAL CYBER

THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

A basic security question:

Can we defend against “X”?

TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

A basic security question:

Can we defend against “X”?

Most of us can’t answer it.

TIDAL CYBER
THREAT-INFORMED DEFENSE

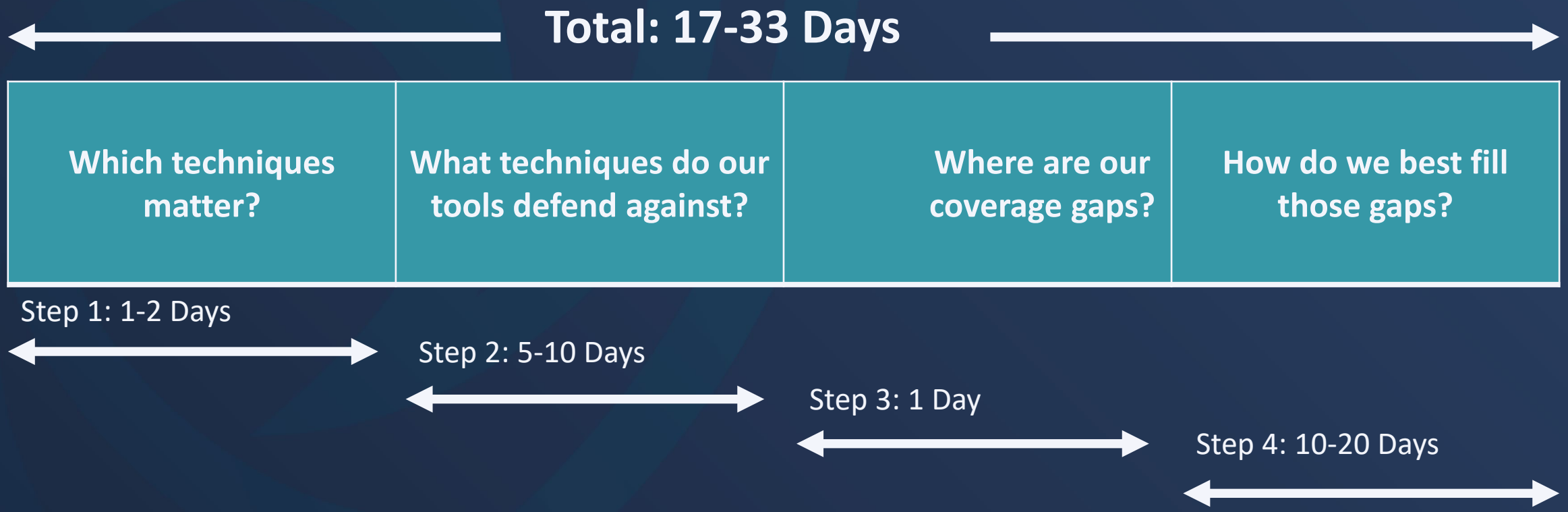
© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

This question is fundamental to security

So why do we struggle to answer it?

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Answering this question is time consuming:



TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Time is money…

The analysis has been prohibitively expensive:

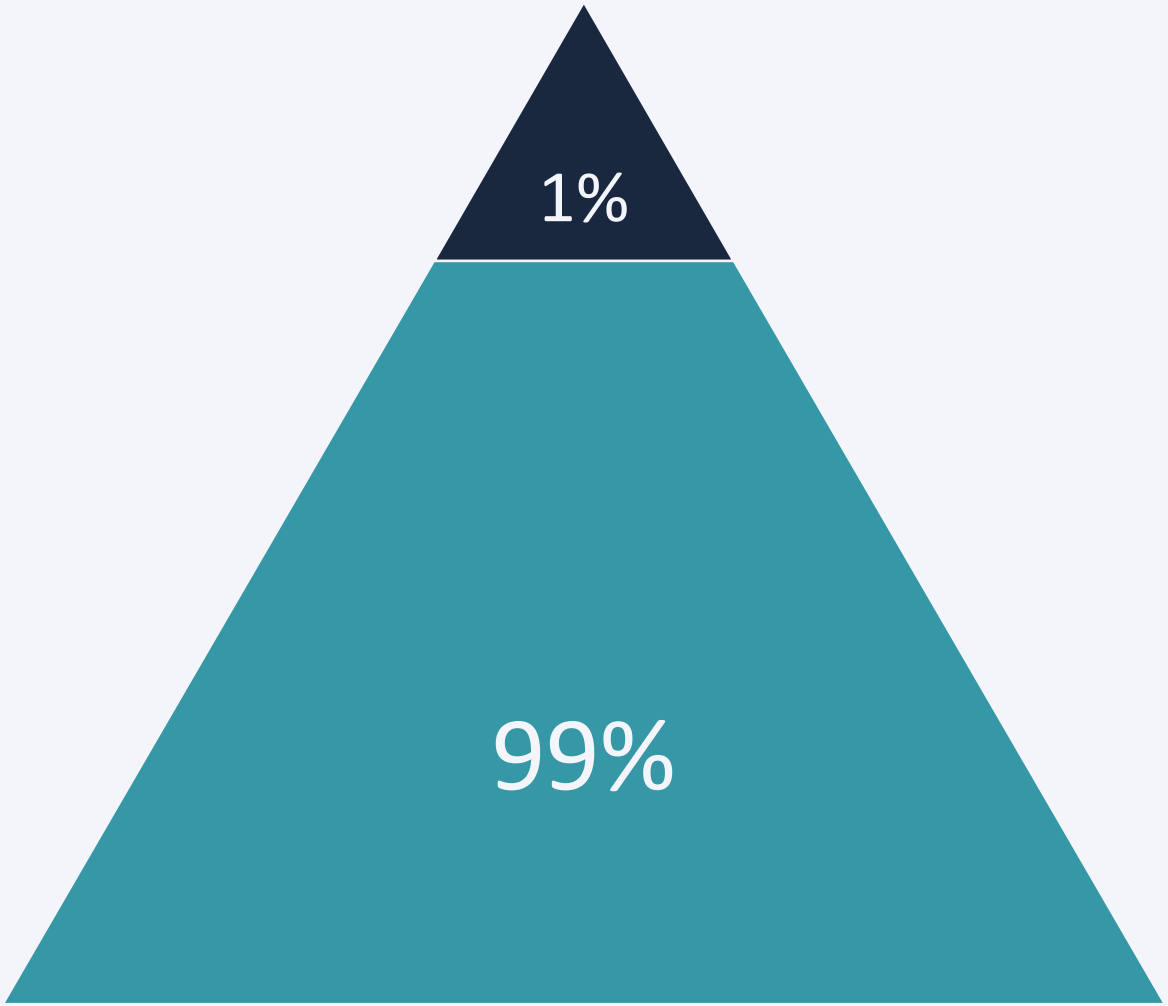
$680K - $1.3M

$100/hr x 17-33 days x 8 hours/day x 50 threats

- Repeat as threats evolve
- Update for new products/feature releases
- Repeat periodically (annually)

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

What is actually happening?



Top 1%

- Coverage Mapping
- Annual and Manual
- Spreadsheets and Weekends
- $$$$

Most of us

- Guess
- Convince ourselves we know

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Stop Guessing

Threat-Informed Defense makes knowing practical

- ✓ Prioritize TTPs that matter most
- ✓ Identify important coverage gaps
- ✓ Recommend the most impactful actions
- ✓ Evolve automatically as adversaries and products evolve

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

A New Approach to Security

The traditional focus on vulnerabilities isn't sufficient for defenses anymore.

Threat-Informed Defense looks at your enterprise from the perspective of the adversary, giving critical insights into how to prioritize your security operations and investments.

Shrink weeks of work into minutes and save time and money.

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Why can’t we answer this basic question?

Threat Intelligence

Most of us don’t know:

- If “X adversary” is targeting us
- What techniques adversary “X” has been using
- If our intelligence is specific enough
- Which techniques are riskier/more important

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

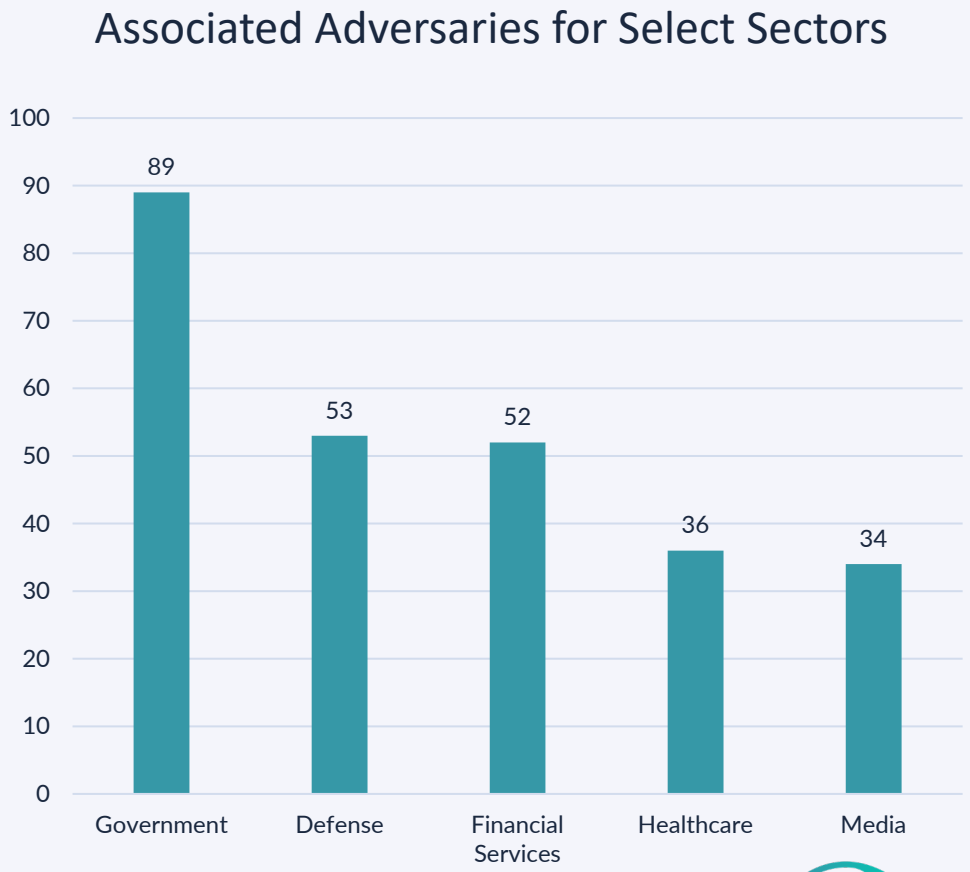
Solution: Threat Profiling

Full methodology: tidalcyber.com/ultimate-guide-to-cyber-threat-profiling

Sector- & geography-based profiling

Refine further (or expand) with:

- Tool & TTP count, density, & importance (Capability)
- Adversary Type, Motivation, Sub-sector (Capability & Intent)
- Reference date (Recency)
- Reference count (Prominence)



TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Why can’t we answer this basic question?

Defensive Intelligence

Most of us don’t know:

- **What techniques are our tools capable of defending against**
- **Whether those capabilities are configured**
- **How effective are those capabilities**
- **The incremental impact of each capability**

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Solution: Defensive Stacking

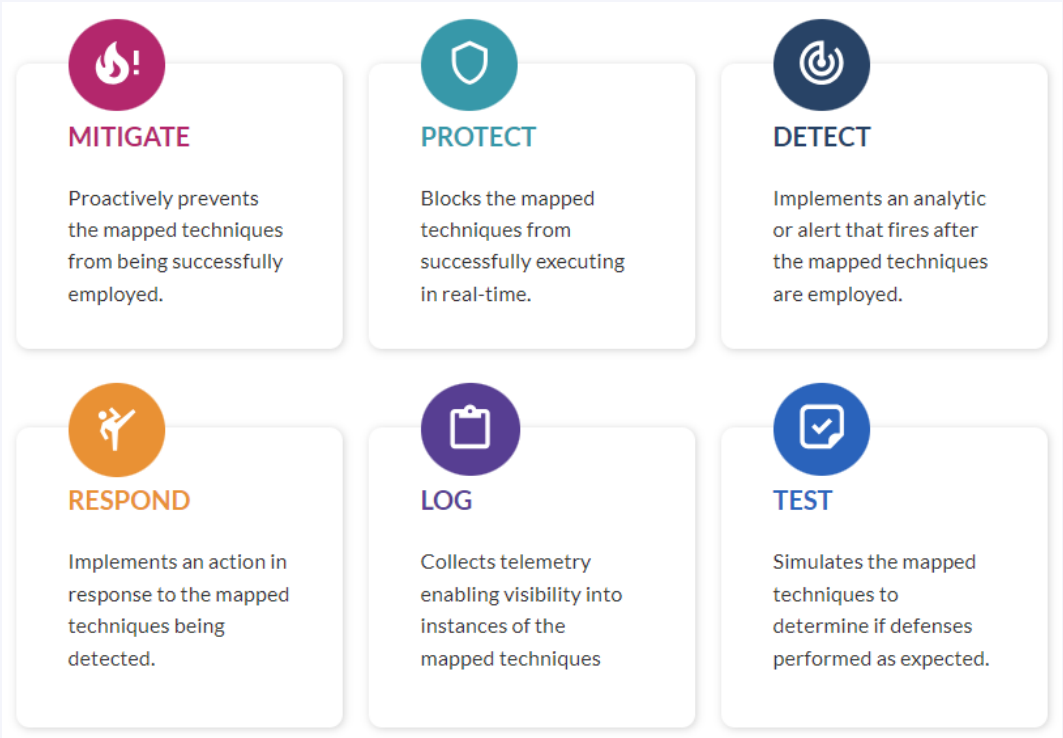
Vendor ATT&CK mapping has increased dramatically: app.tidalcyber.com/vendors

Model defenses *across the spectrum* of capability types

Further granularity via weighting by:

- Tactic & Technique importance
- Capability Type
- Configuration state (default vs. custom)
- Capability effectiveness

Primary Defensive Capability Types



TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Putting it all Together

THREAT PROFILING

THREAT OBJECTS	WEIGHTED TECHNIQUES
Groups	*examples*
Software	Phishing
Campaigns	Drive-by
	Brute Force
	Input Cap
	Net Sniff
	Unsec Cred

Knowledge Base
(Updated/Enhanced ATT&CK Data)

Assess

COVERAGE MAPPING

Calculates residual risk for each technique

DEFENSIVE STACKING

PRODUCT INTEGRATIONS

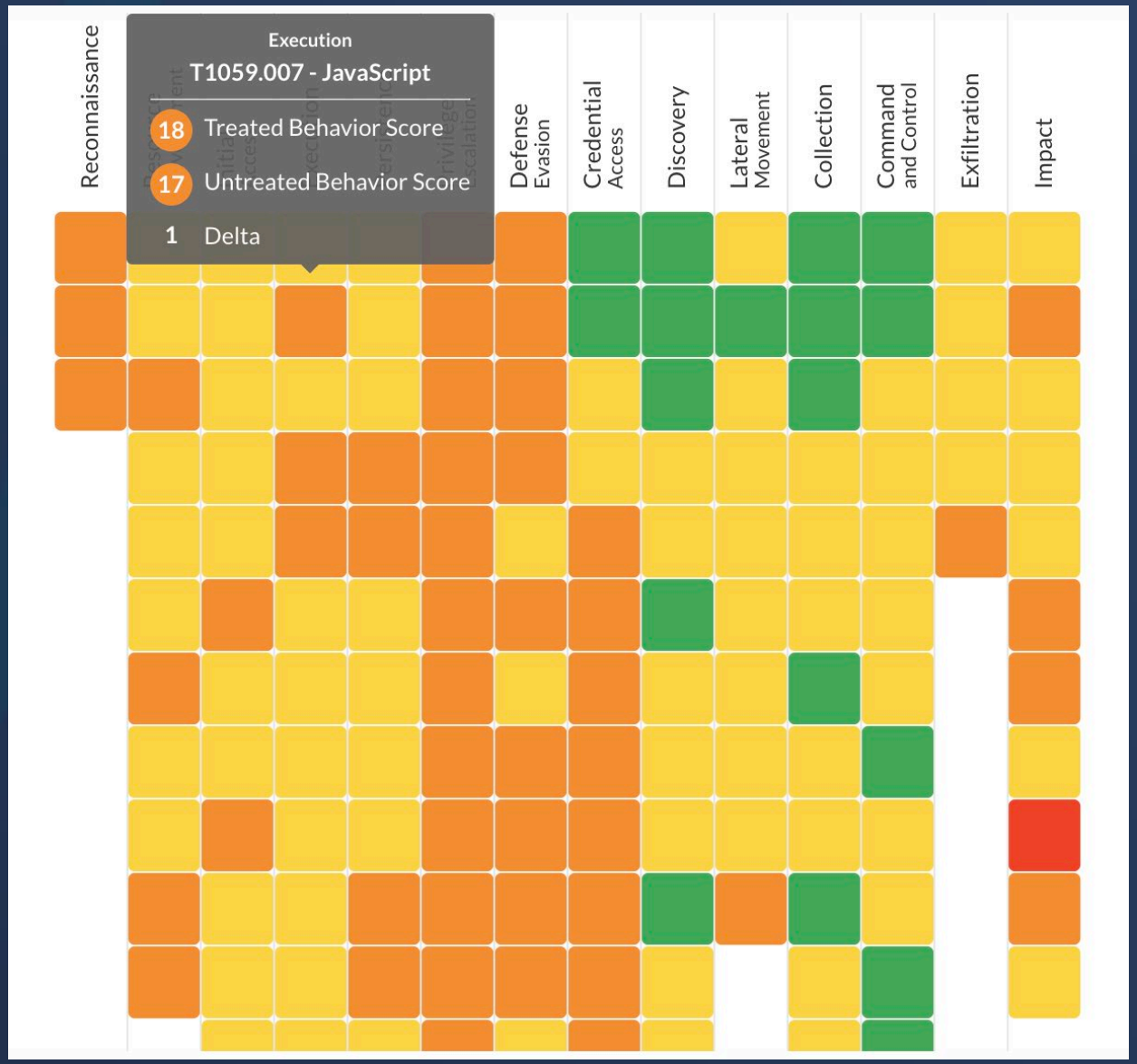
SIEM EDR Analytics Other

Capability Registry
(>15,000 capabilities shared by vendors and valuable analytics)

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Coverage Mapping

- Coverage that is personal
  - ATT&CK is not checkboxes
  - ATT&CK is not a bingo card
- Understand inherent risk
- Automatically calculate residual risk across every technique
- Illuminate high residual risk for prioritization



© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

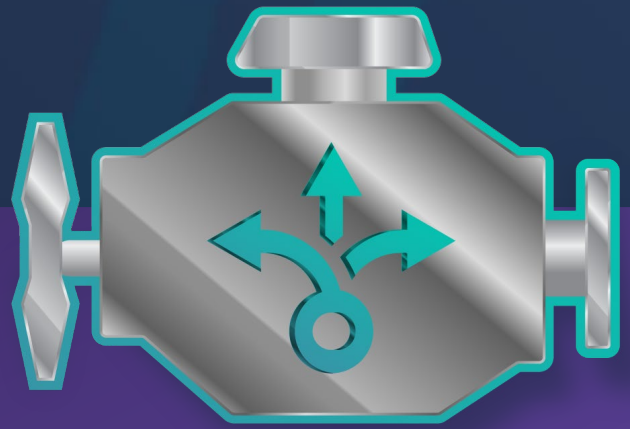
Putting it all Together

THREAT PROFILING

THREAT OBJECTS	WEIGHTED TECHNIQUES
Groups	*examples*
Software	Phishing
Campaigns	Drive-by
	Brute Force
	Input Cap
	Net Sniff
	Unsec Cred

Knowledge Base
(Updated/Enhanced ATT&CK Data)

Improve



RECOMMENDATION ENGINE

Automatically identifies best actions to take

DEFENSIVE STACKING

PRODUCT INTEGRATIONS

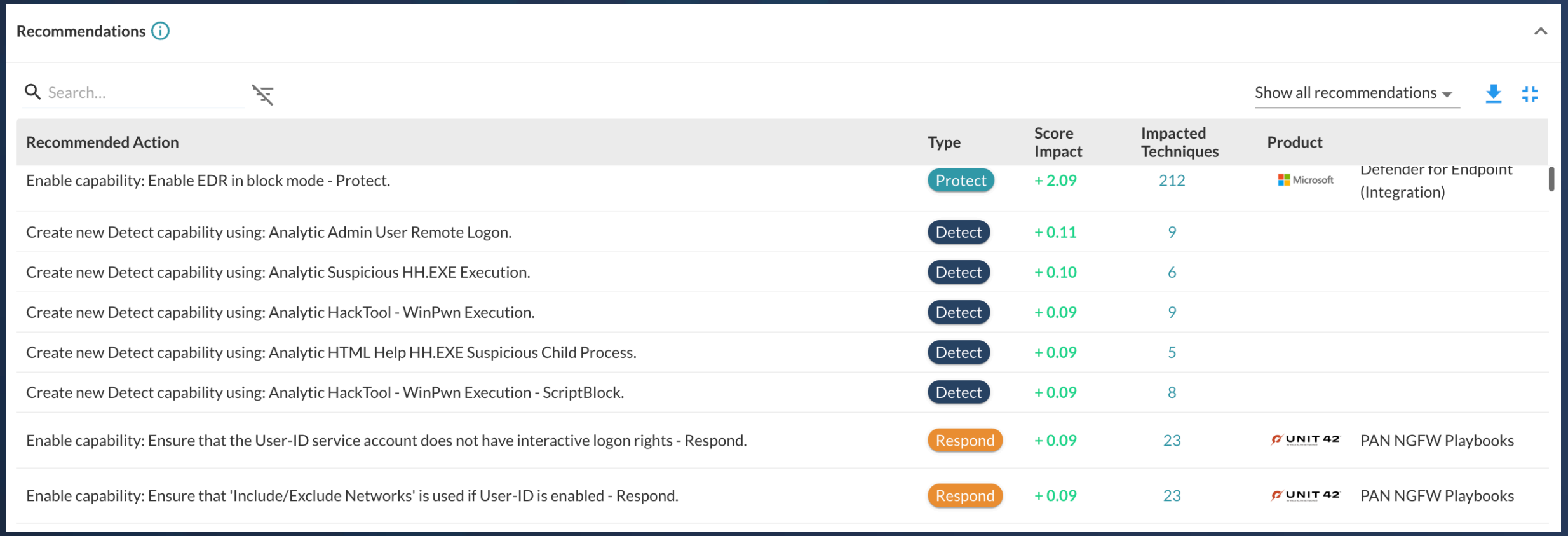
SIEM | EDR | Analytics | Other

Capability Registry
(>30,000 capabilities shared by vendors and valuable analytics)

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Automated Recommendation Engine

- Prioritize actions based on the reduction of residual risk

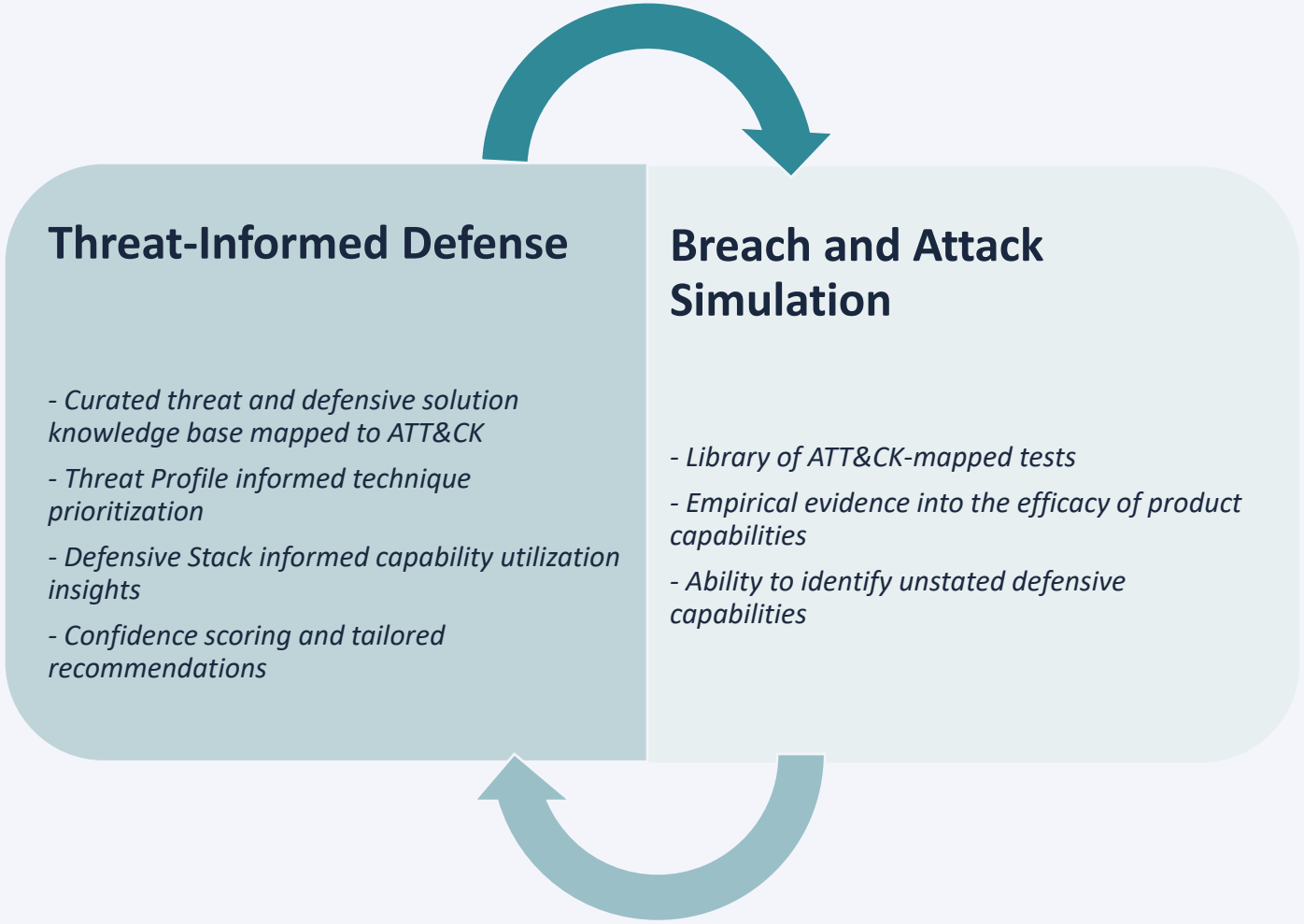


Recommended Action	Type	Score Impact	Impacted Techniques	Product	
Enable capability: Enable EDR in block mode - Protect.	Protect	+ 2.09	212	Microsoft	Defender for Endpoint (Integration)
Create new Detect capability using: Analytic Admin User Remote Logon.	Detect	+ 0.11	9		
Create new Detect capability using: Analytic Suspicious HH.EXE Execution.	Detect	+ 0.10	6		
Create new Detect capability using: Analytic HackTool - WinPwn Execution.	Detect	+ 0.09	9		
Create new Detect capability using: Analytic HTML Help HH.EXE Suspicious Child Process.	Detect	+ 0.09	5		
Create new Detect capability using: Analytic HackTool - WinPwn Execution - ScriptBlock.	Detect	+ 0.09	8		
Enable capability: Ensure that the User-ID service account does not have interactive logon rights - Respond.	Respond	+ 0.09	23	UNIT 42	PAN NGFW Playbooks
Enable capability: Ensure that 'Include/Exclude Networks' is used if User-ID is enabled - Respond.	Respond	+ 0.09	23	UNIT 42	PAN NGFW Playbooks

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Better Together

Threat-Informed Defense and Breach and Attack Simulation

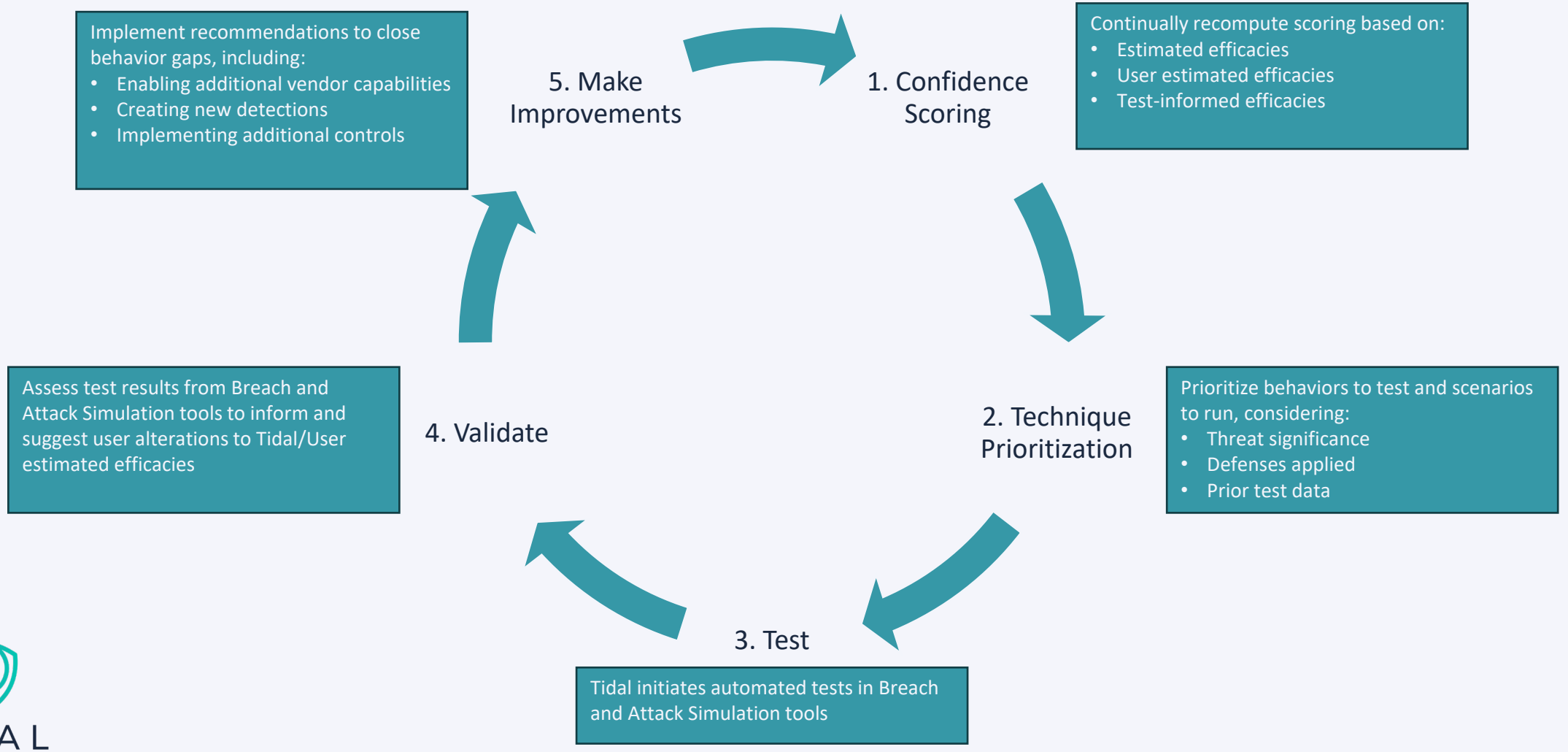


TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

BAS / Test Lifecycle

Improve Confidence Accuracy with Testing



TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Why Keep Guessing?

TIDAL CYBER

THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL

Thank You!

- Tidal Community Edition: app.tidalcyber.com
- Threat Profiling Guide: tidalcyber.com/ultimate-guide-to-cyber-threat-profiling
- Tidal Blog: tidalcyber.com/blog
- Engage with Us!
  - **Tidal Community Slack**
  - **LinkedIn**: Tidal Cyber / Frank Duff
  - **Twitter/X**: @TidalCyber / @frankduff
  - **Email**: contact@tidalcyber.com

TIDAL CYBER
THREAT-INFORMED DEFENSE

© 2023 Tidal Cyber, Inc. All rights reserved | CONFIDENTIAL