Agile and Continuous Improvement Using ATT&CK

Matt Stiak

Jason Sinchak

We are the security “everyman”

Resources

Logs

Blue team structure

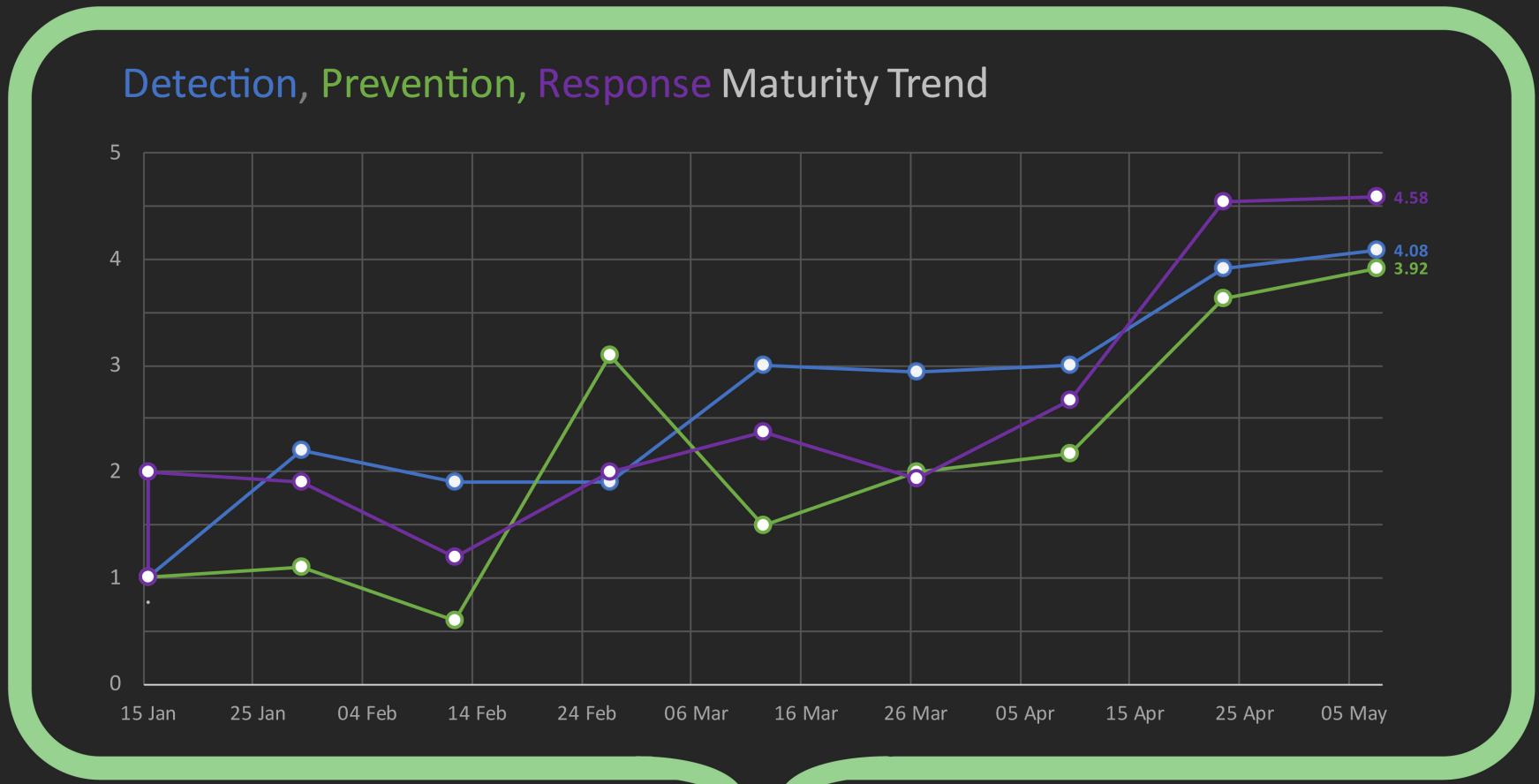
Not scrum masters

Don’t think agile is fun

Shiny objects

The Big Idea

Use ATT&CK to test and improve security. Just like the big players.



What We Wanted

Untangling Reality

Identifying and overcoming obstacles to wider adoption.

Why you can't implement ATT&CK at your company...

The New Way vs The Old Way

Identifying Barriers **Structure Becomes Restricting**

Identifying Barriers
Education Requirements

Identifying Barriers **Resources and Time Management**

How you can overcome all that and implement ATT&CK at your company...

ATT&CKing Barriers

#1 **Use agile to your advantage.**

Agile helps you manage a frantic stop-and-start pace without disrupting progess.
(or your sanity)

Building blocks

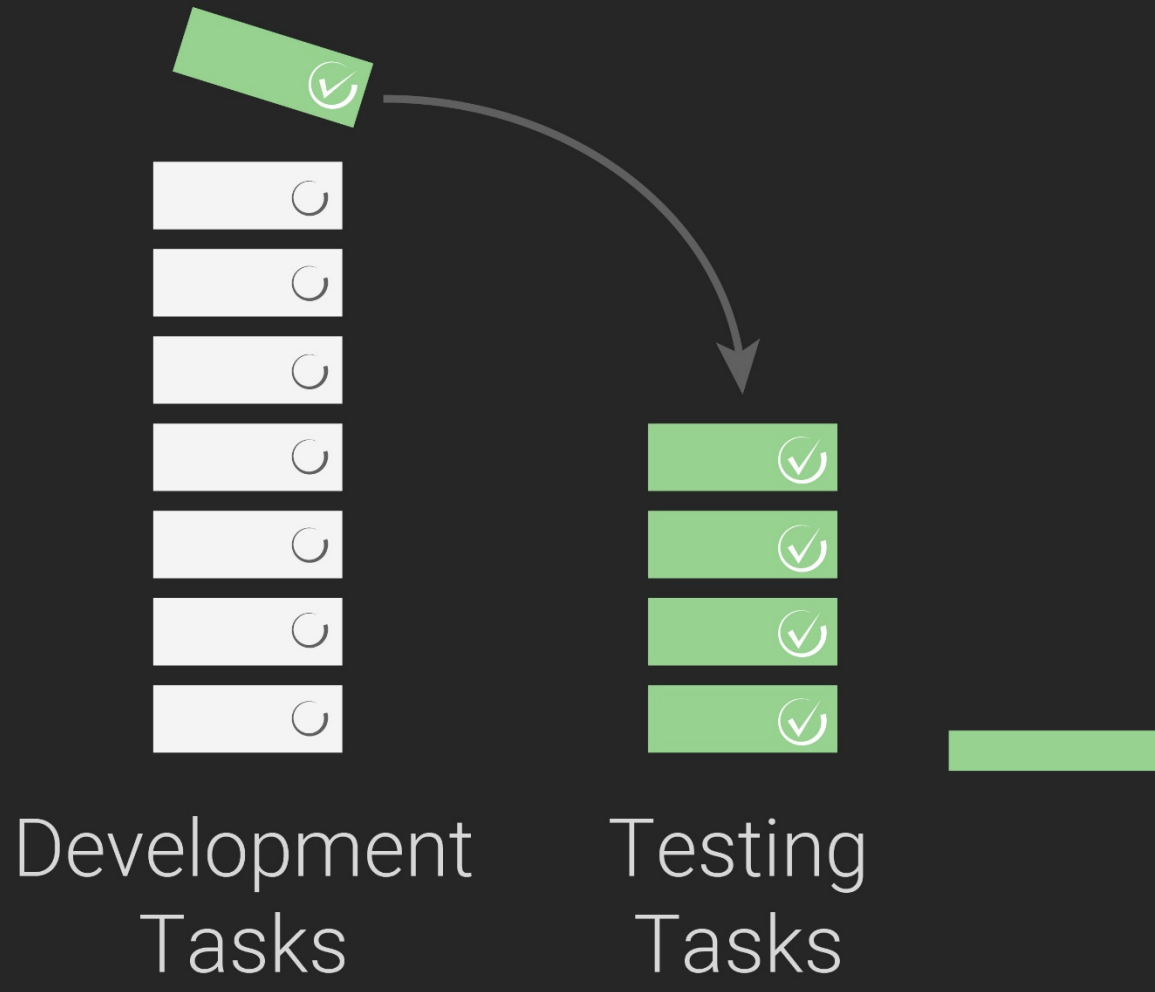
Content

Data

Model

Architecture

Micro-Purple



Building blocks

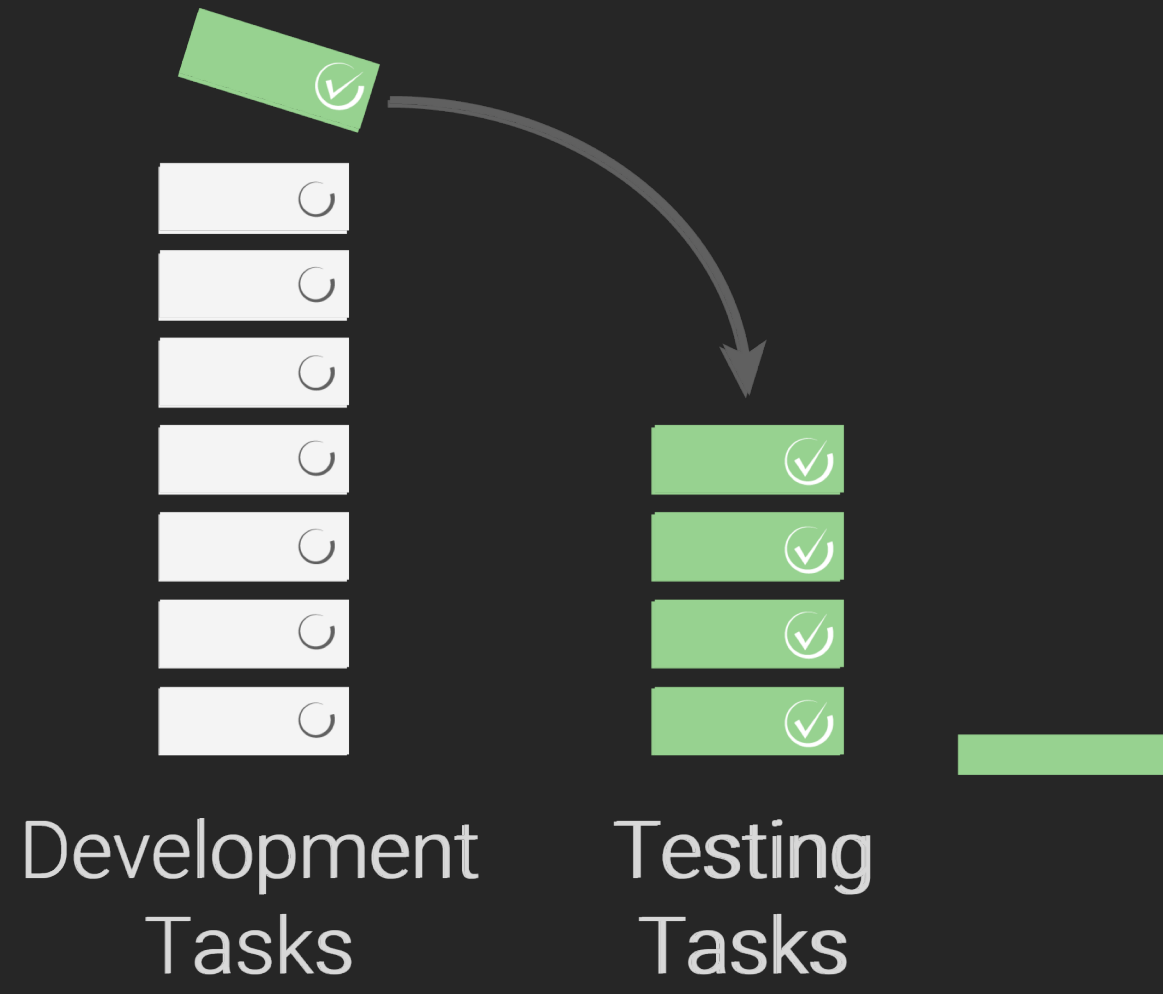
Content

Data

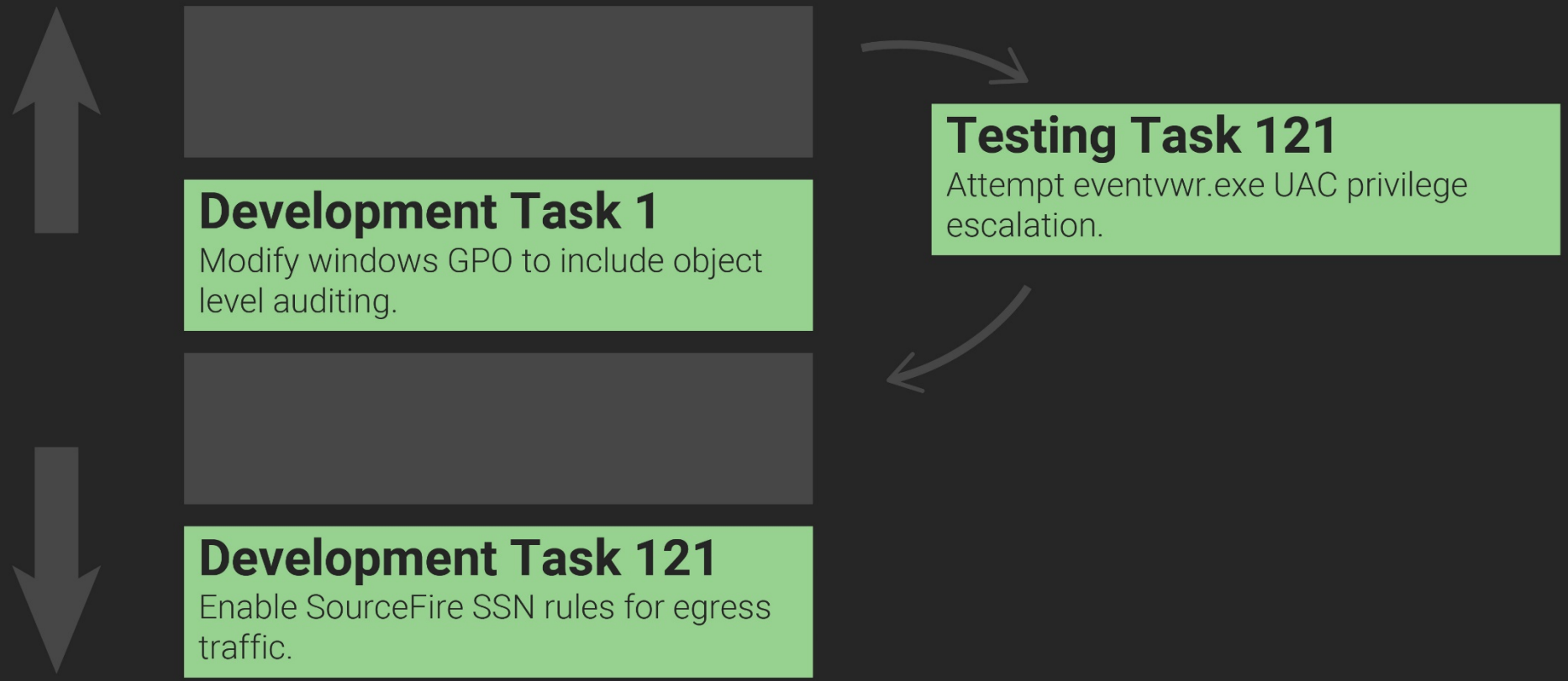
Model

Architecture

Micro-Purple



Populating and grooming the backlog



Winning over the skeptics

ATT&CKing Barriers

#2 Create “micro” purple teams.

Test everything without blowing your red team budget.

Key micro purple features

In-house

Iterative

Low-sophistication

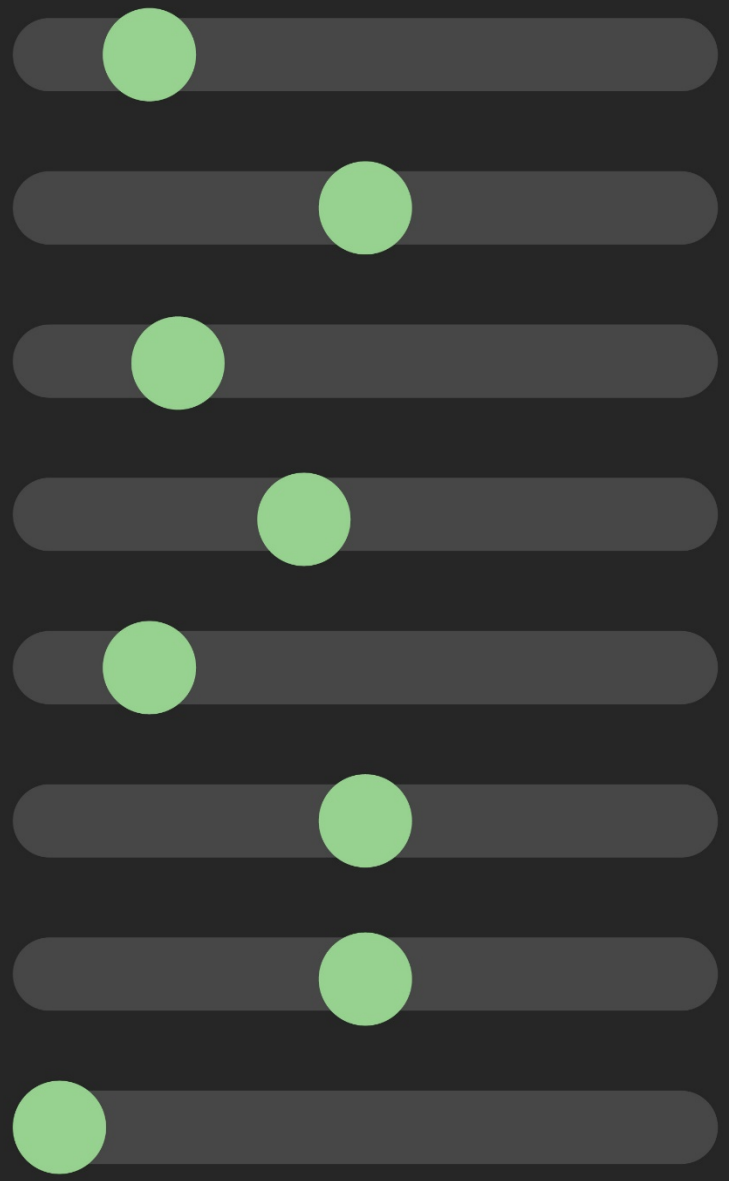
Low-cost

Derive confidence in capabilities by scoring observations about monitoring, preventing, detecting.

ATT&CKing Barriers

#3 **Let the metrics show the way.**

Scoring
Monitoring

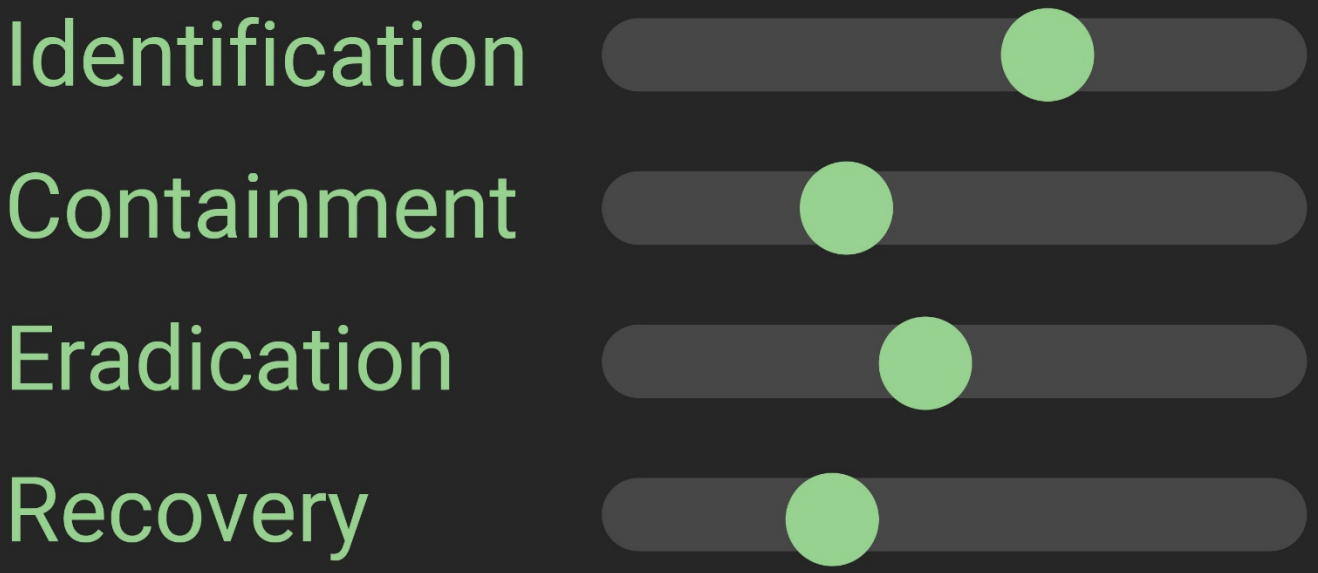


Scoring
Prevention

Result

Complexity

Scoring
Response




Finally have a simple,
evidence-based way to answer:
“Could that happen to us?”

It’s not all or nothing.

Go at your own pace.

Expect interruptions.