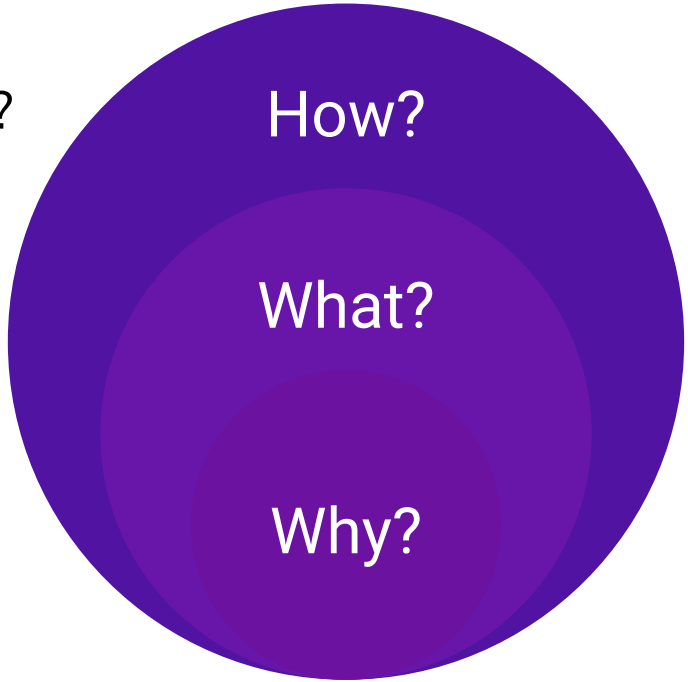
Purple Maturity Model

Tim Schulz - @teschulz
Adversary Emulation Lead

Roadmap

3. How can we use it?



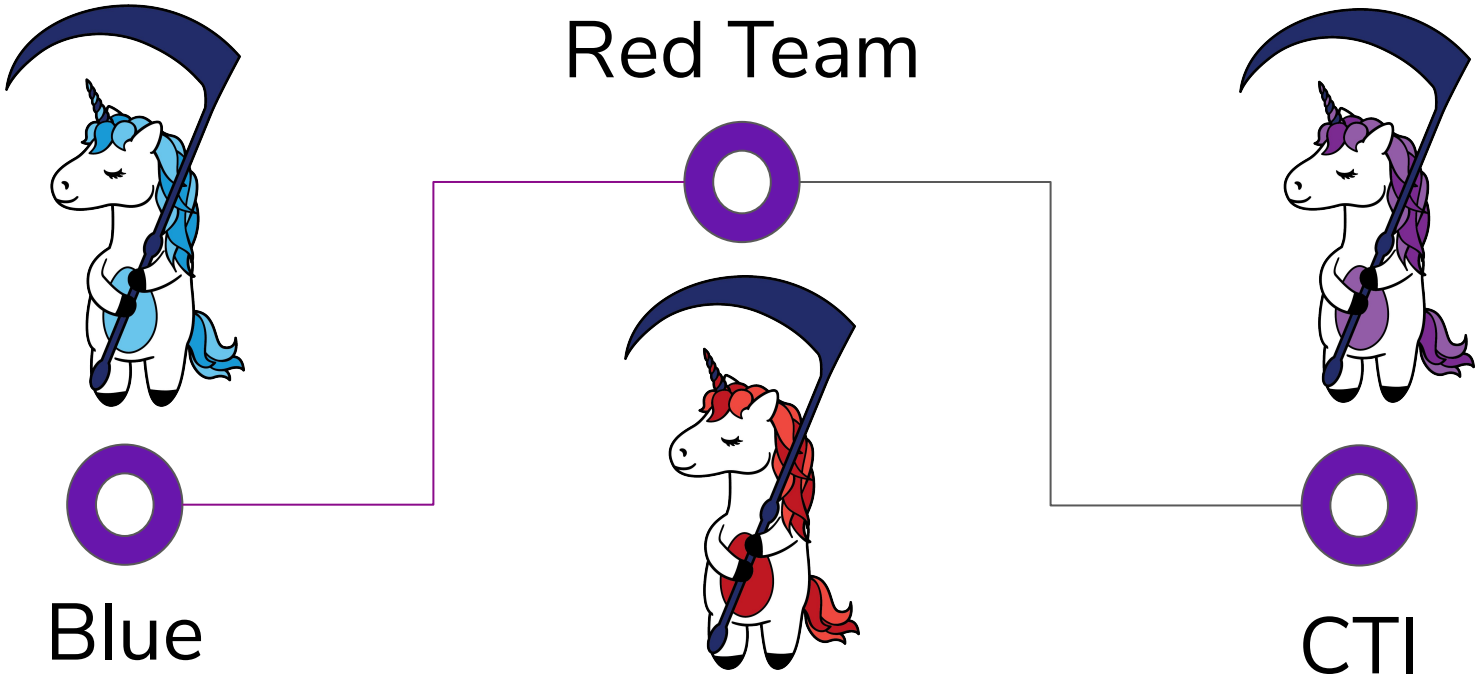
2. What is the maturity model?

1. Why does purple need a maturity model?

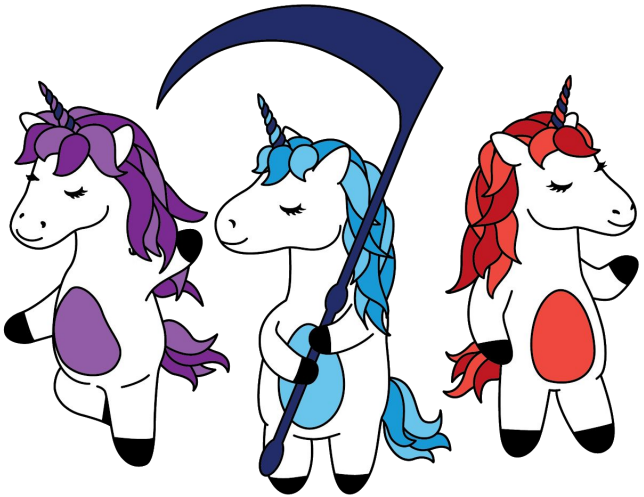
Roadmap

1. Why does purple need a maturity model?

Infosec Teams of Today



Infosec Teams of Tomorrow

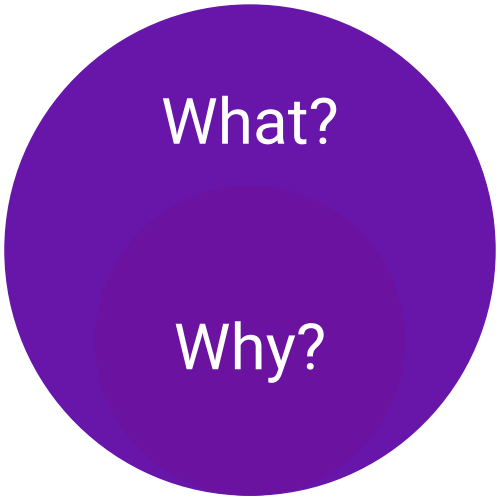


Challenges with current landscape

- Teams develop capability independently
- Communication and cooperation between teams is optional
- Purple teaming is a singular event or exercise

Fundamentally different mentality than red and blue teams

Roadmap



2. What is the maturity model?

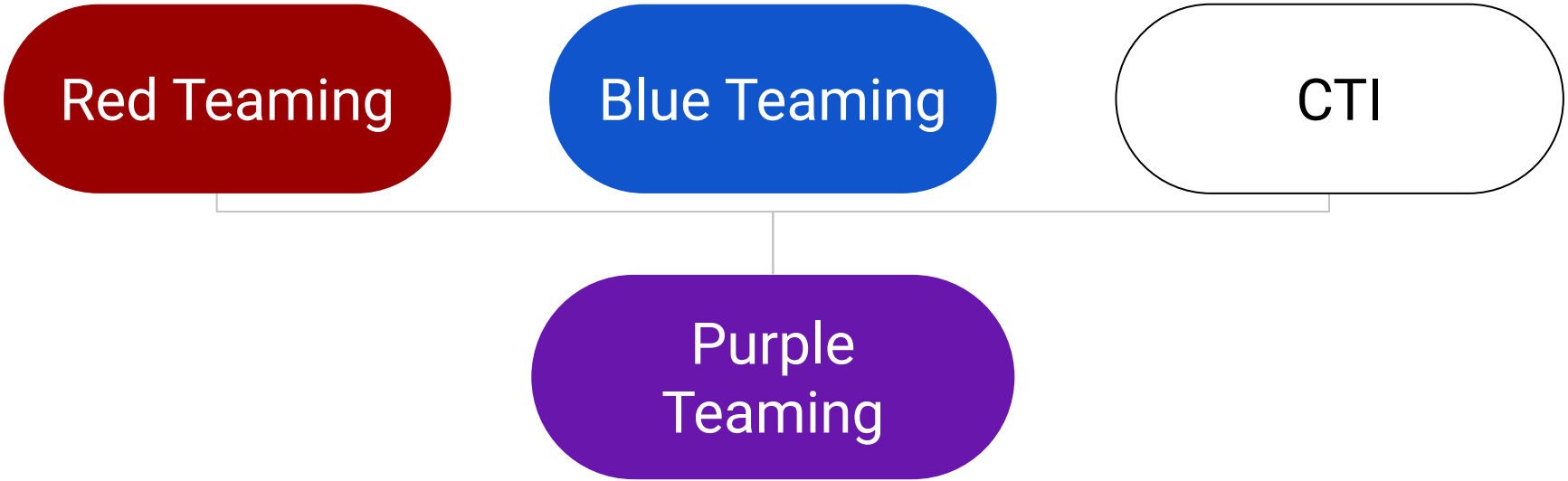
The Purple Story

Red Teaming

Blue Teaming

CTI

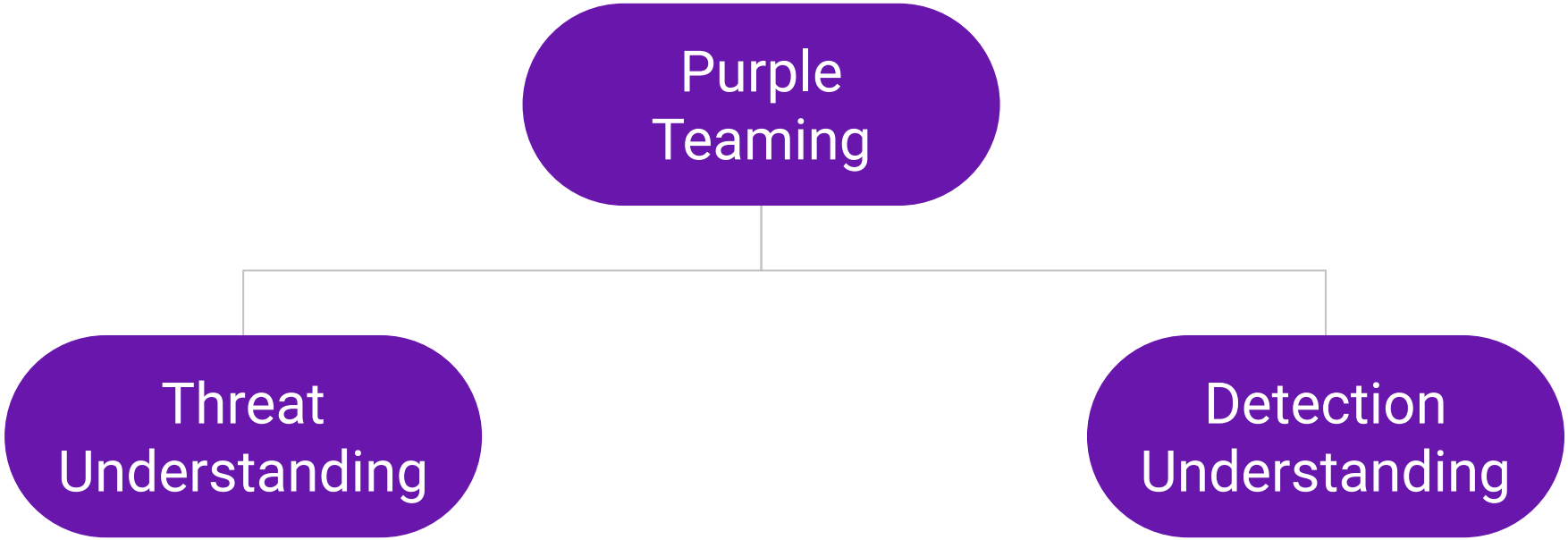
The Purple Story



The Purple Story

Purple Teaming

The Purple Story



Goals for the Breakdown

Threat Understanding

Detection Understanding

- Make the categories easily understandable
- Clear enough that people with current expertise can understand where they fall between them
- General enough that broader context will not be lost by those focused on one area

Detection Understanding

- What log and telemetry data sources do we have?
- What is the process for creating new detections and/or alerts?
- What is our escalation process?
- What detections have been validated?
- Are we lacking any visibility?

Detection Understanding

Threat Understanding

Threat Understanding

- What techniques are adversaries using to target our industry?
- What procedural variance could an adversary use to get around our detections?
- What detections have been validated?
- Are we lacking any test coverage?

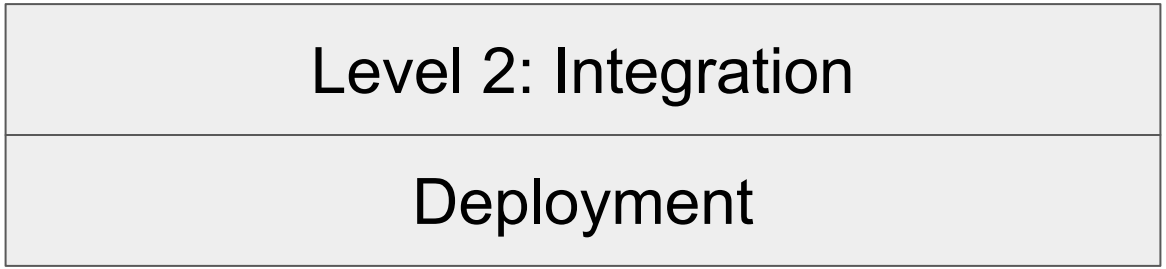
Building our model: Level 1

Level 1: Deployment

Threat Understanding

Detection Understanding

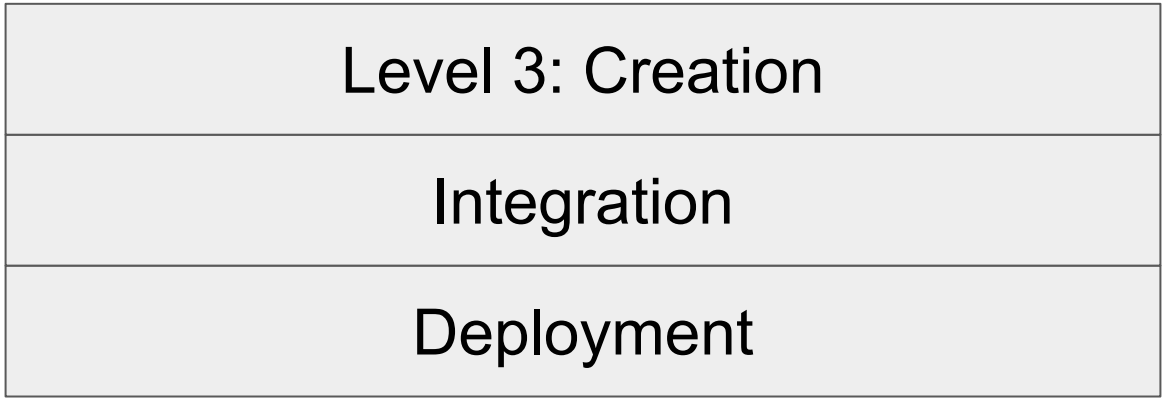
Building our model: Level 2



Threat Understanding

Detection Understanding

Building our model: Level 3

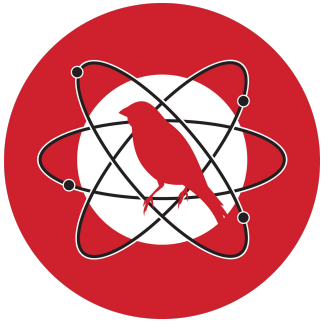


Threat Understanding

Detection Understanding

Project Examples

https://github.com/SigmaHQ/sigma



Atomic Red Team

https://atomicredteam.io

Detection Understanding Example: Sigma

Creation

Integration

Deployment

Deploying SIGMA rules in SIEM

Detection Understanding

SCYTHE

Detection Understanding Example: Sigma

Integrating SIGMA rules into sandbox testing pipeline

Deploying SIGMA rules in SIEM

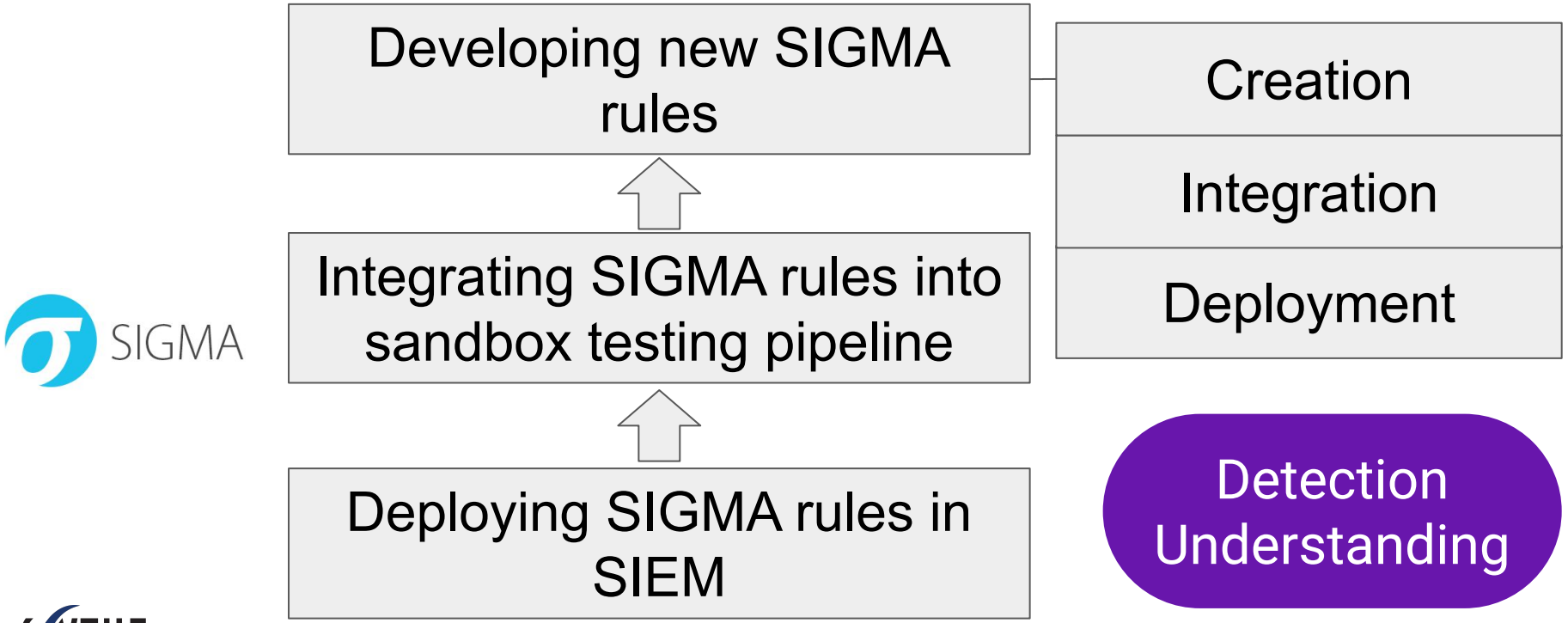
Creation

Integration

Deployment

Detection Understanding

Detection Understanding Example: Sigma



Threat Understanding Example: ART

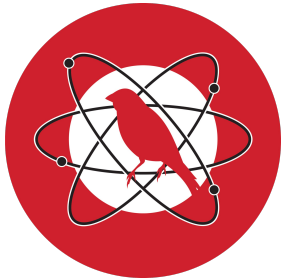
Creation

Integration

Deployment

Threat Understanding

Using ART to test detections



SCYTHE

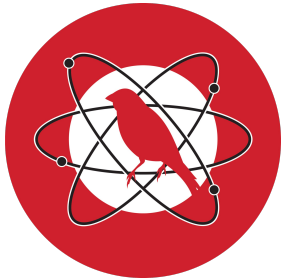
Threat Understanding Example: ART

Creation

Integration

Deployment

Integrating ART into detection development pipeline

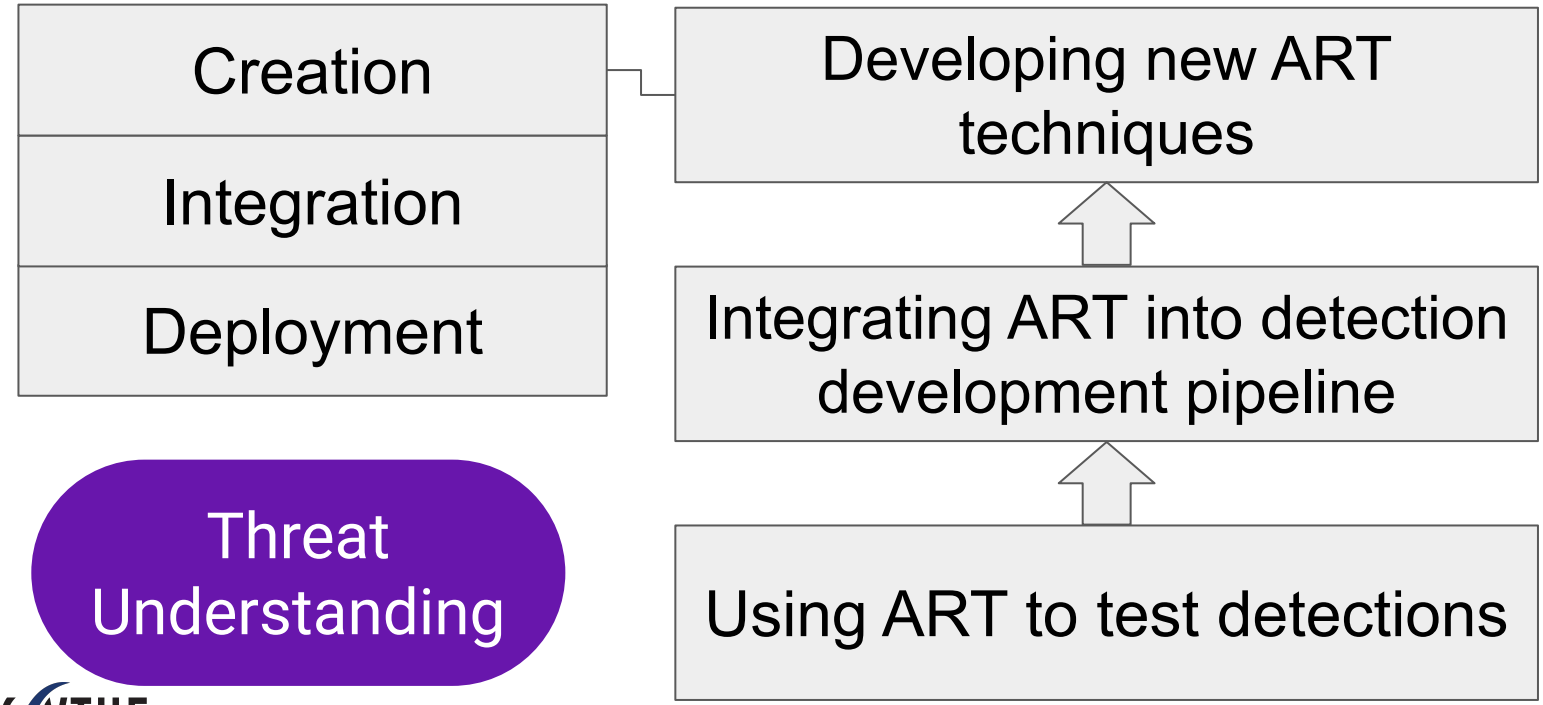


Threat Understanding

Using ART to test detections

SCYTHE

Threat Understanding Example: ART



Foundation in Communication & Collaboration

Communication is an assumption

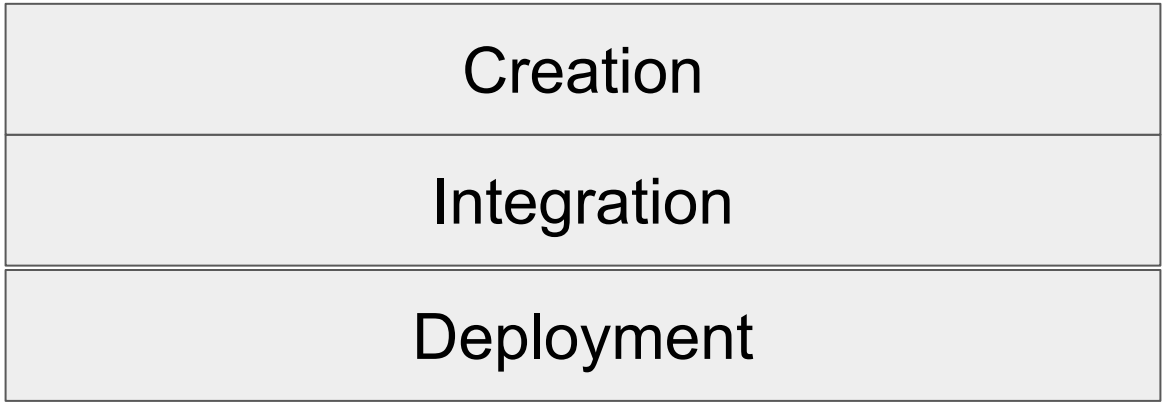
Communication and Collaboration are core

“You are one team”

Responsible for communicating your purple team vision

Communication!

Purple Maturity Model

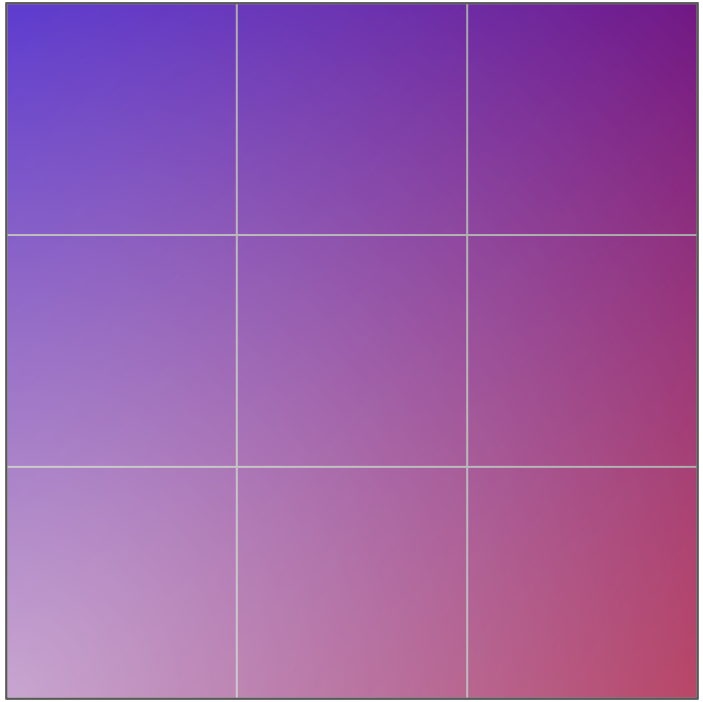


Threat Understanding

Detection Understanding

Purple Maturity Model

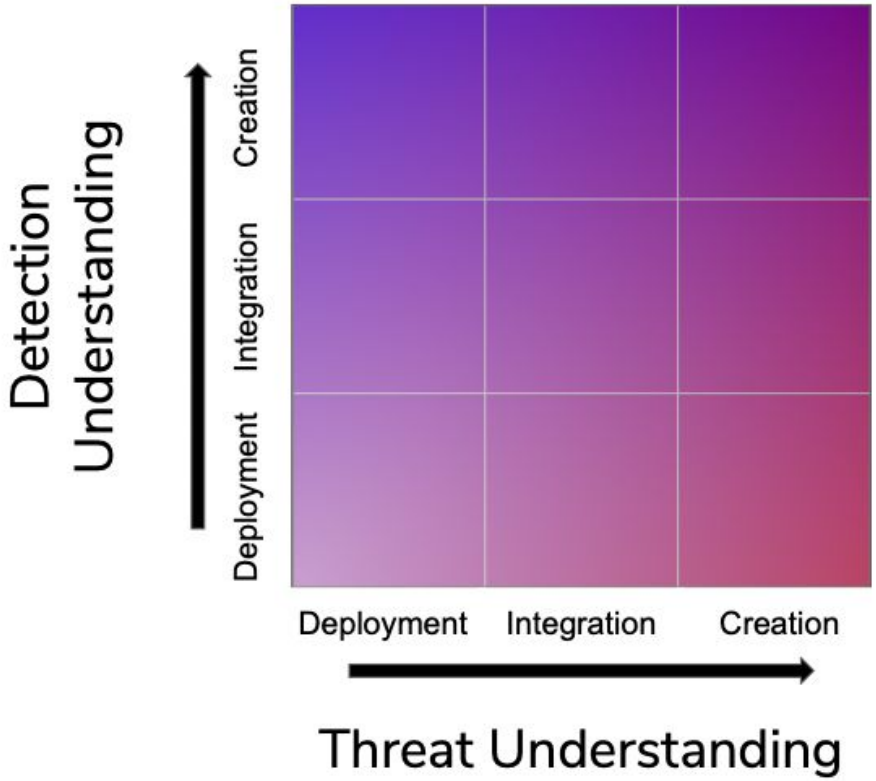
Detection Understanding



Threat Understanding

SCYTHE

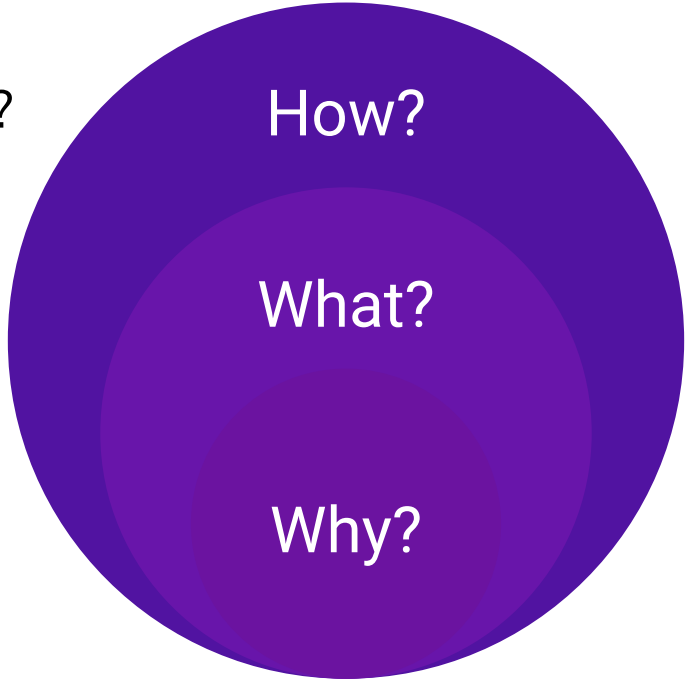
Purple Maturity Model



SCYTHE

Roadmap

3. How can we use it?



Introducing Unicorn Inc

Alex - Blue

Brooke - Red

Casey - CTI

Introducing Unicorn Inc

Alex - Blue

- Builds new detections based based on latest IOCs from Casey's emails

Introducing Unicorn Inc

- Uses the latest and greatest Windows red team tooling and AMSI bypasses from Twitter

Brooke - Red

Introducing Unicorn Inc

Casey - CTI

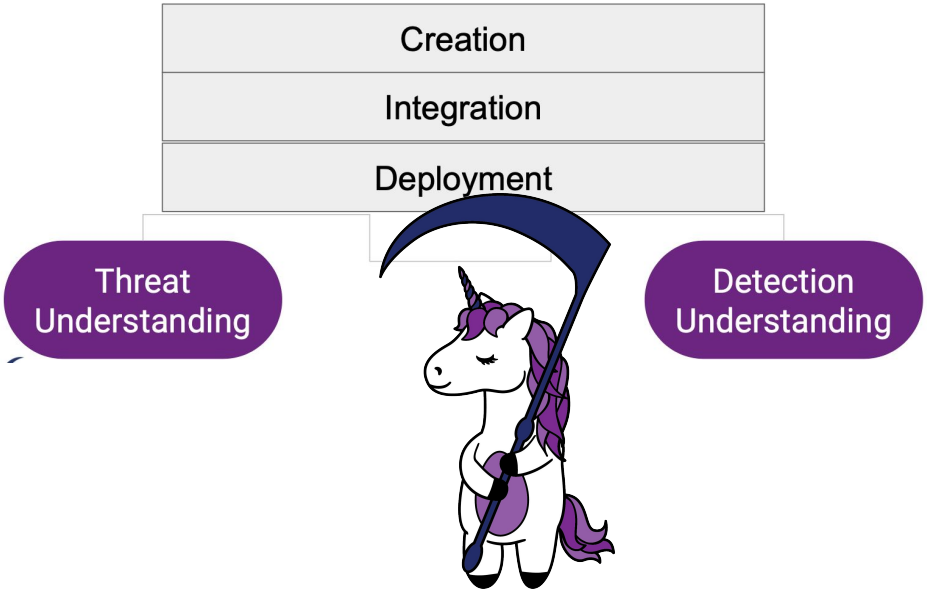
- Reads every CTI vendor’s threat report

Building a roadmap

Brooke

Casey

Alex



SCYTHE

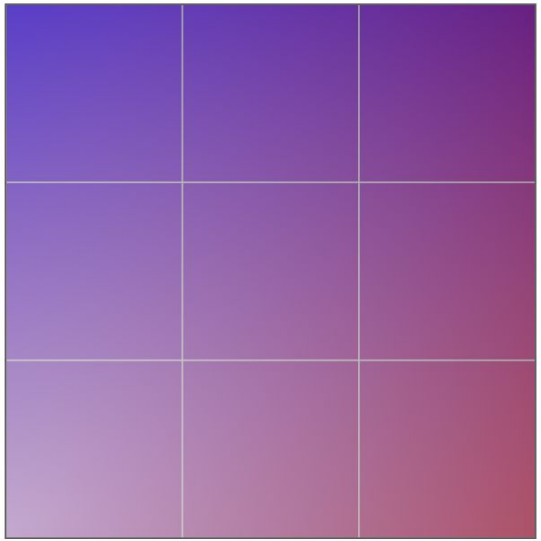
Where are we?

Alex

Brooke

Casey

Detection
Understanding



Threat Understanding

SCYTHE

Shifting Roles

Alex

- Runs new detections by Brooke to ensure they work and are not easily bypassed
- Incorporates detections for new malware techniques identified by Casey
- Researches new integration points and analysis to incorporate in detection logic

SCYTHE

Shifting Roles

Brooke

- Builds tests to validate detections
- Incorporates techniques and procedures from threats identified by Casey
- Passes new techniques from Twitter to Alex and Casey

Shifting Roles

Casey

- Researches attackers that are targeting the Unicorn industry
- Provides reports and guidance to Alex and Brooke on how threats are leveraging specific techniques and technologies
- Clusters malware groups together to better understand similarities

SCYTHE

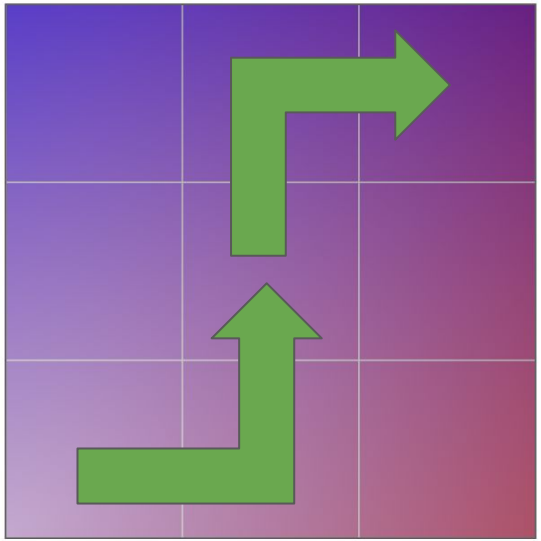
Joint Goals

Alex

Brooke

Casey

Detection
Understanding

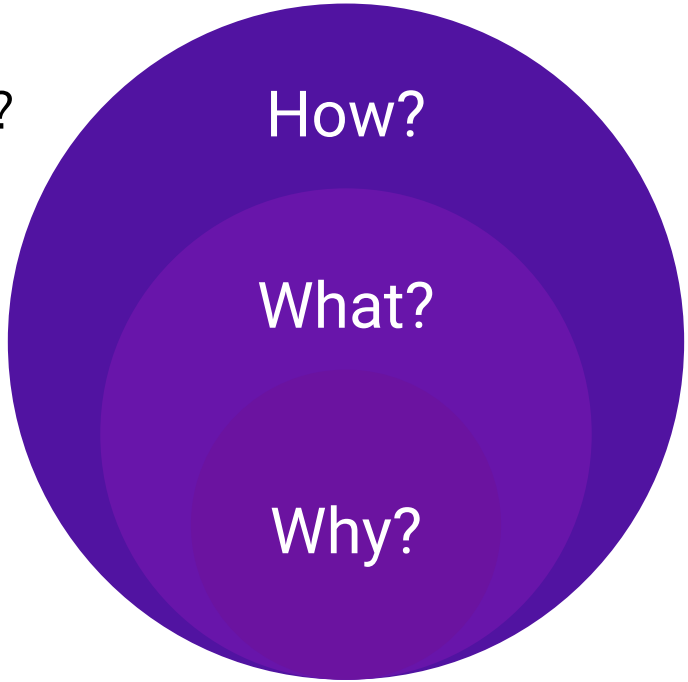


Threat Understanding

SCYTHE

Conclusion

3. How can we use it?



2. What is the maturity model?

1. Why does purple need a maturity model?

Questions?

Thanks for attending!

@teschulz

https://www.scythe.io/authors/tim-schulz

SCYTHE @scythe_io