Welcome to Purple Teaming & Adversary Emulation
DAY 4

SCYTHE

Agenda

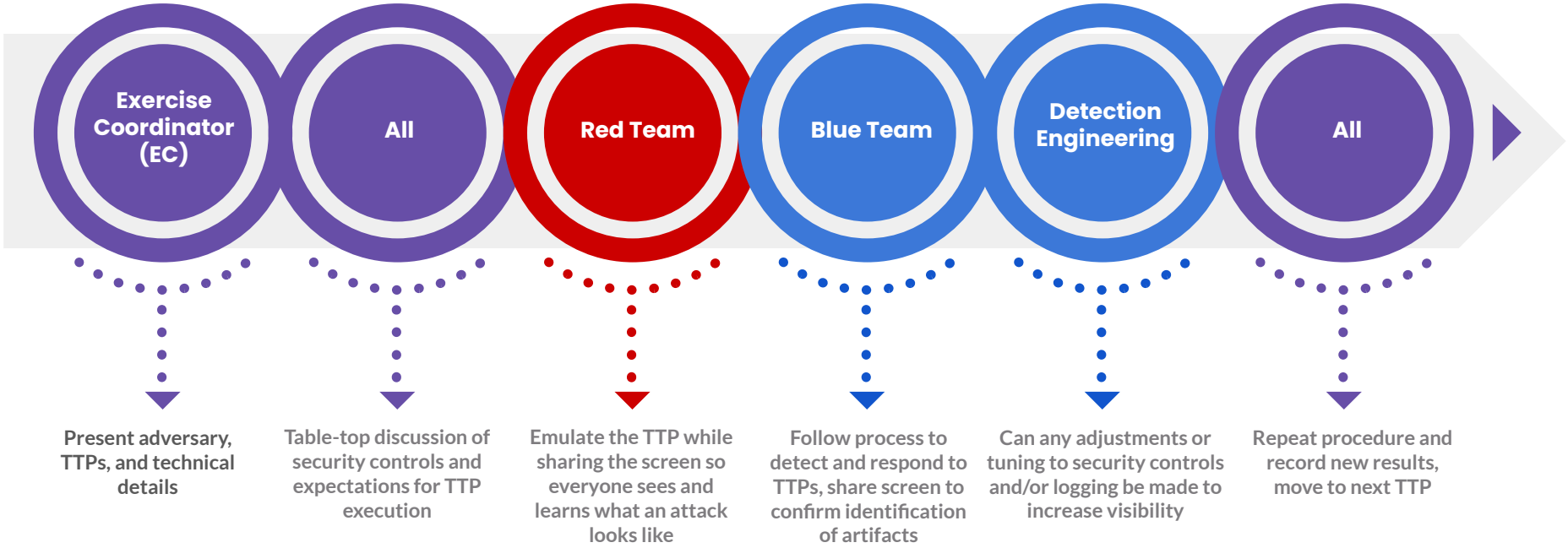
- Purple Team Exercise Framework
- Purple Maturity Model
- Capstone Exercises

Purple Team Exercise Framework

(PTEF)

SCYTHE

Purple Team Exercise Flow



Roles and Responsibilities

Title	Role	Responsibility
Head of Security	Sponsor	Approve Purple Team Exercise and Budget
Cyber Threat Intelligence	Sponsor	Cyber Threat Intelligence
Red Team & Blue Team Managers	Sponsor	Preparation: Define Goals, Select Attendees
Red Team	Attendee	Preparation, Exercise Execution
Blue Team - SOC, Hunt Team, DFIR	Attendee	Preparation, Exercise Execution
Project Manager	Exercise Coordinator	Lead point of contact throughout the entire Purple Team Exercise. Responsible to ensure Cyber Threat Intelligence is provided. Ensures all Preparation steps are taken prior to Exercise Execution. During Exercise Execution, record minutes, notes, action items, and feedback. Send daily emails with those notes as well as guidance for what's planned for the next day. Compile and deliver Lessons Learned.

Table Top

Exercise Coordinator

Are there any preventative measures to stop this plan?

What Defenses are in place?

- Out of the box EDR with no tuning
- Minimal detections are expected, especially for system administration tools

What responses are anticipated from the SOC?

Purple Team Exercise is meant to provide baseline and help future detections through Detection Engineering process.

Table Top

Exercise Coordinator

TTP	Expected Result	Executed Result	Notes
Get-Process T1057 via PowerShell	Logged with Sysmon Event ID 1, No Alert		
Download Mimikatz from Github via PowerShell (Invoke-WebRequest) T1105 Ingress Tool Transfer	Blocked by firewall proxy, high alert from firewall w/ email		
Mimikatz LSASS Dump sekurlsa::LogonPasswords T1003.001 via PowerShell	Blocked, EDR & SIEM Log, High Alert from EDR w/ email		

Table Top

Exercise Coordinator

TTP	Expected Result	Executed Result	Notes
Get-Process T1057 via PowerShell	Logged with Sysmon Event ID 1, No Alert	Execution Success, logged with Sysmon EID 1, No Alert	Sysmon logged locally, but SIEM/EDR did not have log
Download Mimikatz from Github via PowerShell (Invoke-WebRequest) T1105 Ingress Tool Transfer	Blocked by firewall proxy, high alert from firewall w/ email	Download successful, no alert from firewall	EDR logged downloaded file, but no alert
Mimikatz LSASS Dump sekurlsa::LogonPasswords T1003.001 via PowerShell	Blocked, EDR & SIEM Log, High Alert from EDR w/ email	Blocked (then swapped to audit), Logs in EDR/SIEM, high email alert	Variance: User could turn off EDR and execute successfully

Table Top

Exercise Coordinator

TTP	Expected Result	Executed Result	Notes
Get-Process T1057 via PowerShell	Logged with Sysmon Event ID 1, No Alert	Execution Success, logged with Sysmon EID 1, No Alert	Sysmon logged locally, but SIEM/EDR did not have log
Download Mimikatz from Github via PowerShell (Invoke-WebRequest) T1105 Ingress Tool Transfer	Blocked by firewall proxy, high alert from firewall w/ email	Download successful, no alert from firewall	EDR logged downloaded file, but no alert
Mimikatz LSASS Dump sekurlsa::LogonPasswords T1003.001 via PowerShell	Blocked, EDR & SIEM Log, High Alert from EDR w/ email	Blocked (then swapped to audit), Logs in EDR/SIEM, high email alert	Variance: User could turn off EDR and execute successfully

Purple Case Study – Scenario

- 6 week Purple Team Exercise - Assumed Breach scenario
- SCYTHE was hired to perform all major roles (red, blue, CTI)
- **Challenge**: $0 spend on new technology
  - Only tuning current security controls

Purple Case Study – Threats

Week 1 - Baseline testing: access, C2, understand controls

Week 2 - APT19: low sophistication Chinese threat actor

Week 3 - Buhtrap: medium sophistication Russian threat actor

Week 4 - APT33: medium sophistication Iranian threat actor

Week 5 - APT3: high sophistication Chinese threat actor

Week 6 - Free Play: red team plan based on previous weeks

Purple Case Study – Baseline

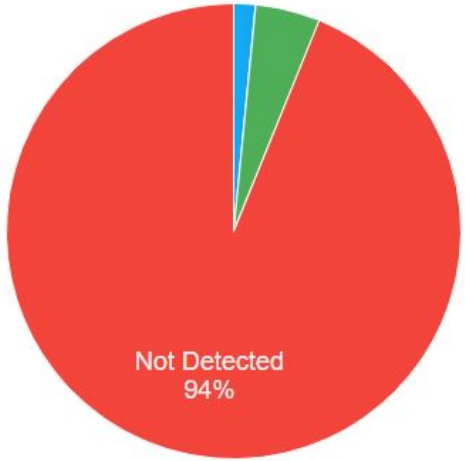
- 94% of Adversary Behavior was undetected
- 3 test cases detected by current controls
- 1 test case blocked

Baseline Result
Known threats have the ability to achieve their objective without being detected

Campaigns Aggregated	5
Test Cases Completed:	65
Test Cases Passed:	4
Detected:	3
Blocked:	1
Test Cases Failed:	61
Not Detected:	61
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Lower



Purple Case Study – Results

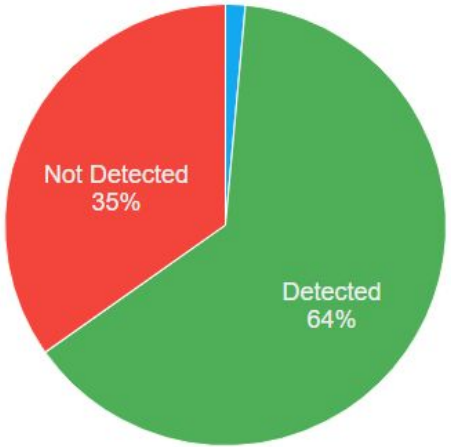
- $0 technology spend to achieve 64% detection rate
- Enabled telemetry (Sysmon)
- Created logic for alerts on EVENTSENTRY

End State Result
Known threats will be detected and responded to before achieving objective

Campaigns Aggregated	5
Test Cases Completed:	69
Test Cases Passed:	45
Detected:	44
Blocked:	1
Test Cases Failed:	24
Not Detected:	24
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score

Above Average



Purple Case Study – YouTube

“The Full Purple Juice, Not the Watered-Down Stuff”

Jorge Orchilles & Bryson Bort
CactusCon 9 2021

https://www.youtube.com/watch?v=tV8TaWMmq2A

SIEM Blog: https://www.eventsentry.com/kb/447

Purple Team Exercise Cheat Sheet

Key Questions	Best Case	Minimum	Notes
Who's involved?	Red Team, Blue Team, CTI Team, Leadership Team	Someone that can execute a test and document a result	Get buy-in or sign off from the highest level possible
What systems are tested?	Production Systems, multiple systems to validate results (servers & endpoints)	Test System	Data generation, data collection, and environment for testing
Logistics?	Remote: Screen share In Person: Shared space	Note keeping tool to record actions	Document/record as much as possible
Security tools?	Everything in SOC & DFIR, tuned for production	A tool that's results can be applied to production	If a tool/control blocks progress, document and shift to audit mode to move through depth

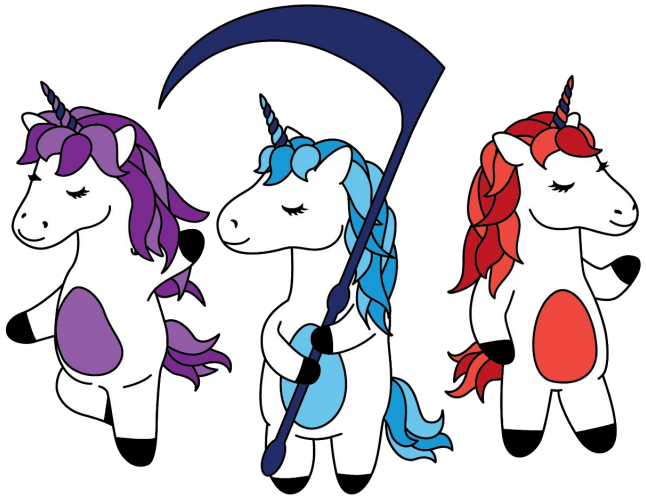
Baselining Discussion

Purple Maturity Model

Challenges with current landscape

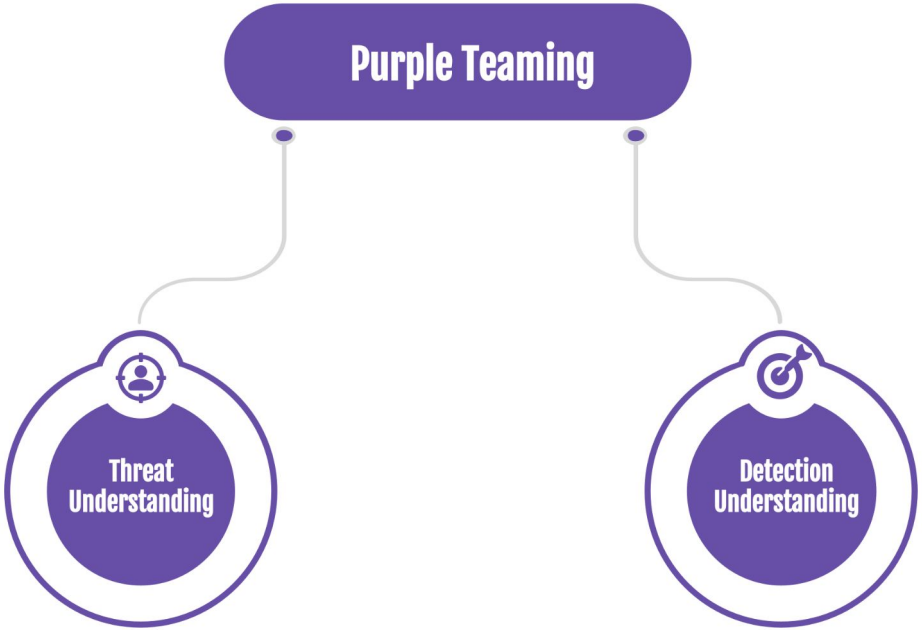
- Purple teaming is a singular event or exercise
- Teams develop capability independently
- Communication and cooperation between teams is optional

Infosec Teams of Tomorrow



Fundamentally different mentality than red and blue teams

Moving Purple Forward



Detection Understanding

Blue + CTI

- 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

Red + CTI

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 the model: Level 1

Red + CTI

Blue + CTI

Level 1: Deployment

Threat Understanding

Detection Understanding

Building our model: Level 2

Red + CTI

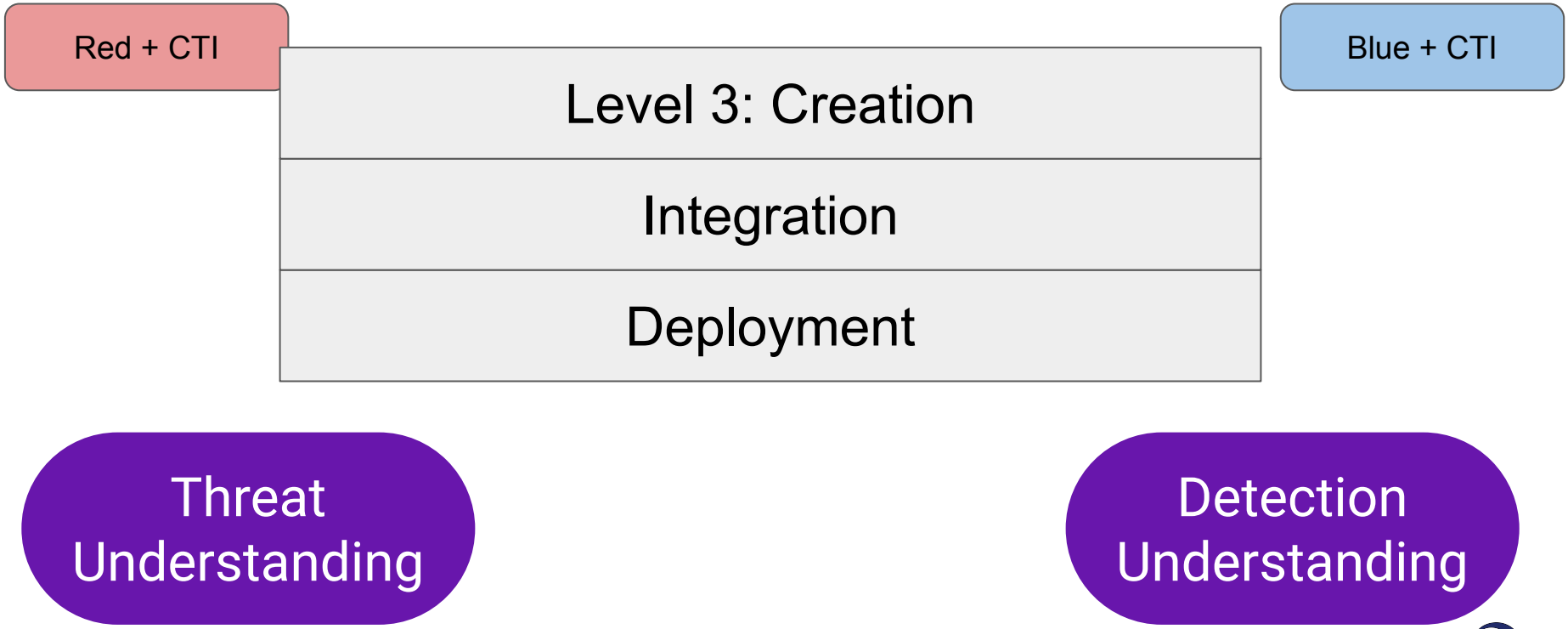
Blue + CTI

Level 2: Integration
Deployment

Threat Understanding

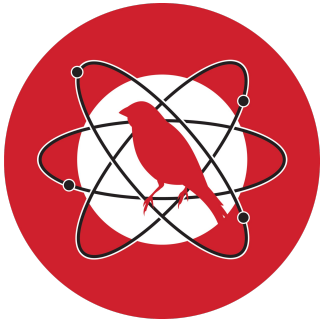
Detection Understanding

Building our model: Level 3



Project Examples

https://github.com/SigmaHQ/sigma



Atomic Red Team

https://atomicredteam.io

Detection Understanding Example: Sigma

Blue + CTI

Creation

Integration

Deployment

Deploying a SIEM/EDR

Detection Understanding

Detection Understanding Example: Sigma

Blue + CTI

Integrating SIGMA rules SIEM/EDR

Creation

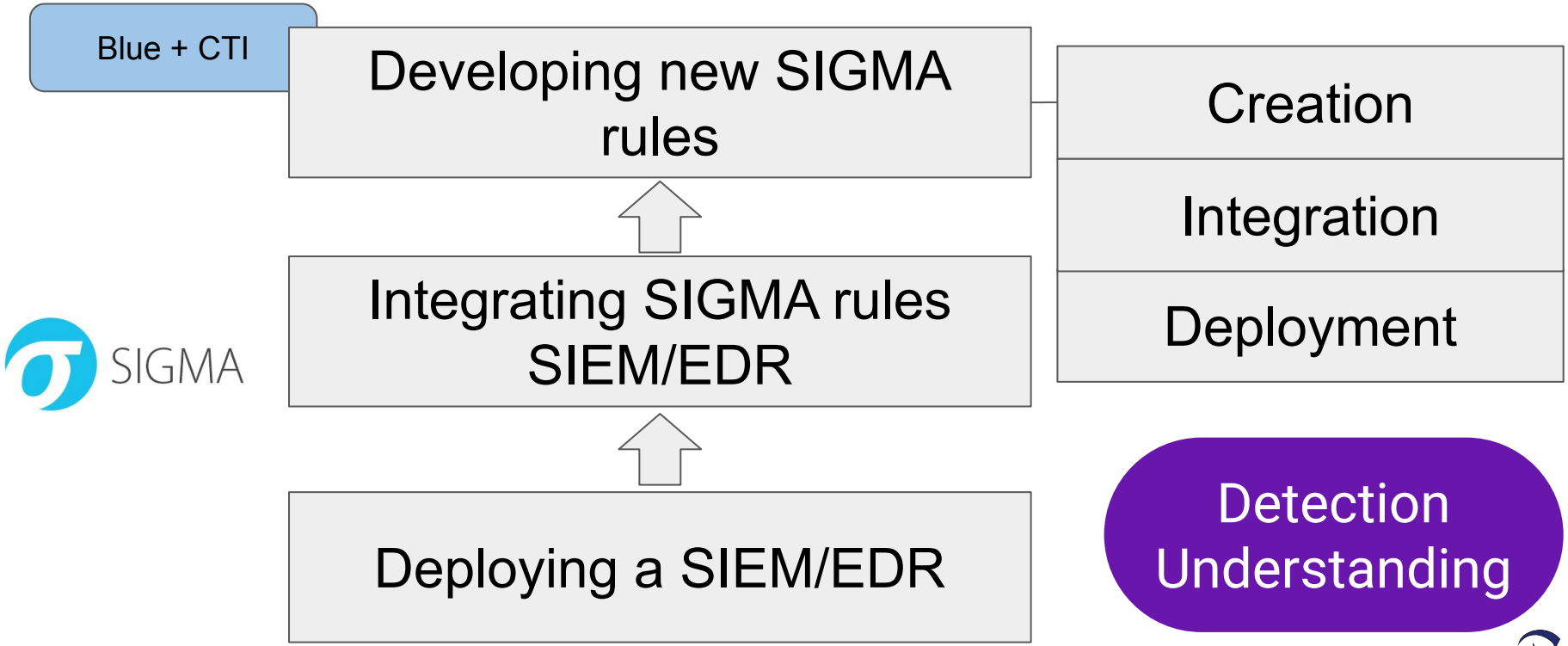
Integration

Deployment

Deploying a SIEM/EDR

Detection Understanding

Detection Understanding Example: Sigma



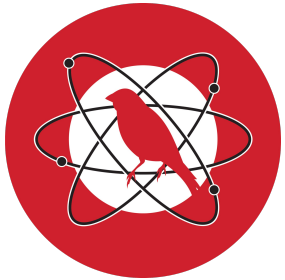
Threat Understanding Example: ART

Red + CTI

Creation

Integration

Deployment



Threat Understanding

Using ART

Threat Understanding Example: ART

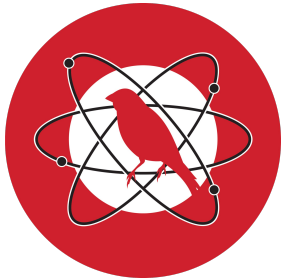
Red + CTI

Creation

Integration

Deployment

Integrating ART to test detections



Threat Understanding

Using ART

Threat Understanding Example: ART

Creation

Integration

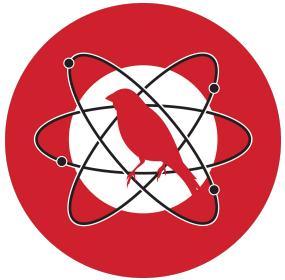
Deployment

Developing new ART techniques

Red + CTI

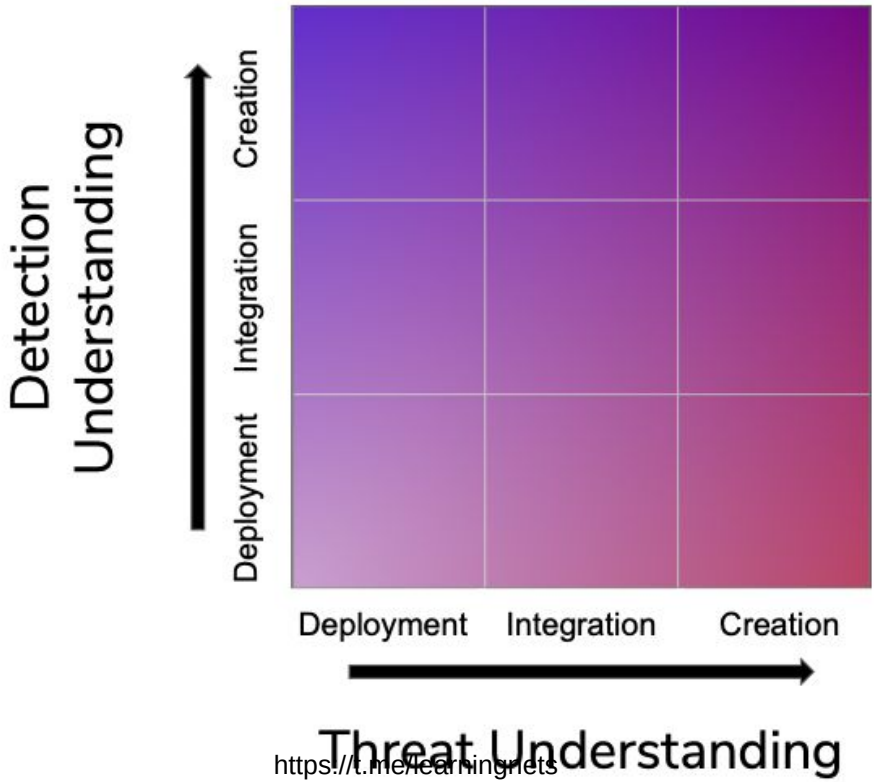
Integrating ART to test detections

Using ART



Threat Understanding

Purple Maturity Model



https://t.me/learningnets

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

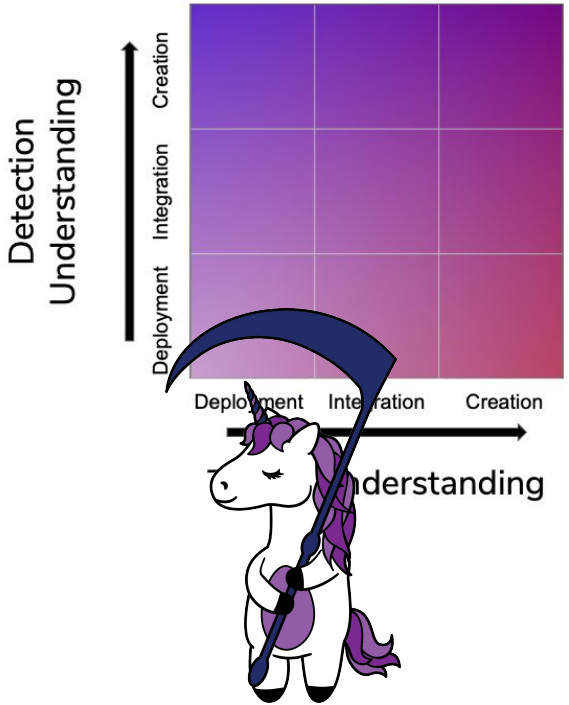
- Reads every CTI vendor’s threat report

Building a roadmap

Brooke

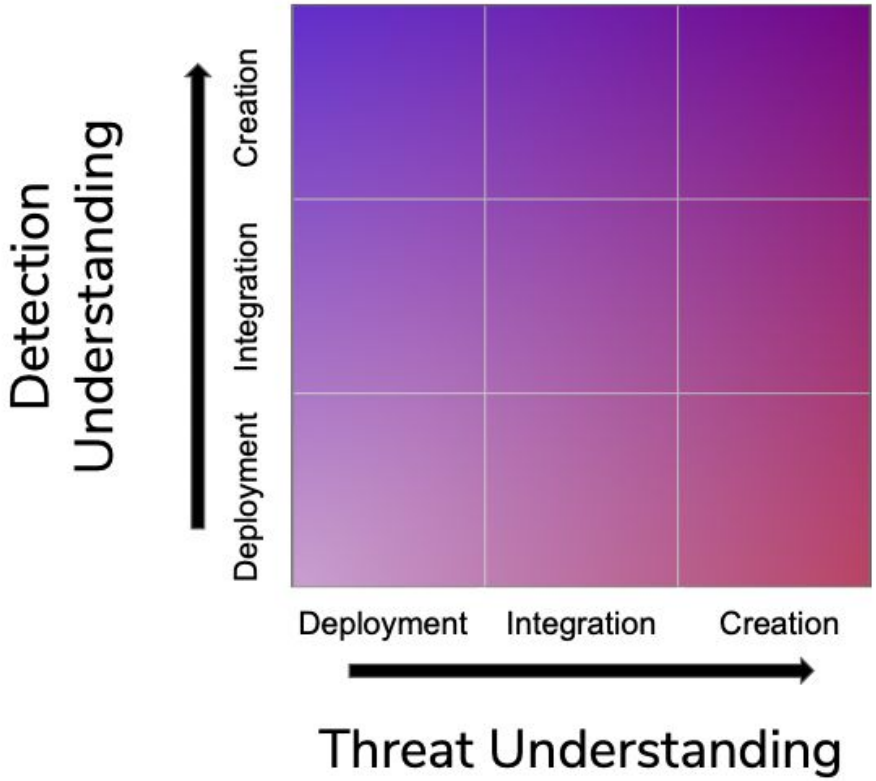
Casey

Alex



https://t.me/learningnets

Where are we?



Shifting Roles (Blue) - New Understanding

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

Shifting Roles (Red) – New Understanding

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 (CTI) - New Understanding

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

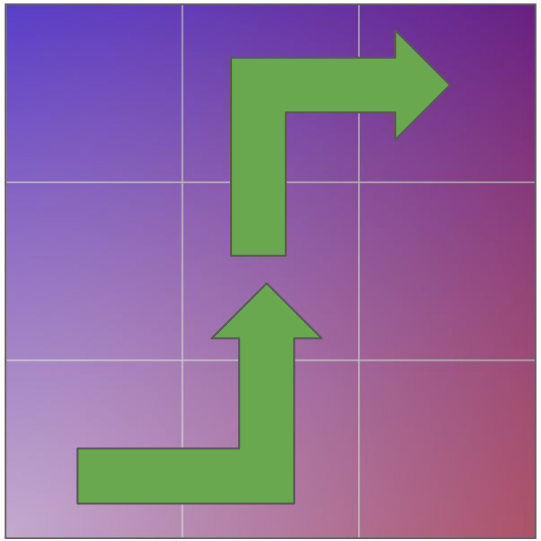
Joint Goals

Alex

Brooke

Casey

Detection
Understanding



Threat Understanding

Questions to Consider with PMM

- Where does your organization (or you) sit within the purple maturity model?
  - Why?
- What steps could your organization (or you) take to move up their maturity in both threat understanding and detection understanding?
  - Is your organization or team heavy in expertise on one side or the other?
  - Is training, hiring, or dedicating resources to gaining more knowledge in one side of the model possible?
- What strategic initiatives could be championed or prioritized to help the team progress in maturity?
  - Are team KPIs helping or hindering the team's ability to mature?
  - Quantity vs Quality, what does your organization reward?

Capstone Exercises

Open Time: Enjoy the Lab Range!

We're around to chat, answer questions, or walk through labs!

Labs are open until August 22nd

Instructor Socials – Connect with Us!

- Jake Williams
  - https://twitter.com/MalwareJake
  - https://www.linkedin.com/in/jacob-williams-77938a16/
- Tim Schulz
  - https://twitter.com/teschulz
  - https://www.linkedin.com/in/tim-schulz/
- Chris Peacock
  - https://twitter.com/SecurePeacock
  - https://www.linkedin.com/in/securepeacock/
- Shawn Edwards
  - https://www.linkedin.com/in/shawn-edwards-7b2564101/

End of Day 4 (and class!)

Blackhat will send you a survey about the course through SurveyMonkey

- Filling this out honestly helps Blackhat understand what you all as the students felt is the value of the course!

Feedback Link for Day 4:
https://freeonlinesurveys.com/s/ThnorXjI

SCYTHE

Thank you all so much for participating and interacting over the past 4 days!

See you in Discord and at future conferences!
Please stop by and say hi if you see us!

SCYTHE

https://t.me/learningnets