Power to the Purple: Intro to Purple Teaming

Tim Schulz
@teschulz

SCYTHE

Tim Schulz – VP of Research & Engineering

SCYTHE

Sandia National Laboratories

- Security Research
- Red Teaming
- Purple Teaming
- ICS/OT

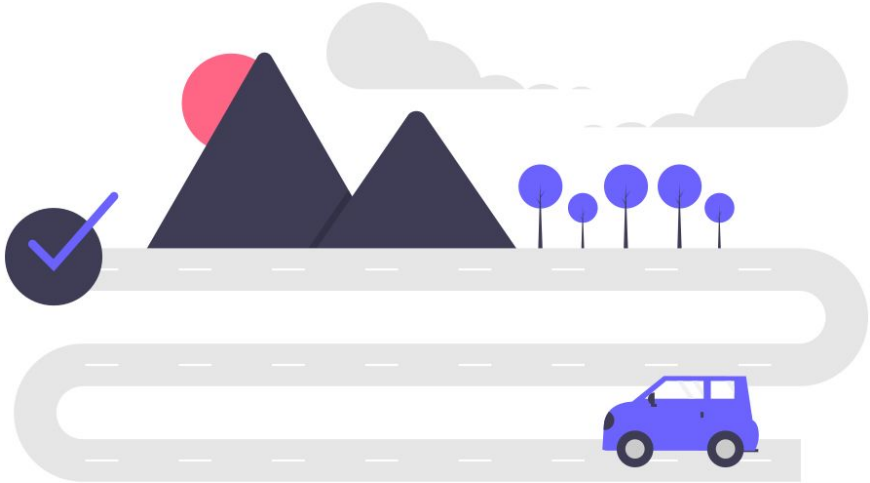
MITRE

MITRE | ATT&CK®

- Adversary Emulation
- Purple Teaming
- Red Teaming

Roadmap: What are we covering today?

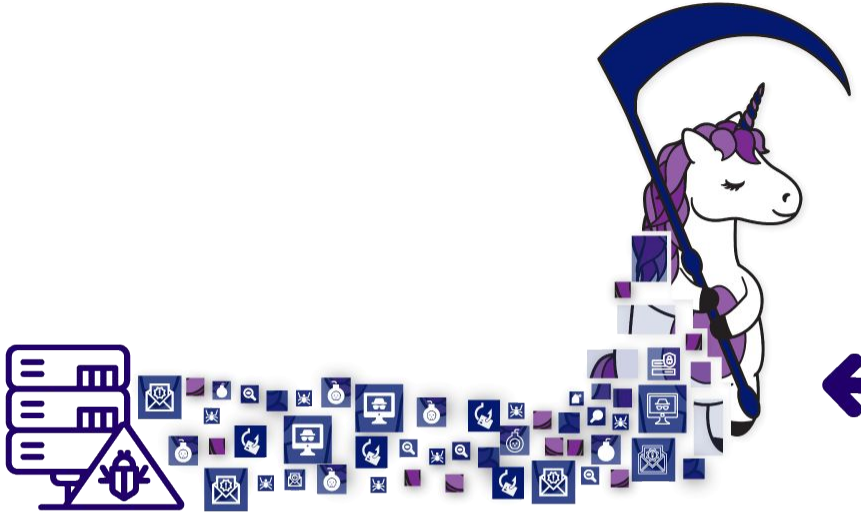
- What is purple teaming?
- Purple Team Process
- Test Execution
- Metrics and Reporting



1. What is Purple Teaming?

SCYTHE

ATTACK. DETECT. RESPOND.



Cyber Threat Intelligence

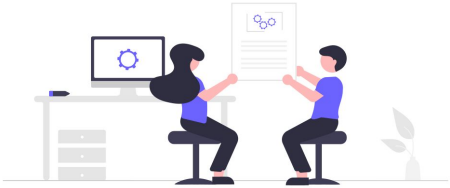
Attack

Tracking

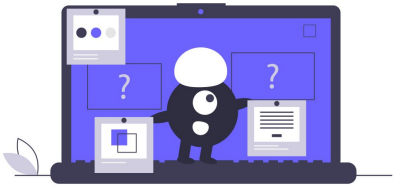
Detect & Respond

What can purple teaming do for you?

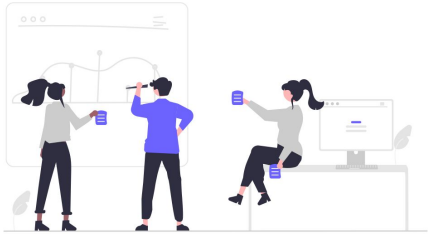
- Train defenders



- Test process between teams



- Test TTPs



- Replay Red Team Engagement

Foster a collaborative culture and mentality!

What is a Purple Team?

Blue Team

Red Team

CTI Team

Purple Team Exercise Cheat Sheet

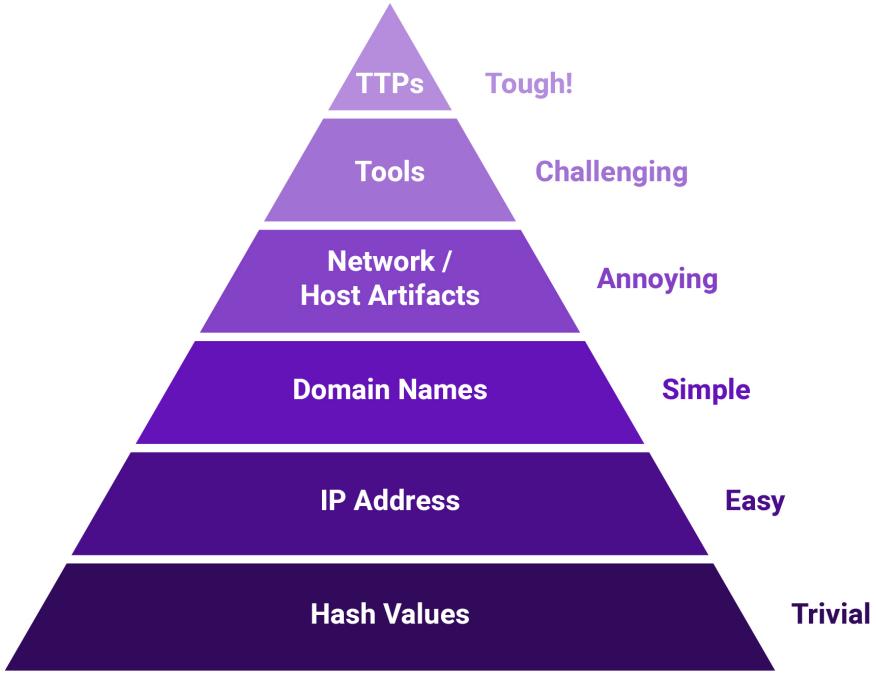
Key Questions	Best Case	Minimum	Notes
Who's involved?	Red Team, Blue Team, CTI Team, Leadership Team	Someone that can execute a test and document a result	Get buy-in or sign off from the highest level possible
What systems are tested?	Production Systems, multiple systems to validate results (servers & 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

2. Purple Process

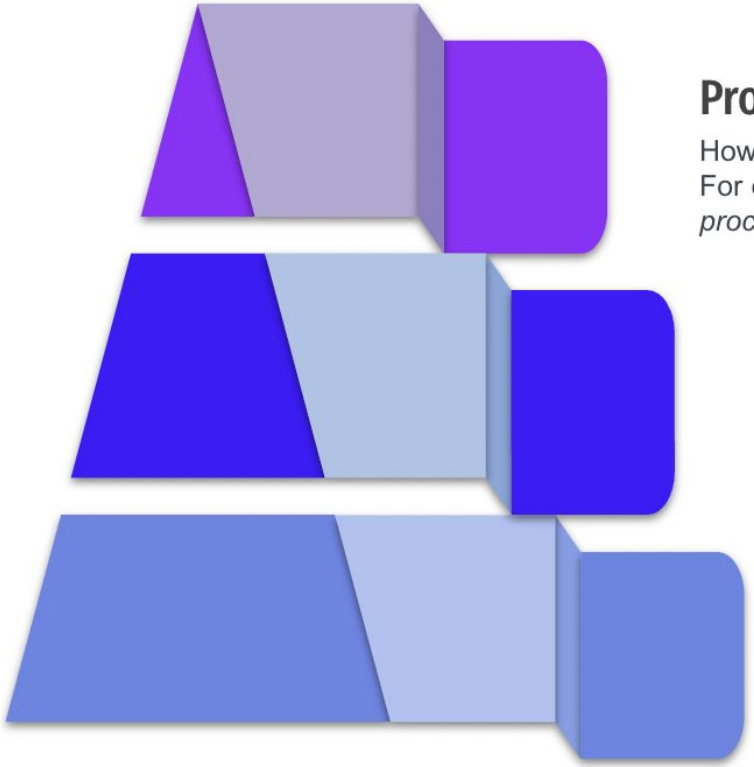
SCYTHE

Pyramid of Pain

David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



SCYTHE Expansion of the Pyramid



Procedures

How the technique was carried out.
For example, the attacker used
procdump -ma lsass.exe lsass_dump

Techniques

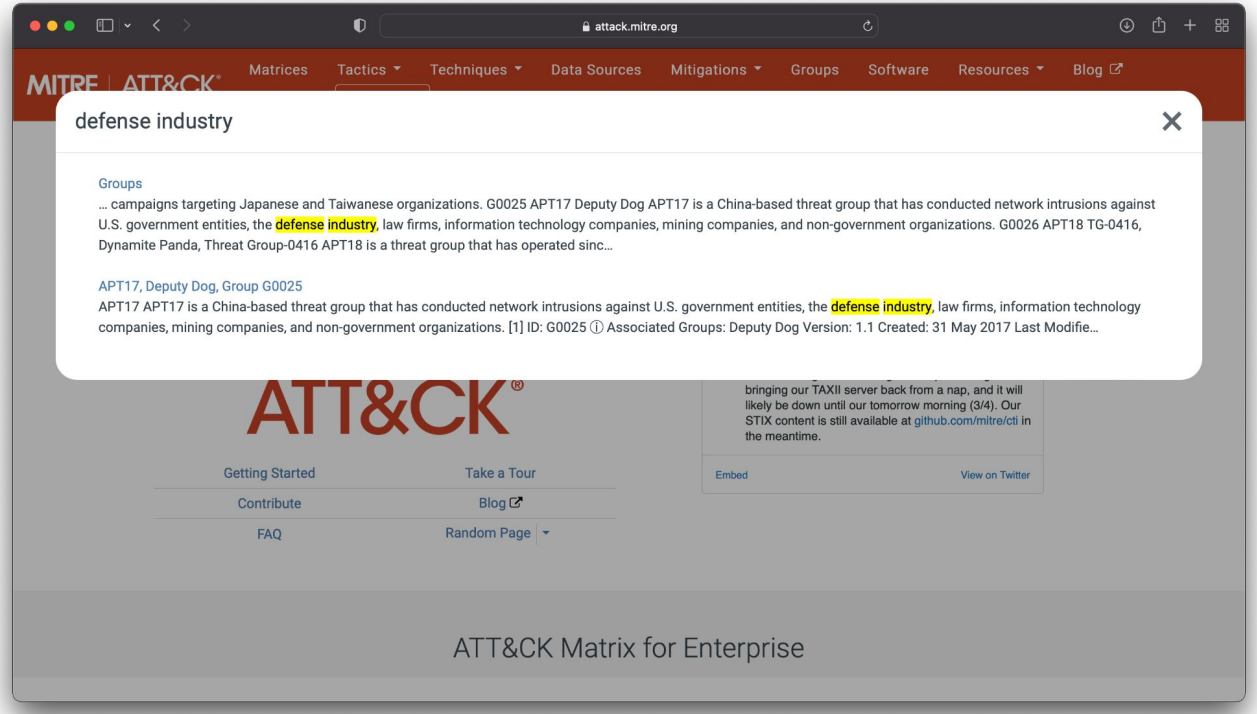
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Chris Peacock: https://scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid

ATT&CK Threat Modeling



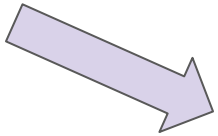
Procedure Variation: Process Discovery (T1057)

Process
Discovery
T1057

Execution Methods: Process Discovery (T1057)

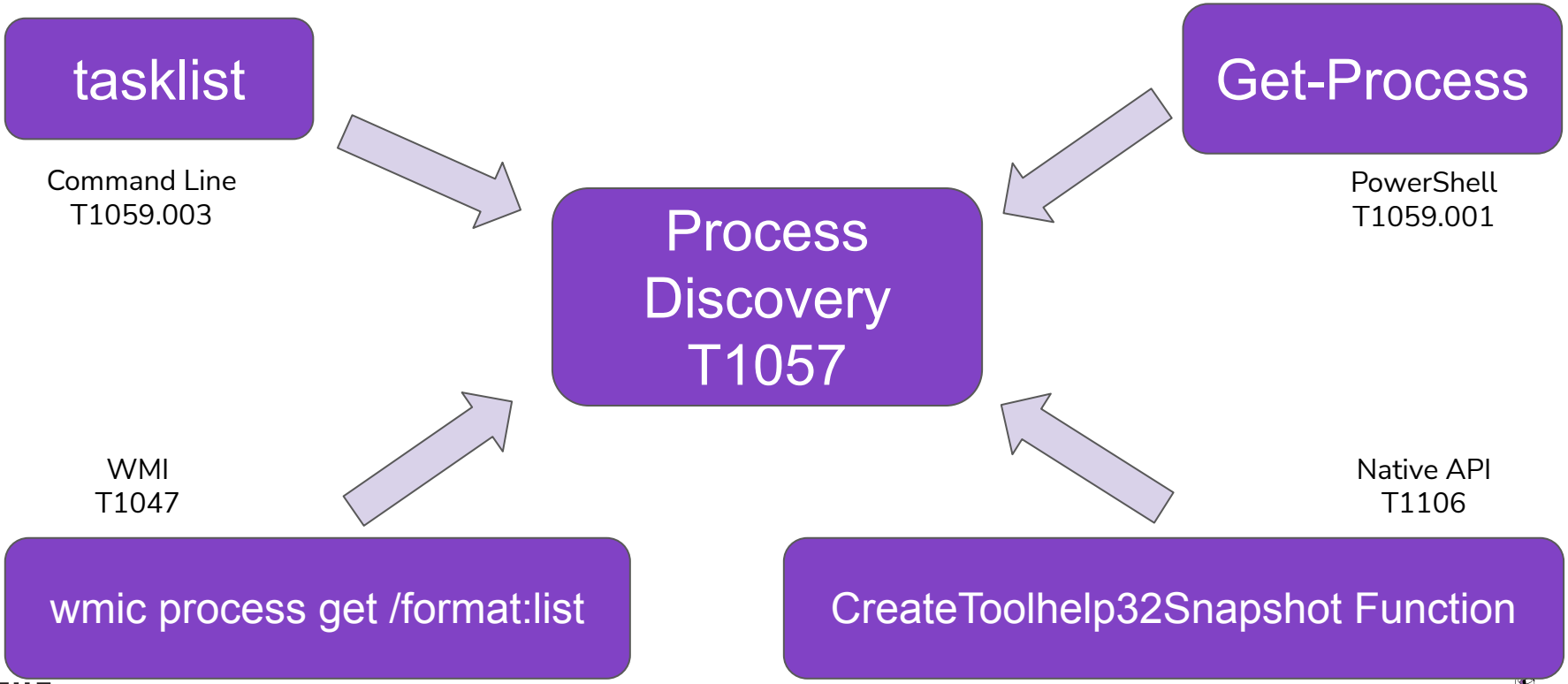
tasklist

Command Line
T1059.003



Process
Discovery
T1057

Execution Methods: Process Discovery (T1057)



2. Purple Process

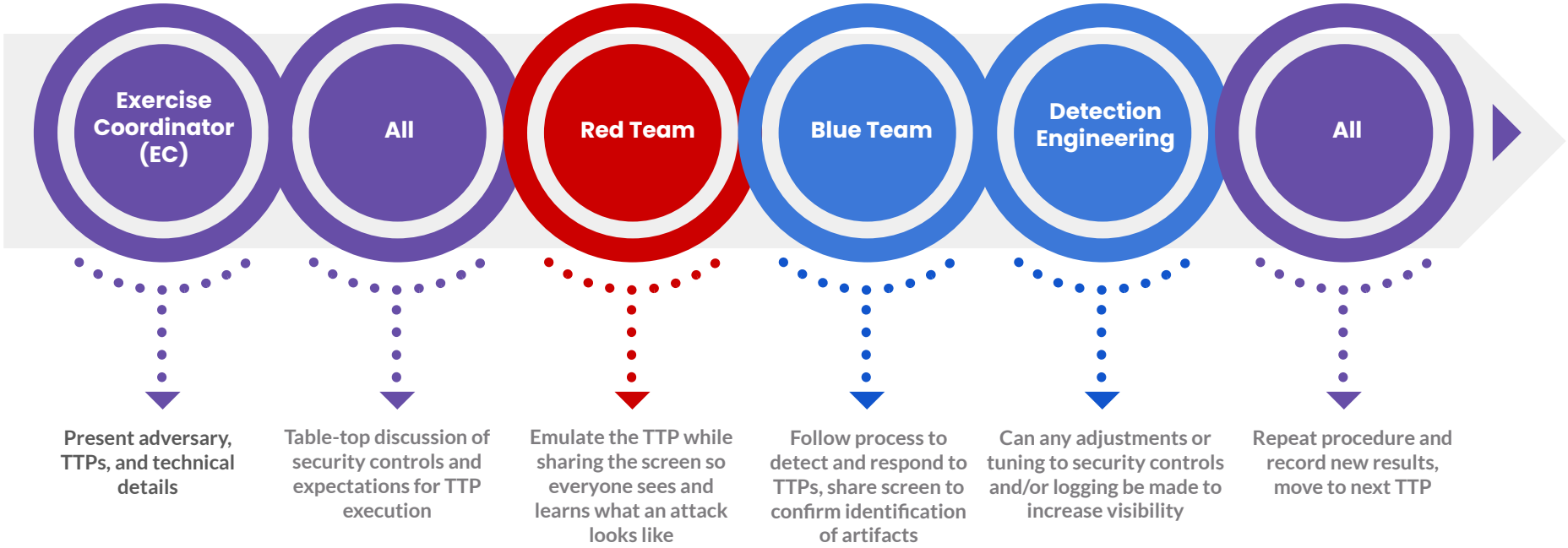
SCYTHE

Purple Team Exercise Framework (v2)

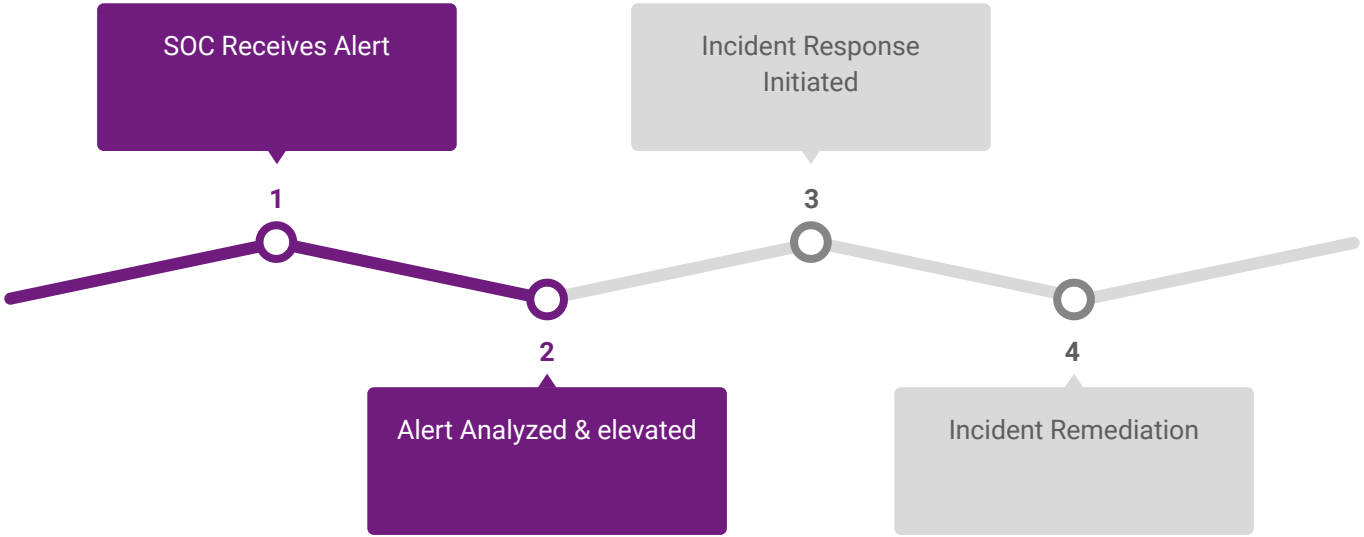
Download the Framework now so you can follow along: https://scythe.io/ptef

Download it now!

Purple Team Exercise Flow

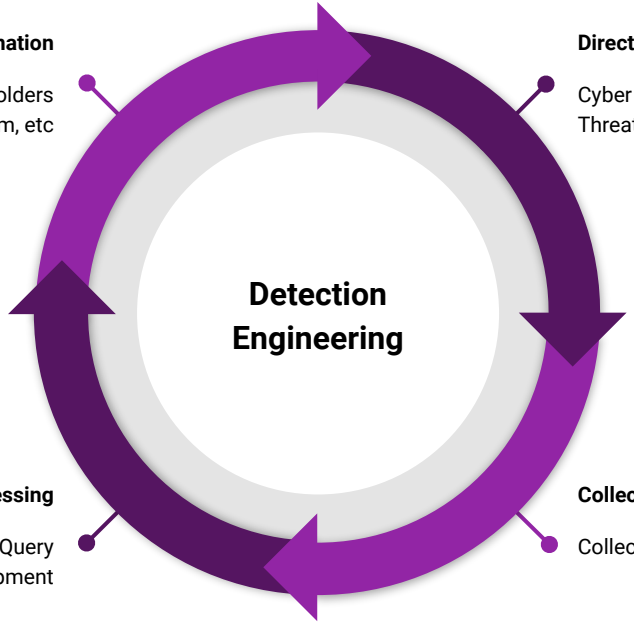


Alert Response Process



How are we evaluating people and process?

Detection Engineering Process



Direction

Cyber Threat Intelligence (CTI) & Threat Understanding

Collection

Collect Emulation Logs

Processing

Processing Logs for Query Development

Dissemination

Distributing to Stakeholders
SOC, Management, Red Team, etc

Efficiency in Testing

Why Assume Breach?

- Cost
- Insider Threat
- Zero Day
- Phishing emails land
- Already breached

Additional Resources

- https://www.scythe.io/library/why-assume-breach
- https://posts.specterops.io/revisiting-phishing-simulations-94d9cd460934

3. Test Execution

Lab time!

SCYTHE

4. Metrics and Reporting

SCYTHE

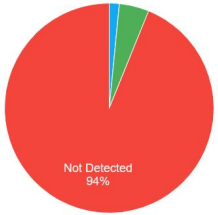
Measuring Outcomes: Metrics

- Collaboration between teams mean certain metrics are easier to measure (especially over time):
  - Time to log
  - Time to detect
  - Time to alert
- Metrics reveal gaps in real time
  - Is the execution method logged at all?
  - Could the team find the context to detect this technique?
  - Does this alert severity mean this is tackled sooner or later?

Overall Score

Lower

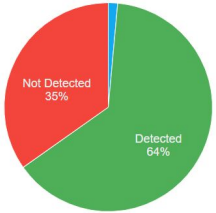
Campaigns Aggregated	5
Test Cases Completed:	65
Test Cases Passed:	4
Detected:	3
Blocked:	1
Test Cases Failed:	61
Not Detected:	61
Test Cases Not Completed:	0
To Be Determined:	0



Overall Score

Above Average

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
	0



Leadership teams like metrics

Thank you!

@teschulz

SCYTHE