RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center


SESSION ID: SBX5-T08

# Purple Is the New Red - Providing the Most Value from Offensive Security



**Jorge Orchilles**

Instructor, Author, Ambassador
SANS Institute
@JorgeOrchilles

# Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

# Agenda



- About Me – relevant projects
- What is a Purple Team?
- Offensive Security Maturity Model
- Purple Team Exercise
- Operationalized Purple Teaming
- Purple Team Maturity Model
- “Apply” Slide

# T1033 – User Discovery: Jorge Orchilles



- SANS Principal Instructor and Author of SEC565: Red Team Operations and Adversary Emulation
- Director – Vulnerability Management, Pen Test, Red Team, Breach and Attack Simulation, Purple Team, and Adversary Emulation
- Creator of Purple Team Exercise Framework and C2 Matrix
- Contributor to ATT&CK, Atomic Red Team, CVSSv3, and others
- ISSA Fellow, NSI Technologist Fellow
- Soccer/Football Fan: HALA MADRID

# What is a Purple Team?



- A **collaboration** between various cyber security skill sets
- A **virtual**, **functional** team working together to test, measure and improve defensive security posture: people, process, and technology
  - Cyber Threat Intelligence - research and provide adversary behaviors or tactics, techniques, and procedures (TTPs)
  - Red Team - offensive team in charge of emulating adversary behaviors or TTPs
  - Blue Team - the defenders: Security Operations Center (SOC), Threat Hunting, Digital Forensics and Incident Response (DFIR), etc.

# Offensive Security Maturity Model

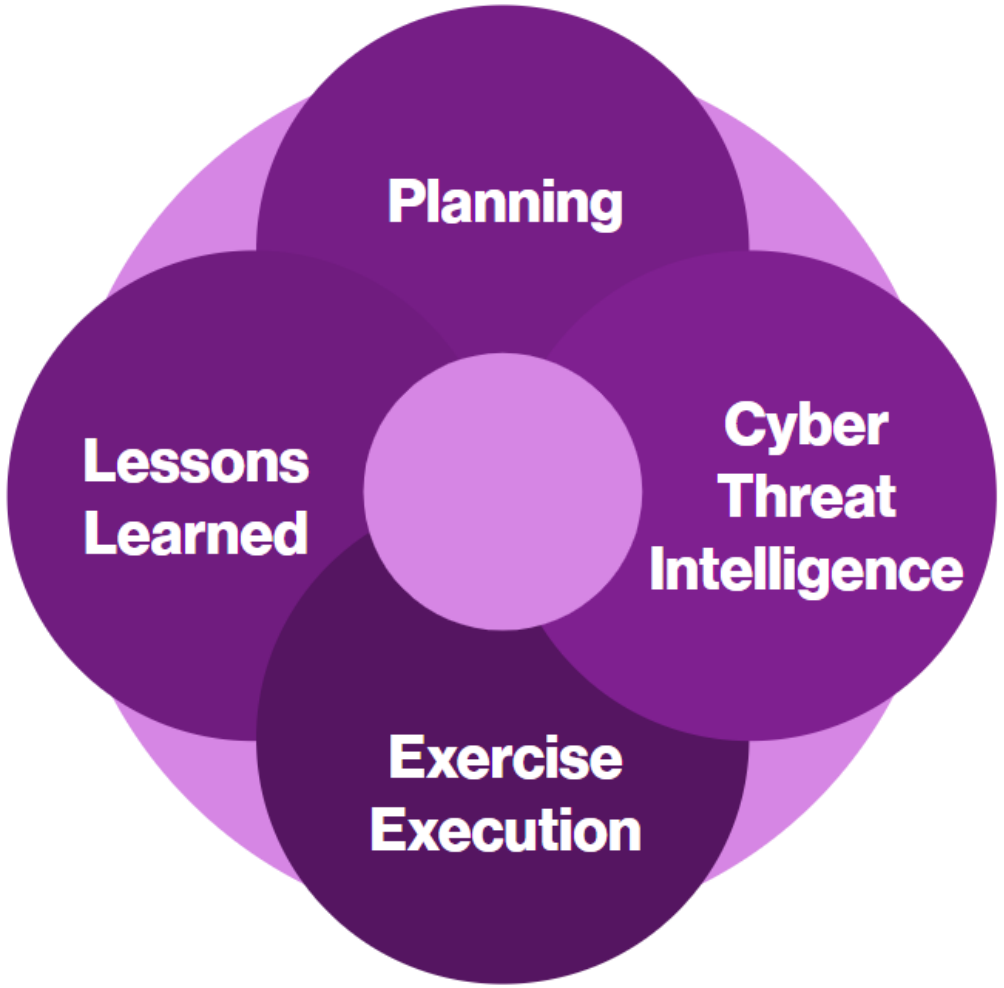


- If asked to build an internal red team, I'd start with Purple first


https://www.sans.org/blog/building-internal-red-team-go-purple-first/

# Start with a Purple Team Exercise (PTX)

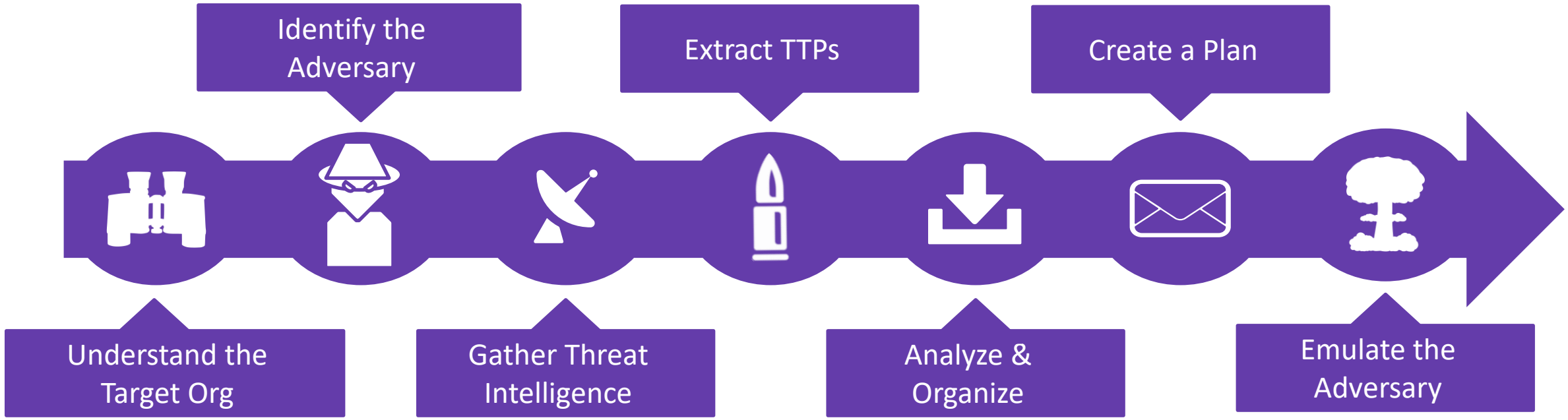





https://github.com/scythe-io/purple-team-exercise-framework

# PTX: CTI for Adversary Emulation





# TTP 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


@SecurePeacock

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

# PTX: Preparation



## Planning Meetings

- Logistics
  - Location
  - Screen Sharing
- Attack Infrastructure
- Target Systems
  - Security tools
  - Accounts
- Blue Team visibility confirmation

## Metrics

- Data Sources
- Detection
  - Telemetry
  - Alerts
- Response
  - Time to Detect
  - Time to Investigate
  - Time to Remediate

# Purple Team Exercise Flow



**Exercise Coordinator**

Introduction of people and exercise process including adversary behaviors/TTPs

**TableTop**

Everyone tabletops the TTP to determine preventive and detective controls and/or possible results

**Red Team**

Emulates the adversary behaviors while sharing screen for everyone to see

**Blue Team**

Follow process to identify alerts or telemetry of emulated behavior

**Detection Engineering**

Build detections by ensuring telemetry and alerts are implemented and tuned.

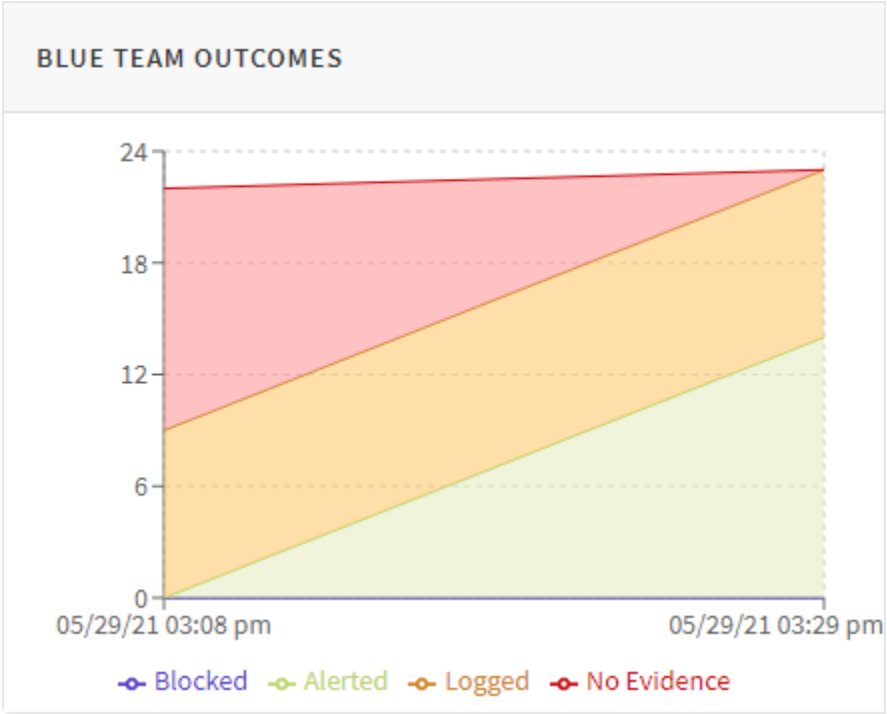
**All**

Learn about the TTP and respond next time it is observed in organization. Repeat for next set of TTPs.

# PTX: Lessons Learned and Action Plan



- Document and show the value
- Track TTPs that were performed, expected result, and actual result
- Track Action Items for further improvement
- PlexTrac (shown) or VECTR

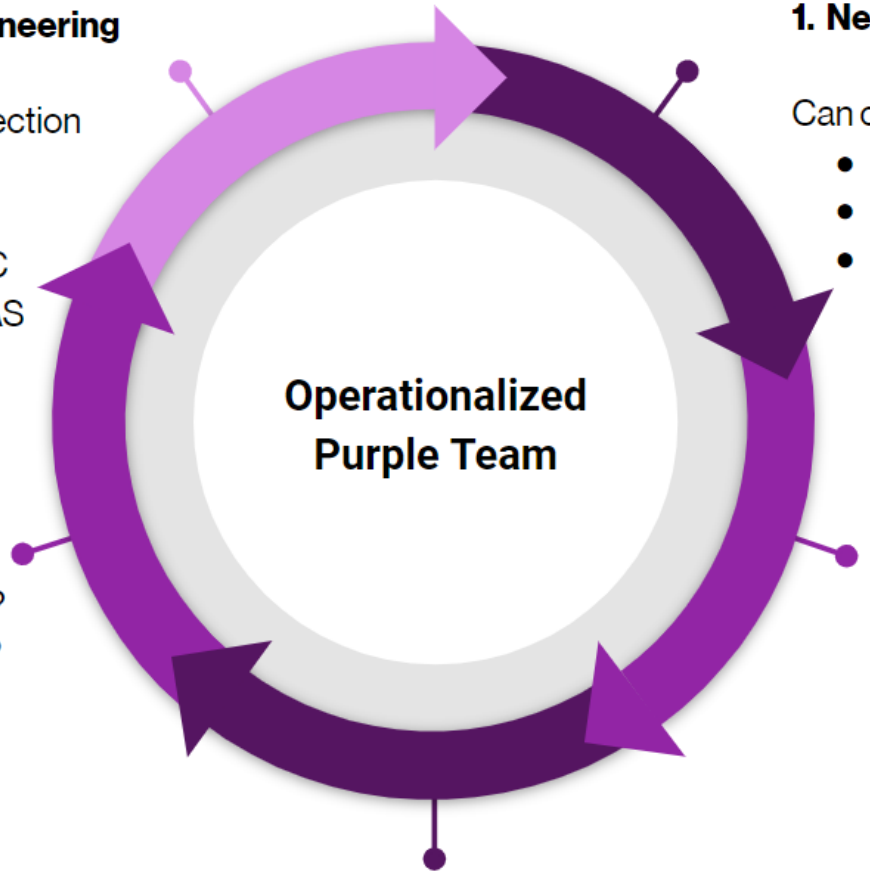


# Success! What next?



# Operationalized Purple Team Process






**1. New Adversary Behavior/TTP**

Can come from anyone:

- CTI
- Red Team
- Blue Team

**2. Analyze & Organize**

- Extract TTPs
- Were these already tested?
- Is there coverage?

**3. Red Team Emulation**

Do the TTPs work here?

**4. Blue Team Result**

- Was there an Alert?
- Is there Telemetry?
- Can we Threat Hunt?

**5. Detection Engineering**

- Build Detection
- Deploy
- Tune
- Train SOC
- Add to BAS

# Step 1: New Adversary Behavior/TTP



- CTI, Red Team, or Blue Team can discover and share new intel or TTPs
- Notification to virtual Purple Team (via new ticket/tracking)
- Assign relevant stakeholders as part of mini-purple team for this item
  - Self assigned or manager assigned

# Step 2: Analyze & Organize the TTPs



- Extract TTPs
- Map to MITRE ATT&CK
- Correlate with previous tests
  - Requires a decent tracking system
  - Excel or Google Sheets as MVP
  - PlexTrac or VECTR
- Hold a tabletop discussion

# Step 3: Emulate TTPs



- Red Team focuses on emulating TTPs
- Sets up attack infrastructure or uses dedicated Purple Team infrastructure
  - Target systems and accounts
  - Standard security tools
- Shares how to emulate with others in purple team
- Does the TTP work in our environment?

# Step 4: Blue Team Results



- Document Blue Team visibility
- Was there an alert?
- Was there telemetry?
  - Are the data sources required being collected?
  - Processing of data sources for queries?
- Can we Threat Hunt?

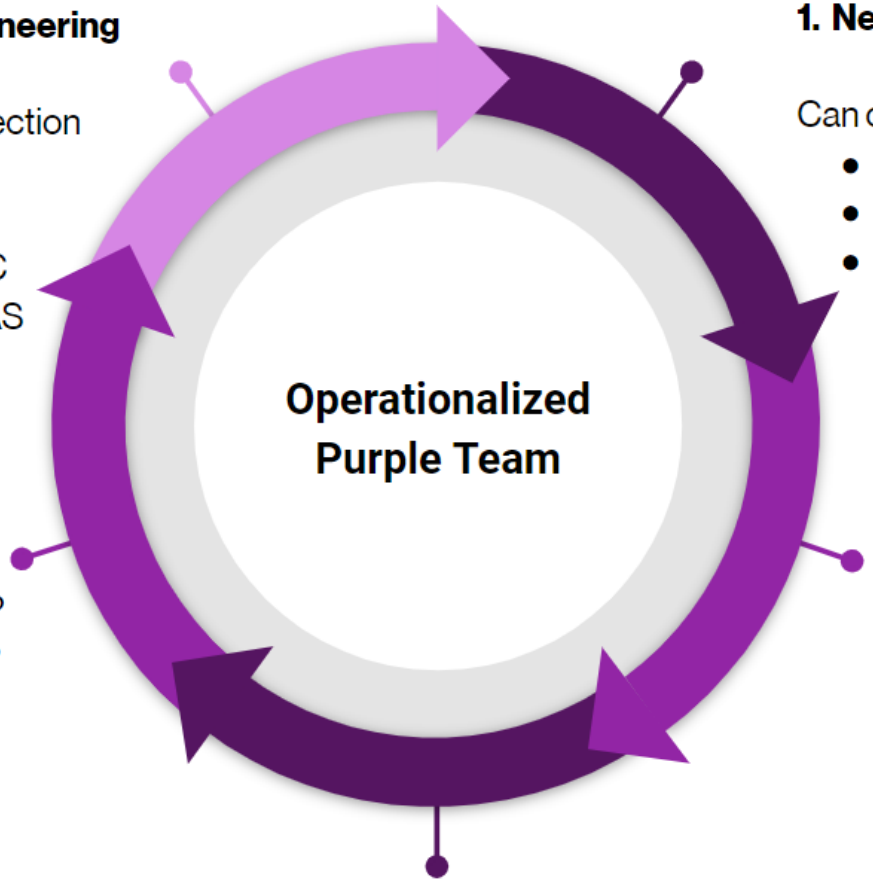
# Step 5: Detection Engineering



- If there are gaps that can be addressed:
  - Build detection
  - Deploy
  - Tune
- Re-run emulation and testing to train the rest of the team
- Add use case to Breach and Attack Simulation solution
  - Only get alerts if real attack or if alerts no longer work

# Continuous Process






**1. New Adversary Behavior/TTP**

Can come from anyone:

- CTI
- Red Team
- Blue Team

**2. Analyze & Organize**

- Extract TTPs
- Were these already tested?
- Is there coverage?

**3. Red Team Emulation**

Do the TTPs work here?

**4. Blue Team Result**

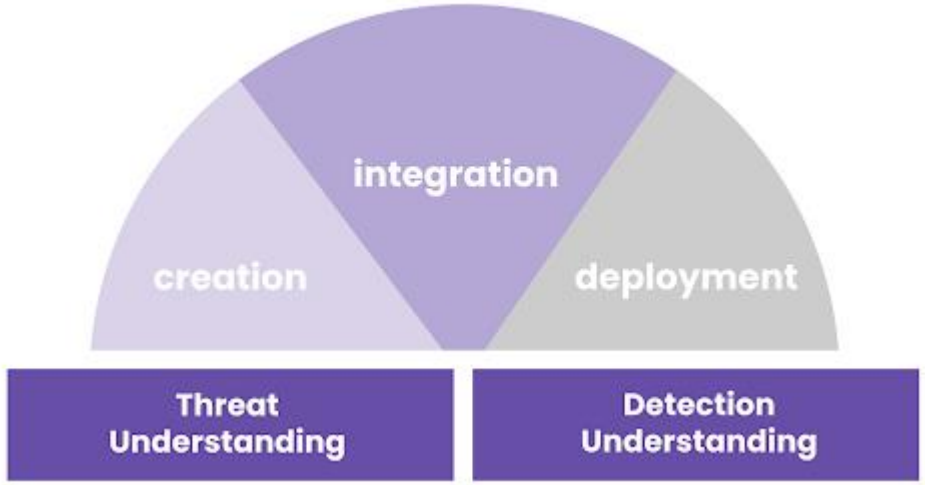
- Was there an Alert?
- Is there Telemetry?
- Can we Threat Hunt?

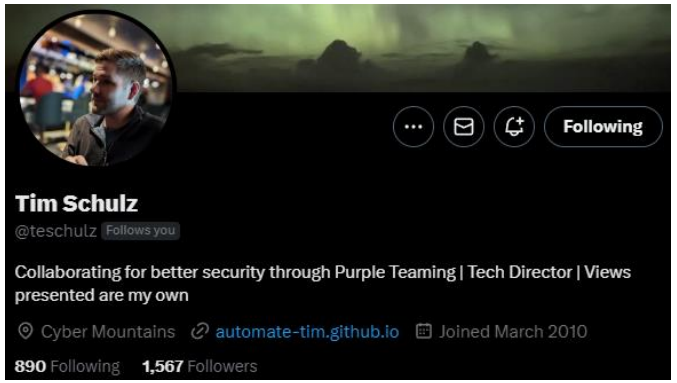
**5. Detection Engineering**

- Build Detection
- Deploy
- Tune
- Train SOC
- Add to BAS

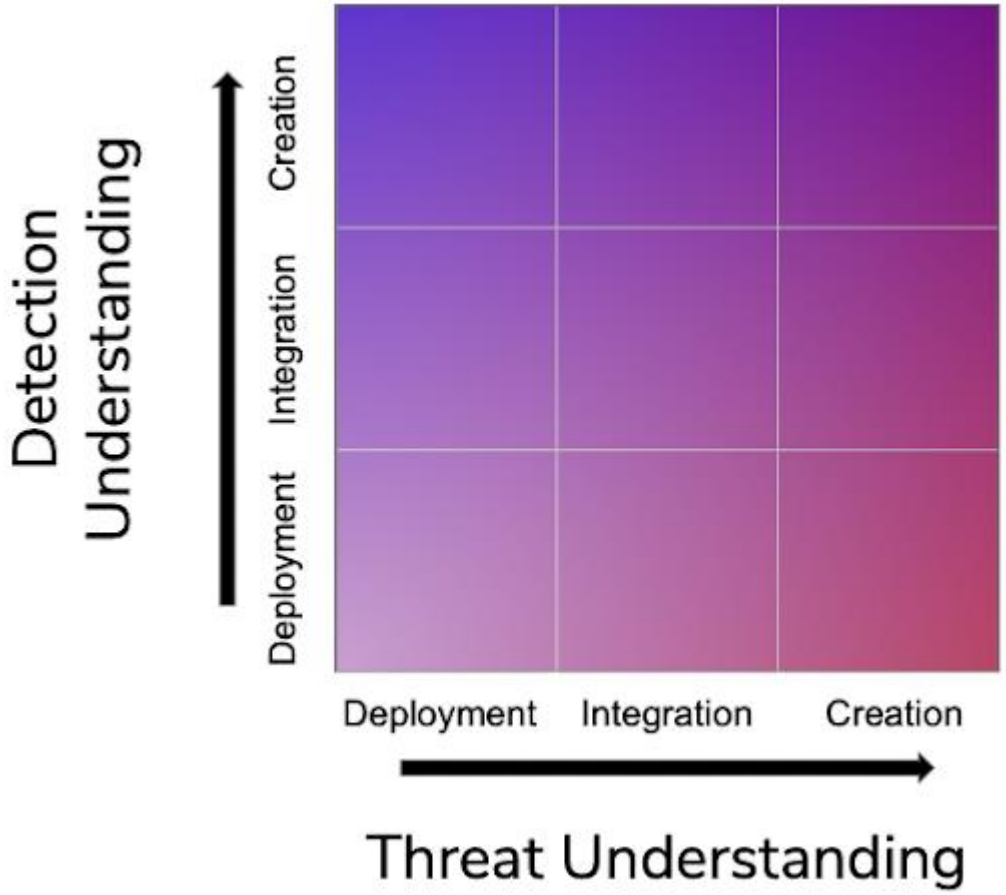
# Purple Team Maturity Model






@teschulz



# “Apply” Slide



- Next week you should:
  - Identify where your organization is in the Offensive Security Maturity Model
- In the first three months following this presentation you should:
  - Run a Purple Team Exercise by collaborating with multiple cybersecurity functions
- Within six months you should:
  - Establish an Operationalized Purple Team process
  - Plan a stealth, end-to-end Red Team engagement

# More Resources



- SANS Purple Team: https://www.sans.org/purple-team/
- Blogs: https://www.sans.org/blog/?focus-area=purple-team
- Purple Team Emulation Plans: https://github.com/scythe-io/community-threats
- SANS Courses
  - SEC565: Red Team Operations and Adversary Emulation
  - SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
  - SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

RSAConference™2023


# Thank You!

**Any questions?**