Purple Team Exercise Framework v2

@JorgeOrchilles

T1033 - System Owner/User Discovery

- Chief Technology Officer - SCYTHE
- Purple Team Exercise Framework (PTEF)
- C2 Matrix Co-Creator
- 10 years @ Citi leading offensive security team
- SANS Certified Instructor: SEC699, SEC560, SEC504
  - SANS SEC564 Author: Red Team Exercises and Adversary Emulation
- Contributor
  - MITRE ATT&CK and Atomic Red Team
  - CVSSv3.1 Working Group Voting Member
  - GFMA: Threat-Led Pentest Framework

@JORGEORCHILLES

Agenda

- History of Offensive Security Assessments
- What is Purple Team
- Purple Team Exercise Framework
- First Purple Team Exercise
- Operationalized Purple Team
- Purple Team Maturity Model

Thanks @bareiss_patrick for meme

My* History of Offensive Security

- *Based on my experience, yours may be different
- Every organization is different and offsec is about bringing **business value**
- If I started today, I would do Purple Team Exercises before Red Team
- Evolve from CVE to TTP

https://www.scythe.io/library/scythes-ethical-hacking-maturity-model

InfoSec Teams Work in Silos

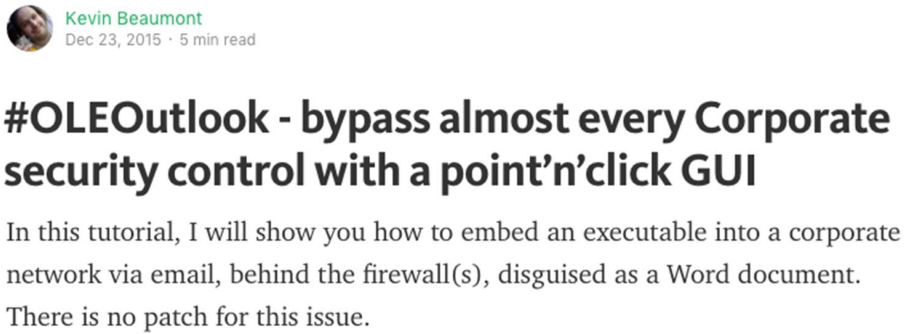
CTI Team

Red Team

Blue Team

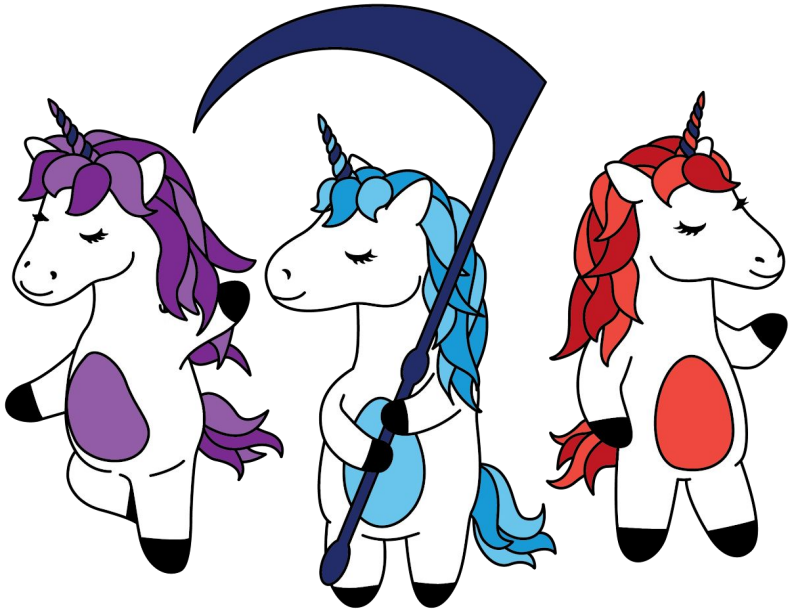
2016 Purple Team Proposal

- 2 Years of Red Teaming and little progress
  - One of the first Red Teams in a major FI - lots of findings, little improvement
- Proposed the Purple Team concept - closed session FS-ISAC Summit 2016
- Mapped to the Cyber Kill Chain (ewww... I know, but that is all we had)
- Case Study used this OLE Outlook issue:
- And meterpreter...



https://github.com/jorgeorchilles/presentations/blob/main/2016-FS-ISAC/PurpleTeam-FS-ISAC.pdf

Towards a Purple Team



@JORGEORCHILLES

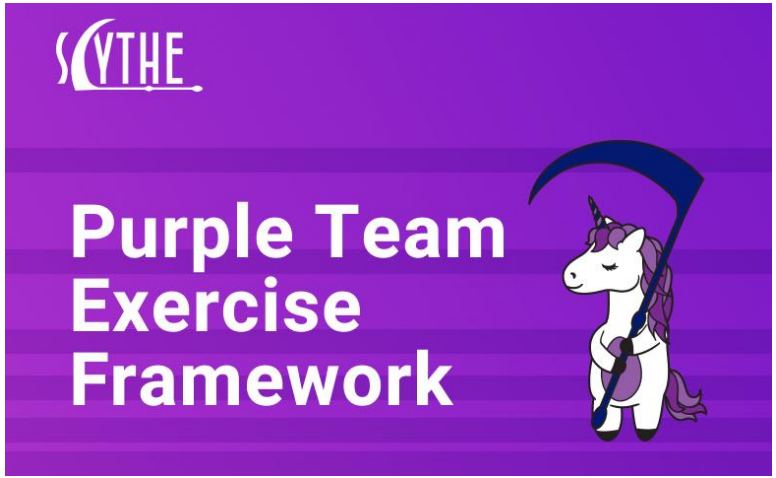
What is a Purple Team?

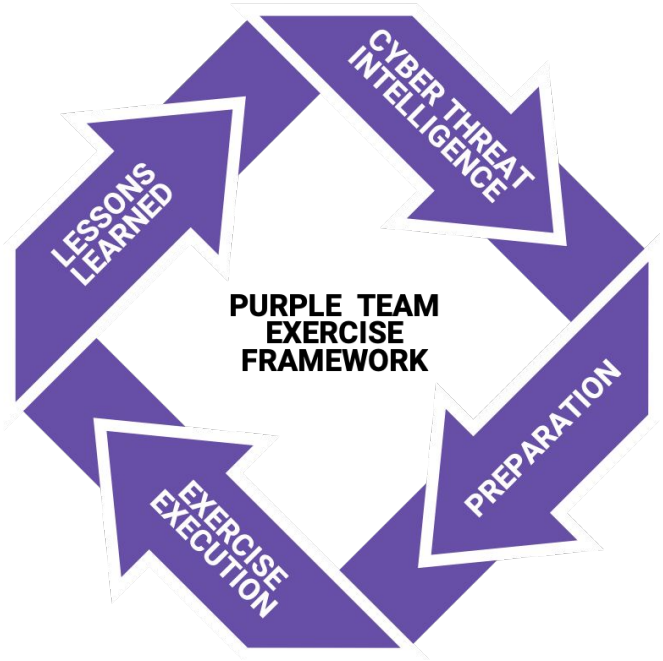
- A Purple Team is a **collaboration** of various information security skill sets.
- Virtual, functional team where teams **work together** to test, measure and improve defensive security posture (people, process, and technology)
  - Cyber Threat Intelligence - research and provide adversary tactics, techniques, and procedures (TTPs)
  - Red Team - offensive team in charge of emulating adversaries and TTPs
  - Blue Team - the defenders. May include but is not limited to Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP).
- Starting to see some dedicated Purple Teams

How do we Purple Team?

Purple Team Exercises	Operationalized Purple Team	Purple Team Maturity Model
• Seperate teams (CTI, Red, Blue) come together for an exercise • Threat informed adversary emulations • Performed on a scheduled basis (e.g. every 3 months)	• Dedicated, internal CTI, Red, and Blue teams work together as virtual team • As new TTPs are discovered, they are analyzed and tested to build detections in a continuous cycle	• Measure threat and detection understanding • Deployment • Integration • Creation

Purple Team Exercise Framework v2

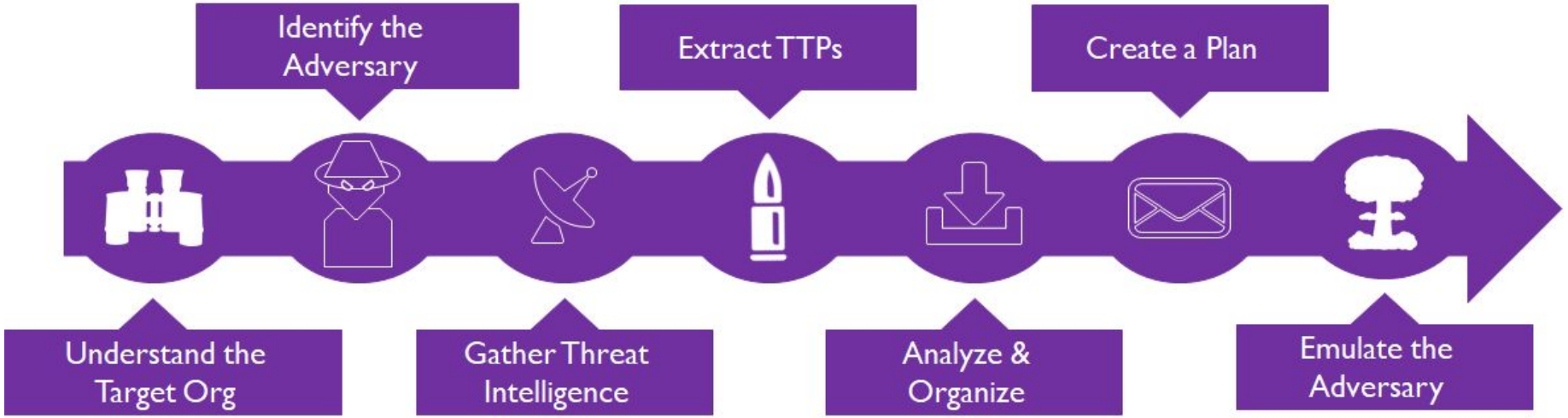




https://github.com/scythe-io/purple-team-exercise-framework

Start with a Purple Team Exercise

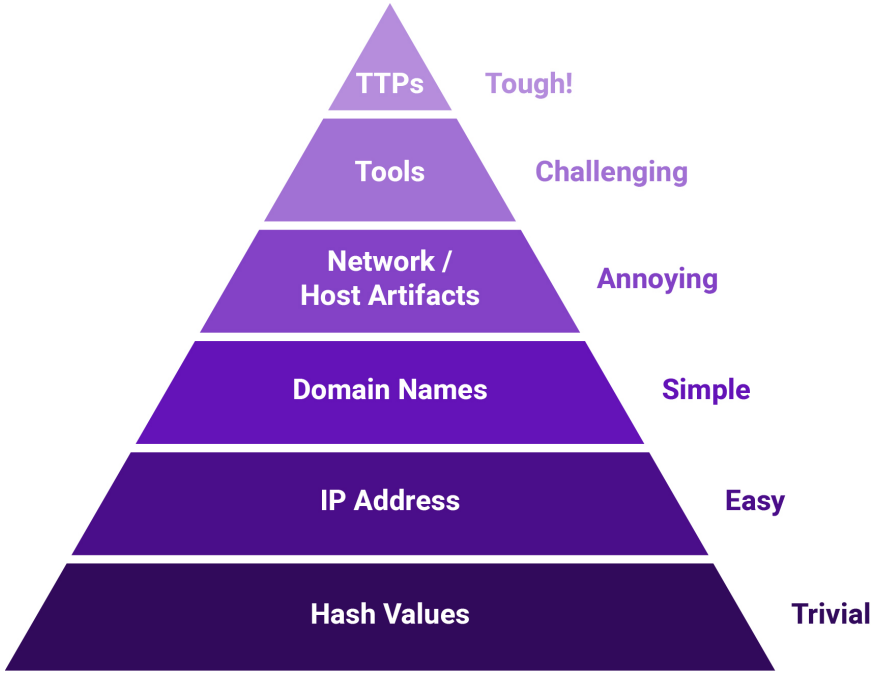
Cyber Threat Intelligence



ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

We want procedure level CTI!

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



Thank You to The DFIR Report

From the domain controller the threat actor ran an encoded PowerShell command to review the size and condition of hard drives across the environment.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0AC
```

Decoded:

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:33242/'); Get-WmiObject -Class win32_logicalDisk -ComputerN
```

Powersploit modules like Get-NetComputer were seen used by the threat actor from the domain controller

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:36595/'); Get-NetComputer -ping -operatingsystem *server*
```

Thank You to The DFIR Report

#ThreatThursday

- Introduce Adversary
- Consume CTI and map to MITRE ATT&CK w/Navigator Layer
- Create Adversary Emulation Plan
  - Share the plan on SCYTHE Community Threat Github: https://github.com/scythe-io/community-threats/
- Attack - Emulate Adversary
- Detect & Respond to the Attack
  - Now with SIGMA rules!
- All free to the community: https://www.scythe.io/threatthursday

Preparation

New to PTEFv2 is considerations for consulting

- Purple Team Pitch
- Planning Meeting 1
- Planning Meeting 2
- Metrics
- Templates: https://github.com/scythe-io/purple-team-exercise-framework/tree/master/Templates

Goals & Objectives

Propose the Purple Team Exercise set goals and objectives

- Foster a collaborative culture within the security organization
- Test attack chains against a target organization
- Train the organization’s defenders (Blue Team)
- Test TTPs that have not been tested before in the organization
- Test the processes between security teams
- Preparation for a zero-knowledge Red Team Engagement
- Red Team reveal or replay after a zero-knowledge Red Team Engagement

Roles & Responsibilities

Title	Role	Responsibility
Project Manager	Exercise Coordinator	Lead point of contact throughout the entire Purple Team Exercise. Responsible for ensuring 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.
Head of Security	Sponsor	Approve Purple Team Exercise and Budget
Cyber Threat Intelligence	Sponsor	Cyber Threat Intelligence
Red Team Manager	Sponsor	Preparation: Define Goals, Select Attendees
Blue Team Manager	Sponsor	Preparation: Define Goals, Select Attendees
Red Team	Attendee	Preparation, Exercise Execution
Blue Team	Attendee	Preparation, Exercise Execution

Time Requirements

- From single day to multi-week exercises
- Preparation time is based on the defined goals, guidance or constraints set by sponsors, and emulated adversary's TTPs

Preparation	Exercise	Lessons Learned
Days-Weeks	Hours-Days-Weeks	TBD

Logistics

- Pick a location
- Virtual or Remote
  - Virtual: Choose a Platform (Zoom, GoToMeeting, etc)
  - For physical locations: SOC locations are ideal as SOC Analysts, Hunt Team, and Incident Response are generally physically present
- Training room or large conference room
- Each attendee should have workstation with media output or screen sharing to show current screen to other participants

Metrics

- Detection
  - Logging events locally
  - Logging events centrally
  - Alerts
  - Telemetry
  - IoCs
  - General Behavior
  - Specific Behavior
- Response
  - Time to Detect
  - Time to Investigate
  - Time to Remediate

Detection

ID	Data Source	Data Component
DS0017	Command	Command Execution
DS0011	Module	Module Load
DS0009	Process	Process Creation
DS0012	Script	Script Execution

https://attack.mitre.org/datasources/

Target Systems

Provision production systems for exercise from golden sources

- Endpoint Operation Systems
  - Standard endpoints - 2 of each (Windows 10, Linux, macOS)
  - Physical systems
  - Virtual Desktop Infrastructure
  - Terminal Services/Citrix
- Server Operating Systems in Environment
  - Windows Servers
  - *nix Servers
  - Include Virtual and Cloud Servers

Security Tools

Request the target systems have production security tools:

- Anti-Virus/Anti-Malware/Anti-Exploit
- Endpoint Detection & Response (EDR)
- Forensic Tools
- Image acquisition
- Live forensics
- Ensure flow of traffic goes through standard, production network-based devices such as firewalls and proxy logs

Blue Team Prep

- Validate security tools are reporting to production security tools from the target systems
- Ensure attack infrastructure is accessible through proxy/outbound controls
- Ensure attack infrastructure is being decrypted (TLS decryption/interception)
- Verify allowlists and notify Red Team
- Work with Red Team as payloads and C2 are tested prior to exercise on non-exercise systems
- Threat Hunting Playbooks - https://threathunterplaybook.com/introduction.html

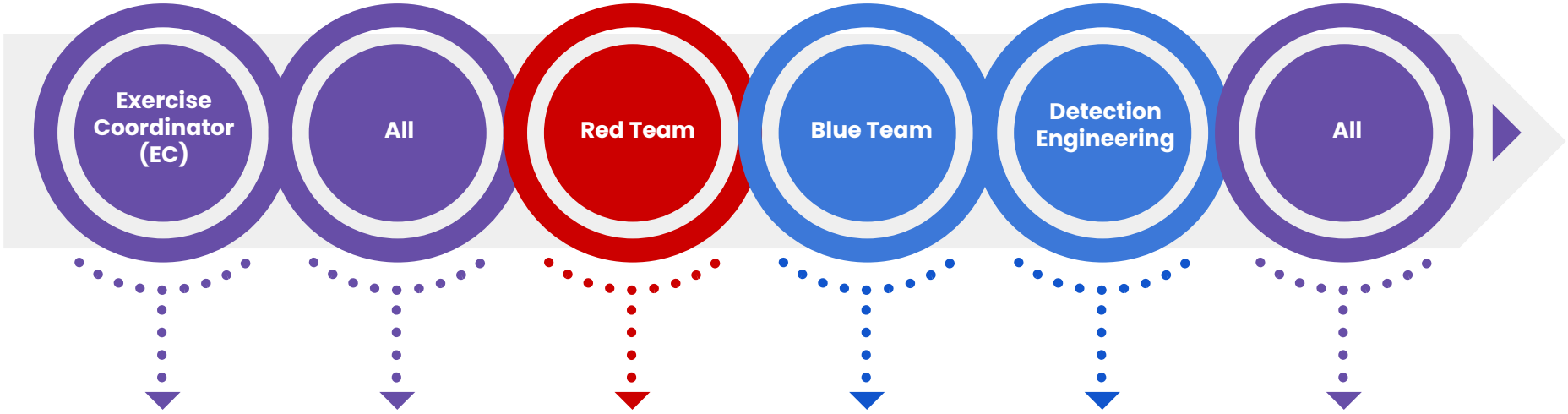
Red Team Prep

- Understand the CTI
- Build the adversary emulation plan
- Do you have to burn your custom stuff?
- Set up attack infrastructure
- Test plan before day of exercise
- Test all access with Blue Team

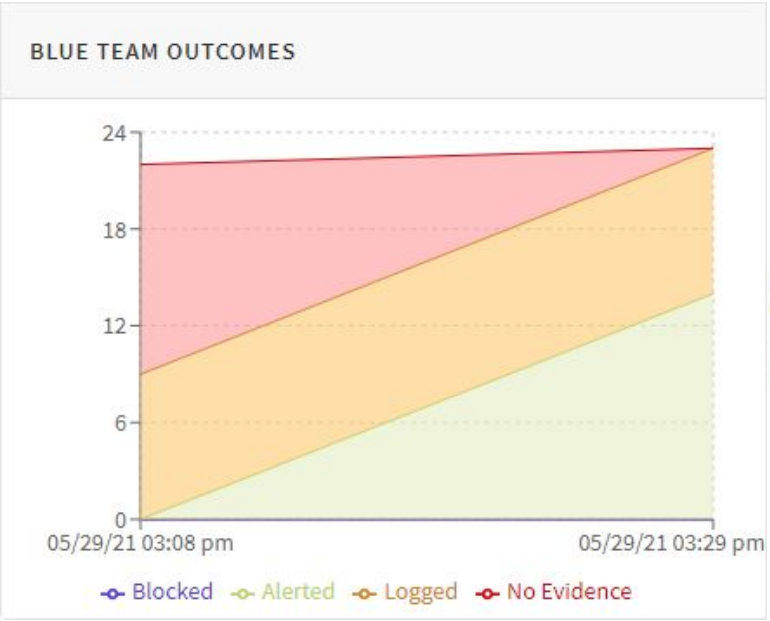
C2 MATRIX

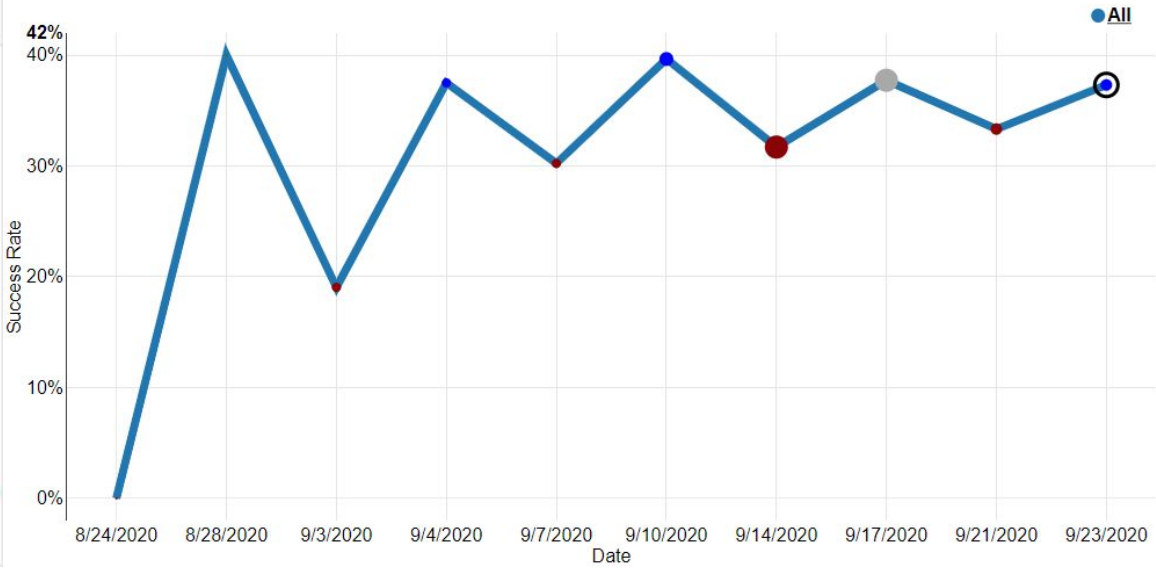
- Google Sheet of C2s
- https://www.thec2matrix.com/
- Find ideal C2 for your needs
- SANS Slingshot C2 Matrix VM
- https://howto.thec2matrix.com
- Follow @C2_Matrix

Purple Team Exercise



Tracking





PlexTrac.com

vectr.io

SHOW VALUE!!!!

- That is what we are here for... providing business value!
- Track each engagement, each improvement, each blue team and red team win!
- Show improvement over time
- This will make you part of the Purple Team Program including people, process, and technology

WILD WEST HACKIN' FEST

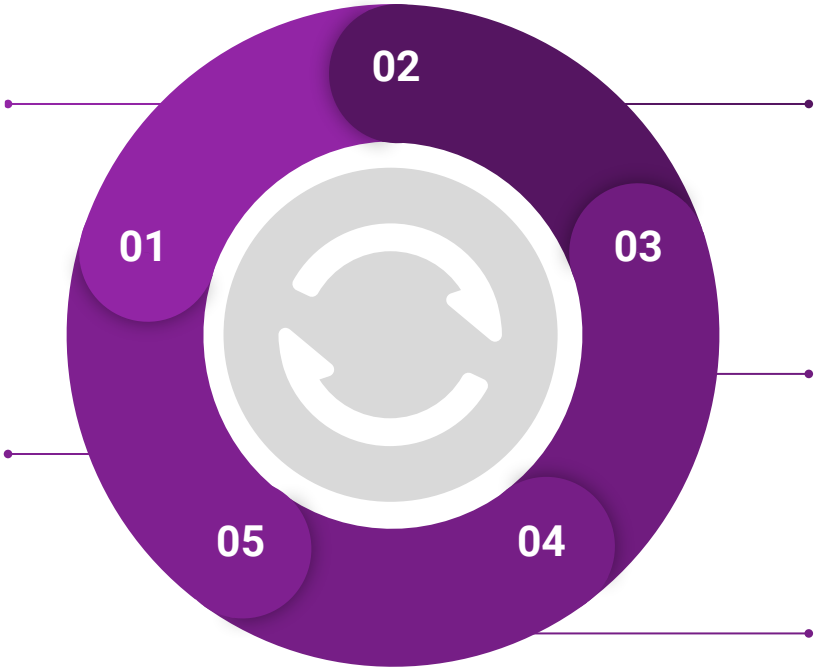
O M G
That worked!
We improved!

What now?

Operationalized Purple Team

New CTI or TTPs
- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Detection Engineering
- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation

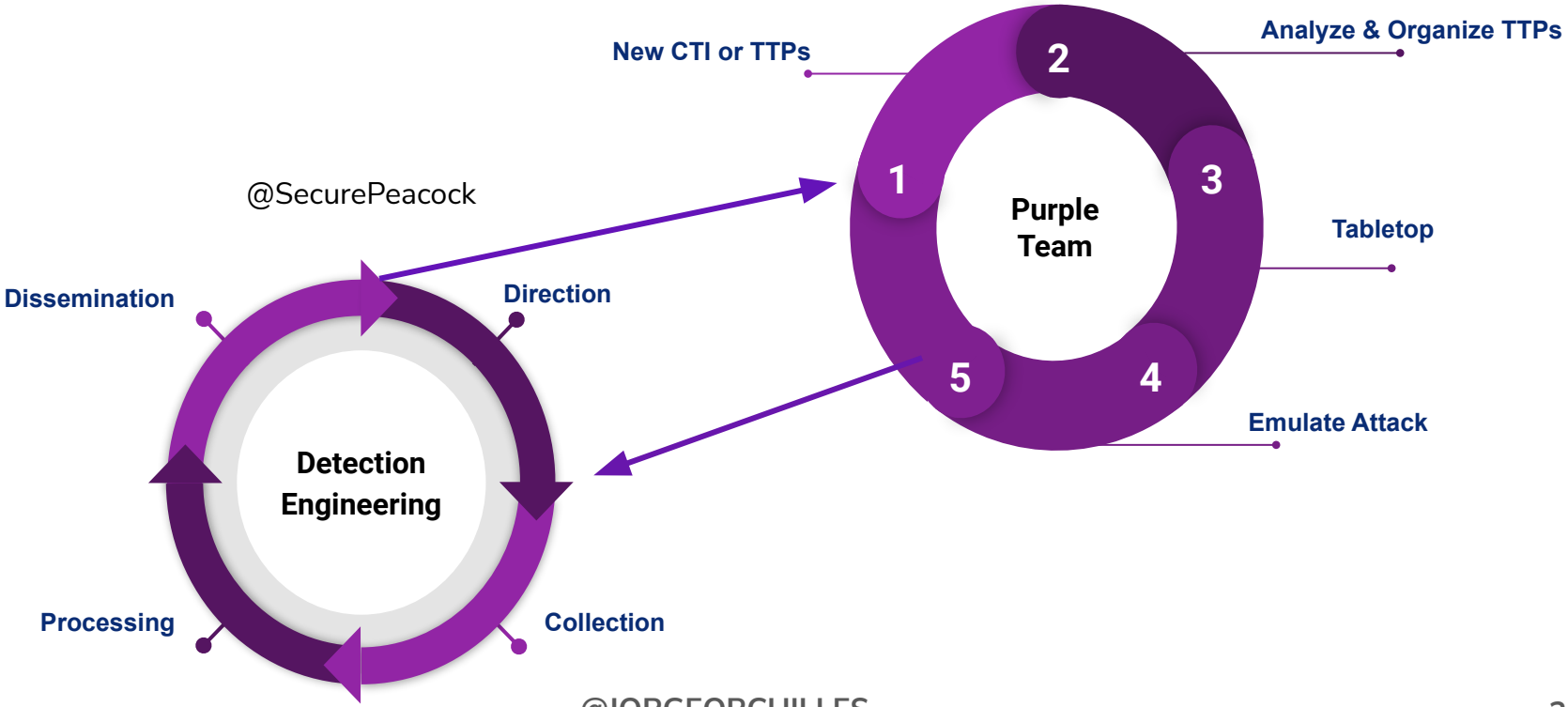


Analyze & Organize TTPs
- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion
- Expected Detection and Response

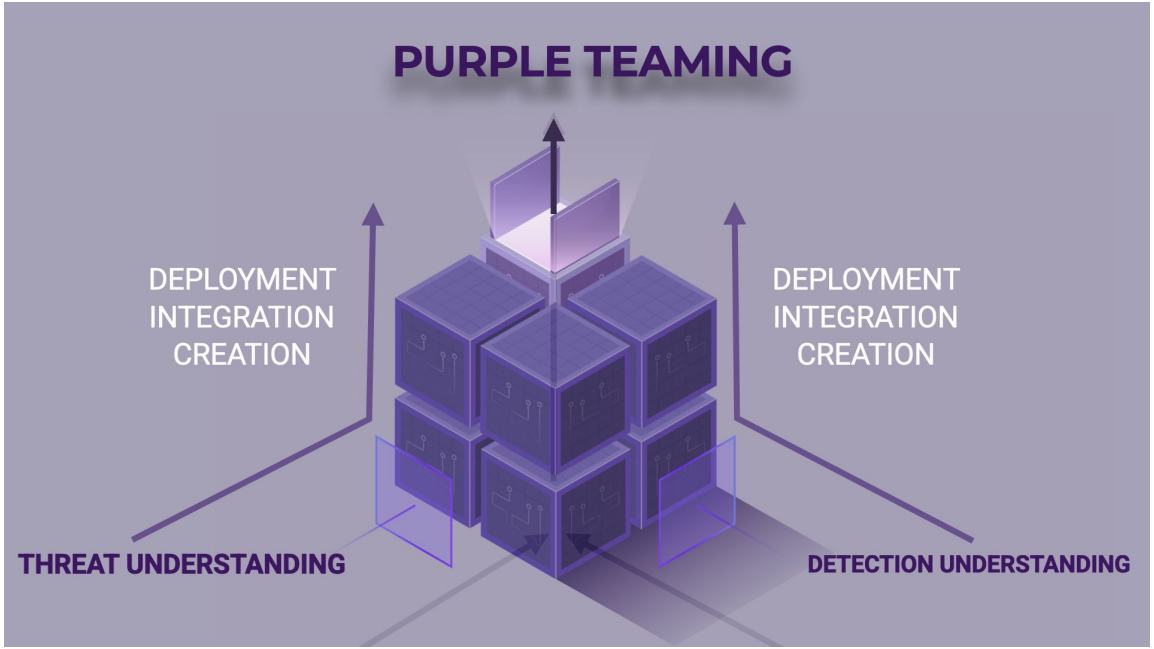
Emulate Attack
- Threat Understanding
- Deployment, Integration, Creation

Detection Engineering



Purple Team Maturity Model

@teschulz



Future

- More Purple Teaming
- Dedicated Purple Teams
- But we need
  - Cyber Threat Intelligence that provides procedure level TTPs
    - ... in machine readable format
  - Larger, standardized Adversary Emulation Libraries
    - MITRE are in YAML: https://github.com/center-for-threat-informed-defense/adversary_emulation_library
    - SCYTHE Community Threats are in JSON: https://github.com/scythe-io/community-threats
    - Atomic Red Team is in YAML: https://github.com/redcanaryco/atomic-red-team/tree/master/atomics

Contribute - Open Invitation

- Edit and submit PRs for the PTEFv2
  - https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv2.md
- Submit Templates
  - https://github.com/scythe-io/purple-team-exercise-framework/tree/master/Templates
- Provide Feedback
  - How are you implementing Purple Teaming in your organization?

References

- Purple Team Exercise Framework: https://github.com/scythe-io/purple-team-exercise-framework
- #ThreatThursday: https://www.scythe.io/threatthursday
- SCYTHE emulation plans: https://github.com/scythe-io/community-threats/
- MITRE emulation plans: https://github.com/center-for-threat-informed-defense/adversary_emulation_library
- Purple Team Maturity Model: https://www.scythe.io/library/introducing-the-purple-team-maturity-model

Thank you!

Questions?