SANS PURPLE TEAM

SANS

Running Your First Purple Team Exercise

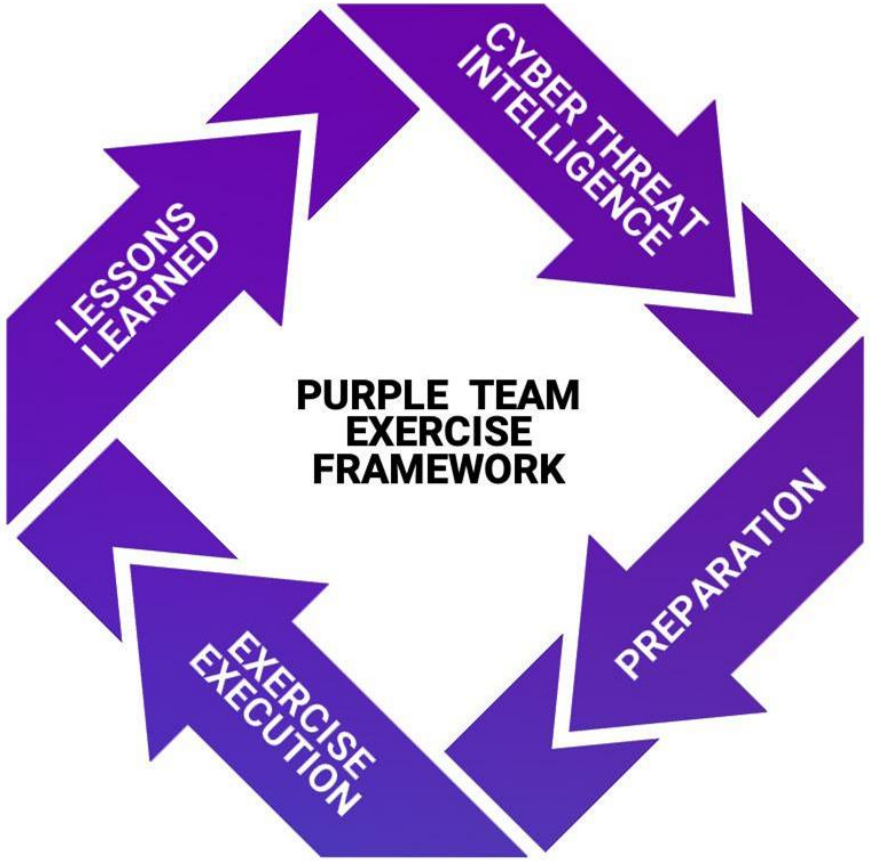
Understand the Cyber Kill Chain, Cyber Threat Intelligence, Attack Emulation, Detection & Response

JORGE ORCHILLES

- Chief Technology Officer
- Certified SANS Instructor: SEC699, SEC599, SEC504
  - Author SEC564: Red Team Exercises and Adversary Emulation
- 10 years @ Citi
- Projects
  - Purple Team Exercise Framework (PTEF)
  - C2 Matrix
  - CVSSv3.1 Voting Member
  - GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow

AGENDA

- What is a Purple Team?
- Purple Team Exercise
  - Framework/Methodology
  - Cyber Threat Intelligence
  - Preparation
  - Purple Team Exercise Flow
  - Tracking & Reporting
- Resources to Learn More



WHAT IS A PURPLE TEAM?

A collaboration between various information 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 tactics, techniques, and procedures (TTPs)
- Red Team - offensive team in charge of emulating adversaries and TTPs
- Blue Team - the defenders. Security Operations Center (SOC), Threat Hunting Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP)

COLLABORATION, WORKING TOGETHER, OH MY…

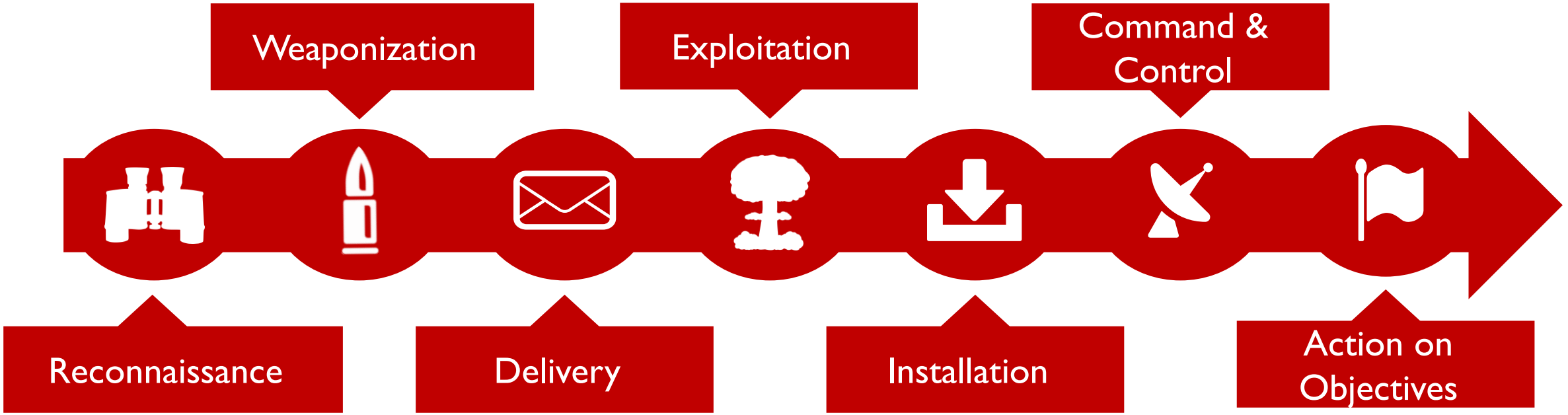
For that, we need a common language

- CVE and CVSS for vulnerabilities in technology
- Understanding attacks:
  - Cyber Kill Chain
  - MITRE ATT&CK
  - Unified Cyber Kill Chain
- Understanding adversary behavior:
  - Pyramid of Pain
  - TTP Pyramid

https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

THE CYBER KILL CHAIN®

One of the first examples of a structured description of attacks was the Cyber Kill Chain®, by Lockheed Martin:



MITRE® ATT&CK™

Adversary Tactics, Techniques, and Common Knowledge

Tactics, Techniques, and Procedures (TTPs) are Adversary Behaviors

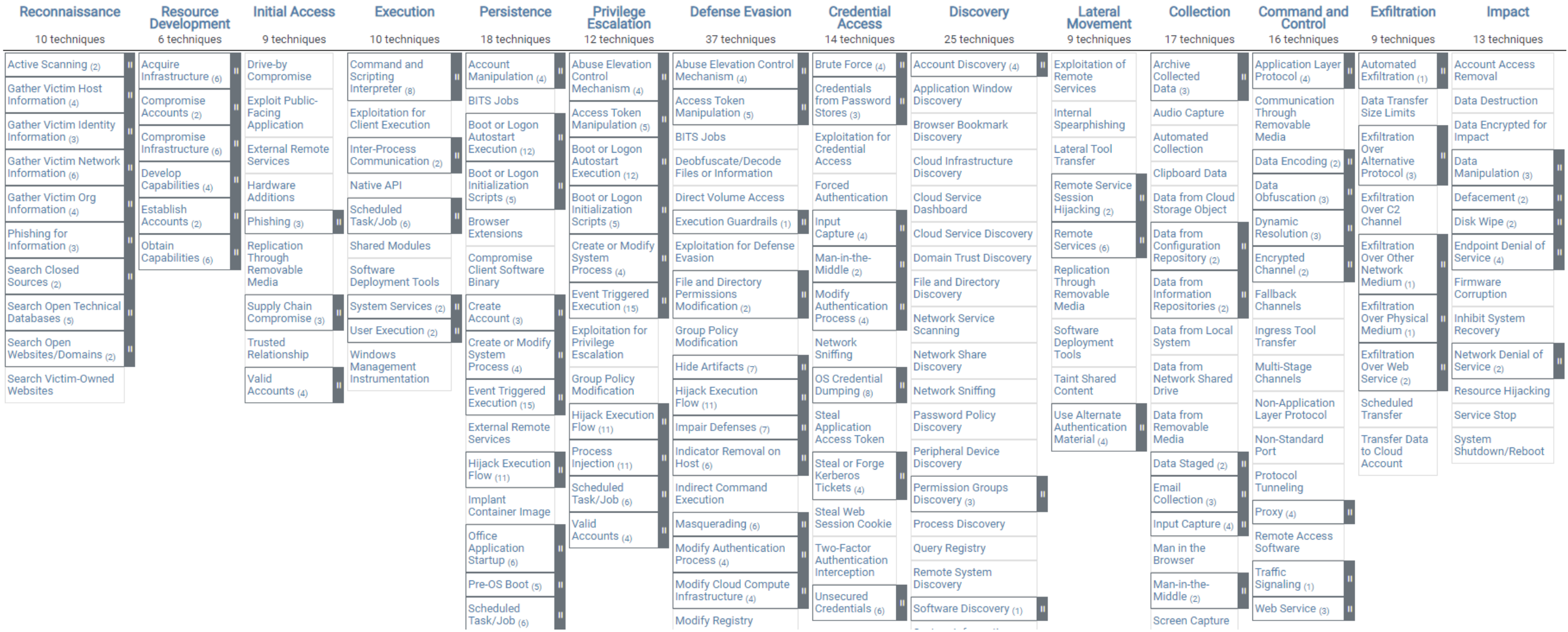
Tactics: 14 high level adversary goals

Techniques: How the adversary achieves their goals

- Sub-Techniques

Procedures: How to perform each technique

MITRE® ATT&CK™ MATRIX



LEVERAGING MITRE ATT&CK

ATT&CK for Adversary Emulation

When organizing adversary emulation (such as red or Purple Team exercises), the emulation plan can be based on MITRE ATT&CK. This facilitates tracking & reporting.

ATT&CK for Threat Intelligence

When consuming or generating Threat Intelligence, observed adversary behavior can be mapped to MITRE ATT&CK. Several platforms support this mapping (e.g., MISP has a MITRE ATT&CK mapping).

ATT&CK for Detection Capability

The overall detection capability of an organization can be mapped to MITRE ATT&CK. This facilitates, for example, reporting on the maturity / scope of the SOC.

ATT&CK for Defense Prioritization

In addition to measuring the detection coverage using MITRE ATT&CK, we can do the same for preventive controls. What MITRE ATT&CK techniques do we actively block?

Organizations should leverage MITRE ATT&CK as the **common language**!

DEFINING ADVERSARY EMULATION

Adversary emulation is an activity where security experts emulate how an adversary operates. The ultimate goal, of course, is to improve how resilient the organization is versus these adversary techniques.

Both Red and Purple Teaming can be considered as adversary emulation.

TTP

Adversary activities are described using TTPs (Tactics, Techniques & Procedures). These are not as concrete as, for example, IOCs, but they describe how the adversary operates at a higher level. Adversary emulation should be based on TTPs. As such, a traditional vulnerability scan or internal penetration test that is not based on TTPs should not be considered adversary emulation.

ATT&CK

Adversary emulation should be performed using a structured approach, which can be based on a kill chain or attack flow. MITRE ATT&CK is a good example of such a standard approach.

PENETRATION TEST VS. ADVERSARY EMULATION

PENETRATION TEST	VS.	ADVERSARY EMULATION
Identify and exploit vulnerabilities on a (series of) system(s) to assess security		Assess how resilient an organization is versus a certain adversary / threat actor
Focused on a specific scope (typically an application or network range)		Focused on the execution of a scenario (typically defined by a number of flags)
Primarily tests prevention, typically less focus on detection		Typically tests both prevention and detection (so is less valuable if there is no Blue Team)

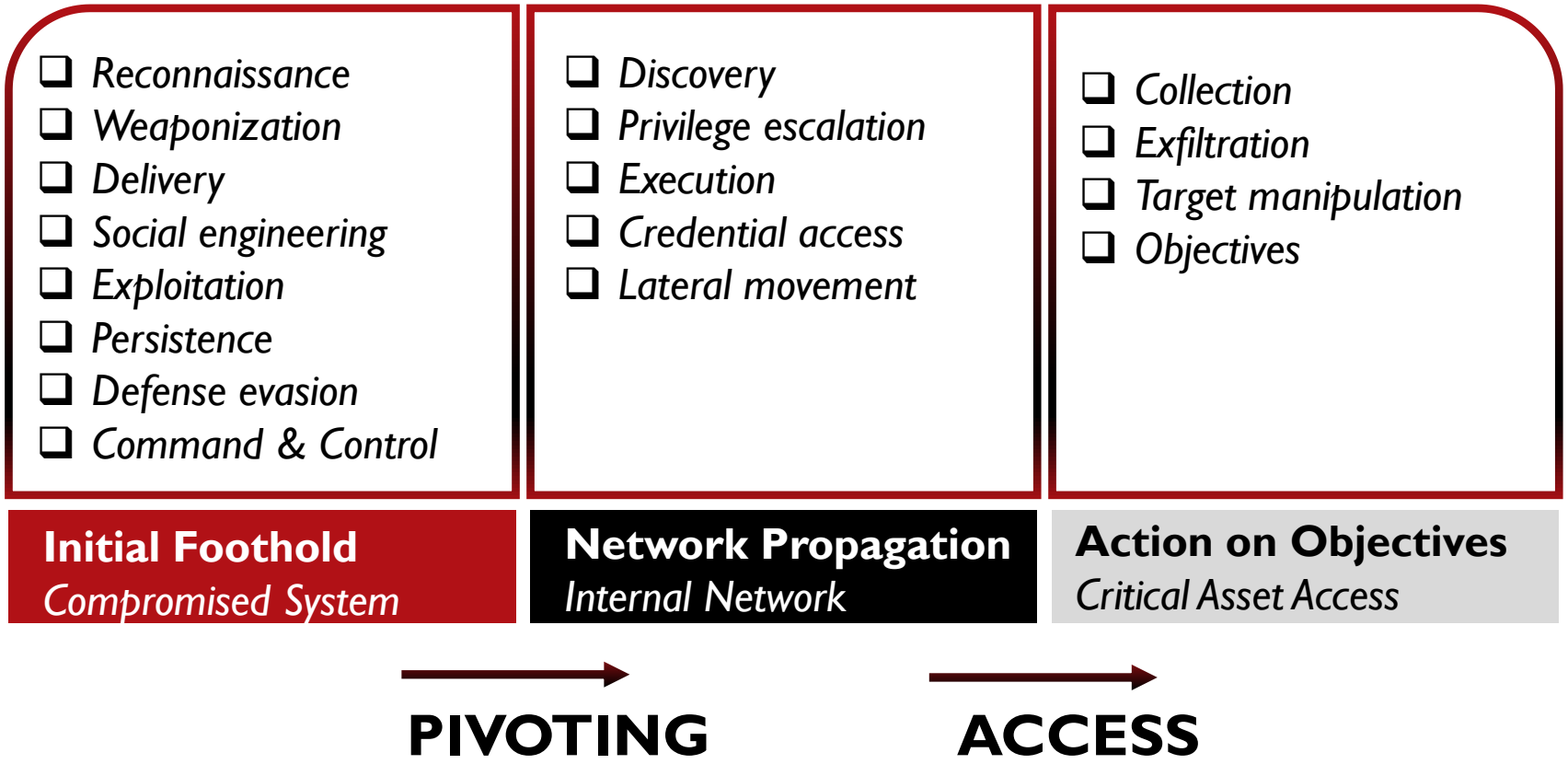
Both Penetration Tests and Adversary Emulation engagements have value. However, it's important to know the difference and the results you can expect!

RED TEAM VS. PURPLE TEAM

RED TEAM	VS.	PURPLE TEAM
A Red Team involves emulation of a realistic threat actor (using TTPs)		A Purple Team involves emulation of a realistic threat actor (using TTPs)
In a typical Red Team, interaction with the Blue Team is **limited** (red vs. blue)		In a typical Purple Team, interaction with the Blue Team is **maximized** (collaboration)
The goal of the Red Team is to **assess** how well the Blue Team prevents and detects		The goal of the Purple Team is to **improve** how well the Blue Team prevents and detects

Both Red Team and Purple Team engagements have value. However, it's important to know the difference and the results you can expect!

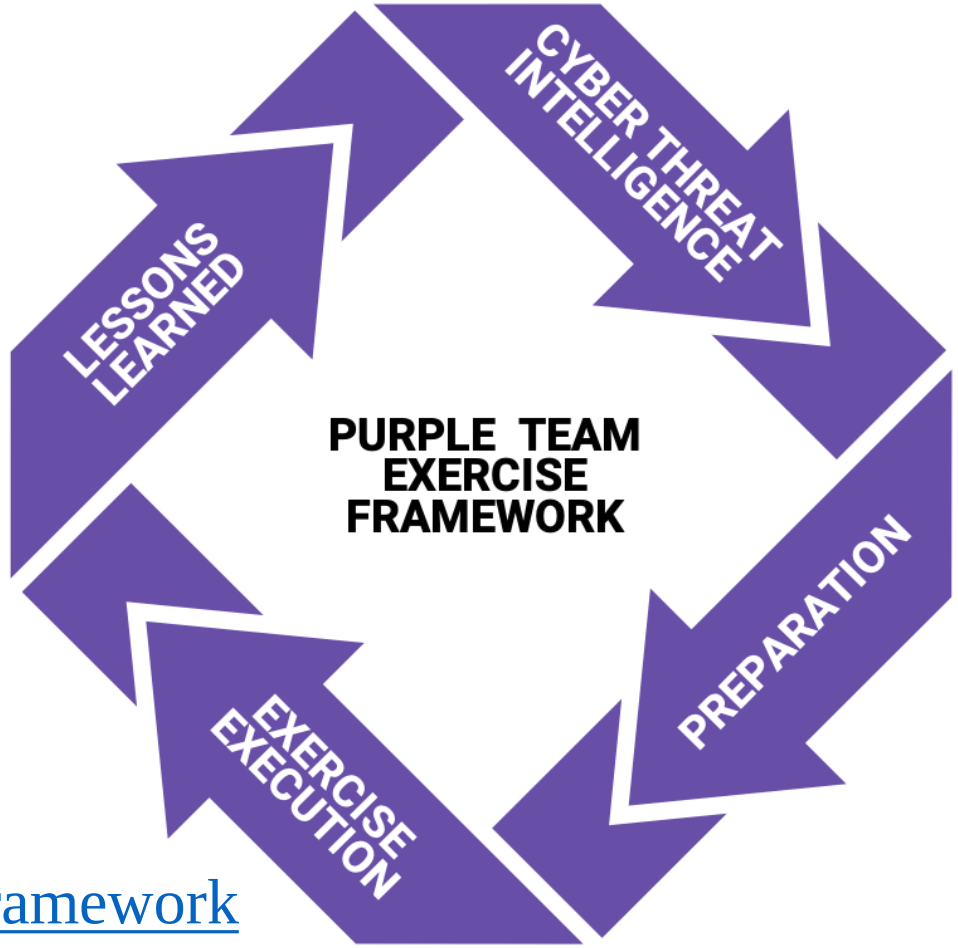
UNIFIED KILL CHAIN – PAUL POLS



The Unified Kill Chain is a good answer to some of the Cyber Kill Chain® limitations!

PURPLE TEAM EXERCISE FRAMEWORK (PTEF)

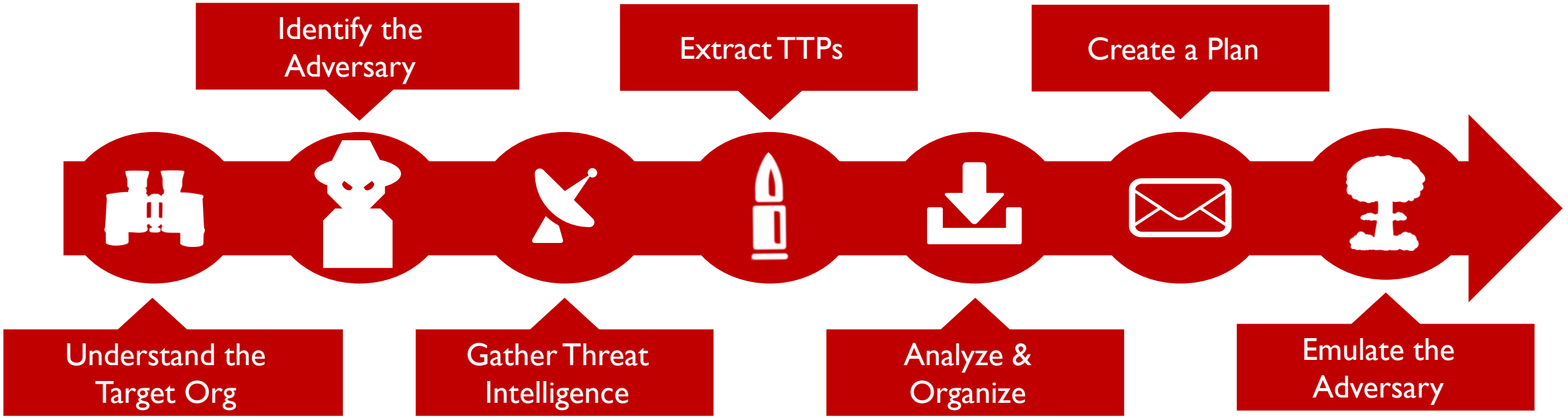
- SCYTHE and industry experts collaborated to create the Purple Team Exercise Framework (PTEF) to facilitate performing adversary emulations as Purple Team Exercises
- Industry led vs. Regulatory led



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

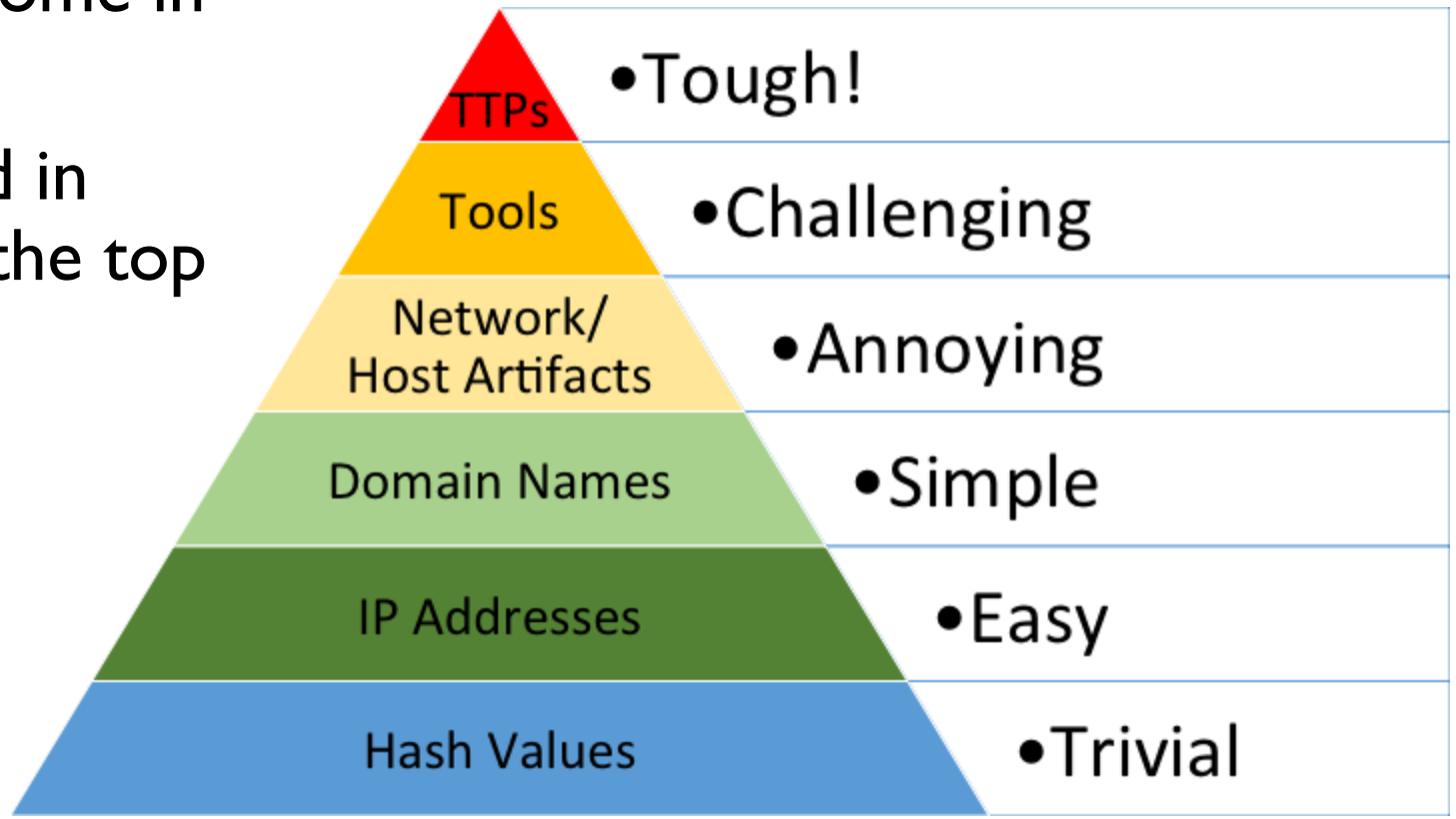
CYBER THREAT INTELLIGENCE FOR ADVERSARY EMULATION

***"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."* (Gartner)**



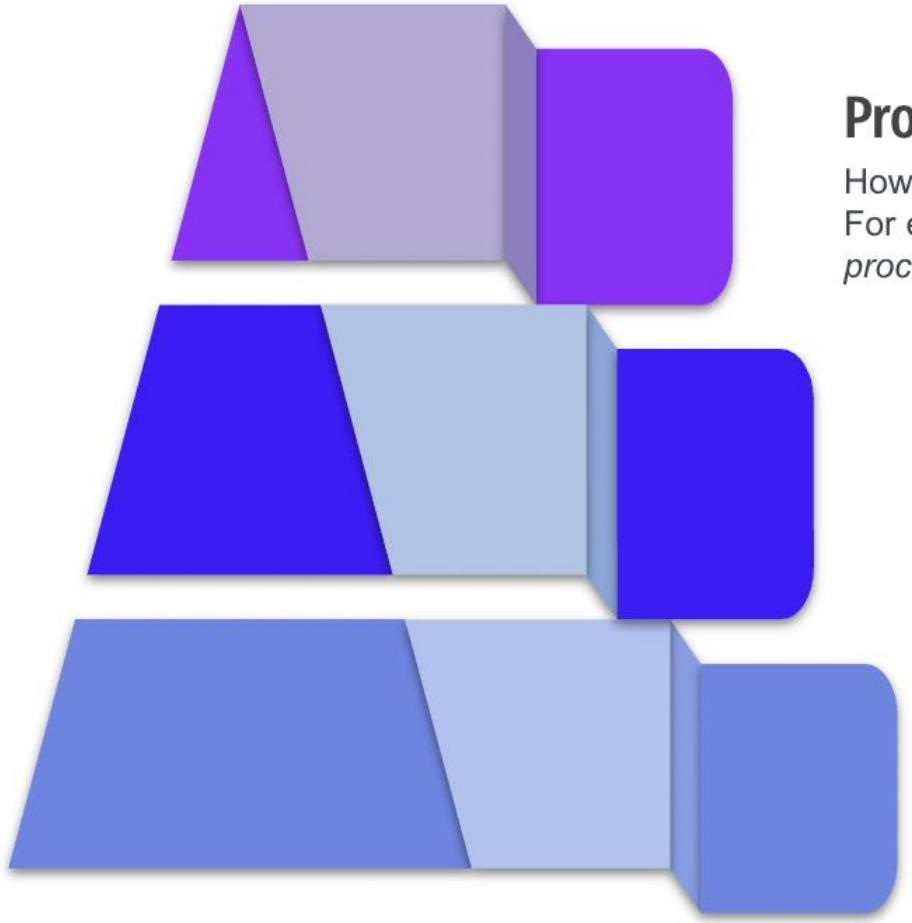
TYPES OF THREAT INTELLIGENCE

- Threat Intelligence will come in various forms
- Purple Team is interested in threat intelligence from the top of the pyramid (TTPs)



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

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.

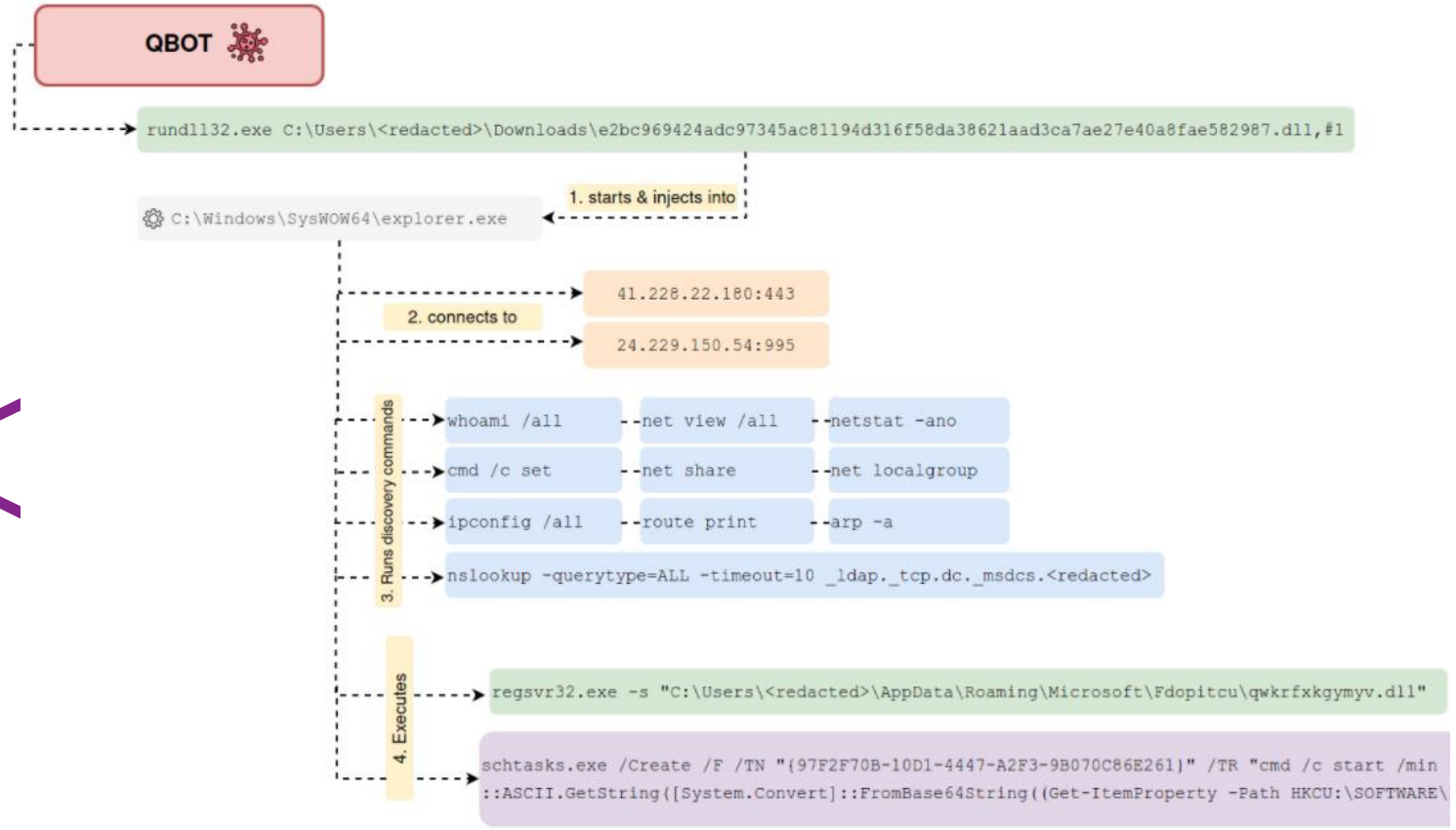
Tactics

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

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

PROCEDURE-LEVEL INTEL

- Exploitation for Privilege Escalation – T1068
- Service Execution – T1569.002
- Network Share Discovery – T1135
- Pass the Hash – T1550.002
- PowerShell – T1059.001
- Windows Command Shell – T1059.003
- Network Share Discovery – T1135
- Obfuscated Files or Information – T1027
- Scheduled Task – T1053.005
- Process Injection – T1055
- Remote System Discovery – T1018
- Obfuscated Files or Information – T1027
- Domain Trust Discovery – T1482
- Domain Groups – T1069.002
- System Owner/User Discovery – T1033
- Network Share Discovery – T1135
- Remote Services – T1021
- Local Account – T1087.001
- Security Software Discovery – T1518.001



https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/

ADVERSARY EMULATION PLAN

Build and document an adversary emulation plan

Examples here: https://github.com/scythe-io/community-threats

- How can we **emulate** the technique? What tools do we need? (Red Team)
- What controls could potentially **stop the technique**? (Blue Team)
- How could we possibly **detect the technique**? (Blue Team)
- Add template fields to **document detection & success** of technique emulation (Red & Blue Team)

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

PREPARATION - 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

PREPARATION – SECURITY CONTROLS

Ensure 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

PREPARATION - METRICS

- Detection
  - Logging events locally
  - Logging events centrally
  - Alerts
- 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

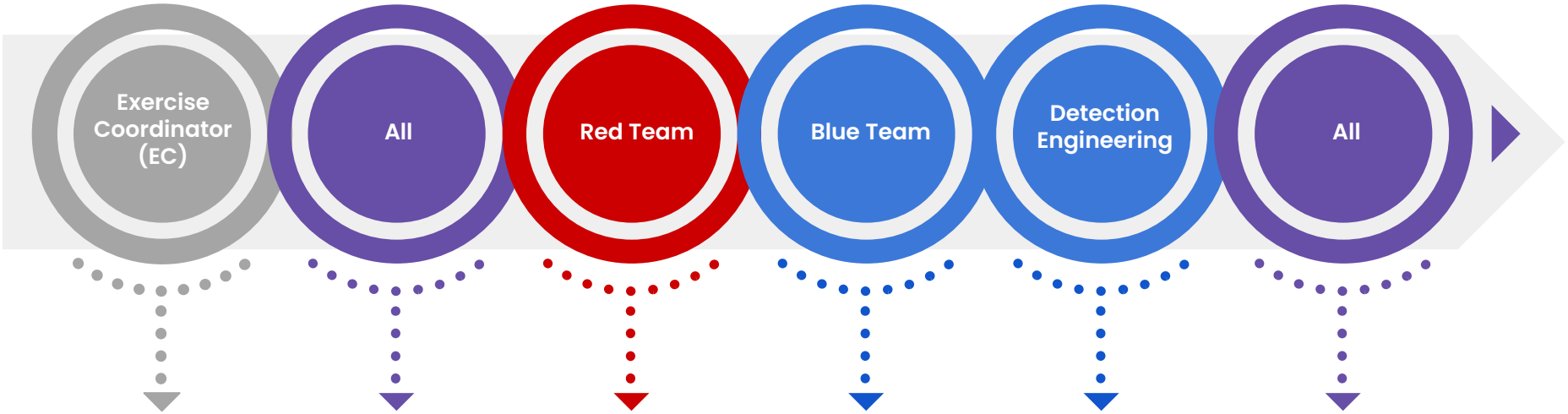
https://attack.mitre.org/datasources/

PREPARATION – RED TEAM

- Understand the CTI
- Build the adversary emulation plan
- Set up attack infrastructure
- Test plan before day of exercise
- Test all access with Blue Team

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

EXERCISE EXECUTION - FLOW

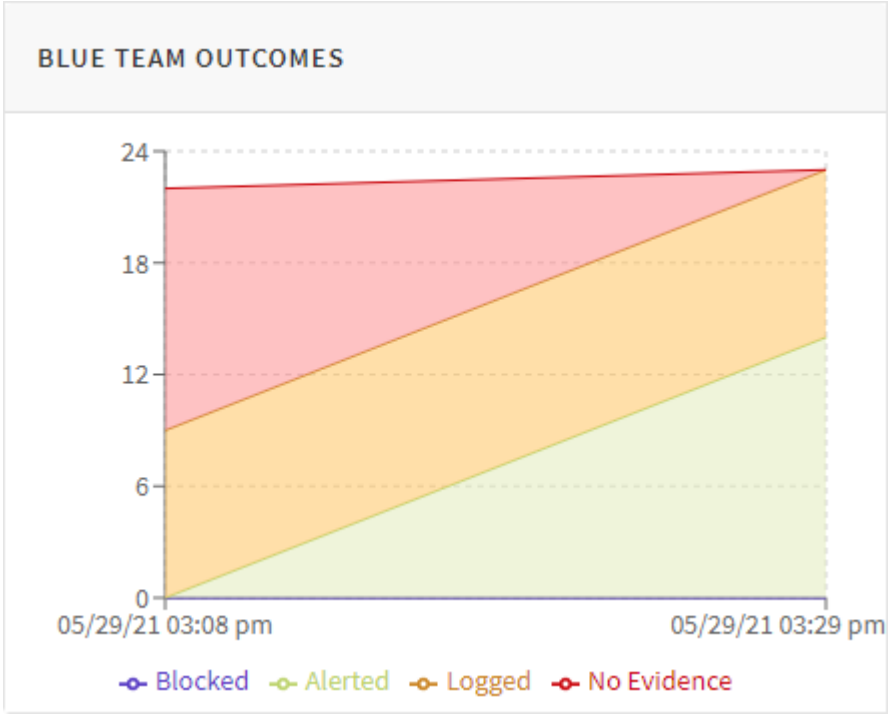


TRACKING AND REPORTING

Show the value!

Track each engagement, each improvement, each blue team and red team win!

Show improvement over time



MORE RESOURCES

- SANS Purple Team: https://www.sans.org/purple-team/
- Blogs: https://www.sans.org/blog/?focus-area=purple-team
- Workshops: https://www.scythe.io/purple-team-workshops
  - Next one on March 31 focusing on Detection Engineering
- SANS Courses
  - SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
  - SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

SANS PURPLE TEAM COURSES

SEC504 -> SEC599 -> SEC699

What are the key differences?

SEC599 Defeating Advanced Adversaries Purple Team Tactics & Kill Chain Defenses	SEC699 Advanced Purple Team Tactics Adversary Emulation for Breach Prevention & Detection
Purple Team class: Focus on Red (20%) & Blue (80%)	Purple Team class: Focus on Red (50%) & Blue (50%)
20% emulation, 50% prevention, 30% detection	50% emulation, 0% prevention, 50% detection
50% lecture - 50% hands-on	40% lecture - 60% hands-on

SANS

Thank You!
Questions?

@JorgeOrchilles