SANS PURPLE TEAM

SANS

Purple Team Interactive Poster Walkthrough

Jorge Orchilles

Erik Van Buggenhout

JORGE ORCHILLES

- Chief Technology Officer
- Principal 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

ERIK VAN BUGGENHOUT

- Co-Founder and Partner at NVISO

  - 2013 – 2016: Pentest / Red Teaming
  - 2016 – 2020: CSIRT / Threat hunting
  - 2020 – NOW: Managed Security Services

- Senior Instructor at SANS

  - 2013 – 2017: Instructor SEC560 / SEC542
  - 2017 – NOW: Instructor & Author SEC599
  - 2019 – NOW: Instructor & Author SEC699

AGENDA

- What is a Purple Team?
- Purple Team Poster
  - Introduction
  - Tools: Red Team & Blue Team
  - Framework: ATT&CK
  - Threat Actors: FIN6, APT28, APT33
  - Emulation & Detection
  - Tracking
  - Purple Team Exercise Framework
- 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)

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!

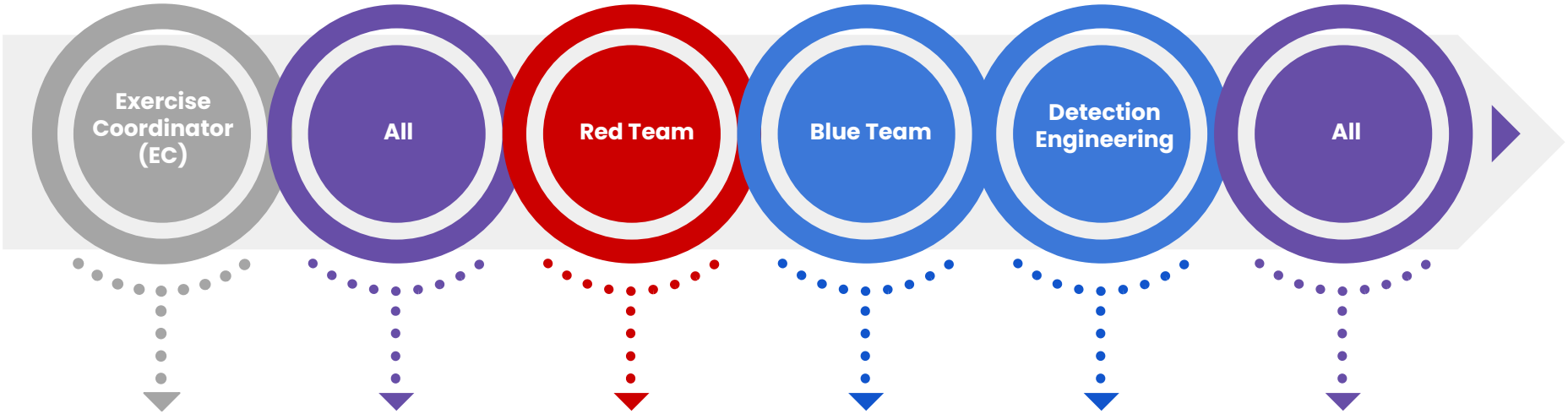
RED TEAM VS. PURPLE TEAM

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!

PURPLE TEAM EXERCISE

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



PURPLE TEAM POSTER WALKTHROUGH

https://www.sans.org/posters/purple-concepts-bridging-the-gap/

MORE RESOURCES

- SANS Purple Team: https://www.sans.org/purple-team/
- Blogs: https://www.sans.org/blog/?focus-area=purple-team
- 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
@ErikVaBu