

An illustration depicting a cybersecurity environment. On the left, five individuals wearing red hoodies and headsets are seated at a desk, representing the Red Team. On the right, five individuals wearing blue hoodies and headsets are seated at a desk, representing the Blue Team. A vertical line, colored red on the left and blue on the right, separates the two teams. The background is dark with subtle lighting effects.

Red Team x Blue Team

Empregabilidade e importâncias nas operações de segurança em ambientes corporativos

Whoami

- Joas Antonio dos Santos
- Head de segurança ofensiva
- Autor de livros ->
- Contribuidor do Mitre



Red Team x Blue Team: Funções



Red Team

- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



Blue Team

- Defensive Security
- Infrastructure Protection
- Damage Control
- Incident Response
- Operational Security
- Threat Hunting
- Digital Forensics

Red Team x Blue Team: Objetivos

Red Team vs. Blue Team Cybersecurity

Red Team

Launches coordinated penetration attacks to test strength and coverage of overall security systems.

Mimics attacks like phishing, social engineering, and employee impersonation.

Operates from a current, "present-moment" view of a company's cybersecurity measures.

Team members need a strong background in software development for custom tool and strategy creation.

Blue Team

Responds to attacks launched by the red team.

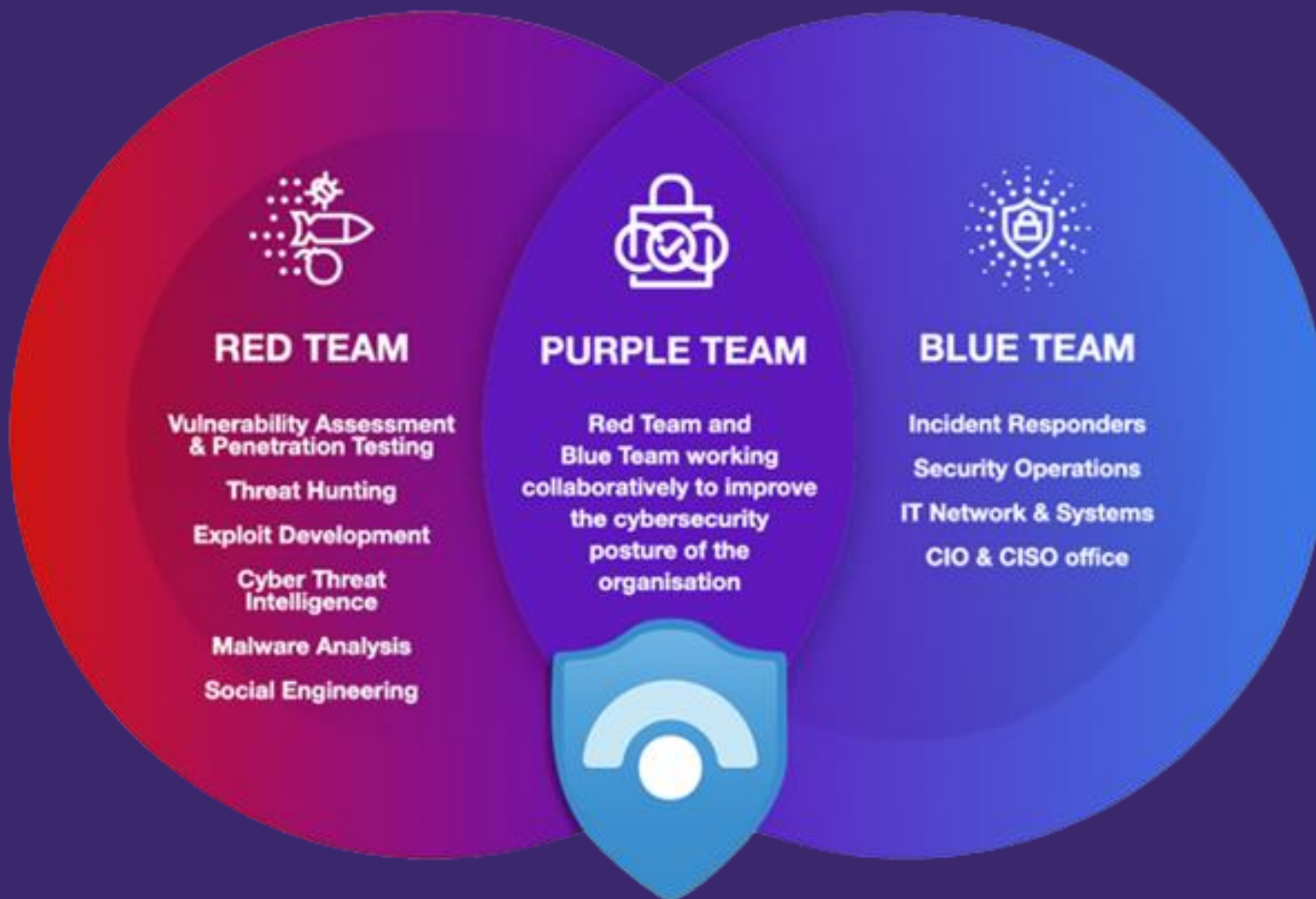
Has to constantly strengthen the overall cybersecurity posture for a company or clients.

Utilizes tools like log and memory analysis, PCAP, risk intelligence, digital footprint analysis and more.

Has a more holistic, "bird's eye" view of a company's entire security strategy.



Purple Team: Conceito

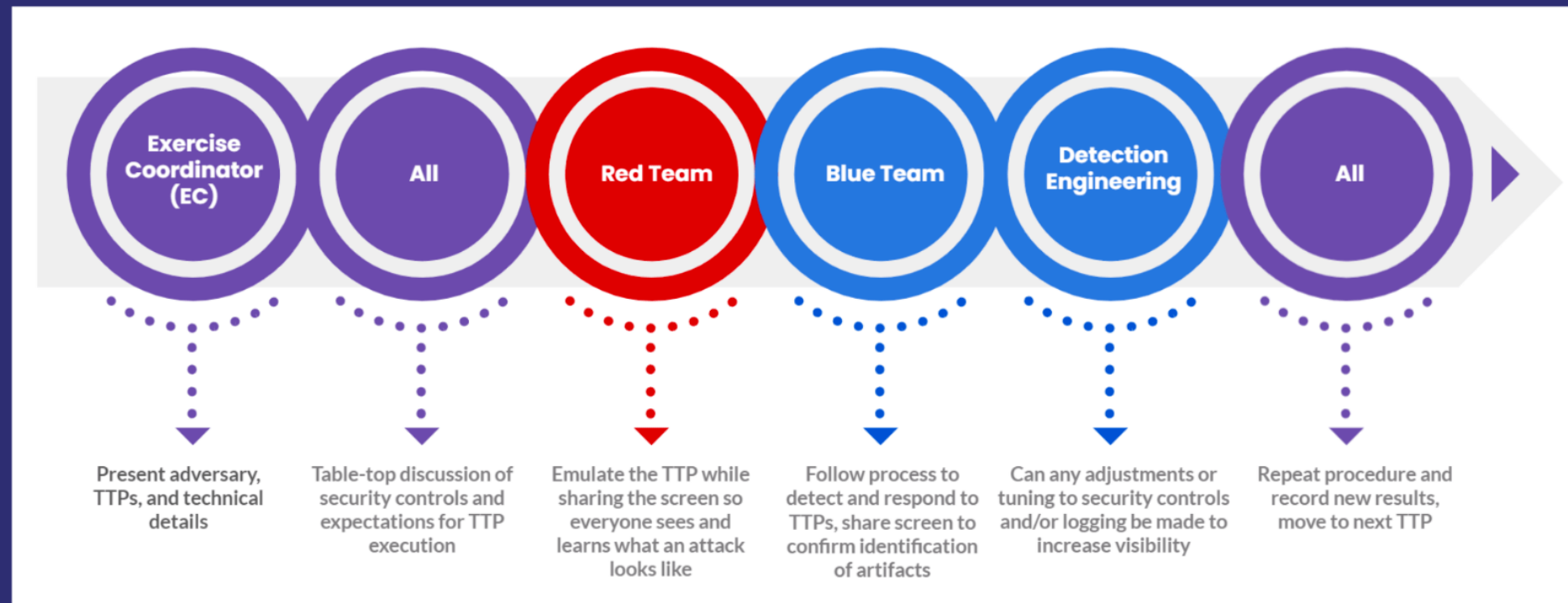


Purple Team: Objetivo

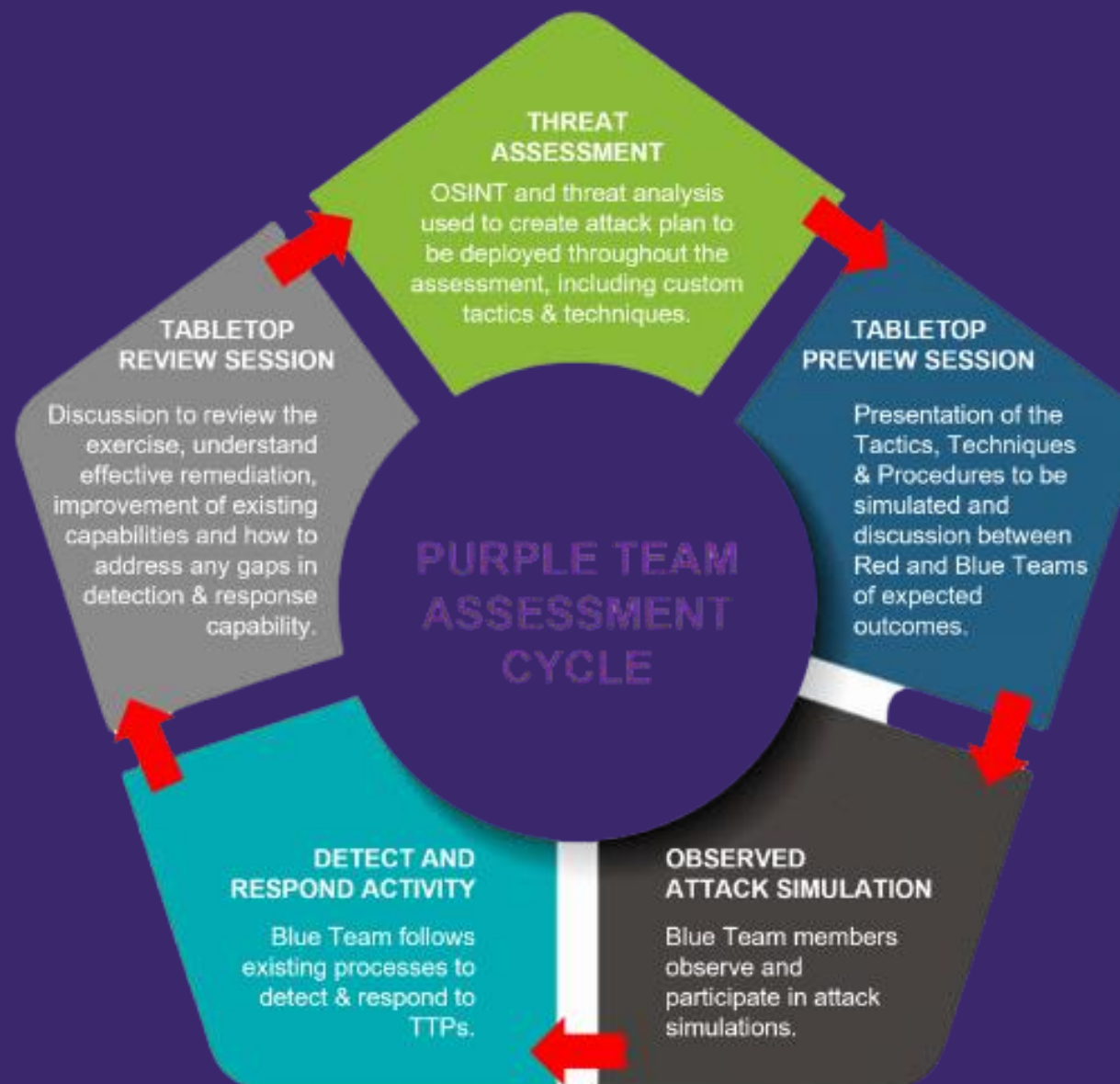
🔗 Purple Teaming What this exercise covers?



Red, Blue and Purple Teaming



Purple Team: Ciclo de avaliação



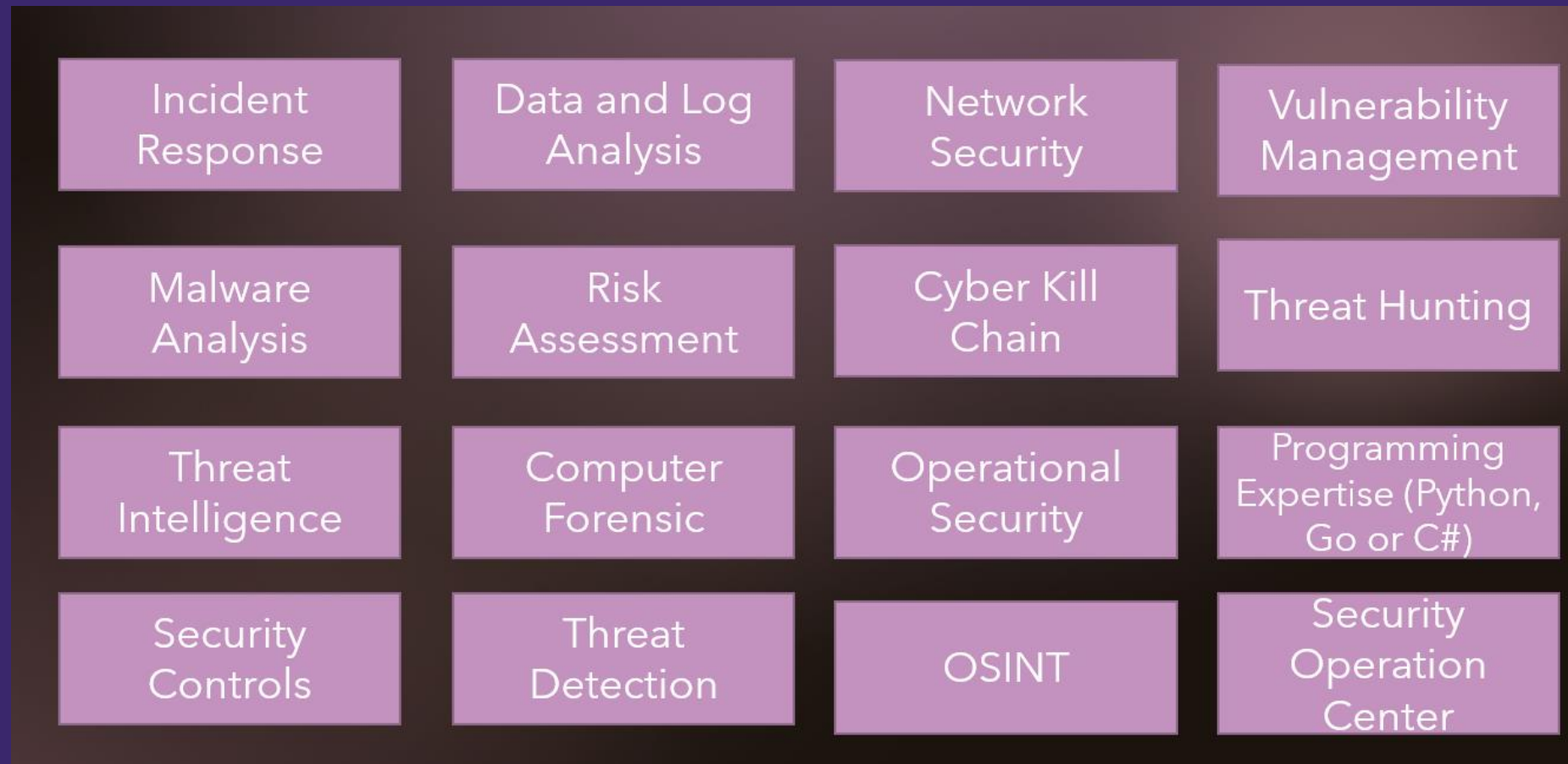
Purple Team: Resultados esperados do Exercícios/Avaliação

Before purple teaming			After purple teaming		
Execution	Persistence	Lateral Movement	Execution	Persistence	Lateral Movement
Hardware additions	AppCert DLLs	Logon scripts	Hardware additions	AppCert DLLs	Logon scripts
Valid accounts	Logon Scripts	Pass the ticket	Valid accounts	Logon Scripts	Pass the ticket
Supply chain compromise	Application shimming	Remote file copy	Supply chain compromise	Application shimming	Remote file copy
		Remote services			Remote services

Empregabilidade do Red Team

PenTest	Social Engineering	Mitre Attack	Physical PenTest
Adversary Emulation	Exploit Development	Cyber Kill Chain	Threat Hunting
Cloud Attack	Defense Evasion	Cyber Threat Intelligence	Programming Expertise (Python, Go or C#)
Threat Modeling	Command and Control	Risk Identified	Hardware Hacking

Empregabilidade do Blue Team



RTFM e BTFM



Na prática

- Wazuh OVA
- Windows Server 2016 Vulnerável
- Kali Linux

OBRIGADO!

