Red Team x Blue Team

Empregabilidade e importâncias nas operações de segurança em ambientes corporativos

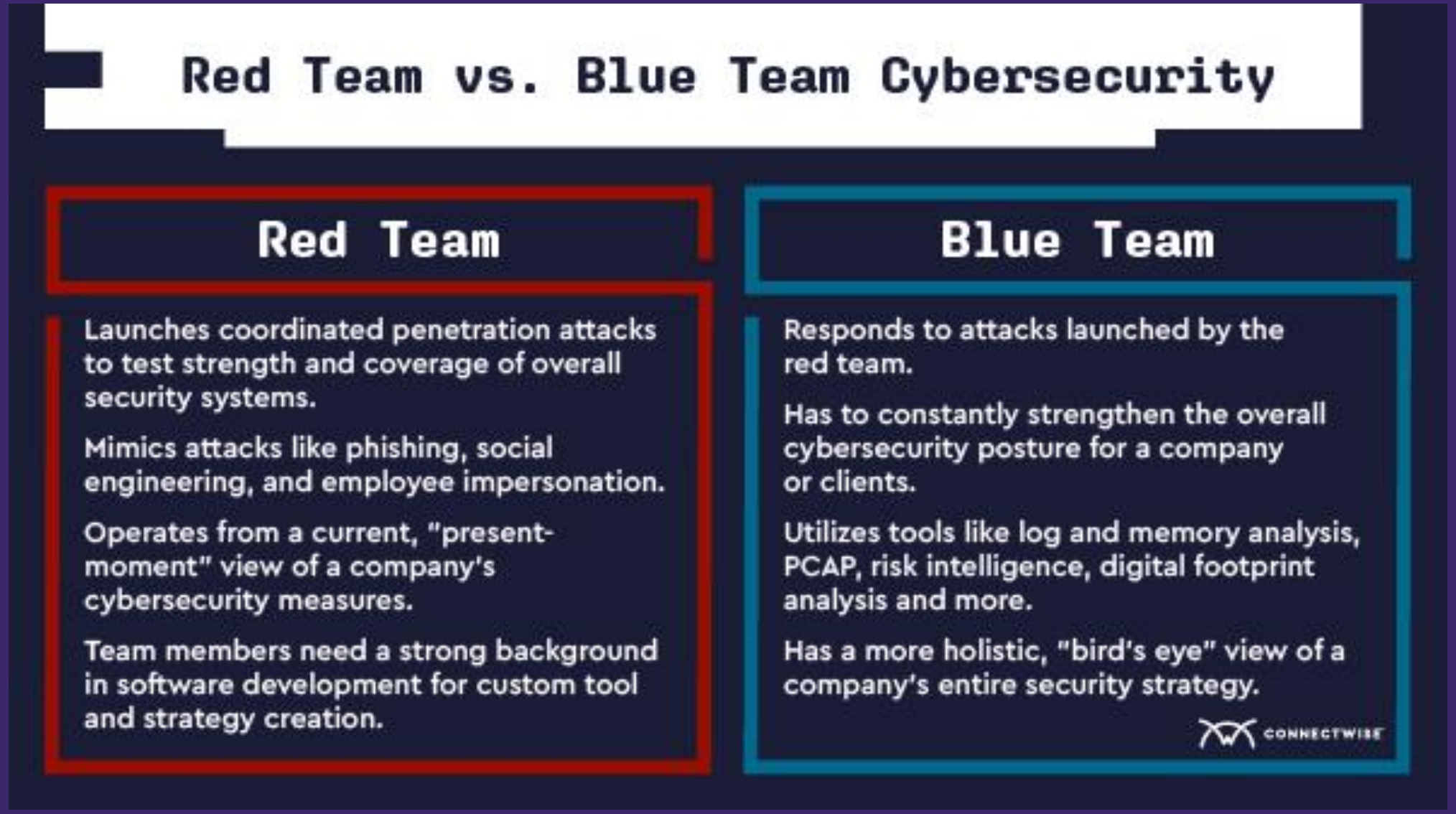
Whoami

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

XIBÉ SEC
Para quem tem fome de Segurança

Red Team x Blue Team: Funções

Red Team x Blue Team: Objetivos



Purple Team: Conceito

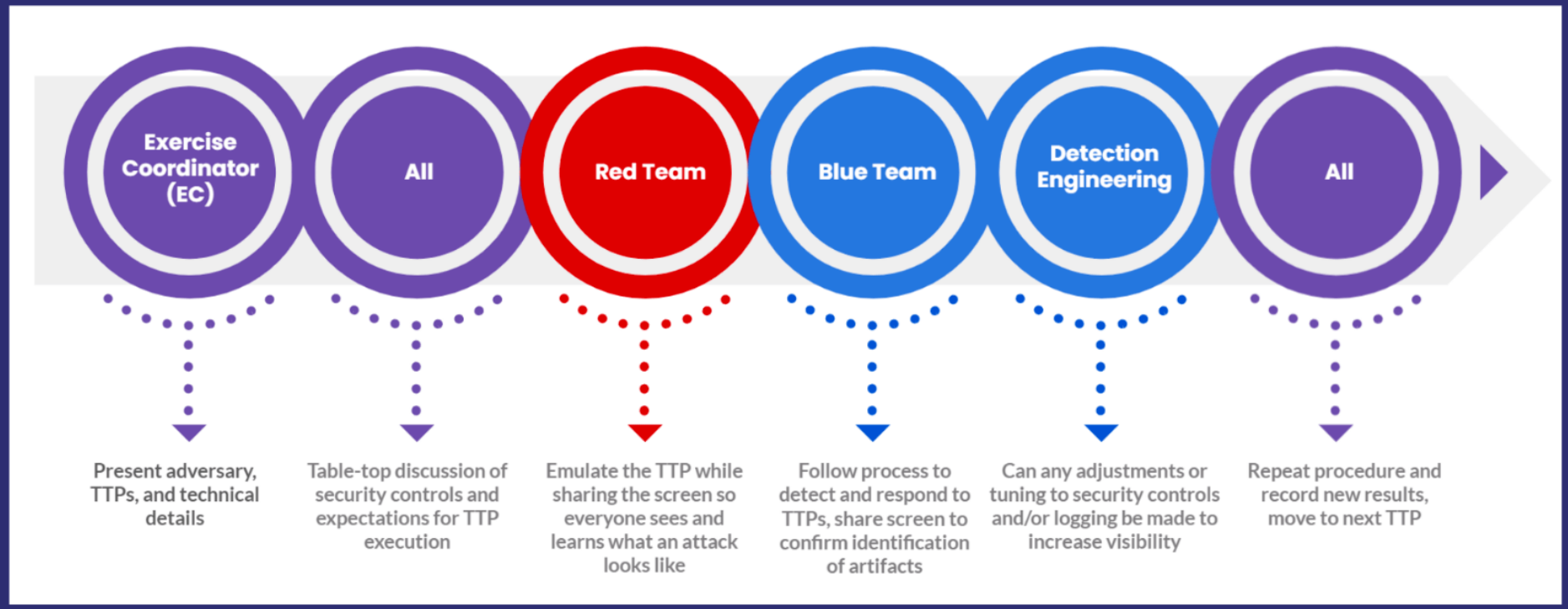
XIBÉ SEC
Para quem tem fome de Segurança

Purple Team: Objetivo

Purple Teaming

What this exercise covers?

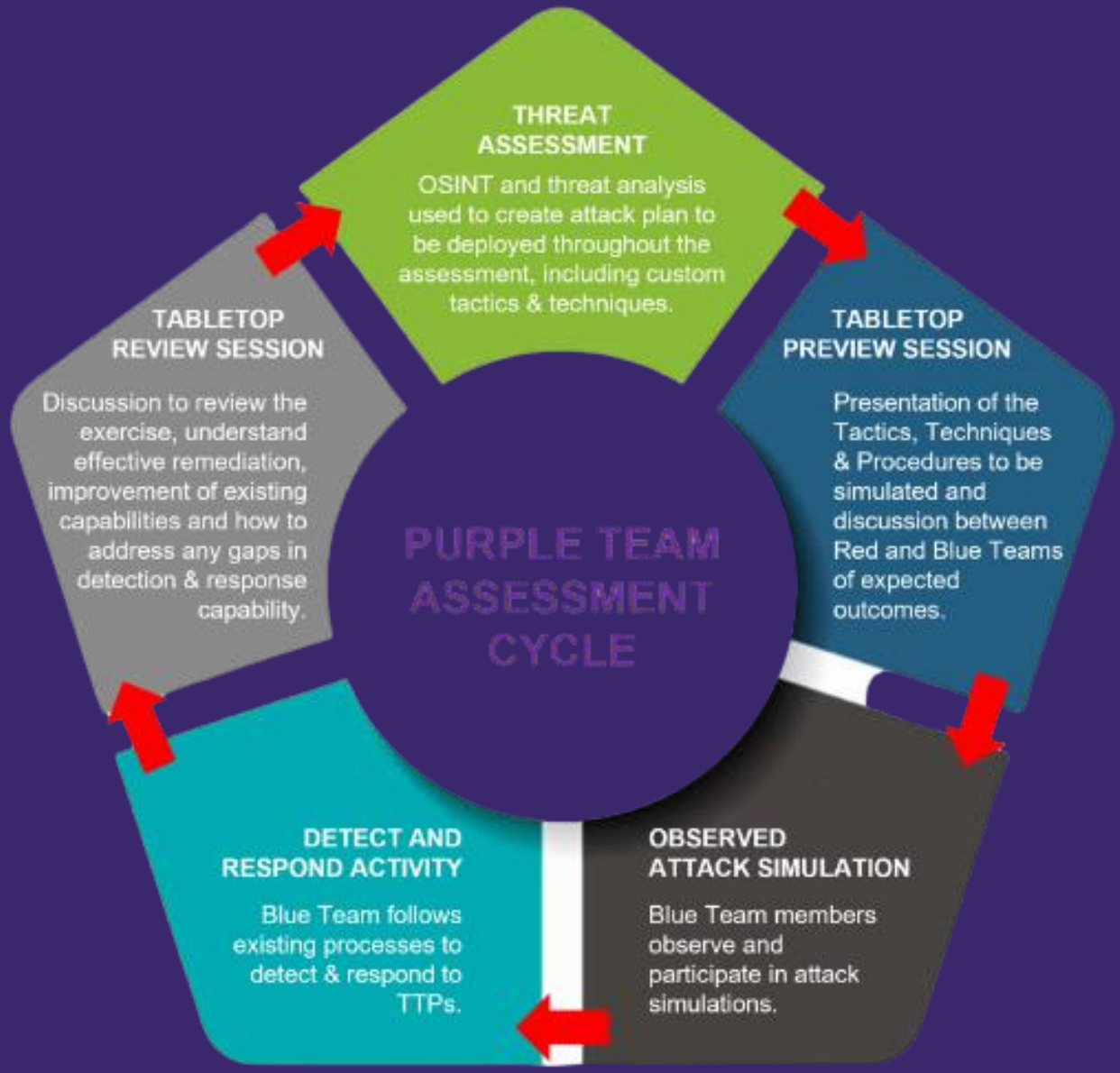
DTS SOLUTION
CYBER SECURITY REDEFINED



Red, Blue and Purple Teaming

XIBÉ SEC
Para quem tem fome de Segurança

Purple Team: Ciclo de avaliação



XIBÉ SEC
Para quem tem fome de Segurança

Purple Team: Resultados esperados do Exercícios/Avaliação

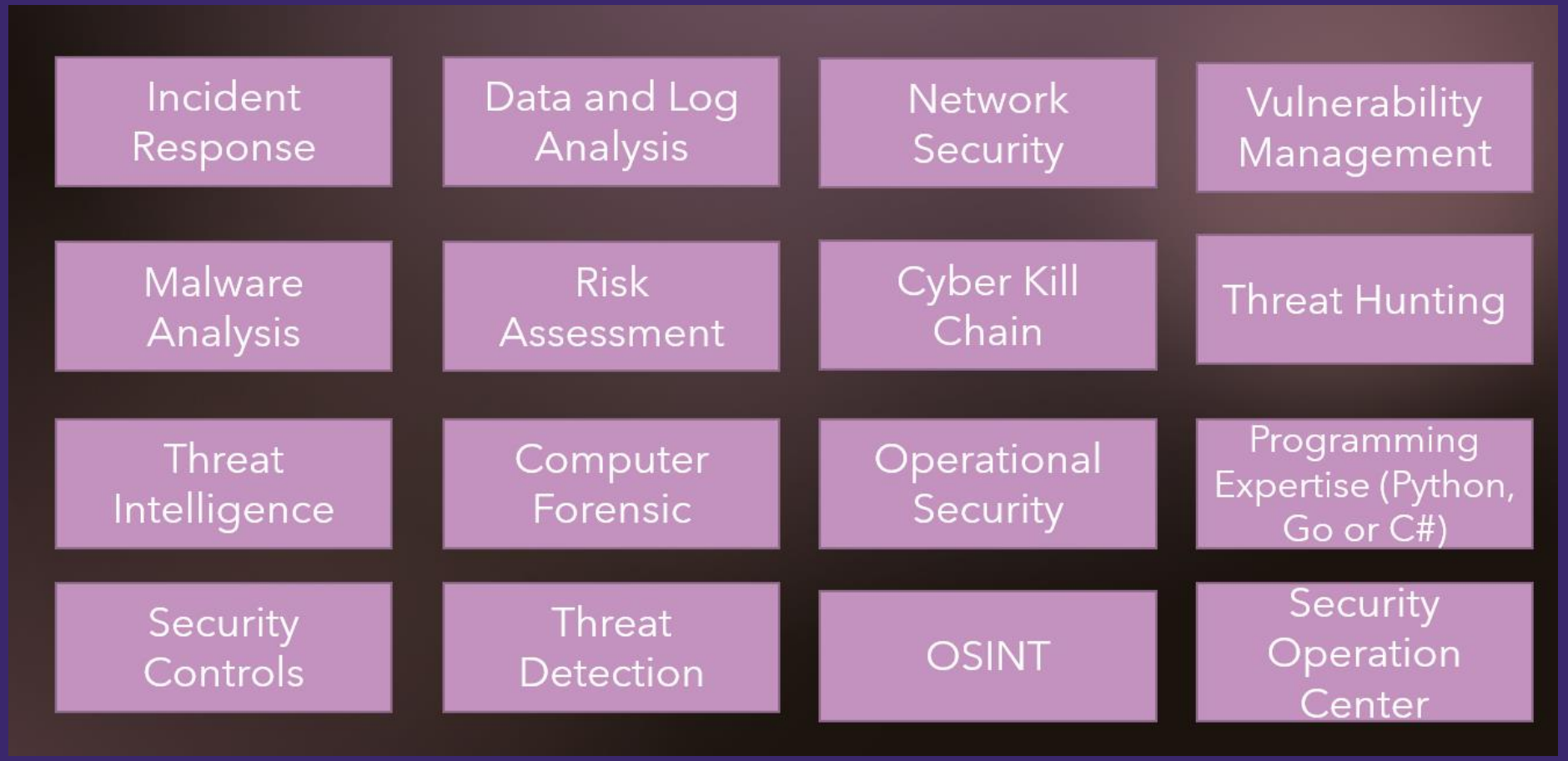
Before purple teaming		
Execution	**Persistence**	**Lateral Movement**
Hardware additions	AppCert DLLs	Logon scripts
Valid accounts	Logon Scripts	Pass the ticket
Supply chain compromise	Application shimming	Remote file copy
		Remote services

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

XIBÉ SEC
Para quem tem fome de Segurança

Empregabilidade do Red Team

Empregabilidade do Blue Team



XIBÉ SEC
Para quem tem fome de Segurança

RTFM e BTFM

Na prática

- **Wazuh OVA**
- **Windows Server 2016 Vulnerável**
- **Kali Linux**

XIBÉ SEC
Para quem tem fome de Segurança

OBRIGADO!

XIBÉ SEC
Para quem tem fome de Segurança