THE DEVELOPER'S CONFERENCE

Trilha – SOFTWARE SECURITY

JOAS ANTONIO

THE DEVELOPER'S CONFERENCE

Introdução ao Mitre Att&ck e ao Cyber Kill Chain

Joas Antonio

Whoami

THE DEVELOPER'S CONFERENCE

Joas Antonio (C0d3Cr4zy)

19 years – Brazil, São Paulo

Apaixonado por tecnologia desde os 7 anos de idade

Asperger/TDAH

PenTester na Inmetrics

Red Team Village, Mitre, Womcy e Hacker Culture Contributor

CEH Master, OSWP, eJPT e eMAPT

Hacking Is Not Crime Advocate

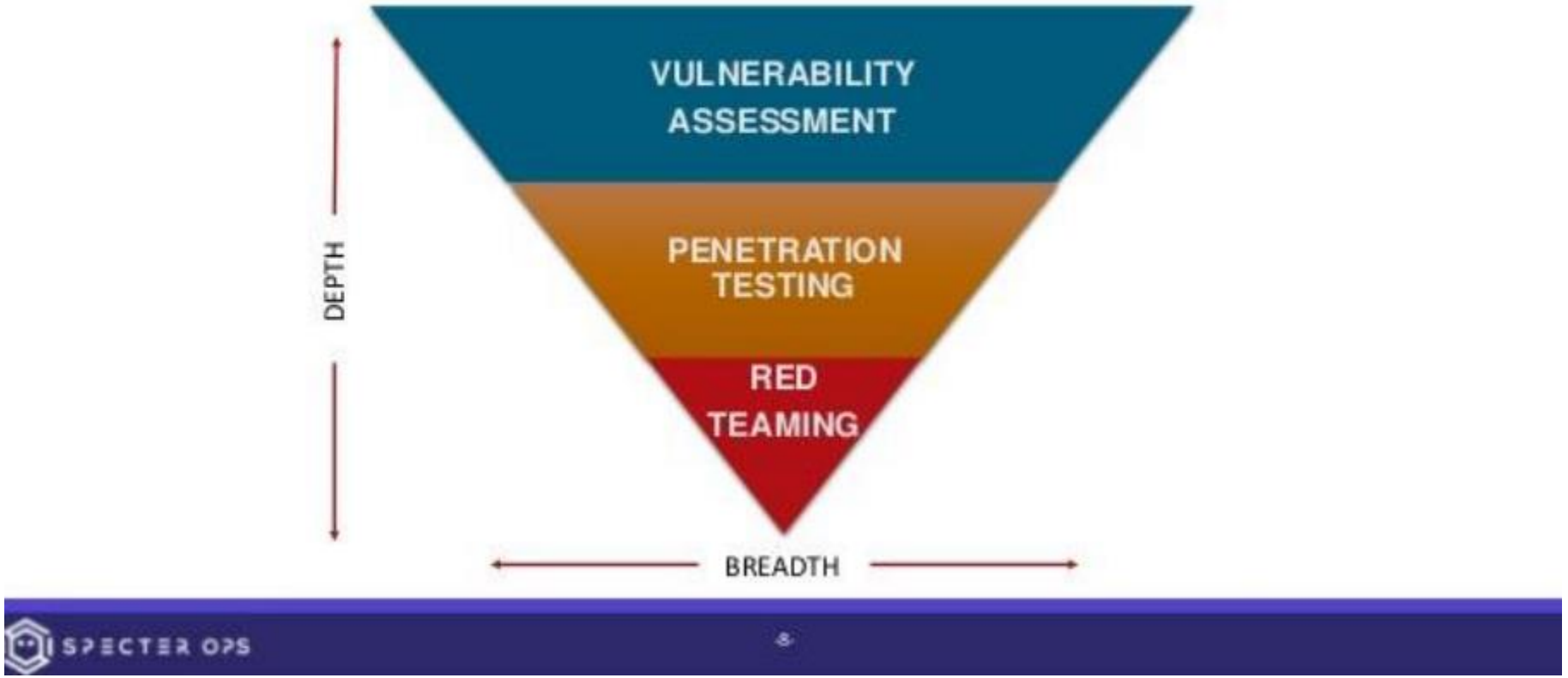
Mitre Contributer

+15 CVE's (XSS, RCE, CSRF, SSRF)

THE DEVELOPER'S CONFERENCE

Red Team vs Other Security Tests

Red Teaming VS Other Security Tests



https://specterops.io/

THE DEVELOPER'S CONFERENCE

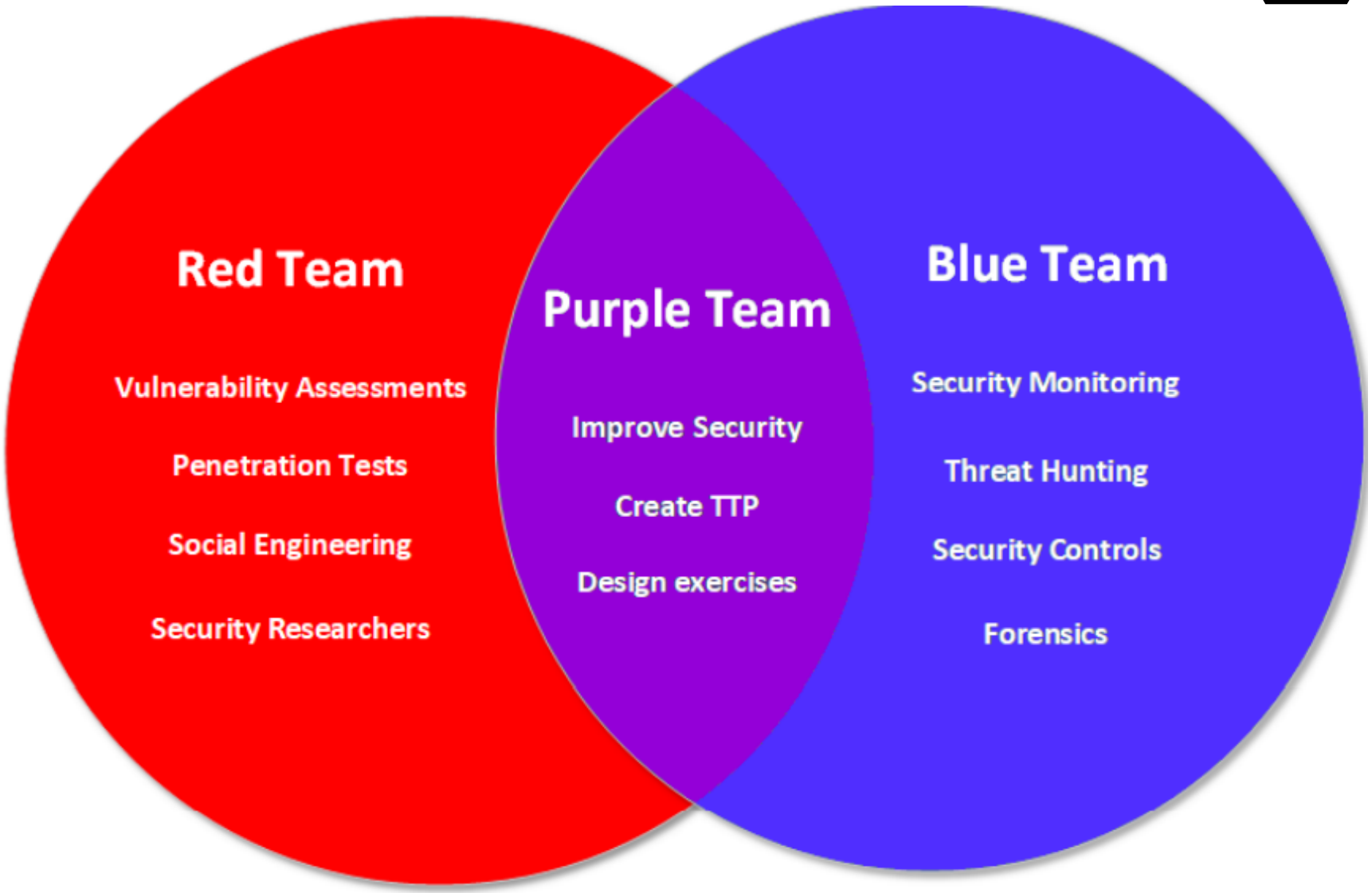
Red Team vs PenTest

CLASSICAL PENTEST	RED TEAMING
Limited timeframe	Comprehensive timeframe
Static methodology	Flexible methodology
Commercial pentest tools are used	All kinds of resources are used
Employees are aware of the test	Except for a few manager, nobody knows while testing
Testers take advantage of known vulnerabilities	Experts try to discover new vulnerabilities
Target is just the technology part	Target is technology, physical and human factors

THE DEVELOPER'S CONFERENCE

RED AND BLUE = PURPLE

Joas Antonio


Red Team
Vulnerability Assessments
Penetration Tests
Social Engineering
Security Researchers
Purple Team
Improve Security
Create TTP
Design exercises
Blue Team
Security Monitoring
Threat Hunting
Security Controls
Forensics

SOBRE PURPLE TEAM

THE DEVELOPER'S CONFERENCE

O Purple Team trabalha em sinergia com Red e Blue Teams, com a missão de alcançar um nível ainda maior de segurança dentro da organização, explorando ao máximo rotinas de ataque e defesa, pensando em como reforçar táticas, técnicas e procedimentos (TTP) de defesa.

Essa abordagem ajuda a desenvolver e melhorar as duas equipes. A equipe azul fica mais informada sobre como priorizar, medir e melhorar sua capacidade de detectar e se defender contra ameaças e ataques, e a equipe vermelha obtém uma visão do setor sobre tecnologias e mecanismos usados na defesa.

THE DEVELOPER'S CONFERENCE

MITRE ATT&CK

Joas Antonio

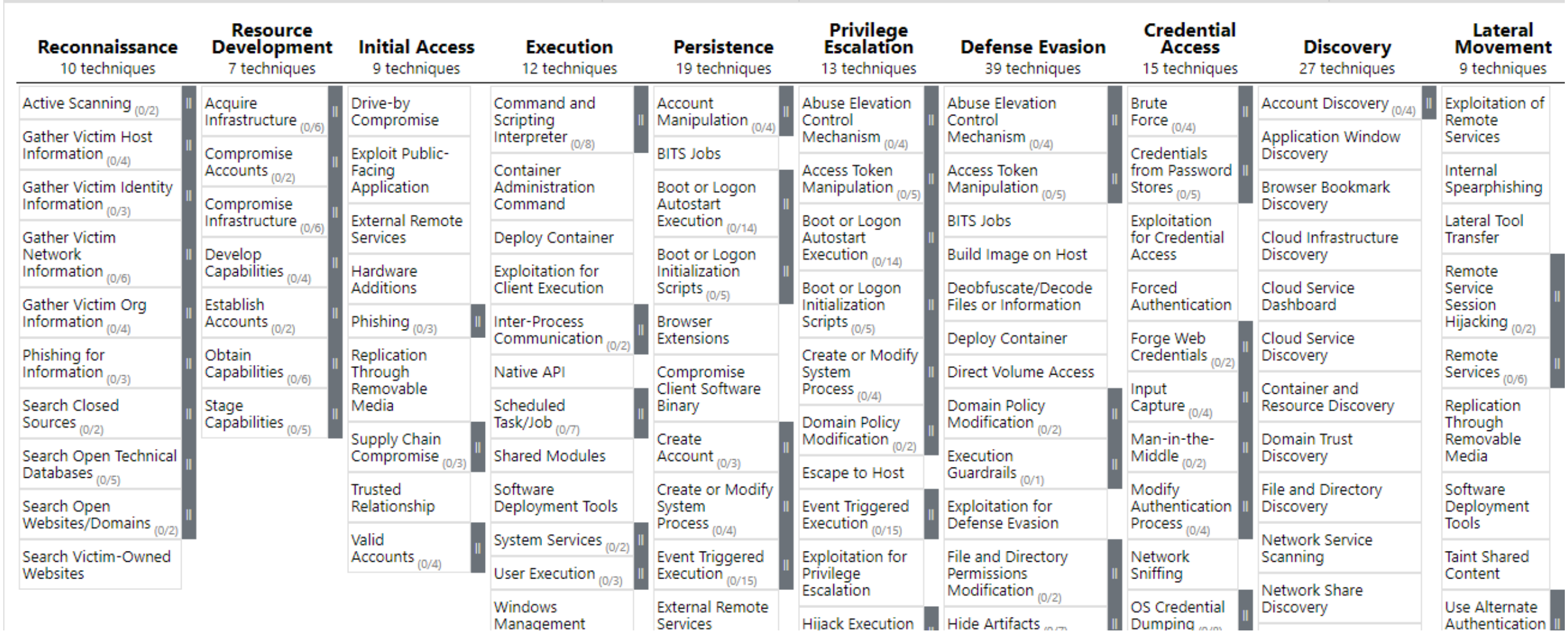
THE DEVELOPER'S CONFERENCE

Mitre Att&ck

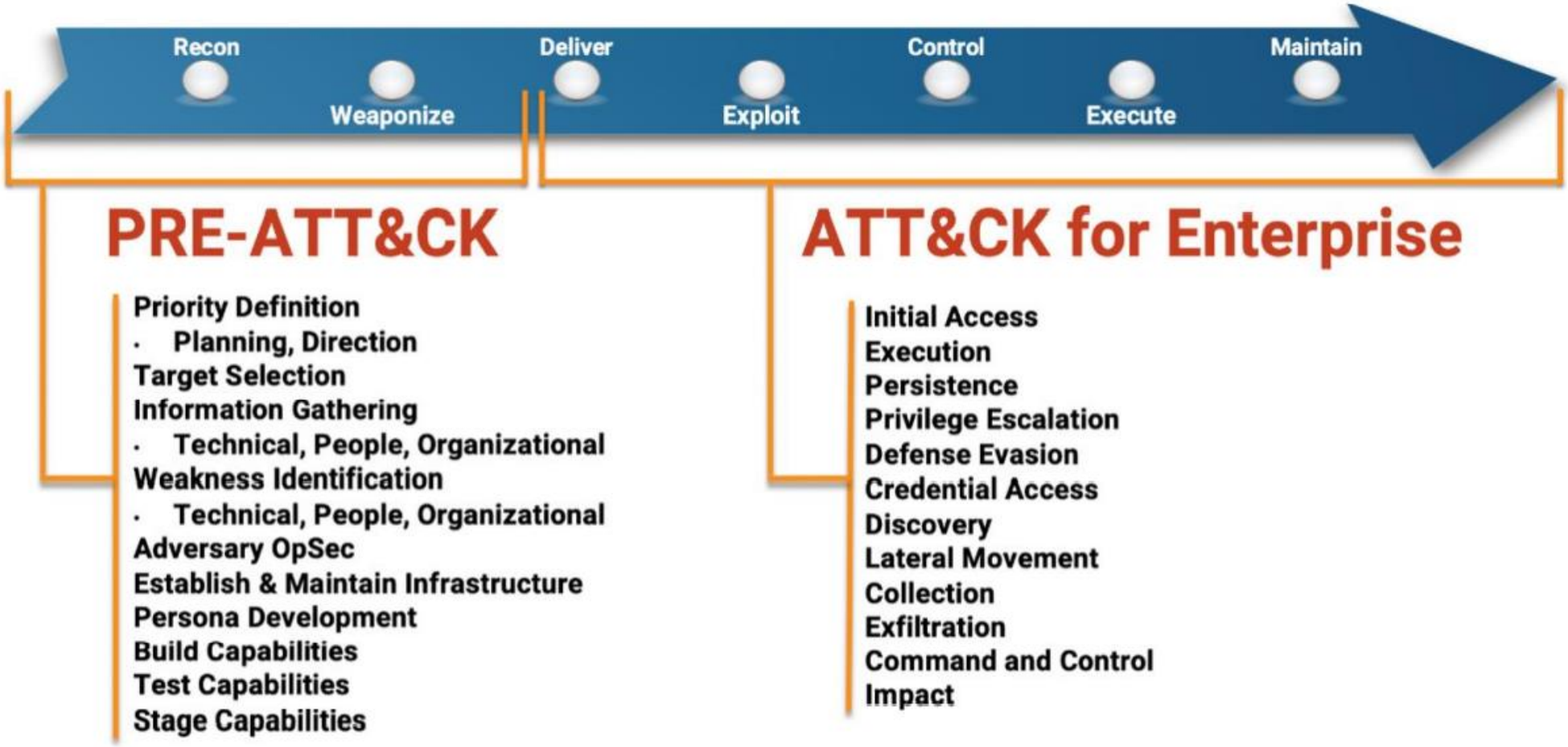
O framework ATT&CK é valoroso para uma série de configurações. Qualquer atividade de defesa pode se beneficiar de aplicar as diretrizes do framework. Além de oferecer uma linguagem comum para os profissionais, o ATT&CK também fornece a fundação para atividades de pentest e Red Team. Isso dá a ambas as equipes um padrão comum de comunicação ao se falar sobre os comportamentos adversários.

Mitre-Att&ck

THE DEVELOPER'S CONFERENCE



Mitre Att&ck


Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain
PRE-ATT&CK
Priority Definition
· Planning, Direction
Target Selection
Information Gathering
· Technical, People, Organizational
Weakness Identification
· Technical, People, Organizational
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities
ATT&CK for Enterprise
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

Mitre Att&ck

THE DEVELOPER'S CONFERENCE

Enterprise ATT&CK

PRE-ATT&CK

It's just ATT&CK

THE DEVELOPER'S CONFERENCE

Cyber Kill Chain

Joas Antonio

CYBER KILL CHAIN vs. MITRE ATT&CK

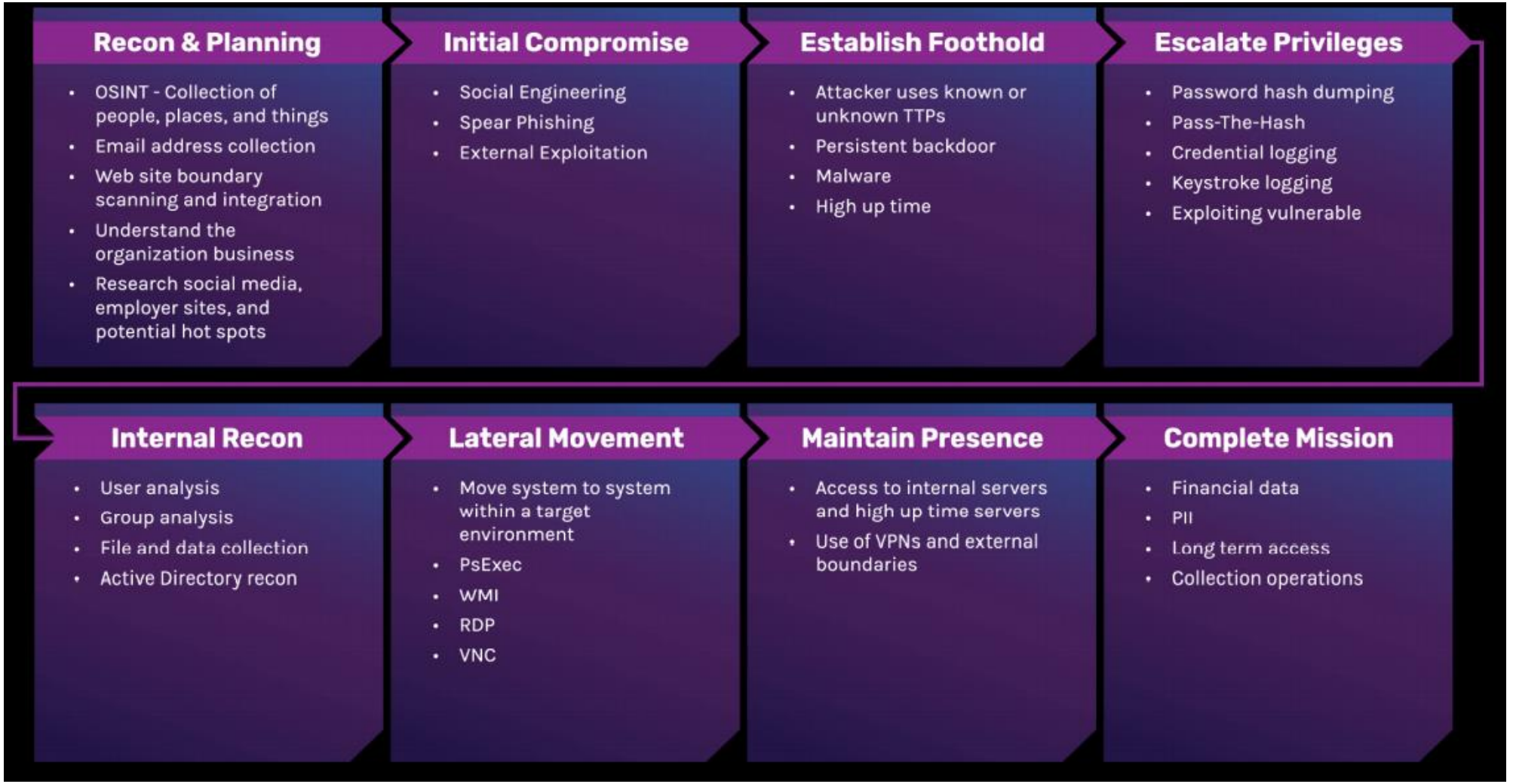
CYBER KILL CHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

Adversary Emulation



Muito obrigado pela oportunidade

Joas Antonio (C0d3Cr4zy)

Credits: Filipi Pires, João Paulo de Andrade and Information Security Community Brazilian