



# Introdução ao Mitre Att&ck e ao Cyber Kill Chain

Joas Antonio

---

# Objetivo do curso

- Red Team vs PenTest
- Purple Team e Red Team
- Red Team Operations
- Conhecendo o conceito de Mitre Att&ck e Cyber Kill Chain
- Como funciona o processo de Adversary Emulation
- Usando o Mitre Att&ck Navigator para estruturar TTPs
- Cracking the Perimeter ou Cracking The Bridge
- Conclusão

# Sobre mim

- Ethical Hacker in Inmetrics, Information Security Researcher, Ethical Hacking and PenTest Independent, OWASP Member and Researcher, Cybrary Teacher Assistant, Microsoft Innovative Educator Instructor, Web Developer (Front-End and Back-End), Bug Hunter by HackerOne and OBB, Python Developer Expert, Shell Script Expert, has over +800 technology courses and +50 certifications, SANS Member, Mitre Att&ck Contributor, Red Team Village Contributor, Texas Cyber Security Summit Contributor, 1000 CEH Hall of Fame, CIS Member and Research, Infosec Competence Leader in Security Awareness, Cyber Security Mentor, Cyber Security Awards Finalist 2020, Article and Book Writer, Cracking The Perimeter Framework Creator, Vulnerable Machine Engineering by Offensive Security, Cyber Security Tutors Founder, Hakin9 Magazine Contributor, Exin Ethical Hacking Foudation Instructor, Exploit Developer and IT lover.

I love computers since I was 7 years old and in love with the information security area since I was 10 years old.

OSWP | CEH ANSI | CEH Practical | CEH Master | eJPT | OSCP (In Progress 99%)  
19years | Asperger

- LinkedIn: <https://www.linkedin.com/in/joas-antonio-dos-santos>

# Red Team vs PenTest

---

Joas Antonio

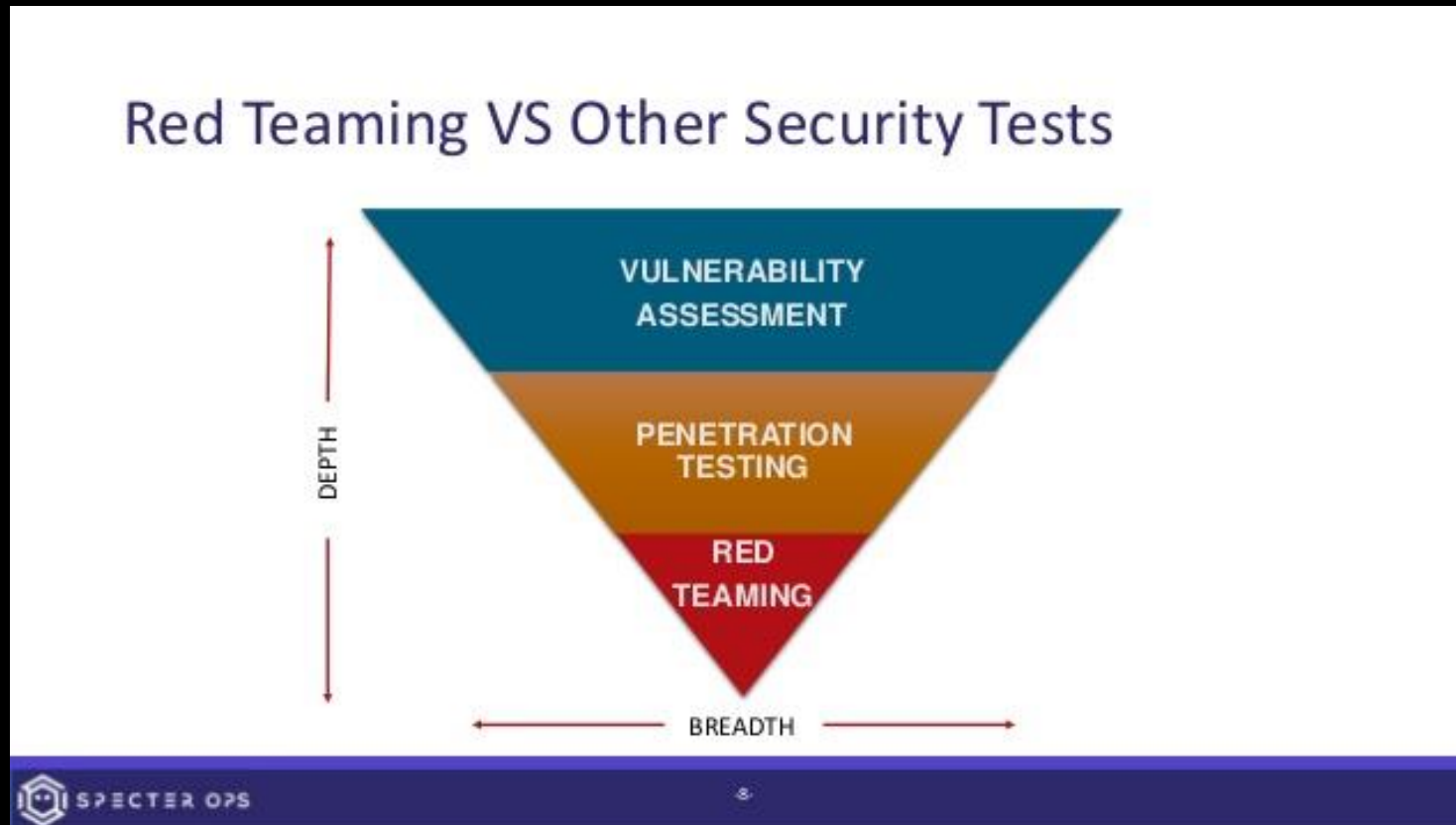
Penetration  
Test

VS

Red Team  
Engagement

# Red Team vs PenTest

Other Security Tests



# 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

# Red Team vs PenTest

Penetration Testing	Red Teaming
It exploits vulnerabilities to achieve a predetermined goal.	Tests the defenses, includes attacking, detection, prevention, and response for the organization.
Identifies issues related to system design and architecture	Provides more opportunities and a broader scope of testing
It is not a stealth operation.	It is a stealth operation.
A point in time technique for detection and response capabilities	This needs to be a continuous process.
Does not provide any suggestions to other security teams	Works in collaboration with blue teams

# O que é PenTest

- Pen testing is a process for testing a system, network, web application, facility or some other resource in order to find as many vulnerabilities and configuration issues as possible within the time allotted. Pen testers then exploit those vulnerabilities to determine the risk of the vulnerabilities.
- Pen testers aren't seeking to discover new vulnerabilities -- zero days. They aim to find already known but unpatched system vulnerabilities.
- During a typical pen test, pen testers aim to find a version of installed software that is known to be vulnerable and then exploit that vulnerability. This process continues: find other vulnerabilities and exploit them, combining the attacks in order to reach the end goal.



# O que é Red Team

- Red teaming shares many similarities with pen testing; however, the goals are different. Red teaming is more scenario-driven than pen testing. The goal of red team engagements is not just to test the environment and the systems within the environment, but to test the people and processes of the organization as well.
- Typical red team scenarios include exploiting lost laptops, unauthorized devices connected to the internal network and compromised DMZ hosts, as well as testing how the security operations center (SOC) or blue team react to an advanced persistent threat. Will the SOC or blue team defenders notice when an employee is exfiltrating data from the network?
- Red teams may also use scenario-driven testing for detection and response, like testing a business's ability to detect and manage external threats, like phishing campaigns, social engineering attempts, attempts to gain physical access to the site, website compromise assessments, protection software evasion, lateral movement across networks and many other attacks, depending on the complexity of an organization's systems.

## Red Team




## Purple Team



## Blue Team




# Purple Team e Red Team

 Penetration Testing


 Threat Emulation


 Social Engineering


 Maximize Red Team.

 Enhance Blue Team.

 Improve Security Posture

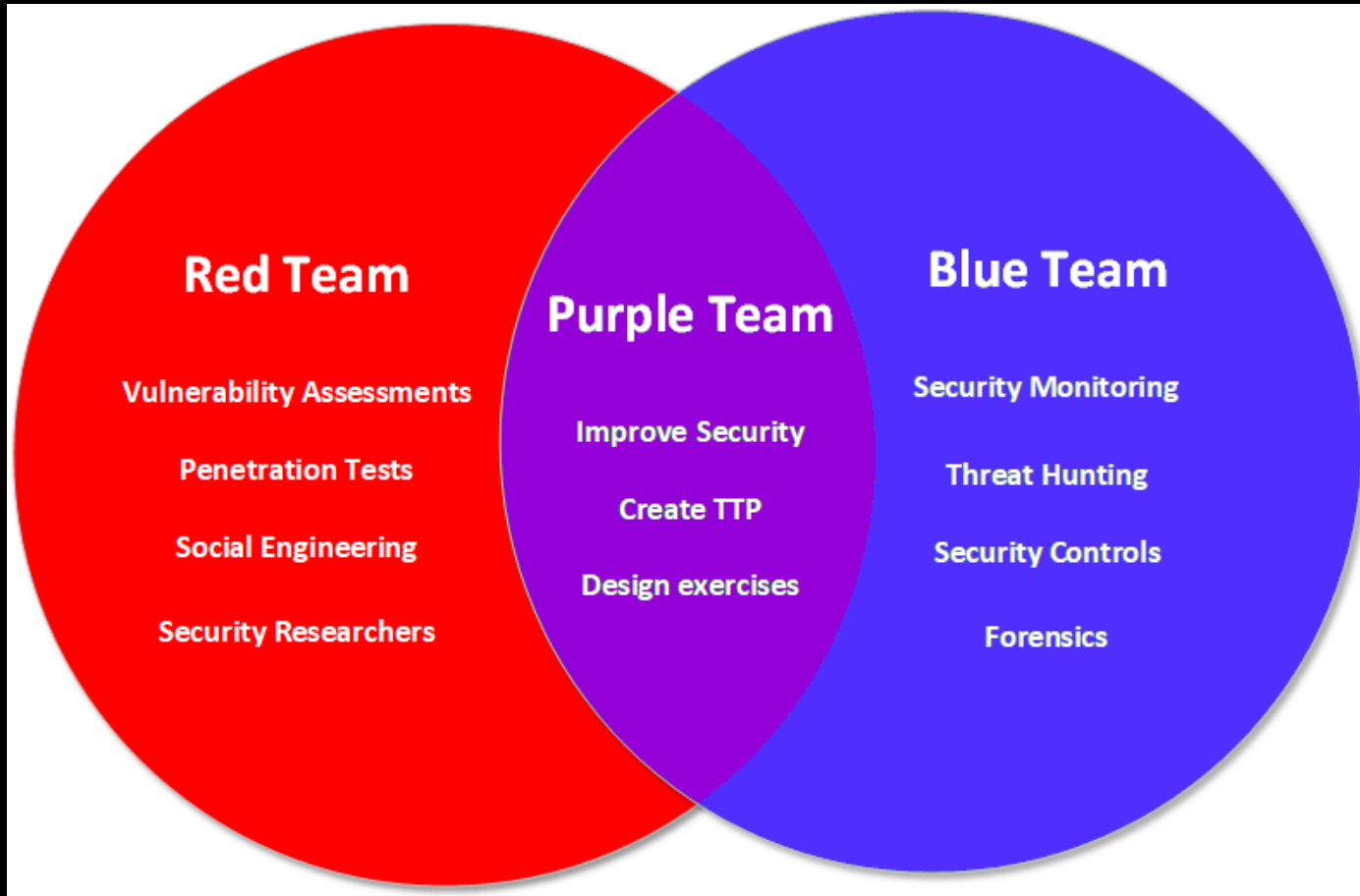
 Proactive Defense

 TTP Based Hunting

 Vulnerability Assessment

Joas Antonio

# Red Team and Blue Team = Purple Team



# Red Team and Blue Team = Purple Team

- 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.
-

# Benefícios do Purple Team

## Comunicação

- Conforme descrito, o objetivo das equipes vermelha e azul é reforçar a segurança de uma organização, assim como a meta da organização é promover a conscientização sobre a segurança cibernética. Com o time roxo, o primeiro objetivo é uma comunicação clara e regular entre os times vermelho e azul, um fluxo constante de informações e esforço simbiótico. Este exercício, recomendado *para ser realizado pelo menos uma vez por ano* e sempre que ocorram mudanças significativas, entre as duas equipas, facilita a comunicação e colaboração constantes entre as equipas, promovendo melhorias constantes na cultura de cibersegurança da organização.

## Perspectiva

- Frequentemente, uma violação pode ocorrer com o invasor evitando todas as defesas, sem qualquer conhecimento ou detecção da equipe azul. Devido ao constante estado de mudança na segurança cibernética, isso nem sempre indica uma falta de habilidade ou tecnologia na equipe azul, mas sim a crescente complexidade dos métodos dos agentes de ameaça e / ou vetores de ataque. O conceito de 'time roxo' efetivamente elimina essa possibilidade.
- As equipes vermelha e azul, trabalhando juntas, fornecem transferência de conhecimento regular e consistente, melhorando a capacidade da organização de impedir cenários de ataque da vida real. No final, a equipe vermelha melhorará os processos de gerenciamento de vulnerabilidade da organização e a equipe azul aprenderá a entrar na mentalidade dos invasores, portanto, a equipe roxa permite o desenvolvimento de melhores programas de resposta a incidentes e processos de detecção de vulnerabilidade.

## Postura

- O último benefício que abordaremos também é o benefício importante, e essa é uma postura de segurança mais saudável para sua organização. Fazendo uso da comunicação constante das equipes roxas, testes anuais de penetração, gerenciamento de vulnerabilidade e desenvolvimento de infraestrutura e políticas de segurança aprimoradas, as organizações colocam seu melhor pé à frente contra a ameaça de uma violação de dados.

# Red Team Operations

Joas Antonio



# Red Team Operations

- Once the objectives are set, the red team starts by conducting initial reconnaissance. Mandiant leverages a combination of proprietary intelligence repositories as well as open-source intelligence (OSINT) tools and techniques to perform reconnaissance of the target environment.
- Mandiant attempts to gain initial access to the target environment by exploiting vulnerabilities or conducting a social engineering attack. Mandiant leverages techniques used by real-world attackers to gain privileged access to these systems.
- Once access is gained, the red team attempts to escalate privileges to establish and maintain persistence within the environment by deploying a command and control infrastructure, just like an attacker would.
- After persistence and command and control systems are established within the environment, the red team attempts to accomplish its objectives through any non-disruptive means necessary

# Red Team Operations

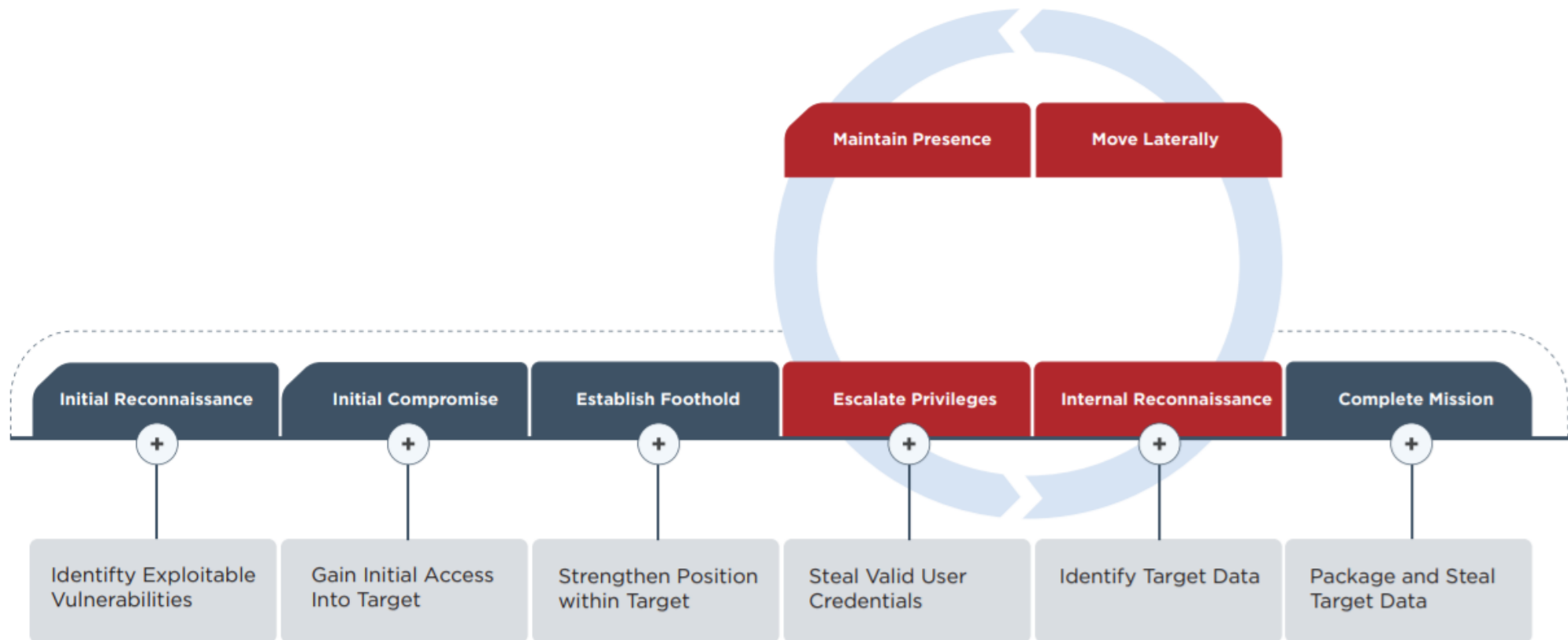
**Red Team Operations are recommended for organizations that want to:**

- Test detection and response capabilities. Security teams prepare for real world incidents, but you need to confirm that they can respond properly — without real risk.
- Raise awareness and show impact. The Mandiant red team behaves like realworld attacker, working n compromise your environment from the Internet by using information only available to the Internet. Successful red team engagements can help justify increased security budgets and identify gaps that require further investment.



# Red Team Operations – Attack Lifecycle

---



# 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

Conhecendo o Mitre Att&ck  
e o Cyber Kill Chain

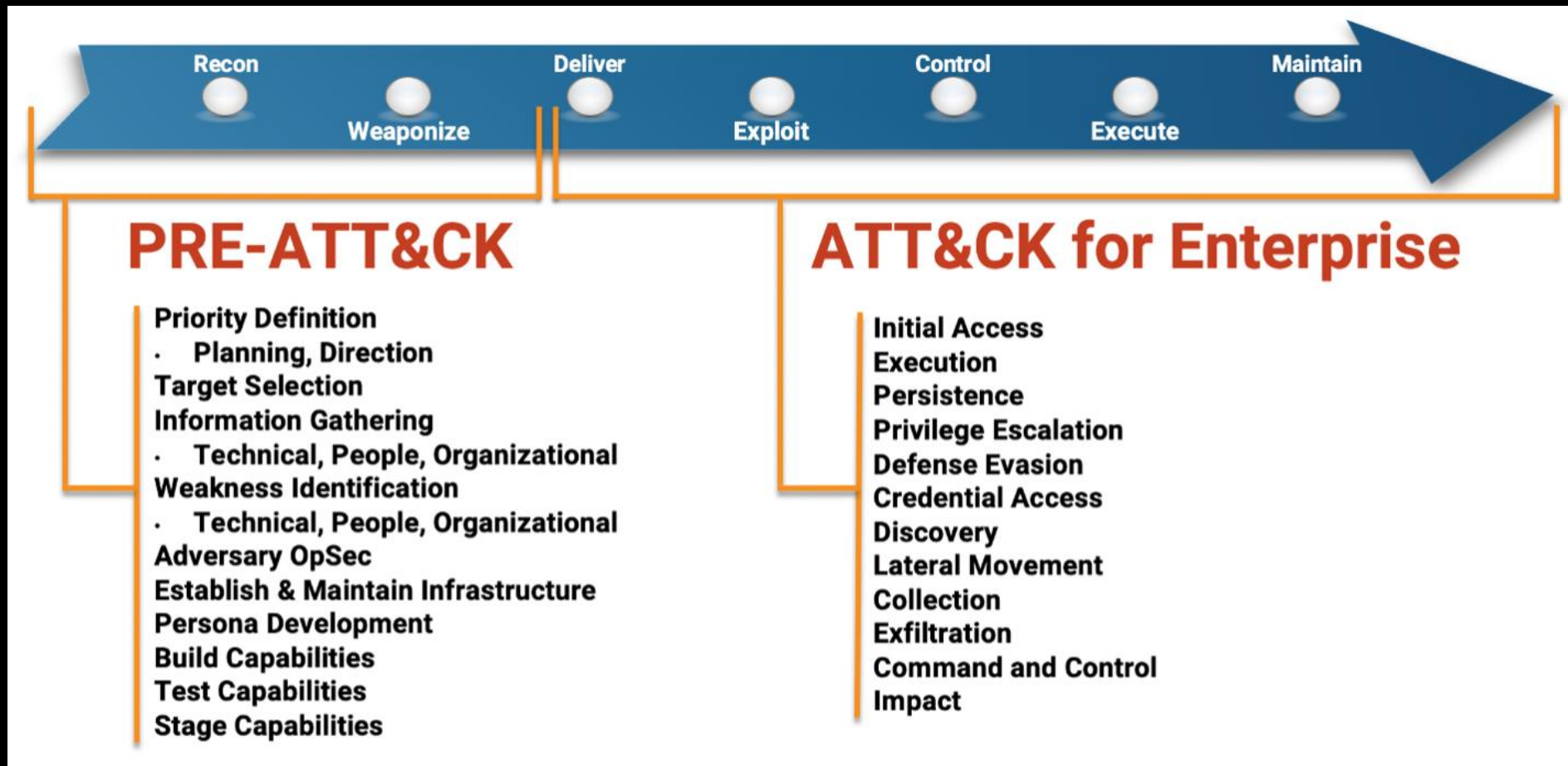
Joas Antonio



# Mitre Att&ck

- O MITRE introduziu o ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) em 2013 como uma forma de descrever e categorizar os comportamentos adversários baseado em observações reais do cenário global. o ATT&CK é uma lista estruturada de comportamentos conhecidos de atacantes que foram compilados em táticas e técnicas, expressados em uma série de matrizes assim como em STIX/TAXII.
- Por ser uma representação compreensiva de comportamentos que os atacantes empregam quando estão comprometendo as redes, tornou-se muito útil para mensurar medidas de defesa e ofensivas.
- O framework ATT&CK é valioso 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.

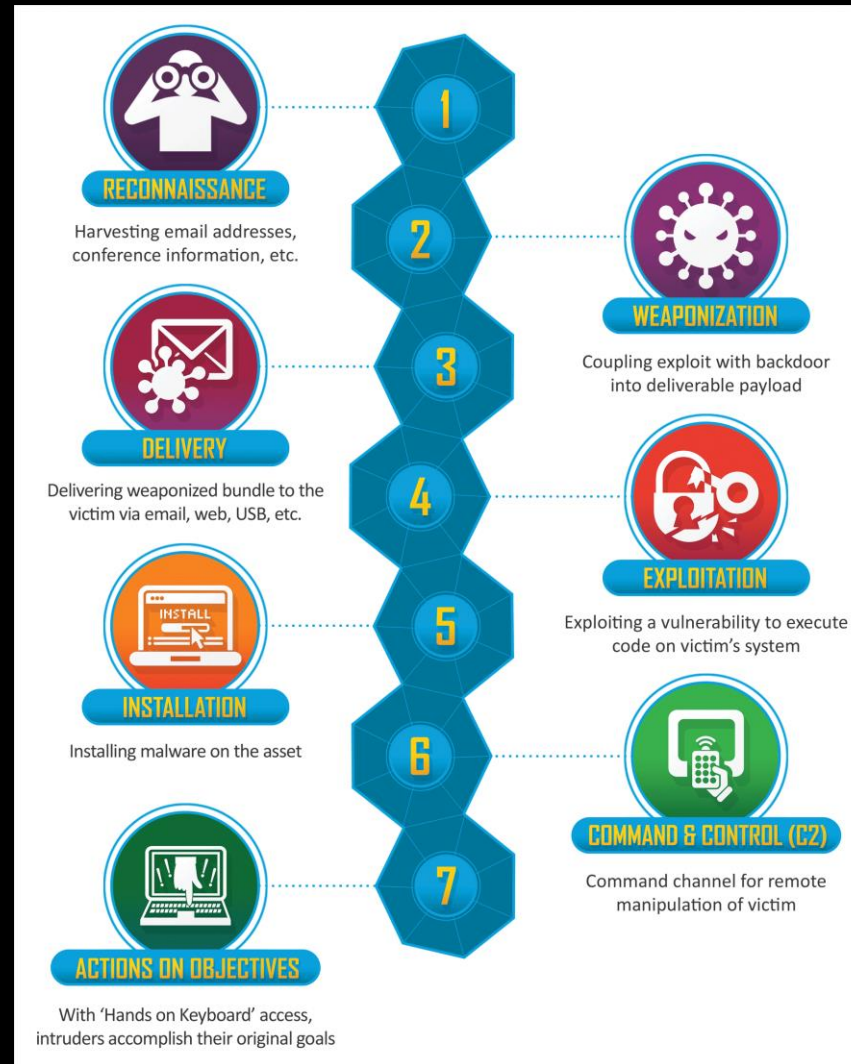
# Mitre Att&ck



# Cyber Kill Chain

Desenvolvido pela Lockheed Martin, a **estrutura Cyber Kill Chain®** faz parte do modelo **Intelligence Driven Defense®** para identificação e prevenção de atividades de intrusões cibernéticas. O modelo identifica o que os adversários devem completar para atingir seu objetivo.

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>



# 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



# Cyber Kill Chain

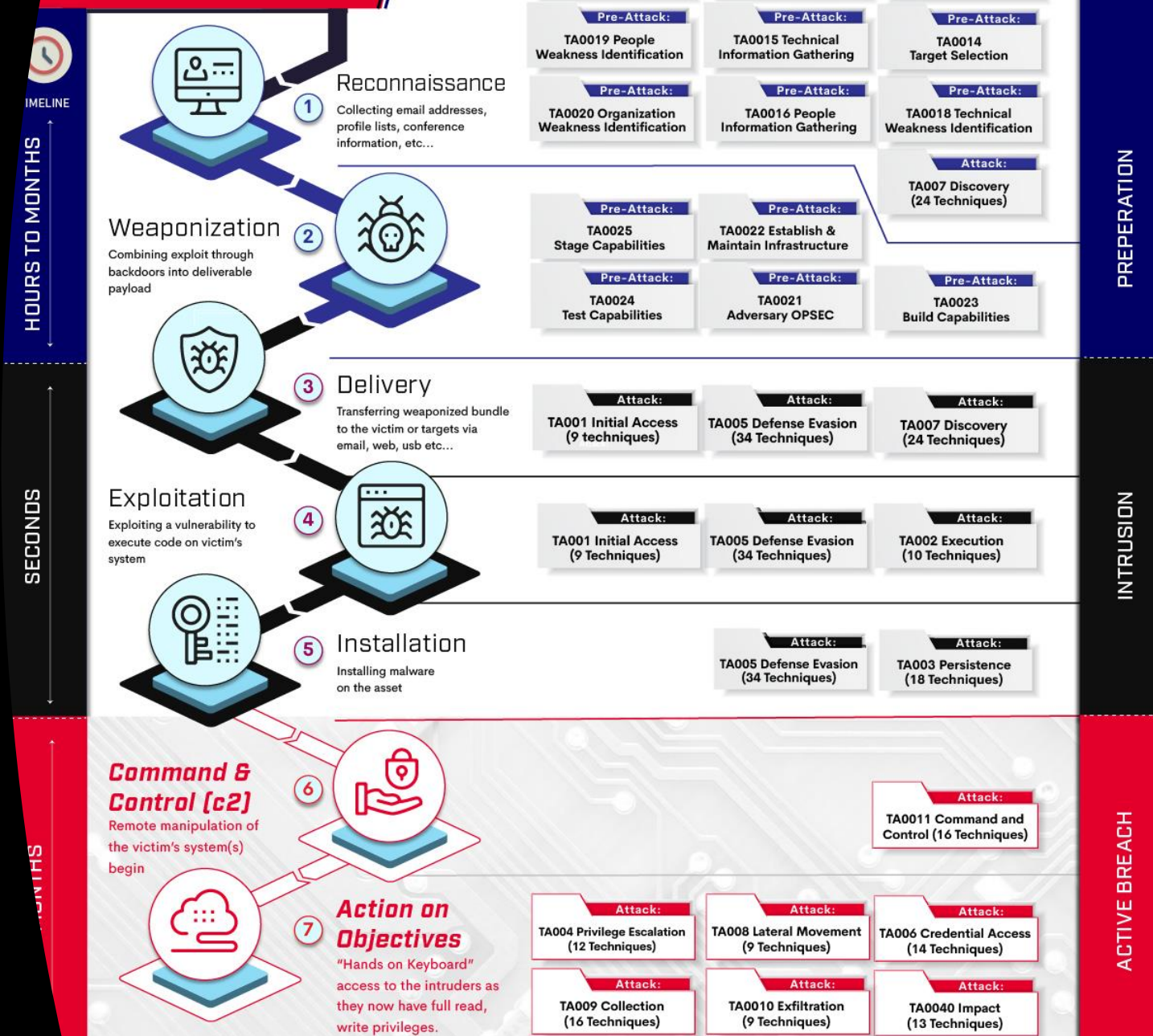
A cadeia de eventos, ou cadeia de destruição, pela qual um invasor externo deve passar é definida no CKC em um nível tático, conforme mostrado:

- **Reconhecimento:** Atividades de reconhecimento passivo ou ativo para identificar alvos para potenciais fraquezas. Avaliação de cada inteligência possível em relação ao melhor curso de ação.
- **Armamento:** criação ou localização de malware de acesso remoto adequado para explorar potenciais fraquezas ou vulnerabilidades, acoplando-o em cargas úteis (como os tipos de arquivo mais usados)
- **Entrega:** entrega a carga útil ao ambiente de destino. Principalmente combinado com quaisquer outras fraquezas descobertas na fase de reconhecimento. Aqui, o vetor de ataque pode ser incluído em e-mails, usando sites mal-intencionados ou hackeados ou usando USB, etc.
- **Exploração:** está provocando a execução da carga útil. Ele pode ser disparado automaticamente, como a execução de um programa de download ou a execução de arquivos em USB ou técnicas mais avançadas, como ataque direcionado usando engenharia social, etc., são possíveis.
- **Instalação:** instalação de carga útil para criar um canal consistente entre a vítima e o invasor. Principalmente o backdoor é implantado para manter a presença neste ponto.
- **Comando e Controle:** Estabelecendo um canal C&C. Isso permite que os invasores tenham um ponto central para direcionar e alcançar os objetivos no ambiente de destino.
- **Ação em Objetivos:** Rodada final para atingir os objetivos originais, o impacto é máximo, como exfiltração de dados confidenciais ou comprometimento da integridade ou disponibilidade dos sistemas.

# Mitre Kill Chain

- Cyber Intrusion Kill Chain, também conhecido como Kill Chain, foi adaptado de conceitos militares. Os engenheiros de Lockheed Martin foram os primeiros a adaptá-lo à área de segurança cibernética. O núcleo da estrutura surgiu da estrutura de ataque. Ele descreve um processo ponta a ponta, ou toda a cadeia de eventos, que é necessário para realizar um ataque bem-sucedido.
- O Kill Chain pode ser usado tanto para conduzir um ataque quanto para detectar, bem como defender um ataque. Quando a defesa está em ação, estamos falando sobre quebrar a cadeia de morte de um oponente, tornando um ataque malsucedido. O modelo CKC da Lockheed Martin serve como o primeiro e o ponto de partida para analisar ataques de APT e malware. De acordo com os pesquisadores da Lockheed Martin, a cadeia de destruição completa pode ser definida como "o agressor deve desenvolver uma carga útil para violar um limite confiável, estabelecer uma presença dentro de um ambiente confiável e, a partir dessa presença, agir em direção aos seus objetivos"

## MITRE Kill Chain





# Como funciona o processo de Adversary Emulation?

Joas Antonio



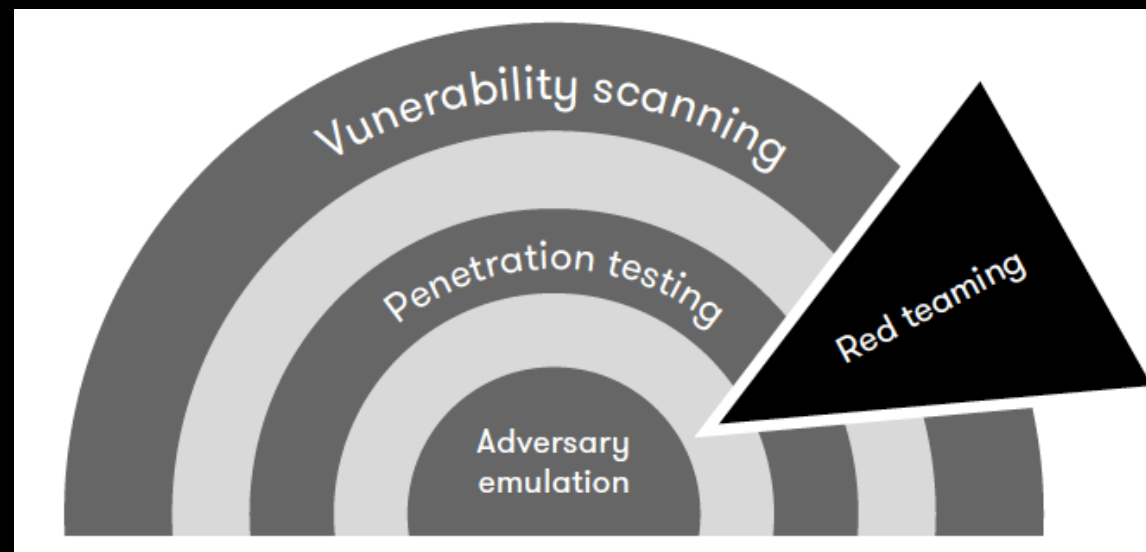
# Adversary Emulation

- Para aqueles que não estão familiarizados com isso, **a emulação do adversário é um tipo de engajamento da equipe vermelha que imita uma ameaça conhecida a uma organização, combinando inteligência de ameaças para definir quais ações e comportamentos a equipe vermelha usa.** Isso é o que diferencia a emulação do adversário dos testes de penetração e outras formas de formação de equipes vermelhas. Emuladores de adversários constroem um cenário para testar certos aspectos das táticas, técnicas e procedimentos (TTPs) de um adversário. A equipe vermelha então segue o cenário enquanto opera em uma rede alvo a fim de testar como as defesas podem se sair contra um adversário emulado.

# Adversary Emulation

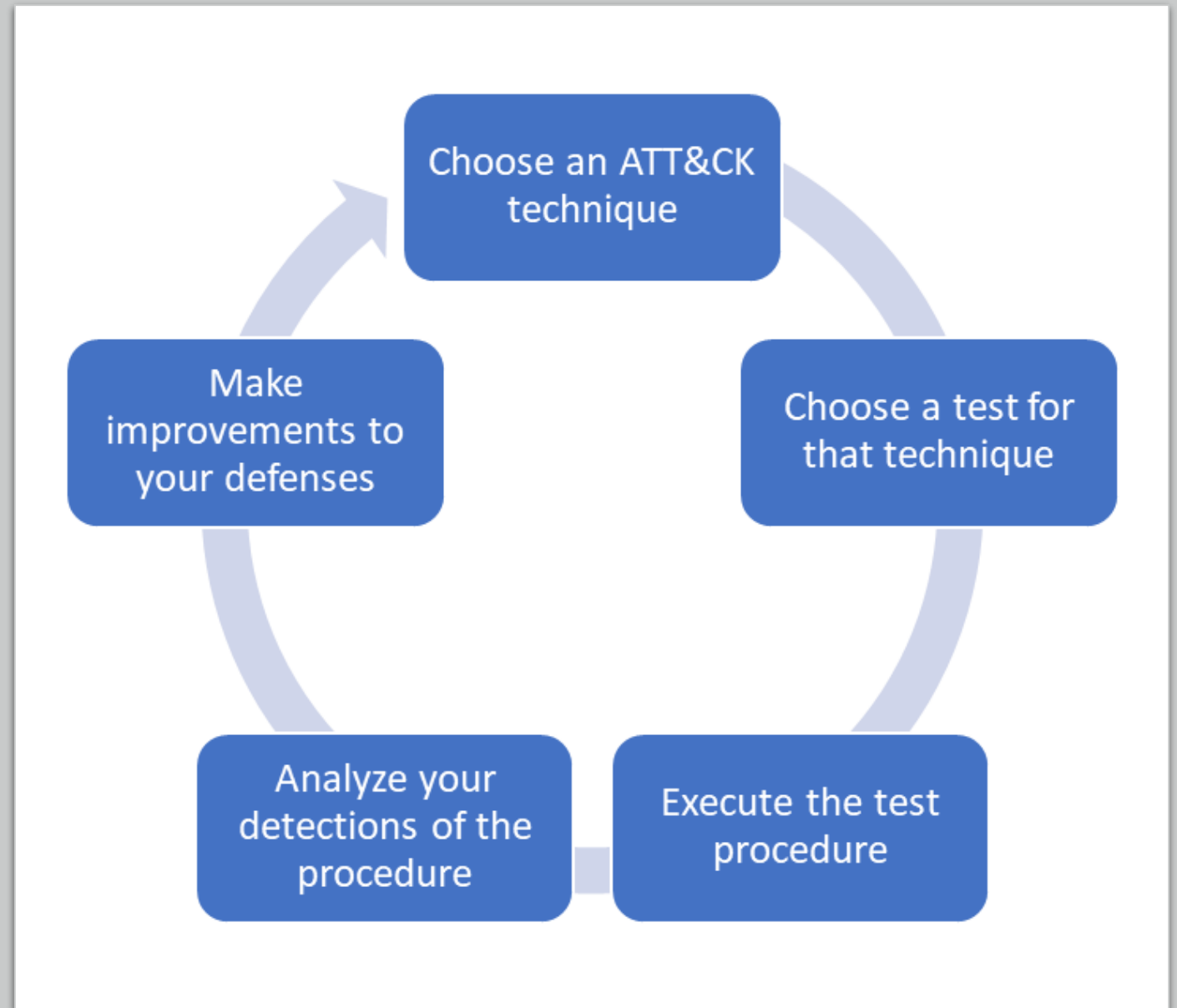
---

- Como a ATT&CK é uma grande base de conhecimento dos comportamentos adversários do mundo real, não é preciso muita imaginação para estabelecer uma conexão entre os comportamentos do adversário ou da equipe vermelha e a ATT&CK. Vamos explorar como as equipes de segurança podem utilizar ATT&CK para emulação de adversário para ajudar a melhorar sua organização!



# Adversary Emulation – Nivel 1

- Equipes pequenas e aquelas voltadas principalmente para a defesa podem obter muitos benefícios com a emulação do adversário, mesmo que não tenham acesso a um Red Team.
- Atomic Red Team , um projeto de código aberto mantido pela Red Canary, é uma coleção de scripts que pode ser usada para testar como você pode detectar certas técnicas e procedimentos mapeados para técnicas ATT&CK.

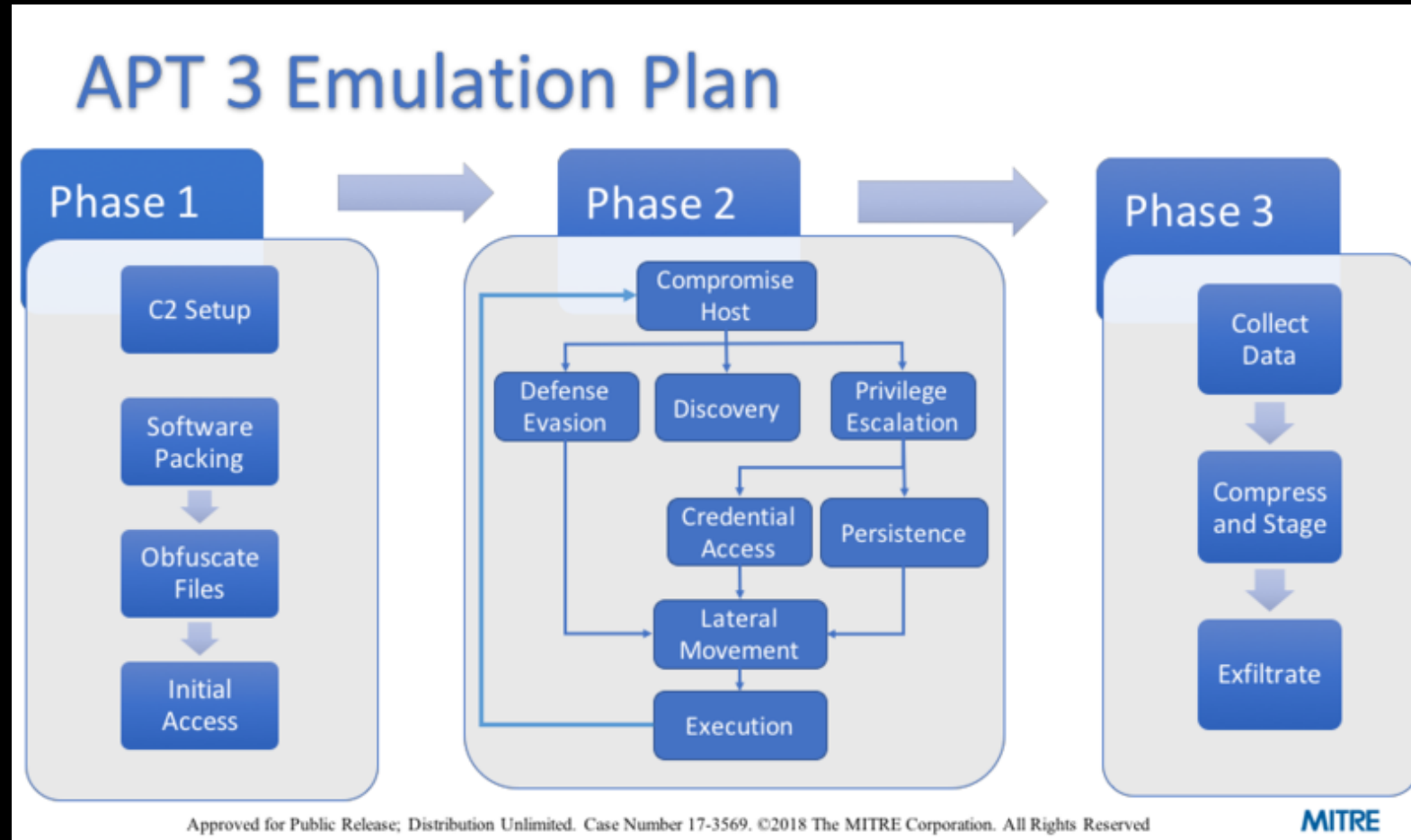


# Adversary Emulation – Nivel 1

- O Atomic Red Team pode ser usado para testar técnicas e procedimentos individuais para verificar se a análise comportamental e os recursos de monitoramento estão funcionando conforme o esperado.
- O repositório Atomic Red Team tem muitos testes, cada um com um diretório dedicado à técnica ATT&CK que é testada. Você pode visualizar o repositório completo no formato ATT&CK Matrix .
- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Indexes-Markdown/index.md>

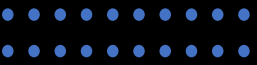
# APT 3 Emulation Plan - Example

Joas Antonio



# Adversary Emulation – Nivel 2

- Para aqueles de vocês que já têm recursos de Red Team, você pode tirar muito proveito da integração da ATT & CK com seus compromissos existentes. O mapeamento das técnicas usadas em uma contratação de equipe vermelha para a ATT & CK fornece uma estrutura comum ao escrever relatórios e discutir mitigações.
- Para começar, você pode pegar uma ferramenta ou operação planejada existente que você usa e mapeá-la para a ATT & CK. O mapeamento dos procedimentos do Red Team para a ATT & CK é semelhante ao mapeamento da inteligência sobre ameaças para a ATT & CK.
- Outro recurso útil para começar a mapear os procedimentos da equipe vermelha para ATT&CK é o [APT3 Adversary Emulation Field Manual](#), que apresenta ações de comando por comando que o APT3 usou, todas mapeadas para ATT&CK.



# Adversary Emulation – Nivel 3



- Nesse ponto, seu Red Team está integrando a ATT & CK nas operações e encontrando valor na comunicação com a equipe azul. Para avançar suas equipes e o impacto que estão tendo ainda mais, você pode colaborar com a equipe de CTI de sua organização para ajustar os compromissos em relação a um adversário específico usando os dados que coletam criando seu próprio plano de emulação de adversário.
- A criação de seu próprio plano de emulação de adversário baseia-se na maior força de combinar equipe vermelha com sua própria inteligência de ameaças: os comportamentos são vistos por adversários do mundo real mirando em você! O Red Team pode transformar essa informação em testes eficazes para mostrar quais defesas funcionam bem e onde os recursos são necessários para melhorar. Há um nível de impacto muito mais alto quando as lacunas de visibilidade e controles são expostas por testes de segurança, quando você pode mostrar uma alta probabilidade de que elas foram aproveitadas por um adversário conhecido. Vincular seu próprio CTI aos esforços de emulação do adversário aumentará a eficácia dos testes e os resultados para que a liderança sênior promova a mudança.



# Adversary Emulation – Service Process



# Adversary Emulation – Tools Examples

- MITRE CALDERA - An automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. <https://github.com/mitre/caldera>
- APTSimulator - A Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised. <https://github.com/NextronSystems/APTSimulator>
- Atomic Red Team - Small and highly portable detection tests mapped to the Mitre ATT&CK Framework. <https://github.com/redcanaryco/atomic-red-team>
- Network Flight Simulator - flightsim is a lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility. <https://github.com/alphasoc/flightsim>
- Metta - A security preparedness tool to do adversarial simulation. <https://github.com/uber-common/metta>
- Red Team Automation (RTA) - RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK. <https://github.com/endgameinc/RTA>



**Breach &  
Attack  
Simulation**

# Usando o Mitre Att&ck Navigator para estruturar TTPs

Joas Antonio

# Fleury Revil - Example

- <https://mitre-attack.github.io/attack-navigator/>
- <https://github.com/CyberSecurityUP/TTPs-Mitre-Attack>

about		domains		platforms									
Fleury Revil		Enterprise ATT&CK v9		Windows, Office 365, SaaS, IaaS, PRE, Network									
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Manipulation	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscate/Decode File or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over CI Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Scheduled Task/job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Pushing for Information	Obtain Capabilities	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification	Input Capture	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Software Deployment Tools	Create Account	Escape to Host	Execution Guardrails	Man-in-the-Middle	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	System Services	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Modify Authentication Process	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	User Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow	Hijack Execution Flow	OS Credential Dumping	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
				Hijack Execution Flow	Process Injection	Process Injection	Steal Application Access Token	Network Sniffing		Data Staged	Non-Standard Port		Resource Hijacking
				Implant Internal Image	Scheduled Task/job	Scheduled Task/job	Steal or Forge Kerberos Tickets	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Valid Accounts	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
				Office Application Startup			Two-factor Authentication Interception	Permission Groups Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot			Masquerading	Process Discovery		Man-in-the-Middle	Traffic Signaling		
				Scheduled Task/job			Modify Authentication Process	Query Registry		Screen Capture	Web Service		
				Server Software Component			Modify Cloud Compute Infrastructure	Remote System Discovery		Video Capture			
				Traffic Signaling			Modify Registry	Software Discovery					
				Valid Accounts			Modify System Image	System Information Discovery					
							Network Boundary Bridging	System Location Discovery					
							Obfuscated Files or Information	System Network Configuration Discovery					
							Pre-OS Boot	System Network Connections Discovery					
							Process Injection	System Owner/User Discovery					
							Rogue Domain Controller	System Service Discovery					
							Rookit	System Time Discovery					
							Signed Binary Proxy Execution	Virtualization/Sandbox Evasion					
							Signed Script Proxy Execution						
							Subvert Trust Controls						
							Template Injection						
							Traffic Signaling						
							Trusted Developer Utilities Proxy Execution						
							Untrusted/Unsupported Protocol Execution						

# Cracking the Perimeter ou Cracking The Bridge

---

Joas Antonio

# Cracking the Perimeter ou Cracking The Bridge – O que é?

---

- O Cracking The Perimeter foca em testar os controles de segurança de defesa de várias formas, sabemos que Oday é constante e uma equipe preparada para validar se seu ambiente está suscetível a ataques dessas ameaças desconhecidas, trabalhando em conjunto com a equipe de Threat Intelligence e Threat Hunter para coletar inteligência de ameaças, novos CVEs, Odays vendidos ao mercado e PoCs de vulnerabilidade. A equipe de quebra de perímetro é precisamente treinada para testar os controles de segurança e se aprofundar na busca de Odays.

<https://github.com/CyberSecurityUP/Cracking-The-Perimeter-Framework/blob/main/CTP%20-%20Framework%201.0%20-%20Portugues%20Version.pdf>

# Conclusão



**My LinkedIn**

<https://www.linkedin.com/in/joas-antonio-dos-santos>

# Referências

- <https://www.packetlabs.net/red-team-vs-blue-team/>
- <https://searchsecurity.techtarget.com/answer/Penetration-testing-vs-red-team-Whats-the-difference>
- <https://www.appknox.com/blog/penetration-testing-vs-red-team-what-is-the-difference>
- <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf>
- <https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3>
- <https://realprotect.net/o-que-e-o-mitre-attck-e-como-ele-pode-melhorar-sua-cybersecurity/>
- <https://www.anomali.com/pt/resources/what-mitre-attck-is-and-how-it-is-useful>
- <https://www.mcafee.com/enterprise/pt-br/security-awareness/cybersecurity/what-is-mitre-attack-framework.html>
- <https://www.rapid7.com/fundamentals/mitre-attack/>
- <https://www.threatq.com/mitre-attack/>
- <https://www.kaspersky.com/enterprise-security/mitre-attack>
- <https://www.redteamsecure.com/approach/red-teaming-methodology>