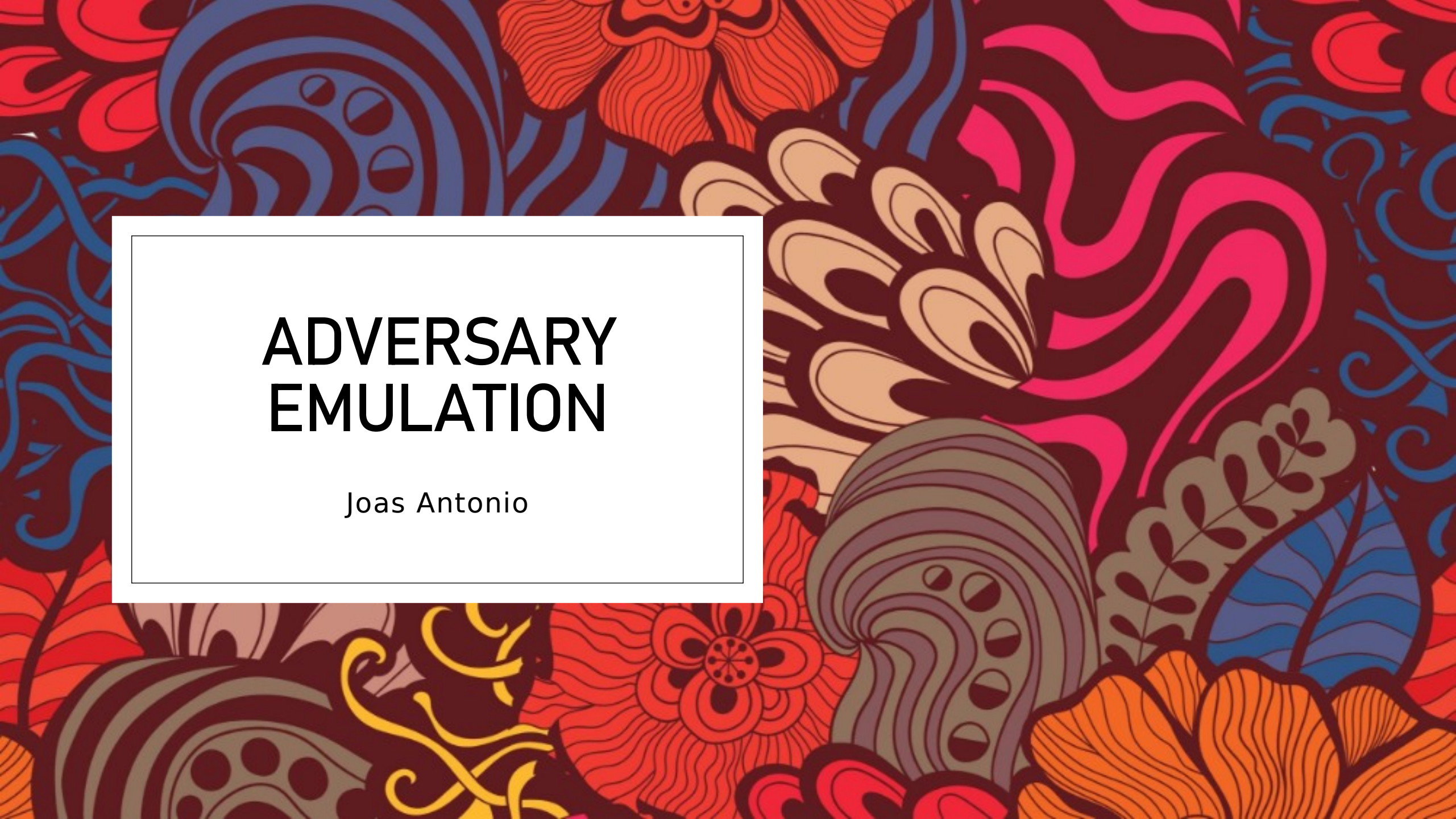

ADVERSARY EMULATION
Joas Antonio

O que é Adversary Emulation?

- Estes são documentos-protótipo do que pode ser feito com relatórios de ameaças disponíveis publicamente e ATT & CK. O objetivo desta atividade é permitir que os defensores testem com mais eficácia suas redes e defesas, permitindo que as equipes vermelhas modelem mais ativamente o comportamento do adversário, conforme descrito pela ATT & CK. Isso faz parte de um processo maior para ajudar a testar produtos e ambientes de maneira mais eficaz, bem como criar análises para comportamentos ATT e CK, em vez de detectar um indicador específico de comprometimento (IOC) ou ferramenta específica.

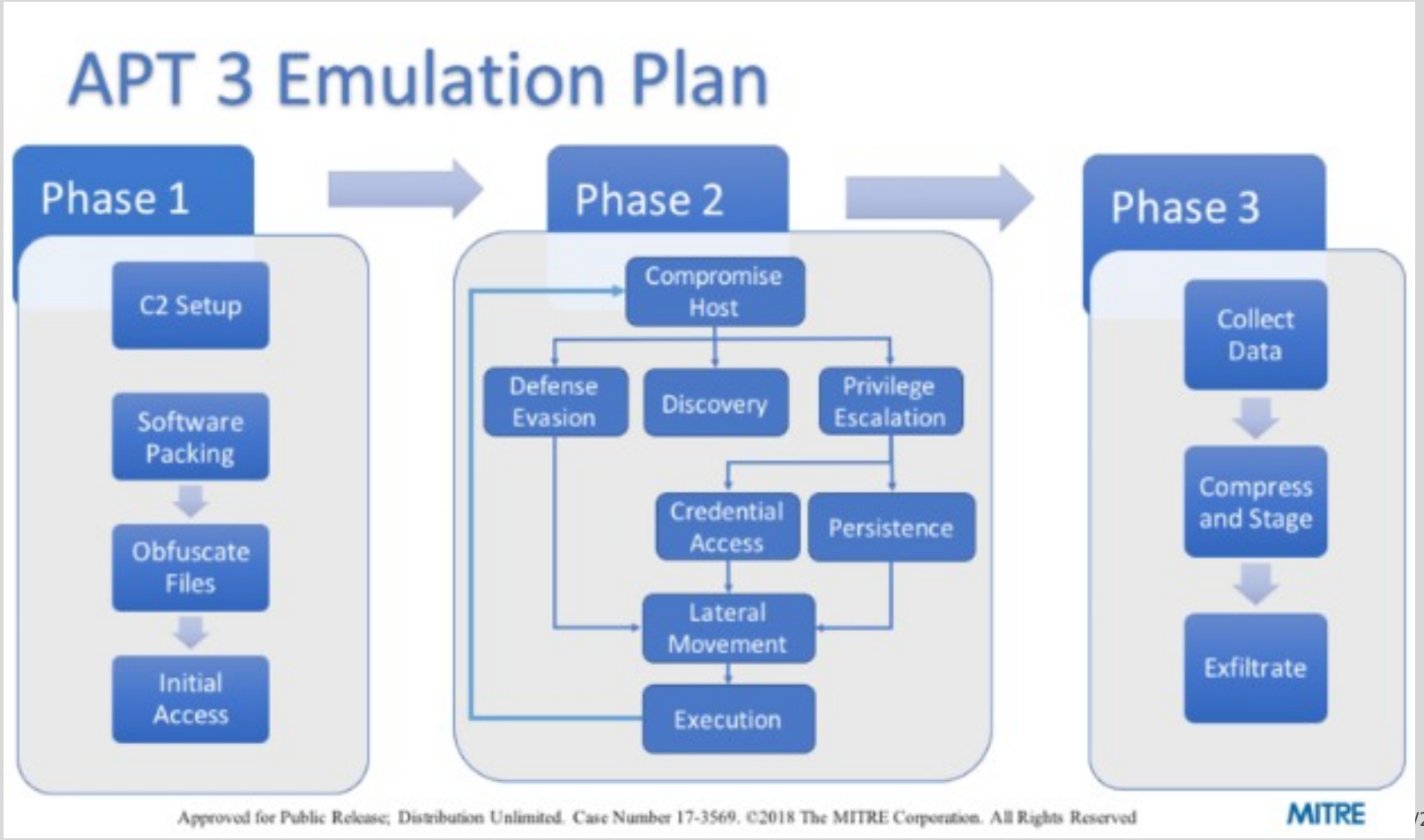
O que é Adversary Emulation?

- Existem muitos relatórios de inteligência de ameaças que se concentram em engenharia reversa de malware, comprometimento inicial e explicações de comando e controle (C2); no entanto, não há muitos relatórios de ameaças sobre como os invasores estão encadeando técnicas ou como os invasores operam no teclado. Como esses protótipos são construídos com base nesses relatórios de ameaças abertos, eles têm as mesmas limitações. Para ajudar com isso, fornecemos um exemplo de forma de encadear as táticas ATT e CK com base na experiência geral de Red Team. Para criar esses planos, a equipe pesquisou grupos APT específicos listados na ATT & CK e ver que tipo de planos poderiam ser gerados para um operador emular esses APTs. Depois de ler quais recursos eram fornecidos pelas ferramentas de um APT, compilamos uma lista de outras maneiras de exibir o mesmo comportamento. Queríamos que os operadores se comportassem geralmente como um adversário específico (aderindo aos TTPs e comportamentos conhecidos desse adversário), mas tendo alguma latitude na implementação real. Para ajudar com isso, também fornecemos uma folha de dicas para comandos que podem ser executados para comportamento semelhante em algumas das ferramentas de formação de equipes vermelhas mais comumente usadas. Um diagrama de amostra de alto nível é destacado abaixo como uma forma possível de estruturar um plano de emulação APT3.

Adversary Emulation x PenTest

- É direcionado à estratégia e orientado a metas para a exfiltração de dados
- Ele opera a partir de um pressuposto de compromisso: nossa equipe assume o papel de um agente de ameaças competente e sofisticado que já se infiltrou em sua rede
- Ele estabelece a persistência do mundo real dentro de sua infraestrutura, fornecendo, assim, indicadores do mundo real de comprometimento para sua equipe de resposta a incidentes
- Ele não emprega metodologias de exploração potencialmente destrutivas em ambientes de produção para estabelecer o acesso, por isso é de baixo impacto nas operações do dia-a-dia e seguro para executar dentro de sua infraestrutura real
- **A simulação de adversários** é a próxima etapa na avaliação de ameaças e preparação para resposta a incidentes. A história recente mostra que a empresa moderna deve manter uma postura de segurança que opere sob o pressuposto de comprometimento. Você ficará comprometido em algum momento e reconhecer esse fato o ajudará a se preparar para o próximo nível de resposta a incidentes: lidar com um invasor ativo e potencialmente avançado dentro de sua infraestrutura.

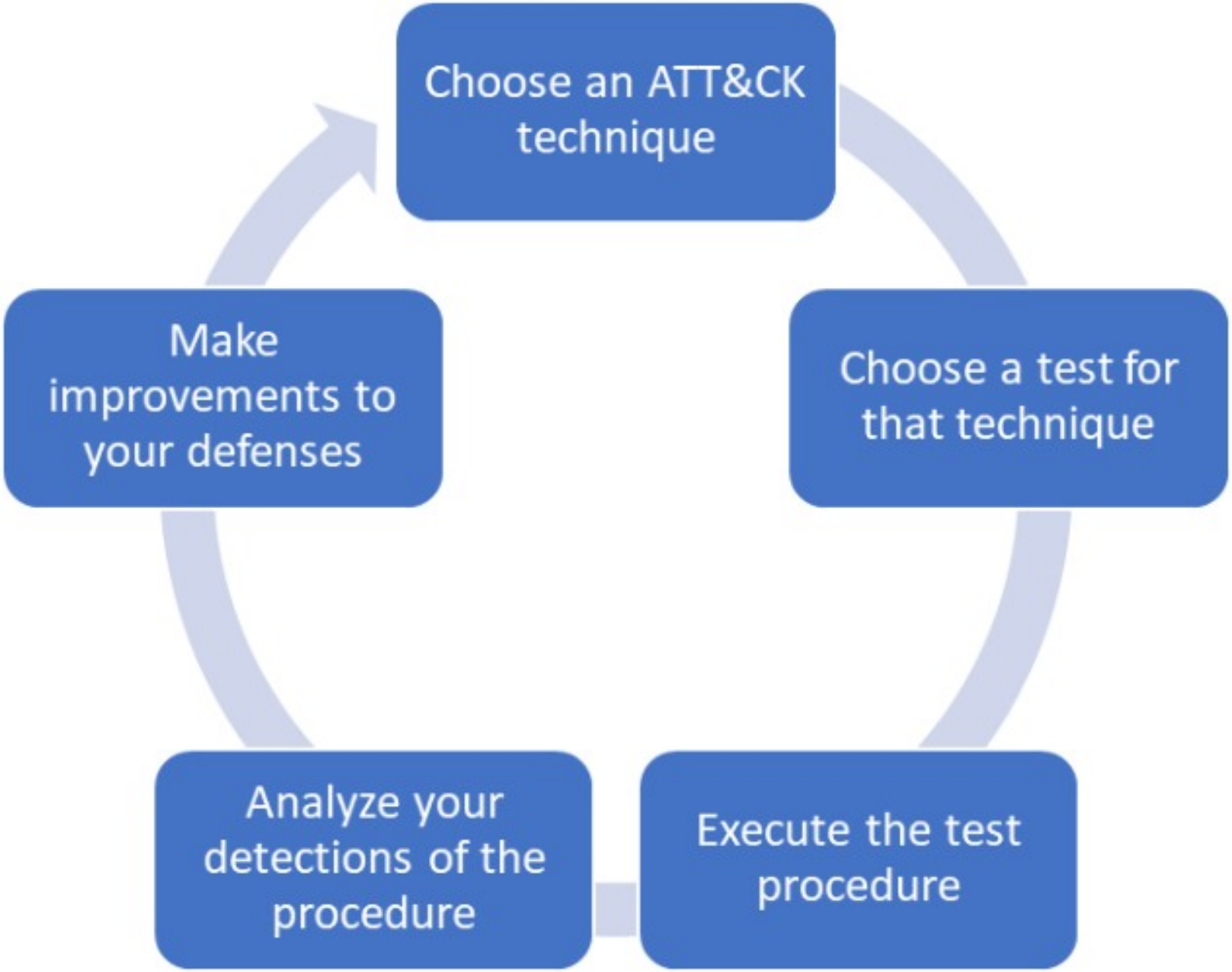
EXEMPLO APT3



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 time vermelho, então não se preocupe! Existem alguns recursos disponíveis para ajudar a iniciar o teste de suas defesas com técnicas alinhadas com ATT e CK. Vamos destacar como você pode mergulhar na emulação do adversário tentando testes simples. 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 e CK. Por exemplo, talvez você tenha seguido o conselho de Katie e examinado as técnicas usadas pelo APT3 , como Network Share Discovery (T1135) . Sua equipe de inteligência passou isso para sua equipe de detecção e, seguindo a orientação de John , eles escreveram uma análise comportamental para tentar detectar se um adversário executou essa técnica. Mas como saber se realmente detectaria essa técnica? 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.

- Ferramenta Atomic: https://github.com/redcanaryco/atomic-red-team
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/Indexes/Indexes-Markdown/index.md



Adversary Emulation: Nivel 1

Ciclo de Teste do ATOMIC

Adversary Emulation: Nivel 1

- *CALDERA é um sistema de emulação de adversário automatizado criado pelo MITER que possui muitos comportamentos embutidos mapeados para técnicas ATT & CK. Ele permite que o operador escolha uma técnica ou encadeie várias ao construir o teste, o que permite que você comece a automatizar sequências de comportamentos para o seu teste, em vez de executar manualmente testes atômicos únicos. Você pode usar um dos cenários pré-construídos ou definir um cenário mais específico, escolhendo os procedimentos (chamados de habilidades no CALDERA) que mapeiam para certas técnicas ATT & CK que você deseja testar.*
- https://github.com/mitre/caldera

Adversary Emulation: Nivel 2

- você pode tirar muito proveito da integração da ATT & CK com seus compromissos existentes. O mapeamento das técnicas usadas em uma contratação de Red Team para a ATT & CK fornece uma estrutura comum ao escrever relatórios e discutir mitigações.
- Para começar, você pode pegar uma operação planejada existente ou ferramenta que você usa e mapeá-la para a ATT & CK. O mapeamento dos procedimentos da Red Team para a ATT & CK é semelhante ao mapeamento da inteligência sobre ameaças para a ATT & CK, portanto, você pode verificar as recomendações de Katie para um processo de 6 etapas descrito em sua postagem de inteligência sobre ameaças .Felizmente, às vezes as técnicas de mapeamento podem ser tão simples quanto pesquisar o comando usado no site da ATT & CK. Por exemplo, se usamos o comando 'whoami' em nossa operação de Red Team, podemos pesquisá-lo no site da ATT & CK e descobrir que duas técnicas provavelmente se aplicam: Proprietário do sistema / Descoberta do usuário (T1033) e Interface de linha de comando (T1059) .

Category	Built-in Windows Command	Cobalt Strike	Metasploit
Discovery			
T1082	ver	shell ver	
T1082	set	shell set	get_env.rb
T1033	whoami /all /fo list	shell whoami /all /fo list	getuid
T1082	net config workstation net config server	shell net config workstation shell net config server	
T1016	ipconfig /all	shell ipconfig	ipconfig post/windows/gather/enum_domains
T1082	systeminfo [/s COMPNAME] [/u DOMAIN\user] [/p password]	systemprofiler kool if no access yet (victim browses to website) or	sysinfo, run winenum, get_env rb

Adversary Emulation: Nivel 2

Outro recurso útil para começar a mapear os procedimentos da Red Team para ATT & CK é o APT3 Adversary Emulation Field Manual , que mostra as ações de comando por comando que o APT3 usou, todas mapeadas para ATT & CK.

Adversary Emulation: Nivel 2

- Está usando ferramentas como Cobalt Strike ou Empire , boas notícias - elas já estão mapeadas para ATT & CK. Armado com seus comandos, scripts e ferramentas individuais mapeados para ATT & CK, agora você pode planejar seu envolvimento.
- Algumas equipes vermelhas têm seus kits de ferramentas e métodos de operação testados e comprovados. Eles sabem o que funciona porque funciona o tempo todo. Mas o que eles nem sempre sabem é quanto de seus TTPs testados e comprovados se sobrepõem (ou não) com ameaças conhecidas que podem ter como alvo a organização. Isso leva a uma pequena lacuna no entendimento de como as defesas se comparam ao que você está realmente tentando se defender, os adversários atacando seu ambiente e não necessariamente o próprio time vermelho.
- Queremos ter certeza de que não estamos fazendo as técnicas apenas porque nossa ferramenta pode executá-las - queremos emular um adversário real com o qual nos preocupamos para fornecer mais valor. Por exemplo, podemos falar com nossa equipe de inteligência de ameaças cibernéticas (CTI) e eles nos dizem que estão preocupados com a segmentação do grupo iraniano conhecido como OilRig. Como tudo está estruturado em ATT & CK, podemos usar o ATT & CK Navigator para comparar as técnicas que poderíamos fazer com uma ferramenta que já temos como Cobalt Strike com as técnicas que sabemos que a OilRig fez com base em relatórios de código aberto. (Você pode verificar uma demonstração do Navigator aqui que mostra como fazer isso.) No gráfico abaixo, as técnicas de Cobalt Strike são vermelhas, as técnicas de OilRig são azuis e as técnicas de Cobalt Strike podem executar *e*OilRig usou são roxos. Essas técnicas roxas nos dão um lugar para começar a usar uma ferramenta que já temos e executar técnicas que são prioritárias para nossa organização.

Adversary Emulation: Nivel 3

- Nesse ponto, sua 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 Red Team com sua própria inteligência de ameaças: **os comportamentos são vistos por adversários do mundo real mirando em você!** A 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.
- Recomendamos um processo de cinco etapas descrito no diagrama abaixo para criar um plano de emulação do adversário, executar a operação e impulsionar melhorias defensivas. (Para obter um esboço mais detalhado do processo, consulte a apresentação de Katie Nickels e Cody Thomas em Threat-Based Adversary Emulation with ATT & CK

Adversary Emulation: Nivel 3

Adversary Emulation: Nivel 3

- 1. **Reúna informações sobre ameaças** - selecione um adversário com base nas ameaças à sua organização e trabalhe com a equipe do CTI para analisar informações sobre o que o adversário fez. Combine o que é baseado no que sua organização sabe, além de informações publicamente disponíveis para documentar os comportamentos do adversário, o que eles perseguem, se eles quebram e agarram ou baixo e lento.
- 2. **Extrair técnicas** - da mesma forma que você mapeou as operações da equipe vermelha para as técnicas ATT e CK, mapeie a inteligência de que você dispõe para técnicas específicas em conjunto com sua equipe da Intel. Você pode indicar à equipe do CTI a postagem do blog de Katie para ajudá-los a aprender como fazer isso.
- 3. **Analise e organize** - agora que você tem um monte de informações sobre o adversário e como ele opera, faça o diagrama dessas informações em seu fluxo operacional de uma forma que seja fácil de criar planos específicos. Por exemplo, abaixo está o fluxo operacional que a equipe MITER criou para o Plano de Emulação Adversário APT3.
- 4. **Desenvolva ferramentas e procedimentos** - Agora que você sabe o que gostaria que a equipe vermelha fizesse, descubra como implementar o comportamento. Considerar:

- Como o grupo de ameaça usou essa técnica?
- O grupo variou a técnica usada com base no contexto do ambiente?
- Quais ferramentas podemos usar para replicar esses TTPs?

Adversary Emulation: Nivel 3

- 5. **Emular o adversário** - Com um plano em vigor, a equipe vermelha agora tem a capacidade de executar e realizar um compromisso de emulação. Como recomendamos para todos os compromissos da equipe vermelha usando ATT & CK, a equipe vermelha deve trabalhar em estreita colaboração com a equipe azul para obter um entendimento profundo de onde estão as lacunas na visibilidade da equipe azul e por que existem.
- Depois que todo esse processo ocorre, as equipes vermelha e azul podem trabalhar com a equipe CTI para determinar a próxima ameaça para repetir o processo, criando uma atividade contínua que testa as defesas contra comportamentos do mundo real.

27/05/2021

ESTRUTURANDO SERVIÇO

FALHA AO DETECTAR ATAQUES SOFISTICADOS

Os invasores podem passar despercebidos por longos períodos de tempo, portanto as organizações precisam testar continuamente a capacidade de sua equipe de segurança de detectar e responder aos sofisticados ataques direcionados de hoje.

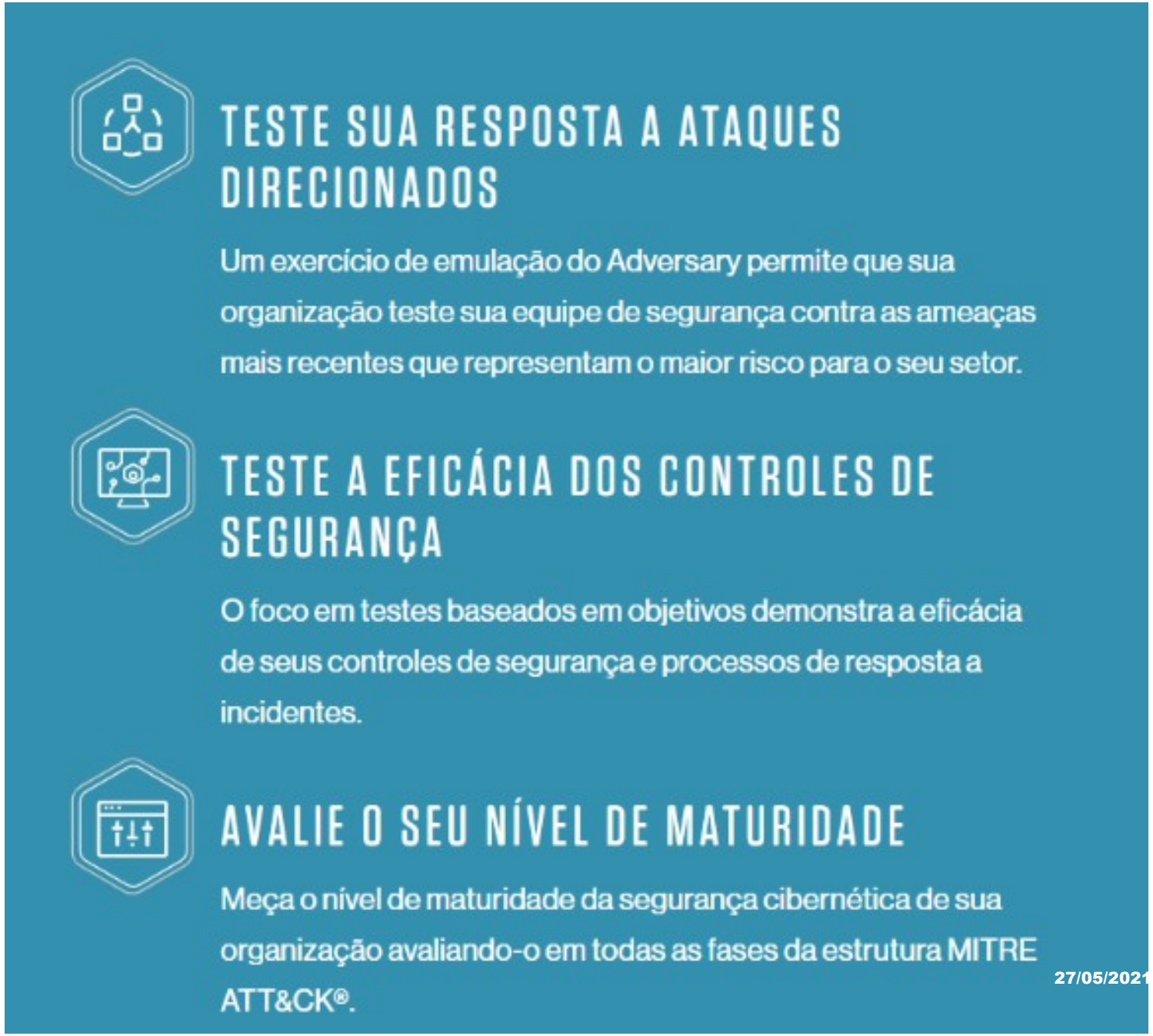
CONTROLES DE SEGURANÇA INEFICAZES

As organizações precisam validar se seus controles e processos de segurança atuais são eficazes contra os TTPs adversários em evolução de hoje.

LACUNAS DE SEGURANÇA

Os adversários podem explorar vulnerabilidades rapidamente e obter movimento lateral em sua rede , e você precisa identificar lacunas em sua postura de segurança atual para entender como um invasor pode violar sua rede.

Adversary Emulation: Desafio



27/05/2021

Adversary Emulation: Benefícios

Adversary Emulation: Ciclo

FASE 1

Integração e escopo

Trabalhar com o cliente para estabelecer um MSA e Regras de Compromisso (ROE) e definir uma Estrutura Analítica do Trabalho (WBS). Isso permite que nossa equipe se aproxime das partes interessadas e da equipe de segurança para estabelecer um cronograma de testes para garantir que atendemos aos seus requisitos de negócios. Nossa equipe gastará tempo para entender completamente seus objetivos, para que possamos atender totalmente às suas necessidades.

Adversary Emulation: Fase 1

Adversary Emulation: Fase 2

Adversary Emulation: Fase 3

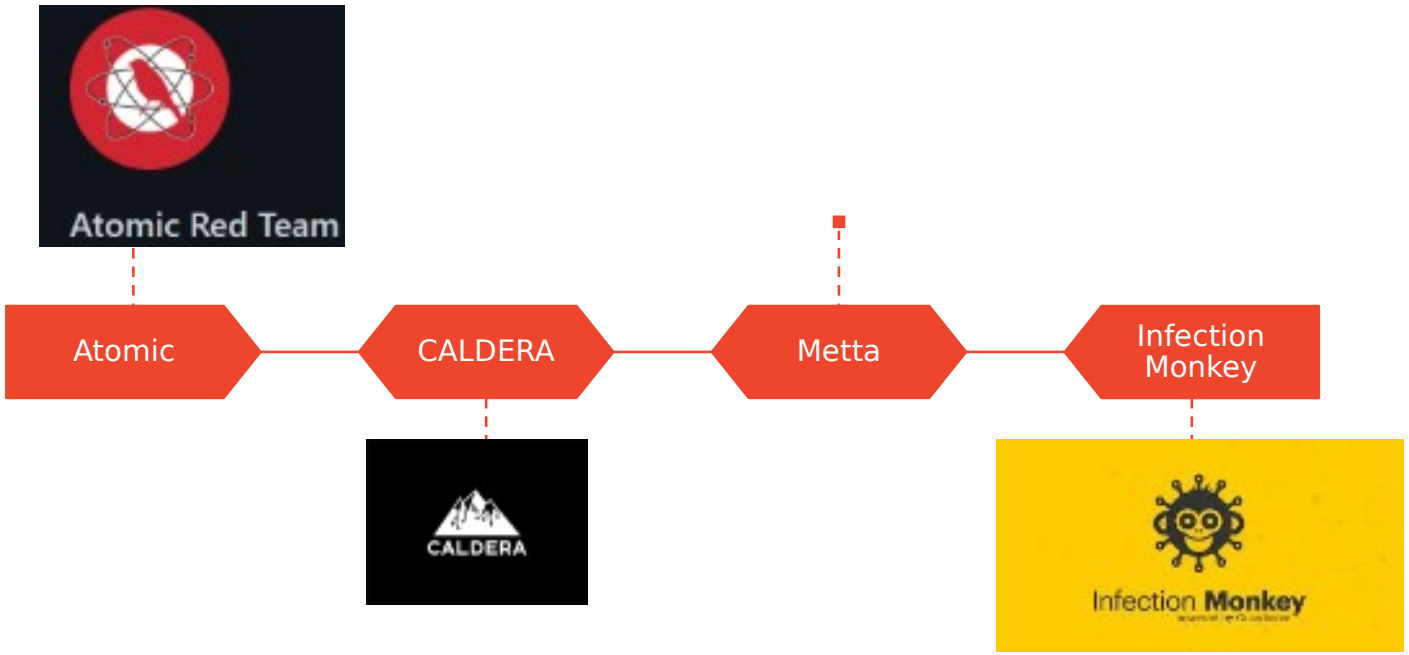
Adversary Emulation: Fase 4

Adversary Emulation: Fase 5

Adversary Emulation: Fase 6

Adversary Emulation: Fase 7

Adversary Emulation: Ferramentas



https://pentestit.com/adversary-emulation-tools-list/

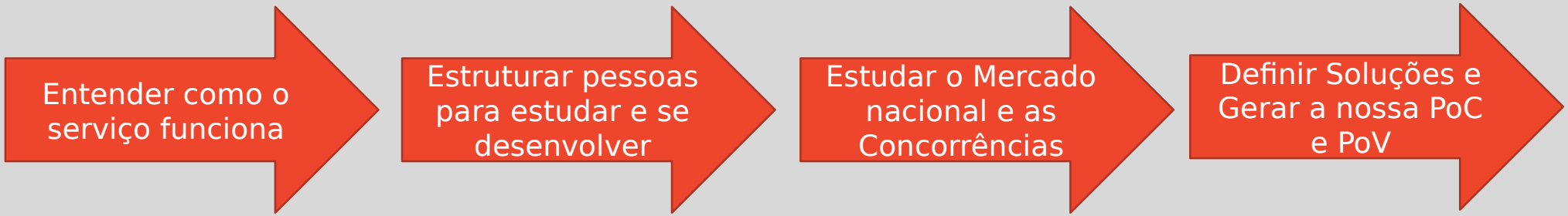
27/05/2021

CONCLUSÃO

Dentro do negócio

Estruturar um serviço do tipo, além de pessoas, precisamos de ferramentas e realizar uma Prova de Conceito e uma Prova de Valor internamente, para assim vendermos esse tipo de serviço para outras empresas.

Fluxo de negócio:



Por fim, vender!