1.Introdução

Threat Intelligence (TI) ou Cyber Threat Intelligence (CTI) são as informações, ou TTPs (Táticas, Técnicas e Procedimentos), atribuídas a um adversário, comumente usadas por defensores para auxiliar em medidas de detecção. A célula vermelha pode alavancar CTI de uma perspectiva ofensiva para auxiliar na emulação do adversário.

2.O que é Threat Intel

Cyber Threat Intelligence pode ser consumido (para tomar medidas sobre dados) coletando IOCs (Indicadores de Compromisso) e TTPs comumente distribuídos e mantidos por ISACs (Centros de Análise de Informação e Compartilhamento). Plataformas e estruturas de inteligência também auxiliam no consumo de CTI, focando principalmente em um cronograma abrangente de todas as atividades.

Tradicionalmente, os defensores usam inteligência de ameaças para fornecer contexto ao cenário de ameaças em constante mudança e quantificar descobertas. IOCs são quantificados por rastros deixados por adversários, como domínios, IPs, arquivos, strings, etc. A equipe azul pode utilizar vários IOCs para construir detecções e analisar comportamento.

Da perspectiva da equipe vermelha, você pode pensar em inteligência de ameaças como a análise da equipe vermelha sobre a capacidade da equipe azul de alavancar adequadamente o CTI para detecções.

3.Aplicações de CTI em Red teams

Conforme mencionado anteriormente, o *red team* utilizará o CTI para auxiliar na emulação do adversário e dar suporte às evidências dos comportamentos do adversário. Para ajudar no consumo de CTI e na coleta de TTPs, os *red teams* geralmente usam plataformas e estruturas de inteligência de ameaças, como MITRE ATT&CK, TIBER-EU e OST Map.

Essas estruturas cibernéticas coletarão TTPs conhecidos e os categorizarão com base em características variadas, como:

- Threat group (grupo de ameaças)
- Kill chain phase (fase de kill chain)
- Táticas
- Objetivos

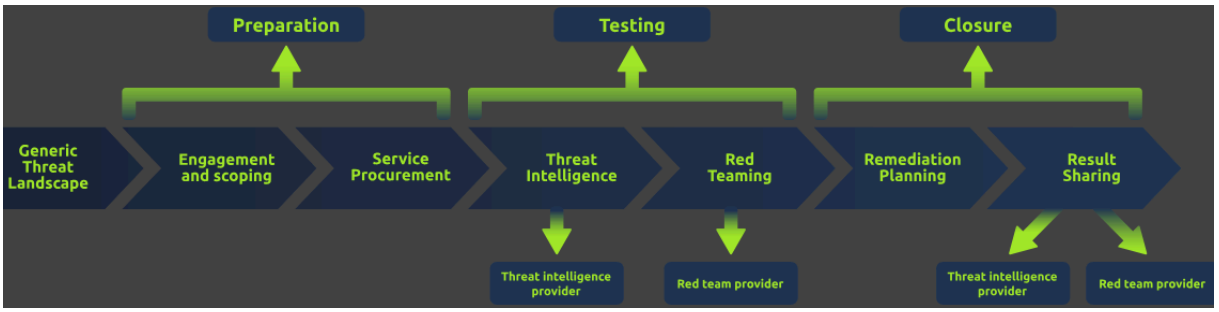
Aproveitar TTPs é usado como uma técnica de planejamento em vez de algo em que uma equipe se concentrará durante a execução do engajamento. Dependendo do tamanho da equipe, uma equipe CTI ou um operador de inteligência de ameaças pode

ser empregado para reunir TTPs para o *red team*. Durante a execução de um engajamento, o *red team* usará inteligência de ameaças para elaborar ferramentas, modificar tráfego e comportamento e emular o adversário visado.

4.O Framework TIBER-EU

TIBER-EU (Threat Intelligence-based Ethical Red Teaming) é uma estrutura comum desenvolvida pelo Banco Central Europeu que se concentra no uso de inteligência de ameaças.

Do white paper do ECB TIBER-EU, "O Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) permite que autoridades europeias e nacionais trabalhem com infraestruturas e instituições financeiras (doravante denominadas coletivamente como 'entidades') para implementar um programa para testar e melhorar sua resiliência contra ataques cibernéticos sofisticados."



Essa estrutura abrange uma prática recomendada e não algo acionável da perspectiva de um *red team*.

5.Mapeamento TTP

O Mapeamento TTP é empregado pela *red cell* para mapear TTPs coletados pelos adversários para uma cadeia de destruição cibernética padrão. O mapeamento de TTPs para uma cadeia de destruição auxilia a equipe vermelha no planejamento de um engajamento para emular um adversário.

Para começar o processo de mapeamento de TTPs, um adversário deve ser selecionado como alvo. Um adversário pode ser escolhido com base em:

- Ramo do alvo
- Vetores de ataques envolvendo funcionários
- País de origem
- Outros fatores

6.Outras aplicações de CTI para Red Team

O CTI também pode ser usado durante a execução do engajamento, emulando as características comportamentais do adversário, como:

- Tráfico C2
- Ferramentas e malwares

O primeiro uso comportamental do CTI que mostraremos é a manipulação de tráfego C2 (Comando e Controle). Um *red team* pode usar o CTI para identificar o tráfego dos adversários e modificar seu tráfego C2 para emulá-lo. Um exemplo de um red team modificando o tráfego C2 com base no CTI coletado são os perfis maleáveis. Um perfil maleável permite que um operador do *red team* controle múltiplos aspectos do tráfego do listener de um C2.

As informações a serem implementadas no perfil podem ser coletadas de ISACs e IOCs coletados ou capturas de pacotes, incluindo:

- Host headers
- POST URIs
- Respostas de servidores e headers

O tráfego coletado pode ajudar um *red team* a fazer com que seu tráfego pareça semelhante ao do adversário visado para se aproximar do objetivo de emulação do adversário.

O segundo uso comportamental do CTI é analisar o comportamento e as ações do malware e das ferramentas de um adversário para desenvolver ferramentas ofensivas que emulem comportamentos semelhantes ou tenham indicadores vitais semelhantes. Um exemplo disso poderia ser um adversário usando um dropper personalizado. A equipe vermelha pode emular o dropper por:

- Identificação de tráfego
- Observação de *syscalls* e API *calls*
- Identificar o comportamento geral do *dropper* e o objetivo
- Adulteração de assinaturas de arquivos e IOCs

A inteligência e as ferramentas coletadas a partir da inteligência de ameaças comportamentais podem ajudar uma equipe vermelha a preparar as ferramentas específicas que serão usadas para executar os TTPs planejados.

7.Criando uma campanha de Threat Intel impulsionada

Uma campanha baseada em informações sobre ameaças usará todo o conhecimento e tópicos abordados anteriormente e os combinará para criar uma campanha bem planejada e pesquisada. O fluxo de tarefas nesta sala segue logicamente o mesmo caminho que você tomaria como uma equipe vermelha para começar a planejar uma campanha:

- Identificação do framework e *kill chain* geral

- Determinar o adversário alvo
- Identificar a TTP e IOC do adversário
- Mapear informações de *threat intelligence* para um framework ou *kill chain*
- Elaborar e manter a documentação de engajamento necessária
- Determinar e usar os recursos de engajamento necessários (ferramentas, modificação de C2, domínios, etc.)