Fundamentos da Análise de Intrusão:

Uso da Cyber Kill Chain e do Modelo Diamante para interpretação de Incidentes

Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

Sumário

Introdução

- **Definições de Incidentes e Indicadores**

Desenvolvimento

- **Overview da Gestão, Tratamento e Resposta a Incidentes**
- **Cyber Kill Chain e Modelo Diamante**
- **Integração da CKC e do Modelo Diamante**
- **Linhas de Ação**
- **Exemplos de Análise Preliminar**

Conclusão

Introdução

Uma organização precisa de uma definição compartilhada e compreendida de incidentes de segurança de computadores.

Critérios comuns para determinar o que é e o que não é um incidente devem ser estabelecidos.

Avaliar e decidir: alguém deve avaliar a situação para determinar se ela é de fato um incidente;

Definições de Incidentes

IT Infrastructure Library (ITIL) 2011

> “uma interrupção não planejada de um Serviço de TI ou redução na qualidade de um serviço de TI”

ISO/IEC 27035-1:2023

> “evento(s) de segurança da informação relacionados e identificados que podem prejudicar os ativos de uma organização ou comprometer suas operações”

SANS Computer Security Incident Handling Step-by-Step Guide

> “um evento adverso em um sistema de informação e/ou rede, ou a ameaça da ocorrência de tal evento”

NIST Computer Security Incident Handling Guide

> “uma violação ou ameaça iminente de violação de políticas de segurança de computadores, políticas de uso aceitável ou práticas de segurança padrão”

Definições de Incidentes

Um incidente cibernético é definido como um evento que leve a um **impacto real ou potencial**, comprometendo pelo menos uma das características dos ativos da informação: a disponibilidade, a integridade, a confidencialidade ou a autenticidade.

O incidente cibernético também pode ser caracterizado pela tentativa de exploração de vulnerabilidade em sistema da informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso, conforme inciso V do art. 4º do Nº 10.748, de 16 de Julho de 2021.

https://www.gov.br/ctir/pt-br/canais_atendimento/orientacoes-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov

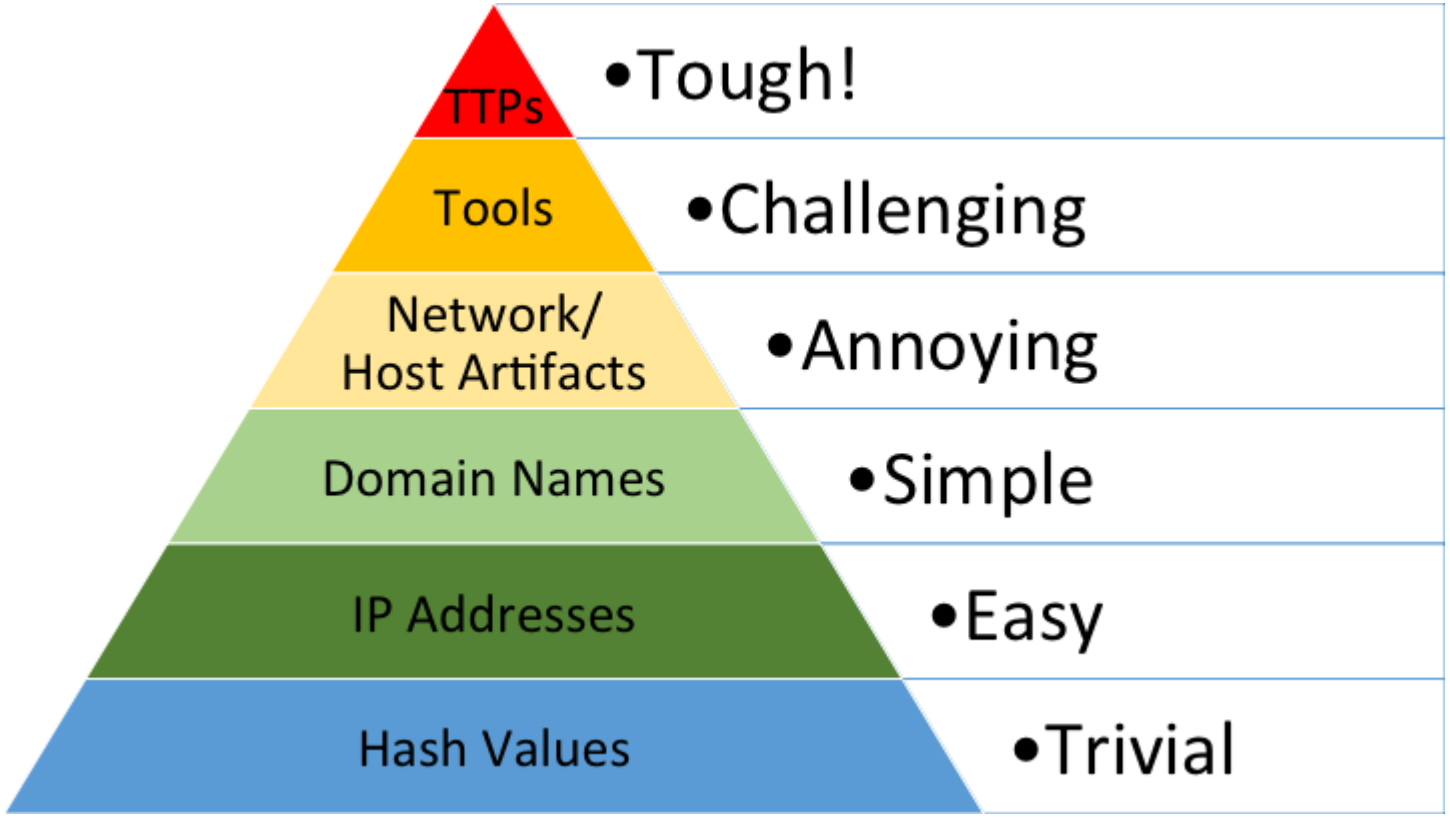
Indicadores e Incidentes

A identificação de um Incidente Cibernético se dá por meio da percepção ou detecção de sinais ou indicadores que caracterizem, com alto nível de probabilidade e confiança, a ocorrência de do comprometimento de computadores, redes ou sistemas, com impactos nas informações processadas, armazenadas ou transmitidas.

Esses indicadores podem estar relacionados às tecnologias, técnicas ou infraestruturas utilizadas por atores maliciosos nos seus ataques ou aos impactos ou danos decorrentes das ações de atores maliciosos.

https://www.gov.br/ctir/pt-br/canais_atendimento/orientacoes-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov

Indicadores e Incidentes



Nem todos os indicadores são criados iguais, porém, e alguns deles são muito mais valiosos do que outros.

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html, por David Bianco.

Sumário

Introdução

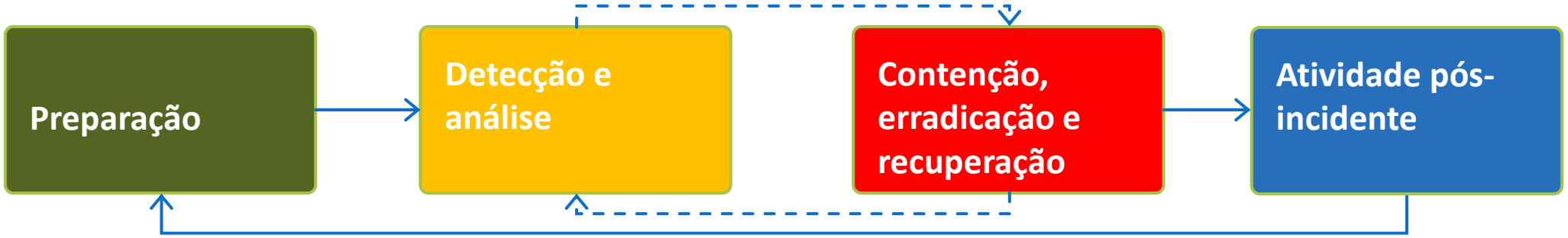
- Definições de Incidentes

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

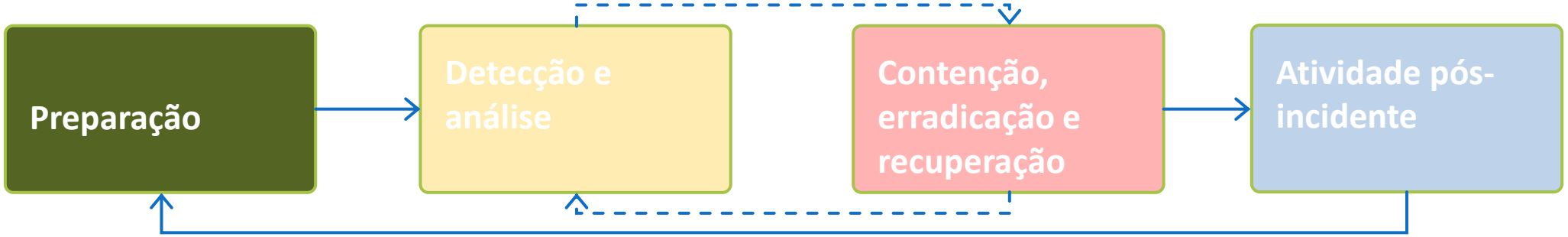
Desenvolvimento



A <u>Gestão de Incidentes</u> envolve as ações que a organização toma para prevenir ou conter o impacto de um incidente, enquanto ele está ocorrendo ou logo após sua ocorrência.

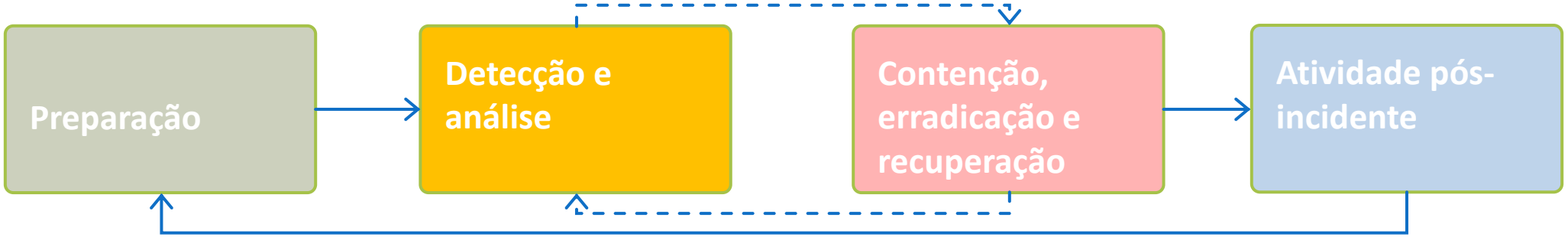
Guia de gerenciamento de incidentes NIST SP 800-61 r2, NIST https://csrc.nist.gov/pubs/sp/800/61/r2/final

Fases da Gestão de Incidentes



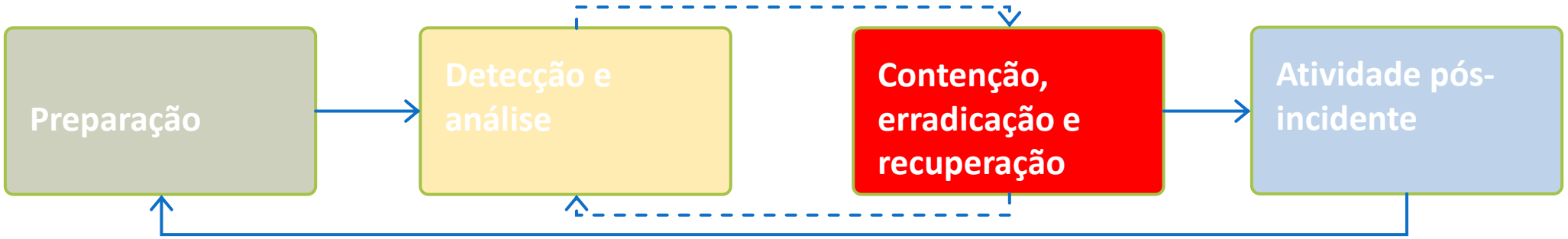
1. Preparação:
   - Estabelecer uma política e um plano de resposta a incidentes
   - Construir uma equipe de resposta a incidentes e definir funções e responsabilidades
   - Adquirir ferramentas e recursos necessários
   - Fornecer treinamento para a equipe de resposta a incidentes

Fases da Gestão de Incidentes



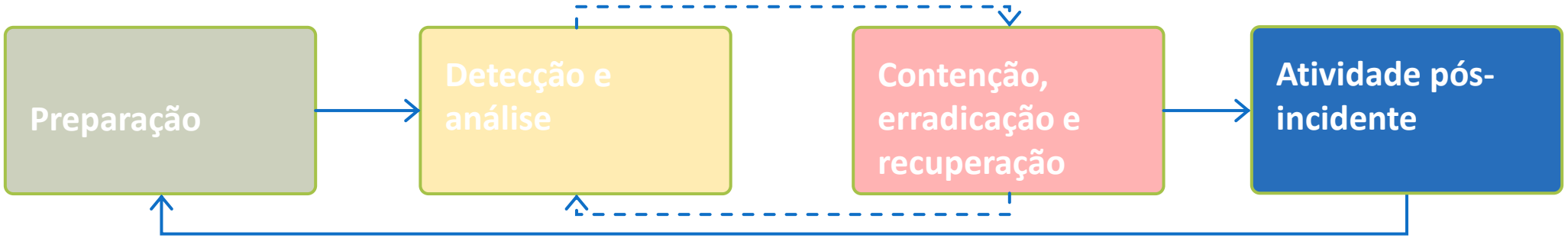
2. Detecção e **<u>análise</u>**:
   - Monitorar sistemas e redes em busca de possíveis incidentes
   - Analisar precursores e indicadores de um incidente
   - Determinar o escopo do incidente, contê-lo se possível
   - Documentar todas as ações tomadas durante esta fase

Fases da Gestão de Incidentes



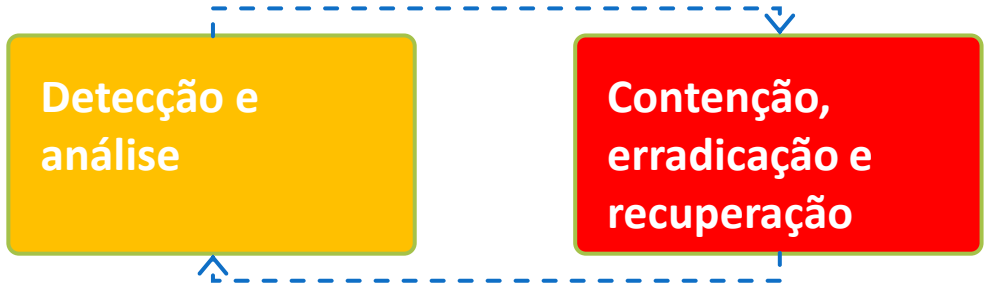
3. Contenção, erradicação e recuperação (Resposta ao Incidente):
   - Contenção de curto prazo para limitar o impacto do incidente
   - Identificar e remediar as vulnerabilidades exploradas pela ameaça
   - Erradicar completamente o incidente do ambiente
   - Recuperar sistemas e serviços para um estado operacional
   - Realizar análise de causa raiz e coletar evidências

Fases da Gestão de Incidentes



4. Atividade pós-incidente:
   - Documentar as lições aprendidas com o incidente
   - Atualizar políticas, planos, ferramentas e treinamento com base nas lições aprendidas
   - Preservar evidências e preparar-se para possíveis ações legais
   - Realizar uma revisão pós-incidente para avaliar a eficácia da resposta

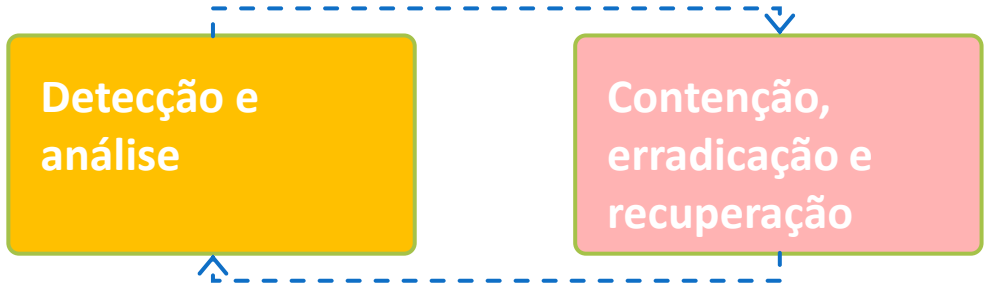
Tratamento de Incidentes



O <u>Tratamento de Incidentes</u> é o subconjunto de serviços relacionados à gestão de um evento cibernético: detecção, análise (triagem), resposta (contenção, erradicação e recuperação).

O tratamento de incidentes fornece uma visão mais aprofundada das relações entre os processos de Detectar, Analisar (Triagem) e Responder.

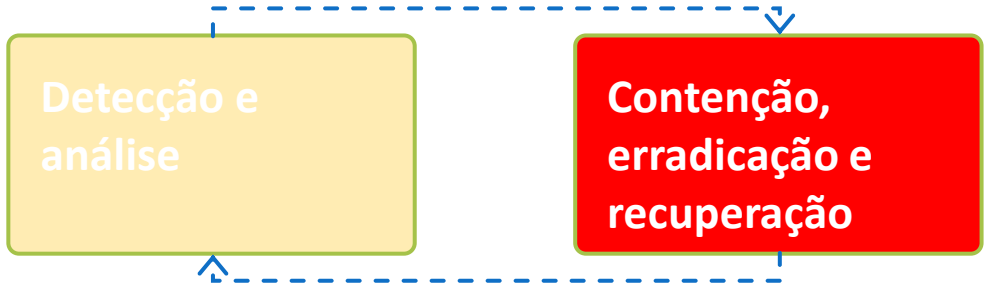
Tratamento de Incidentes



Triagem – *as ações tomadas para categorizar, priorizar e atribuir eventos e incidentes*

Análise – a tentativa de determinar o que aconteceu, qual impacto, ameaça ou dano resultou e quais etapas de recuperação ou mitigação devem ser seguidas.

Resposta a Incidentes



A <u>Resposta ao Incidente</u> são as ações reativas a um incidente. Elas visam resolver o incidente e mitigar os impactos.

Desafios na Triagem

A triagem de incidentes demanda uma capacidade de realizar a interpretação e avaliação das informações disponíveis para:

- **Validação (há IOC ? / é incidente ?)**
- **Classificação (Risco ou Impacto?)**
- **Categorização (Taxonomia ?)**
- **Priorização ?**
- **Correlação com outros ?**
- **É outro tipo de assunto ?**

Desafios na Triagem

A triagem de incidentes frequentemente recai sobre profissionais menos experientes, o que pode levar a erros críticos, como:

- **Classificação incorreta da categoria do incidente**
- **Priorização inadequada**
- **Interpretação equivocada**
- **Falta de correlação entre eventos**

Esses equívocos podem comprometer a eficácia da resposta a incidentes, aumentando o risco para a organização.

Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

Cyber Kill Chain

É um processo de sete etapas que os adversários precisam executar para cumprir sua missão com sucesso. As sete etapas são:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command-and-Control (C2)
7. Actions on Objectives

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

Cyber Kill Chain

Essas etapas são determinísticas, seguem uma premissa que para cada intrusão o adversário precisa executar as etapas, permitindo inferências nas ações anteriores e posteriores a um determinado “momento”.

Vale ressaltar que há exceções, mas essa regra geral geralmente se aplica as a grande parte das intrusões. “O Impacto” ocorre quando há uma conclusão bem-sucedida.

A utilização da na triagem facilita a interpretação dos eventos, enquadrando os indicadores de comprometimento (IOC) relacionados aos incidentes dentro de um **modelo cronológico de ações realizadas pela ameaça, como uma linha do tempo**.

1. Reconnaissance

Relacionada a coleta de informações sobre a organização alvo.

Suporta o planejamento do da intrusão, não apenas do acesso inicial.

Muitas vezes é executado por meio de OSINT e Enumeração ou Escaneamento da infraestrutura, como redes e sistemas, bem como de pessoas relacionadas ao alvo.

Nessa etapa, a visibilidade das ações do adversário muitas vezes está “mascarada” por as ações comuns na rede (não destoa do baseline e da normalidade).

2. Weaponization

Envolve a **criação, obtenção e preparação das ferramentas (código ou software malicioso)** e infraestrutura que serão usadas pela ameaça contra as vítimas.

Um exemplo é obter ou desenvolver um código malicioso (como malware), para explorar vulnerabilidades.

Normalmente, ferramentas são usadas para auxiliar esse processo, parcial ou totalmente.

Essas ferramentas frequentemente deixam rastros ou impressões digitais.

3. Delivery

Relacionada ao **vetor usado para entrega** do objeto transformado em “arma” para a vítima.

Os vetores de entrega mais comuns ocorrem por meio de ativos de rede, como HTTP, SMTP e outros sistemas Web. De forma menos comum temos entrega por meio de mídia física (ou espectro eletromagnético).

É importante destacar que geralmente ocorre uma ofuscação para mascarar o código malicioso ou verdadeira intenção da entrega.

4. Exploitation

Nela há a exploração das vulnerabilidades na infraestrutura da vítima.

Exploit: Técnica para violar a segurança de uma rede ou sistema de informação, violando a política de segurança.

O Exploit pode ser feito em vulnerabilidades de software bem como em configurações ruins ou erros humanos.

A fase de *Exploitation* pode ocorrer em ciclos com a de Delivery, na exploração de pessoas e tecnologias (engenharia social + código malicioso).

5. Installation

A execução de código pelo atacante na infraestrutura da vítima. O adversário busca o controle operacional de um sistema.

Envolve muitas vezes série de etapas executadas automaticamente, usando chamadas de sistema padrão, para organizar o código malicioso no sistema de forma que ele seja instalado e invocado da maneira pretendida pelo atacante.

As propriedades da instalação incluem: arquivos criados ou modificados, diretórios, configurações de sistema e configurações para comunicação.

6. Command-and-control

O Comando e controle (C2) descreve todas as maneiras pelas quais a comunicação é estabelecida entre a vítima e o atacante.

Nela é usada a persistência que foi estabelecida na infraestrutura da vítima**. Isto é, a manutenção do acesso inicial feito.**

Os IoCs da fase de C2 são relacionados a comunicação periódica entre uma infraestrutura utilizada pelo atacante e a vítima.

7. Actions on Objectives (AO)

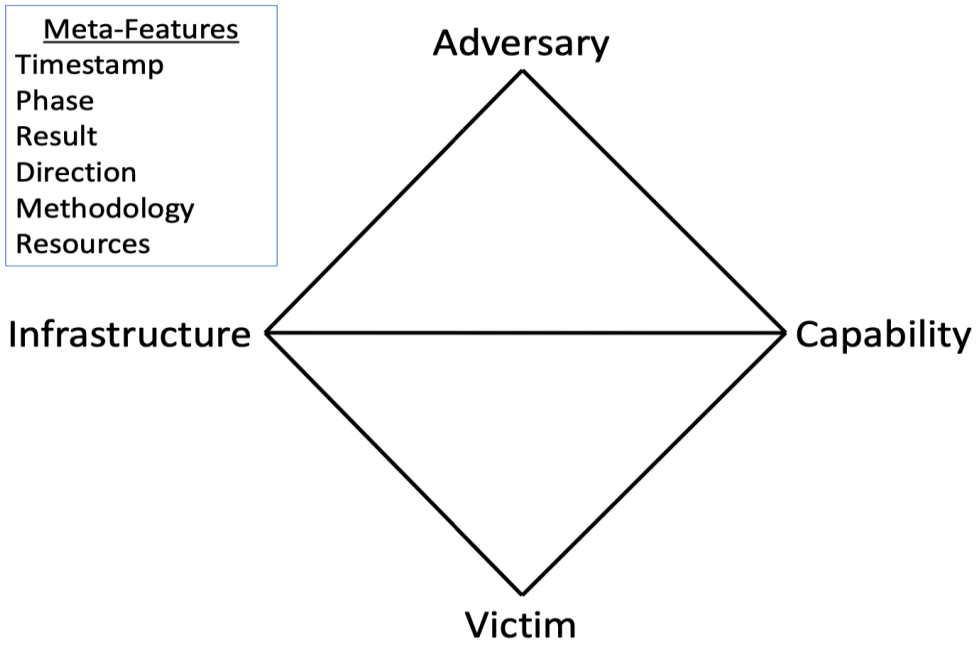
As ações nos objetivos podem incluir exfiltração de dados, comprometimento do sistema ou interrupção de serviços.

Os IoCs dessa fase são relacionados aos impactos ou danos. (Vazamento de dados, Perda de integridade e indisponibilidade).

Modelo Diamante

A CKC por si só é insuficiente para qualificar adequadamente toda as informações sobre uma intrusão.

Este modelo adiciona uma camada de profundidade aos dados já caracterizados pela CKC, categorizando as **informações do Ameaça, Capacidade, Infraestrutura e Vítima**, que se tornam necessária para orientar a conclusão da análise de uma única intrusão, bem como a correlação entre intrusões.



https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Modelo Diamante

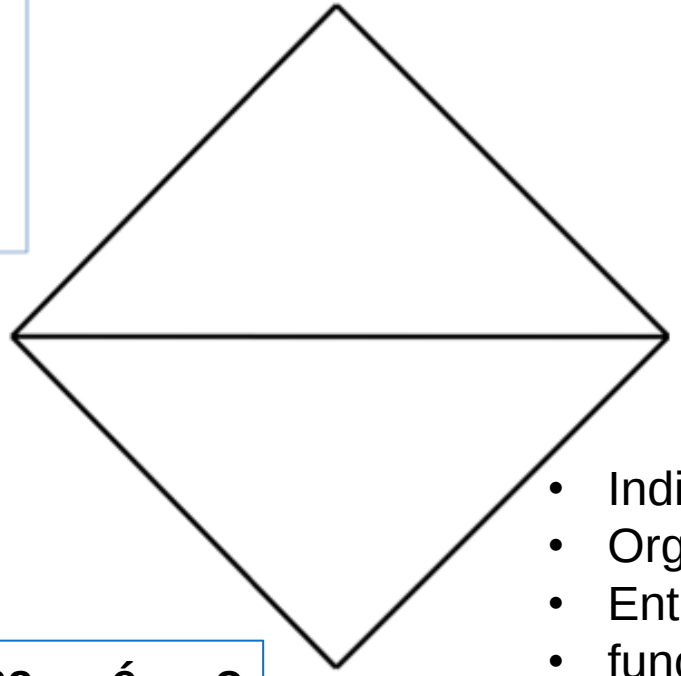
Quaisquer dados relacionados ao atacante como:

- Indivíduo
- Organização
- Operador
- Cliente

A Infraestrutura envolve meios em que o adversário interage com a vítima.

- Ativos
- IPs, Servidores
- Domínios, Sites
- Emails
- Serviços

Meta-Features
Timestamp
Phase
Result
Direction
Methodology
Resources



O adversário usa as capacidades, por meio de uma infraestrutura, contra a vítima.

- Técnicas, Táticas
- Comportamentos
- Ferramentas (Exploits, Malware)

A vítima é o destinatário das ações dolo adversário.

- Indivíduo
- Organização
- Entidade
- funcionário-alvo
- empresa-alvo
- Ativo
- Laptop do funcionário
- WAN da empresa

Premissas do Modelo Diamante

Axioma 1: **Em cada** evento de **intrusão**, **um adversário dá um passo** em direção a um objetivo pretendido, **usando uma capacidade sobre a infraestrutura contra uma vítima para produzir um resultado**.

Axioma 2: Existe um conjunto de **adversários que buscam comprometer** sistemas ou redes de computadores **para promover seus objetivos e satisfazer suas necessidades**.

Axioma 3: Todo sistema e, por extensão, todo ativo da vítima, **possui vulnerabilidades e exposições**.

Axioma 4: Toda **atividade maliciosa contém duas ou mais fases que devem ser executadas em sucessão, com sucesso,** para atingir o resultado desejado.

Premissas do Modelo Diamante

Axioma 5: Todo evento de **intrusão requer que um ou mais recursos externos sejam satisfeitos** antes do sucesso.

Axioma 6: Sempre **existe um relacionamento entre o Adversário e sua(s) Vítima(s),** mesmo que distante, passageiro ou indireto.

Axioma 7: Existe um subconjunto do conjunto de **adversários que possui motivação, recursos e capacidades para sustentar efeitos maliciosos por um período significativo** contra uma ou mais vítimas, resistindo aos esforços de mitigação. As relações Adversário-Vítima neste subconjunto são chamadas de relações de adversário persistentes.

Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

Integração CKC + Diamante

Cada fase da CKC pode ter um Modelo Diamante associado.

Cada IoC coletado e relacionado a uma única fase da intrusão será uma evidência associada a um adversário, uma vítima, uma capacidade ou infraestrutura.

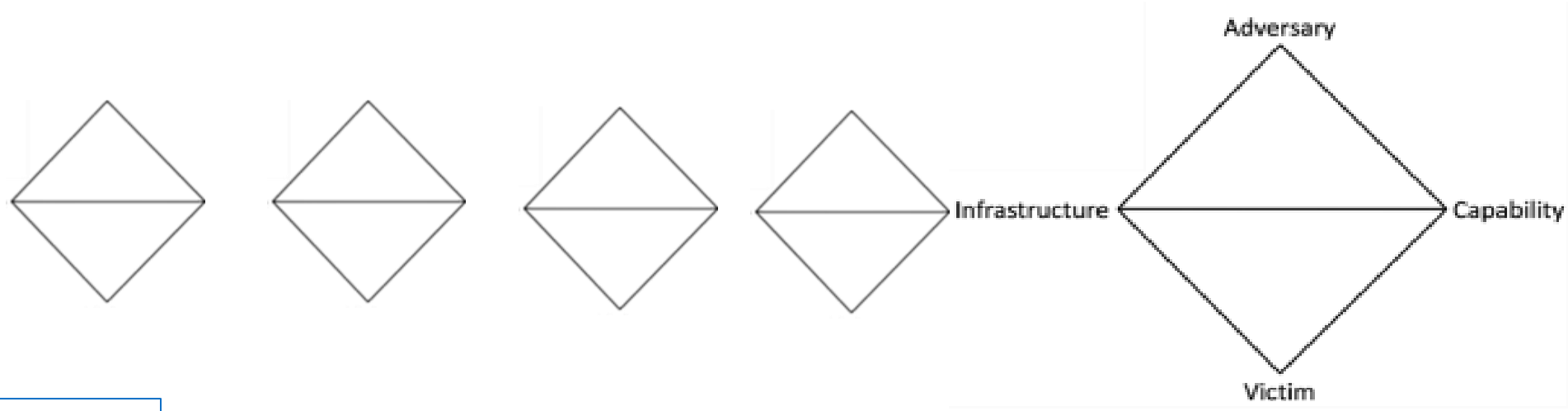
Para descrever completamente uma intrusão, o maior número possível de vértices do modelo diamante deve ser preenchido em TODAS as fases da CKC.

É claro que isso quase nunca é possível e, **em algumas fases, simplesmente não haverão informações suficientes**.

Recon | Weap | Deliv | Exp | Inst | C2 | Actions

Integração CKC + Diamante

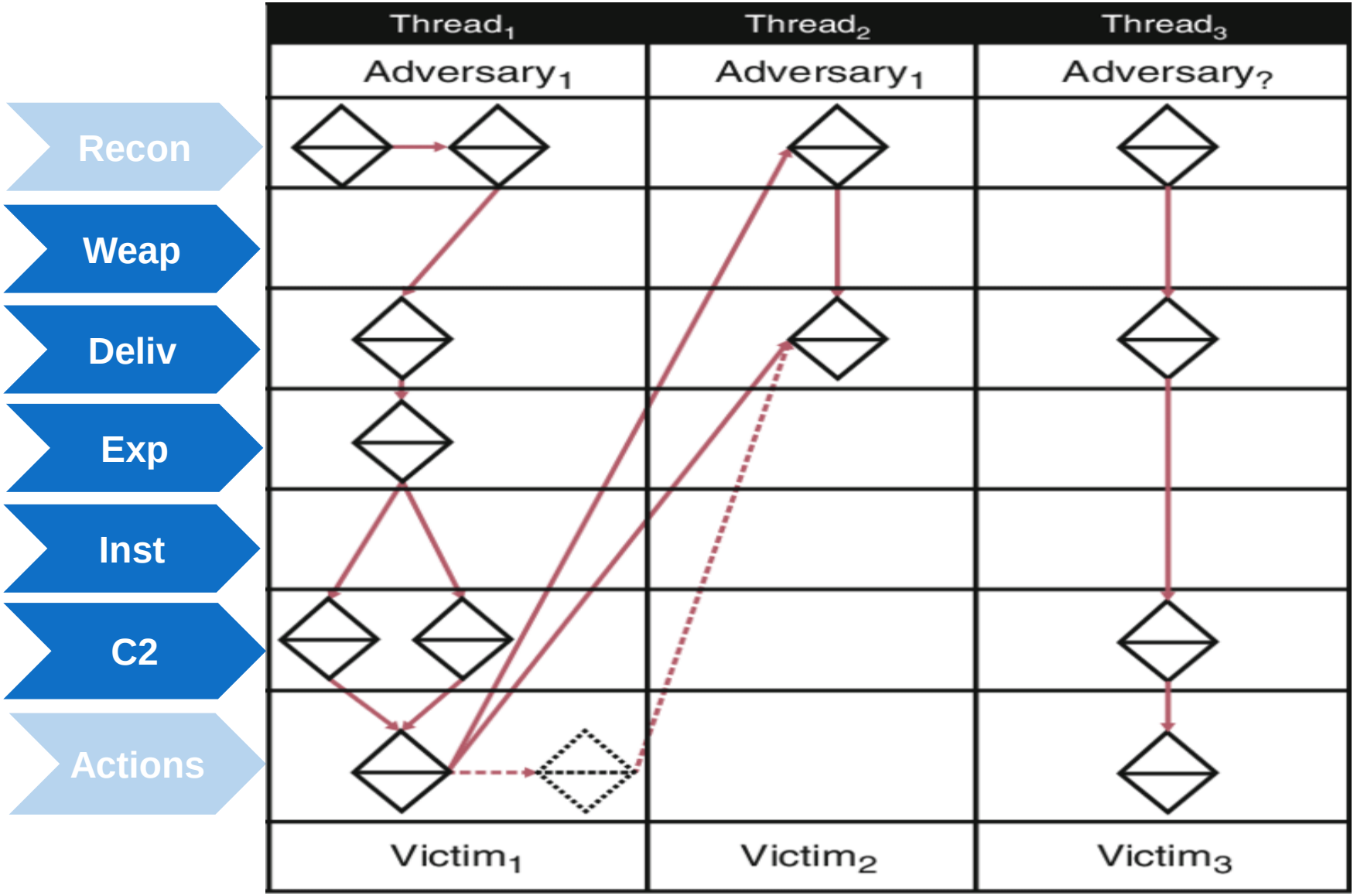
Pelo menos um vértice deve ser preenchido em cada fase da CKC, entre as fases 2 e 6, **para declarar a análise de um incidente completa.**



Ocorrem fora da Infraestrutura da vítima

Recon | Weap | Deliv | Exp | Inst | C2 | Actions

Correlação - CKC + Diamante



Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

Linhas de Ação

Ações que podem ser tomadas pelos defensores da rede (Modelo 7D).

1. **Descobrir** – Verificar nos registros determinados IoCs (passado) .
2. **Detectar** – Identificar a ocorrência de IoCs (regras, assinaturas - futuro).
3. Negar – Interromper ataques assim que eles ocorrerem (Sandbox, Filtrar).
4. **Interromper** – Interceptar comunicações de dados realizadas pelo invasor e interrompê-las. (Desligar, Quarentena, Bloquear, Isolar)
5. Degradar – Criar medidas que limitem ou atrasem um ataque (Tempo, Volumetria).
6. Enganar – Enganar um invasor fornecendo informações falsas ou configurando recursos de distração (Honeypoy / Honeynet).
7. Destruir – Neutralizar capacidades da ameaça (Hacking Back, Takedown, Denial of Service, Prisão, Apreensão)

Linhas de Ação

Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Descobrir	Detectar	Negar	Interromper	Degradar	Enganar	Destruir

As linhas de ação possíveis de serem adotadas podem ser estruturadas no formato de matriz, junto com a CKC, para facilitar a organização e planejamento.

Linhas de Ação

Detect	Deny	Disrupt	Degrade	Deceive
Web analytics	Firewall ACL			
NIDS	NIPS			
Vigilant User	Proxy filter	Inline AV	Email Queuing	
HIDS	Vendor Patch	EMET, DEP		
HIDS		AV		
NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
Audit log			Quality of Service throttle	Honeypot

Figure 1: Countermeasures

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

Uso da na Análise / Triagem

Recapitulando a situação do Analista na Triagem, são muitas perguntas e muita responsabilidade.

- O que aconteceu ?
- É um incidente ? Temos IOC ?
- Quando aconteceu ? Como ? Onde ?
- Temos Impacto ?
- Temos Ameaça ? Quem ?
- Qual a prioridade ? Qual a categoria ?
- O que pode ser feito ?

Uso da na Análise / Triagem

A partir do entendimento que a identificação de um Incidente geralmente se inicia a partir de detecção de um IoC que é validado na Infraestrutura da vítima.

O uso da CKC com aplicação das informações no Modelo Diamante permite apoiar a Triagem, ajudando a diminuir a incerteza e apontando para as lacunas de conhecimento.

Intervalo

Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

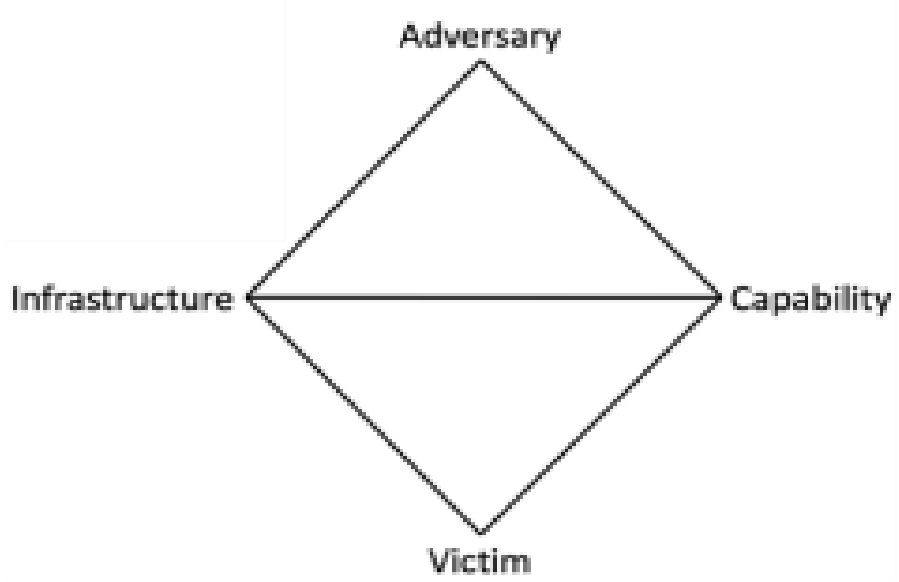
Conclusão

Exemplo de Análise Preliminar

Foram relatados pelos usuários da sua organização várias tentativas de phishing no email da sua organização.

Não foram identificados elementos de código malicioso. Havia um redirecionamento dos usuários para um site que simulava o login institucional.

O MFA é implementado por padrão na sua organização.



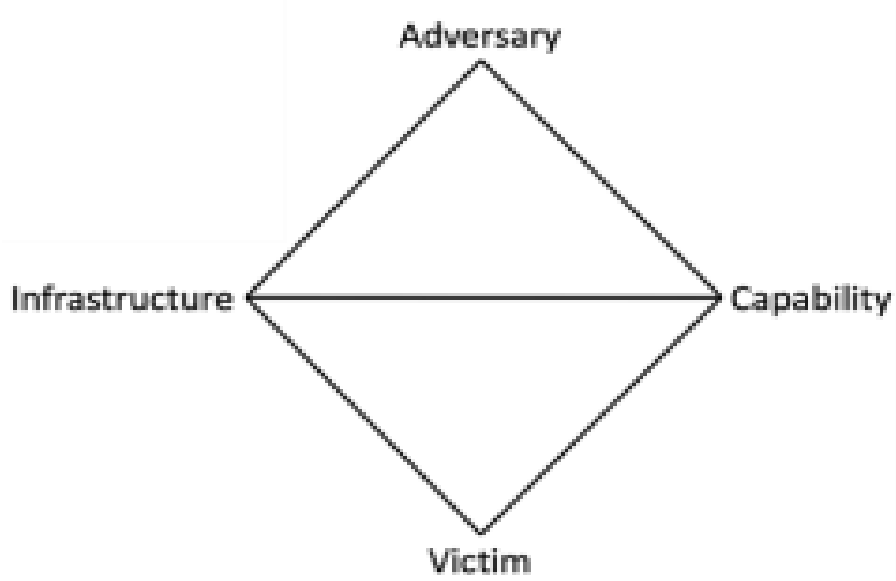
Recon | Weap | Deliv | Exp | Inst | C2 | Actions

Exemplo de Análise Preliminar

Ferramenta “T” identificou e bloqueou executável com assinatura “Mimikatz”.

O registro da detecção apontou para o executável “LaZagne.exe” em um sistema Windows.

Um pesquisa no “google” permitiu LaZagne é uma ferramenta de código aberto pós-exploração usada para recuperar senhas armazenadas em um sistema.

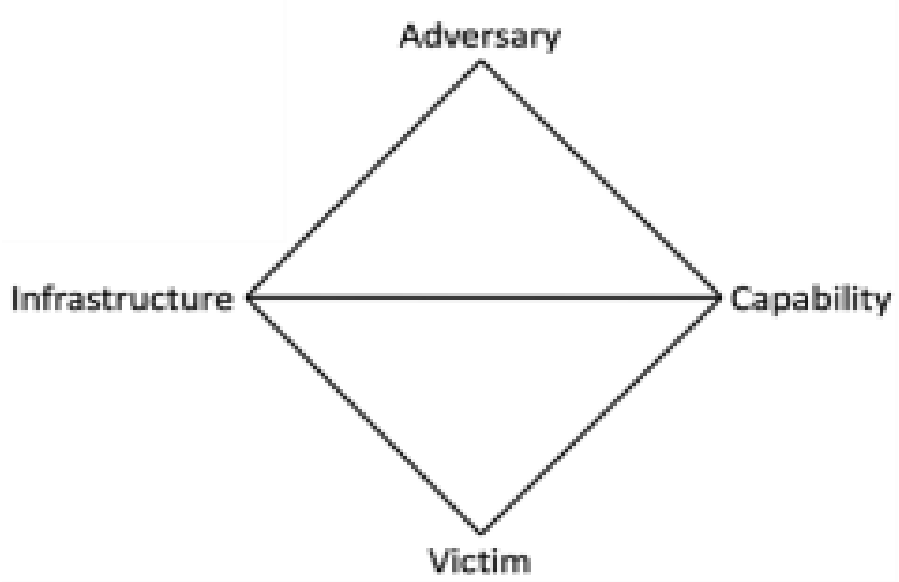


Recon | Weap | Deliv | Exp | Inst | C2 | Actions

Exemplo de Análise Preliminar

O CTIR Gov notificou provável comunicação entre um ativo de rede em sua infraestrutura com um domínio de IP malicioso.

Uma verificação preliminar validou tráfego entre sua rede e o IP.

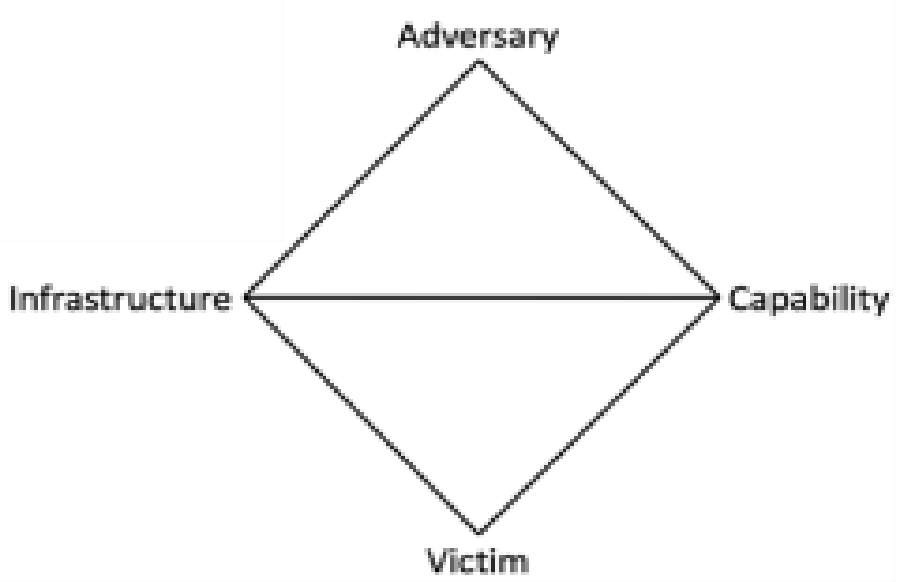


Exemplo de Análise Preliminar

O CTIR Gov notificou credenciais vazadas com o domínio da sua organização.

As credenciais foram sanitizadas e não foram encaminhada as senhas.

Uma verificação na base de dados identificou usuários válidos.



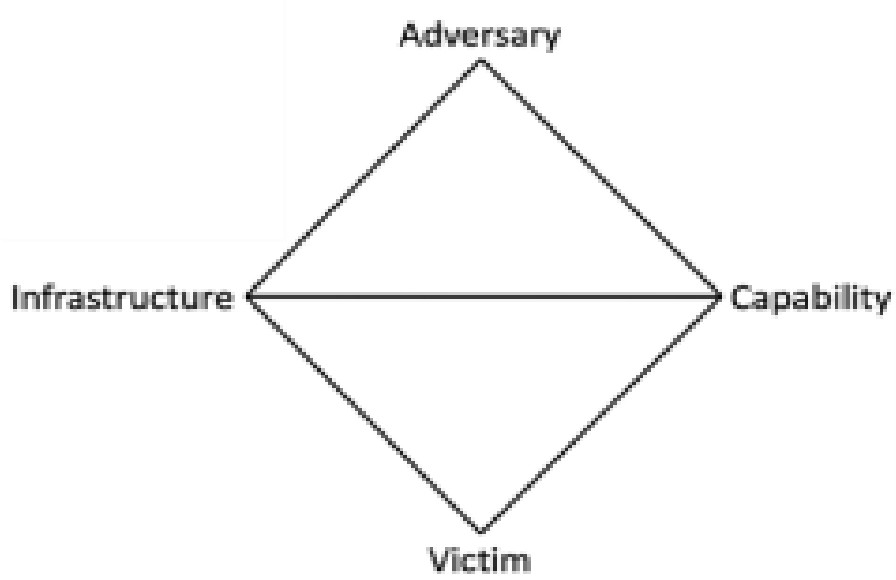
Recon | Weap | Deliv | Exp | Inst | C2 | Actions

Exemplo de Análise Preliminar

Analista “João” identificou uma anomalia no comportamento da sua rede.

Um grande volume de dados está sendo exfiltrado de sua infraestrutura em direção a internet.

Foi associado a essa anomalia o uso da ferramenta RClone.



Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Cyber Kill Chain e Modelo Diamante
- Integração da CKC e do Modelo Diamante
- Linhas de Ação
- Exemplos de Análise Preliminar

Conclusão

Perguntas

Muito obrigado!

Avaliação do 8º Webinário

CESAR MONTENEGRO JUSTO

Tenente Coronel (EB) - Assessor Militar

Cyber Threat Intelligence Analyst (GCTI)

cesar.montenegro@presidencia.gov.br

ctirgov@presidencia.gov.br

ctir@ctir.gov.br