O uso da Cyber Kill Chain para apoiar a interpretação, categorização e priorização de incidentes na triagem.

Apresentação

CESAR MONTENEGRO JUSTO

Militar do Exército

Especialista em Gestão da Segurança da Informação e Comunicações

GIAC Cyber Threat Intelligence Analyst (GCTI)

https://www.linkedin.com/in/cesarmontenegrojusto/

Sumário

Introdução

- Definições de Incidentes e Indicadores

Desenvolvimento

- Overview da Gestão, Tratamento e Resposta a Incidentes
- Desafios na Triagem
- Cyber Kill Chain
- Linhas de Ação
- Interpretação, Categorização e Priorização com a CKC
- Estudo de Caso

Conclusão

Introdução

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"

Introdução

Indicadores e Incidentes

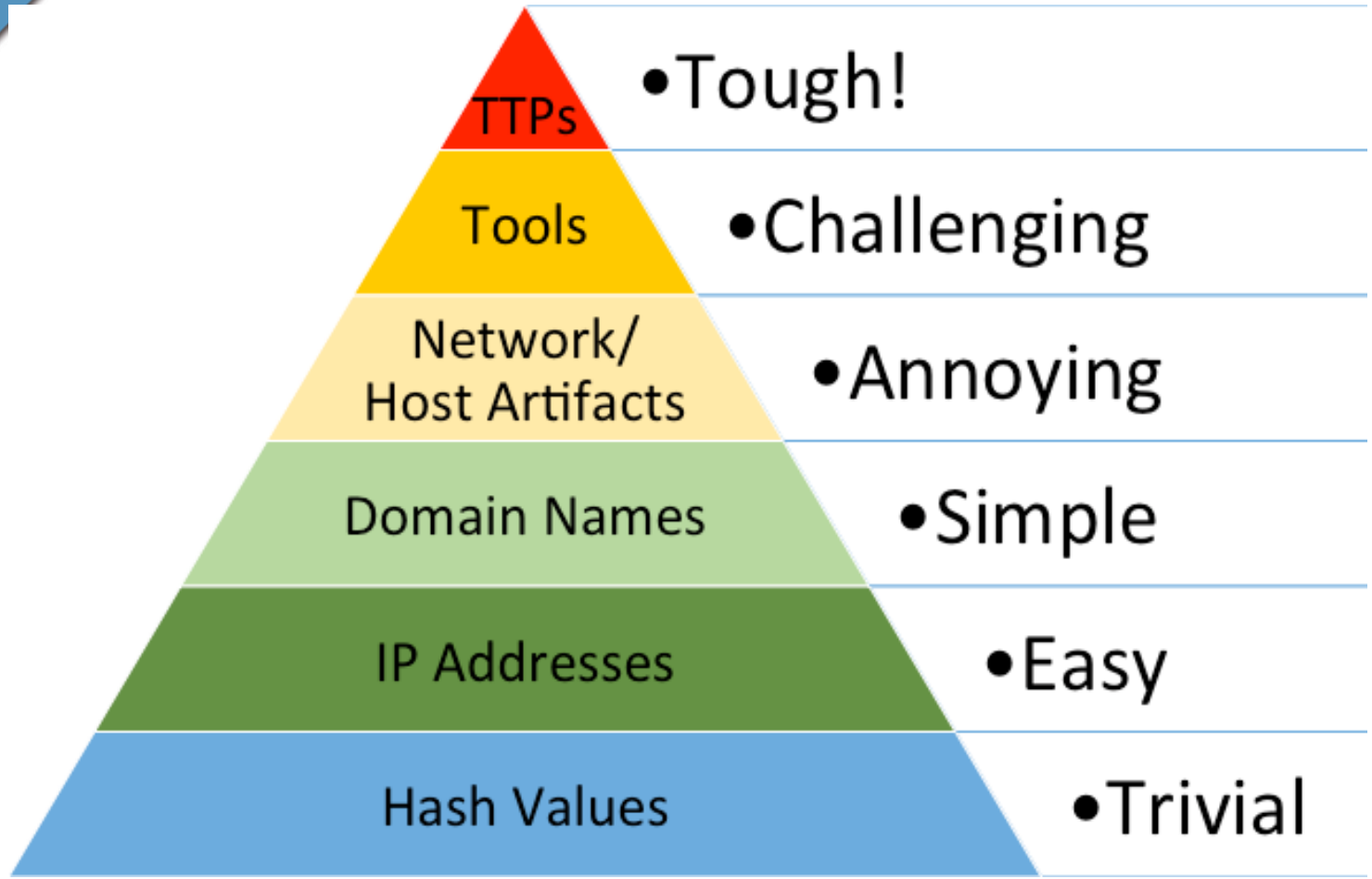
A identificação de um Incidente Cibernético se dá por meio da **percepção** de **sinais ou indicadores** que caracterizem**,** com alto nível de probabilidade e confiança, a ocorrência de do comprometimento de computadores, redes ou sistemas, com impactos nas informações processadas, armazenadas ou transmitidas.

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.

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

Introdução

Indicadores e Incidentes

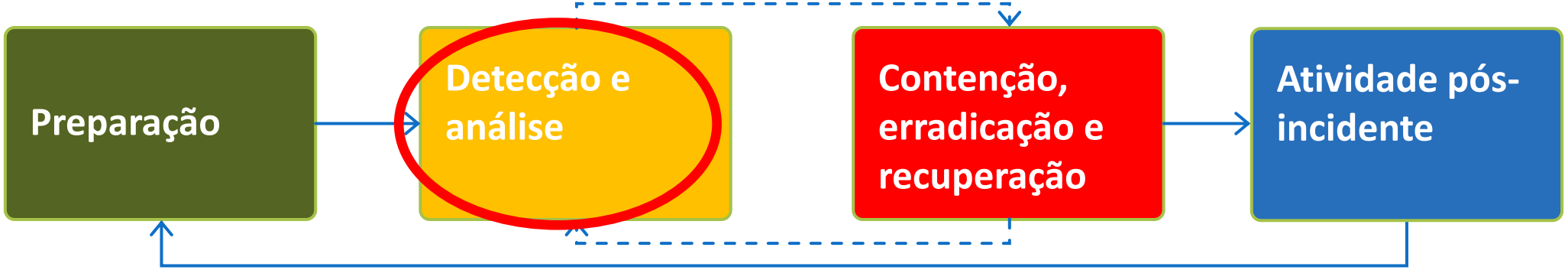


Nem todos os indicadores são criados iguais, porém, e alguns deles são muito mais valiosos do que outros.

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

Desenvolvimento

Gestão, Tratamento e Resposta a Incidentes



No NIST SP 800-61r2 – O processo de triagem é apresentado como parte crítica da fase de "Detecção e Análise".

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

Desenvolvimento

Triagem como processo Decisório

A Triagem é um Ponto de Decisão, no qual é definido como a equipe vai intervir nas ações adversas.

A Triagem compreende *as ações tomadas para categorizar, priorizar, correlacionar e atribuir eventos e incidentes.*

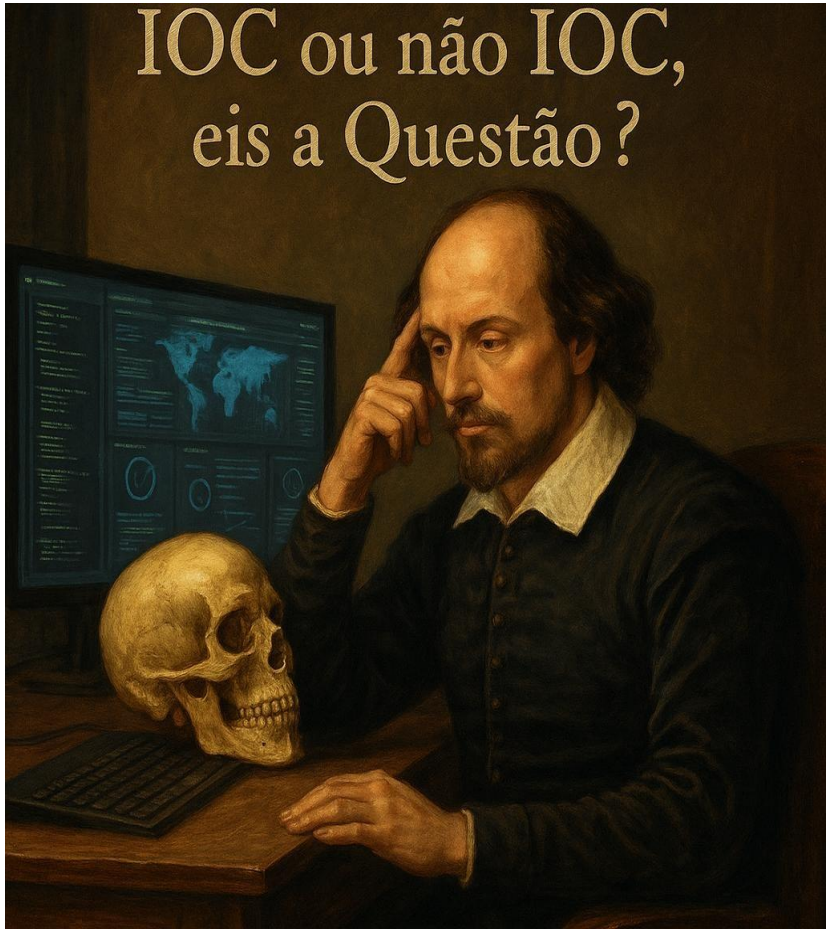
A Triagem influencia todas as ações da <u>Resposta a Incidentes.</u>

Desenvolvimento

Desafios na Triagem

A triagem de incidentes demanda uma capacidade de realizar a interpretação e avaliação das informações disponíveis, com oportunidade verificar:

- **<u>Validação (há IOC ? / é incidente?)</u>**
- **<u>Outros assuntos</u> ?**
- **Categorização (Taxonomia) ?**
- **Classificação (Impacto, Risco) ?**
- **Priorização ?**
- **Correlação?**
- **Atribuição (Quem ?)**



Desenvolvimento

Desafios na Triagem

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

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

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

Desenvolvimento

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

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

Desenvolvimento

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**.

Desenvolvimento

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).

Desenvolvimento

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.

Desenvolvimento

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.

Desenvolvimento

4. Exploitation

Nela há a exploração das vulnerabilidades na infraestrutura da vítima.

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.

Desenvolvimento

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.**

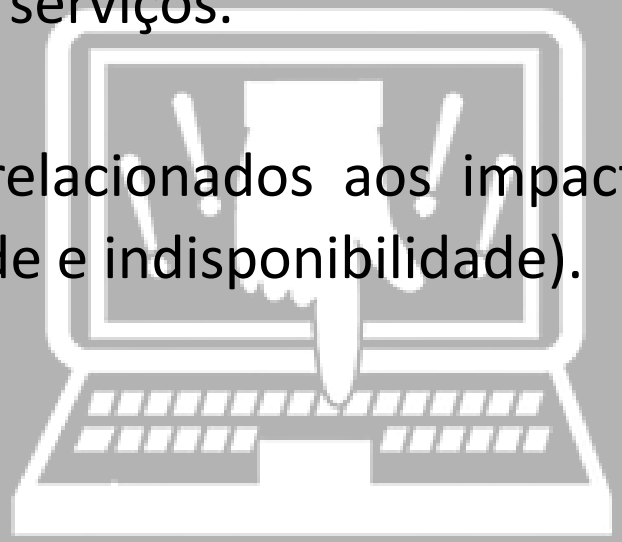
Os IoCs da fase de C2 são relacionados a comunicação periódica entre uma infraestrutura utilizada pelo atacante e a vítima.

Desenvolvimento

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).



Desenvolvimento

Linhas de Ação

Ações que podem ser tomadas pelos defensores da rede .

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 (Takedown, Prisão, Apreensão)

Fonte: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Desenvolvimento

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

Fonte: 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

Desenvolvimento

Linhas de Ação

Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Descobrir	Detectar	Negar	Interromper	Degradar	Enganar	Destruir
Histórico >	TIP	NGFW, ACL				
TIP	TIP	NGFW, ACL				
Histórico > Email	NIDS, NGFW	NGFW, Proxy	WAF	Email Filtering	DNS Redirect	
Histórico >	EDR/XDR, WAF	EDR	EDR/XDR		Honeypot	
Histórico > Forense	EDR/XDR, UEBA	EDR	EDR/XDR		Honeypot	
Netflow DNS passivo	NIDS, EDR/XDR, UEBA	Firewall, ACL, ZTNA	NIPS, SOAR	Tarpit	Honeynet, DNS Redirect	
Histórico > SIEM, DLP	SIEM, Audit Log	DLP	NIPS, SOAR	Qos, Bandwidth throttling	Honeynet, Decoys	

Fonte: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Desenvolvimento

Interpretação dos Incidentes

Em uma Interpretação de Incidentes usando a Kill Chain, **o estado do incidente e sua criticidade são determinados verificando a fase da CKC relacionada ao IOC e *timestamp* detectados**.

Existem até 6 oportunidades | momentos para agir antes da concretização dos Impactos.

Incidentes ainda não concretizados são geralmente detectados entre as fases 2 e 6.

Incidentes concretizados são os detectados na fase 7.

Desenvolvimento

Correlação entre Incidentes

	Incidente 1	Incidente 2	Incidente 3
Recon	?	?	?
Weap	Malware 1	Phishing Site	Malware 1
Deliv	Email	Email	Email
Exp	Vulnerabilidade A	Usuário	Vulnerabilidade A
Inst	?		
C2	Domínio Malicioso	Formulário	?
Actions	Roubo de Senhas	?	?
	Vítima 1	Vítima 1	Vítima 2

Fonte: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Desenvolvimento

Priorização dos Incidentes

Utilizando a “fotografia” do incidente com a fase da CKC que se enquadra o IOC, com contexto e *timestamp* que foram detectados consegue se responder se houve impacto (fase 7) ou projetar um impacto potencial.

A CKC como *timeline* ajuda na métrica temporal.

Outros fatores devem ser associados baseados no modelo de negócio.

Desenvolvimento

Estudo de Caso

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

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

O *timestamp* do Incidente foi de 72 horas atrás.

O analista além do bloqueio do da ferramenta “T”, informou que sanou o incidente restaurando o backup.

Desenvolvimento

Estudo de Caso

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

A presença dele no sistema caracteriza que houve um acesso inicial anterior. Não foi identificado o vetor nem a data desse acesso.

Não foi identificado se o backup estava comprometido.

Fonte: https://github.com/AlessandroZ/LaZagne
Fonte: https://attack.mitre.org/software/S0349/

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

Desenvolvimento

Estudo de Caso

Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Descobrir	Detectar	Negar	Interromper	Degradar	Enganar	Destruir
	As Ações tomadas resolveram o Incidente ?				O uso da CKC poderia ter apoiado o Analista?	

Recon → Weap → Deliv → Exp → Inst → C2 → Actions

Conclusão

Muito obrigado!

Email funcional: cesar.montenegro@presidencia.gov.br

Email administrativo: ctirgov@presidencia.gov.br

Email incidentes: ctir@ctir.gov.br

Website: https://www.gov.br/ctir/pt-br