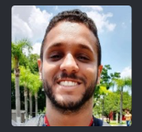
CSIRT Orquestrado: Evoluindo com NIST SP 800-61r3

Quem somos

TLP:CLEAR



Thiago Amparo

- CSIRT
- Graduado em Análise e Desenvolvimento de Sistemas e pós-graduado em Segurança da Informação.
- Foco em resposta à incidentes e Forense digital.

Vinicius Souza

- CSIRT
- Graduado em Redes de Computadores e pós-graduado Forense Digital e Investigação Cibernética.
- Foco em projetos de Cybersegurança e resposta à incidentes.

TLP:CLEAR

Ficando na mesma página com o NIST SP 800-61

O NIST SP 800-61 foi criado em 2004 e é um guia oficial de boas práticas para estabelecer e operar um CSIRT

Revisão 1 (Março 2008)

Estabeleceu os fundamentos para resposta a incidentes, com foco na preparação das equipes, detecção de incidentes, e a importância da documentação e comunicação eficiente ao longo do processo.

Revisão 2 (Agosto 2012)

Consolidou o ciclo de vida em 4 fases (Preparation; Detection & Analysis; Containment, Eradication & Recovery; Post-Incident).

Revisão 3 (Abril 2025)

Alinhou-se ao Cybersecurity Framework 2.0 e ao cenário atual (Cloud, supply-chain, ataques que podem levar um tempo maior para ser concluído). Além de fazer com que todas as etapas tenham oportunidade de melhorias e correções durante ou ao final do tratamento.

TLP:CLEAR

Ficando na mesma página com o NIST SP 800-61

O NIST SP 800-61 é um guia oficial que define boas práticas para o estabelecimento e operação de equipes de resposta a incidentes de segurança da informação (CSIRTs).

Revisão 2 (2012)

- Ciclo de vida em 4 fases
- Foco em execução técnica
- Pós-Incidente = etapa final de melhoria no processo de resposta
- Cenário tradicional (On-premise, resposta rápida)

Revisão 3 (abril 2025)

- Ciclo contínuo baseado nas 6 funções do CSF 2.0
- Foco em orquestração, integração e estratégia
- Melhoria distribuída em todo o ciclo
- Adaptado para ambientes multicloud, supply-chain e ataques persistentes

Por que a revisão 3 veio?

- Para alinhar ao CSF 2.0
- **Para posicionar o CSIRT como orquestrador estratégico, e não só como executor** técnico;
- Porque os ataques são mais longos, complexos e silenciosos;
- Porque vivemos em um mundo multicloud, híbrido e cheio de interdependências;
- E porque melhoria contínua agora é parte do ciclo, não só uma etapa final.
- Para transformar cada incidente em combustível para melhoria, da governança à prevenção;

TLP:CLEAR

Ficando na mesma página com o CSF 2.0

O NIST CSF 2.0 (Cybersecurity Framework 2.0), é um framework que apoia na gestão do risco relacionado à segurança cibernética, e o NIST 800-61r3 está alinhado com as funções principais, ou pilares. Ele era um framework especificamente de gestão de riscos e foi incorporado ao 800-61 nessa nova revisão

O que é:

São funções de alto nível que representam o ciclo completo da gestão de segurança, desde o entendimento do que proteger até a melhoria contínua baseada em lições aprendidas. Elas servem como ponto de partida para priorizar e organizar ações de segurança

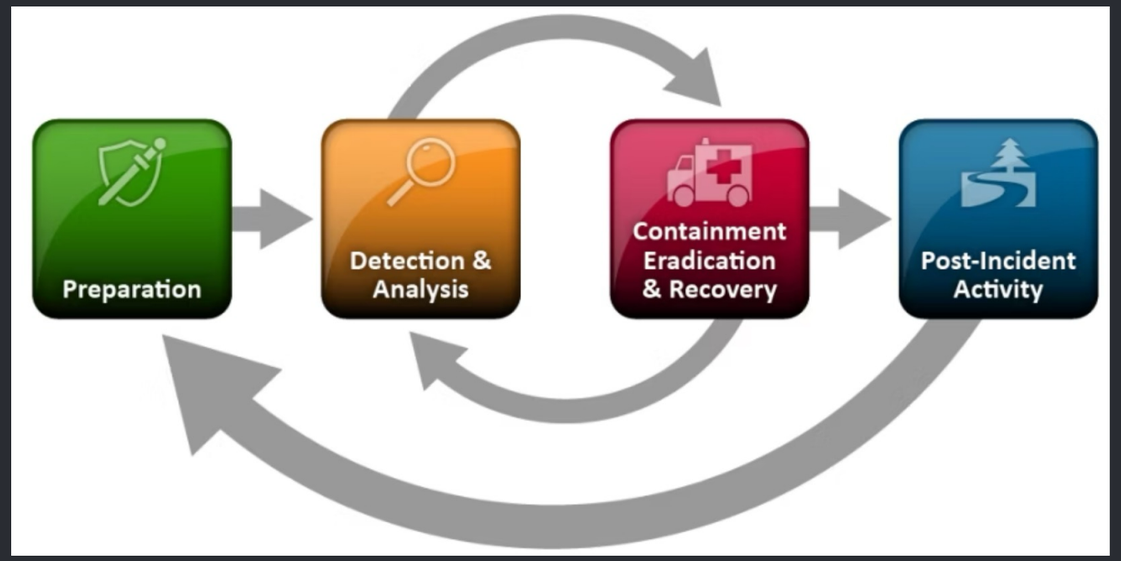
Quais são os pilares:

Govern, Identify, Protect, Detect, Respond e Recover

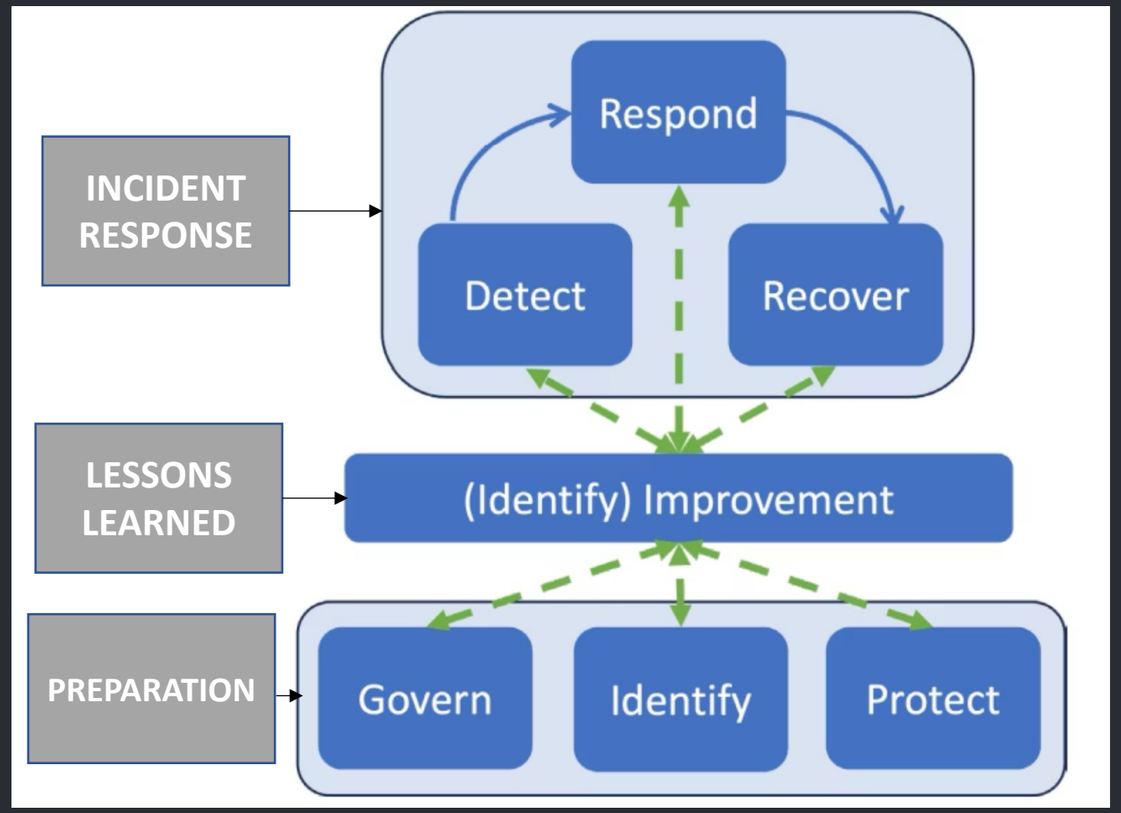
Mudanças do ciclo de vida

TLP:CLEAR

Revisão 2



Revisão 3



TLP:CLEAR

Abandono o que estou fazendo e começo de novo?

Revisão 2

Fluxo linear com 4 fases sequenciais.
Moldou a respostas a incidentes de diversas empresas e profissionais em IR.
O ciclo é adaptado para cada organização e isso não deve ser alterado.

Revisão 3

Ciclo contínuo alinhado às seis funções do CSF 2.0.
CSIRT como direcionador estratégico implícito pela função **GOVERN**.

Lessons Learned

Trilha de melhoria contínua falando com todas as fases em todos os momentos e alimentando as áreas de governança, prevenção e arquitetura.

Isso significa que:

- A melhoria pode (e deve) começar **antes** do incidente **iniciar**.
- A melhoria pode (e deve) começar **antes** do incidente **acabar**.
- O CSIRT pode (e deve) direcionar **todos** os insumos às áreas chaves.

TLP:CLEAR

Analise de causa raiz

Causa raiz é o fator principal que originou o incidente de segurança, permitindo sua ocorrência ou facilitando seu impacto.

Por que investigar a causa raiz?

- Para evitar recorrência de incidentes;
- Gerar insumos de melhoria no processo ou ferramentas;
- Para identificar e corrigir a origem e não apenas os sintomas

Exemplos de causa raiz

- Falta de monitoração adequada;
- Política de acesso mal definida;
- Políticas de conscientização ou treinamentos;
- Configuração incorreta ou faltante;
- Falta de controles definidos à nível de endpoint, redes, etc.

Como classificar causa raiz:

- Utilizem frameworks como Veris, por exemplo, onde poderá classificar: Actor, Asset, Attributes e Action.

Importante salientar que todas as áreas tem papeis e responsabilidades em todas as etapas da Resposta à Incidentes

Obrigado!

Perguntas?

🔗 **Thiago Amparo**
linkedin.com/in/thiagoamparosilva

🔗 **Vinicius Souza**
linkedin.com/in/vinicius-souza-l