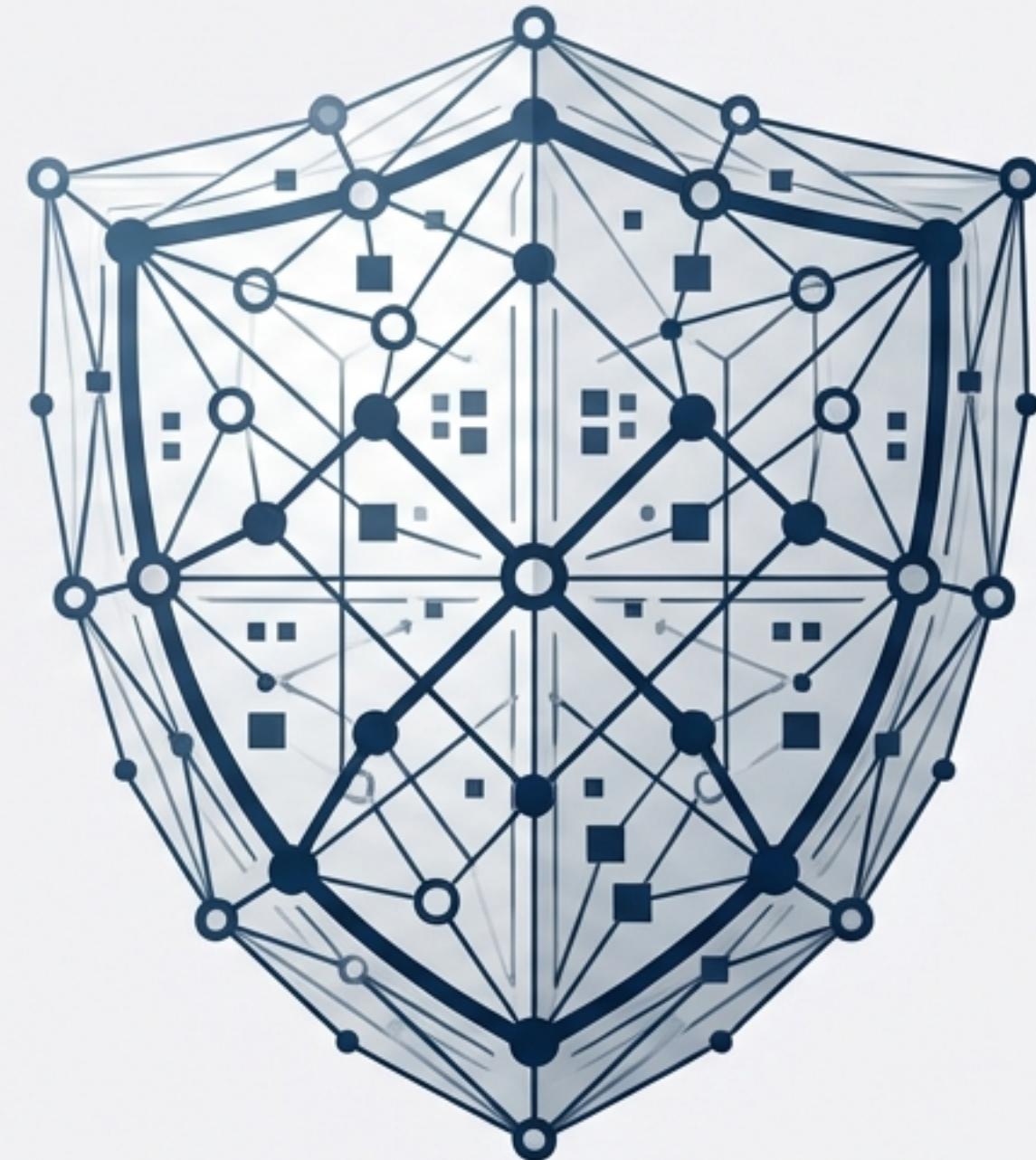


Resposta a Incidentes de Segurança Computacional & Defesa Cibernética

Um guia estratégico baseado no NIST SP 800-61r2 e melhores práticas de mercado.



A Necessidade de uma Capacidade Formal

Define a prontidão organizacional para enfrentar desafios digitais com precisão e eficácia.

EVENTO



Qualquer ocorrência observável em um sistema ou rede (ex: conexão a um servidor, recebimento de email).

Impacto no Negócio: Incidentes comprometem dados e reputação. A resposta organizada minimiza danos, cumpre requisitos legais (FISMA/Compliance) e restaura serviços.

INCIDENTE



Uma violação ou ameaça iminente de violação das políticas de segurança, políticas de uso aceitável ou práticas de segurança padrão.

“ "A prevenção total é impossível. Incidentes são inevitáveis." ”

Organizando a Capacidade de Resposta (CSIRC)

Centralizado



Um único time lida com incidentes para toda a organização.

Política (Policy):

Define o que é um incidente e a estrutura organizacional.

Distribuído



Múltiplos times (por divisão/geografia) coordenados por uma entidade única.

Plano (Plan):

O roteiro para implementação e metas.

Coordenado



Um time central aconselha times locais sem ter autoridade direta.

Procedimentos (Procedures):

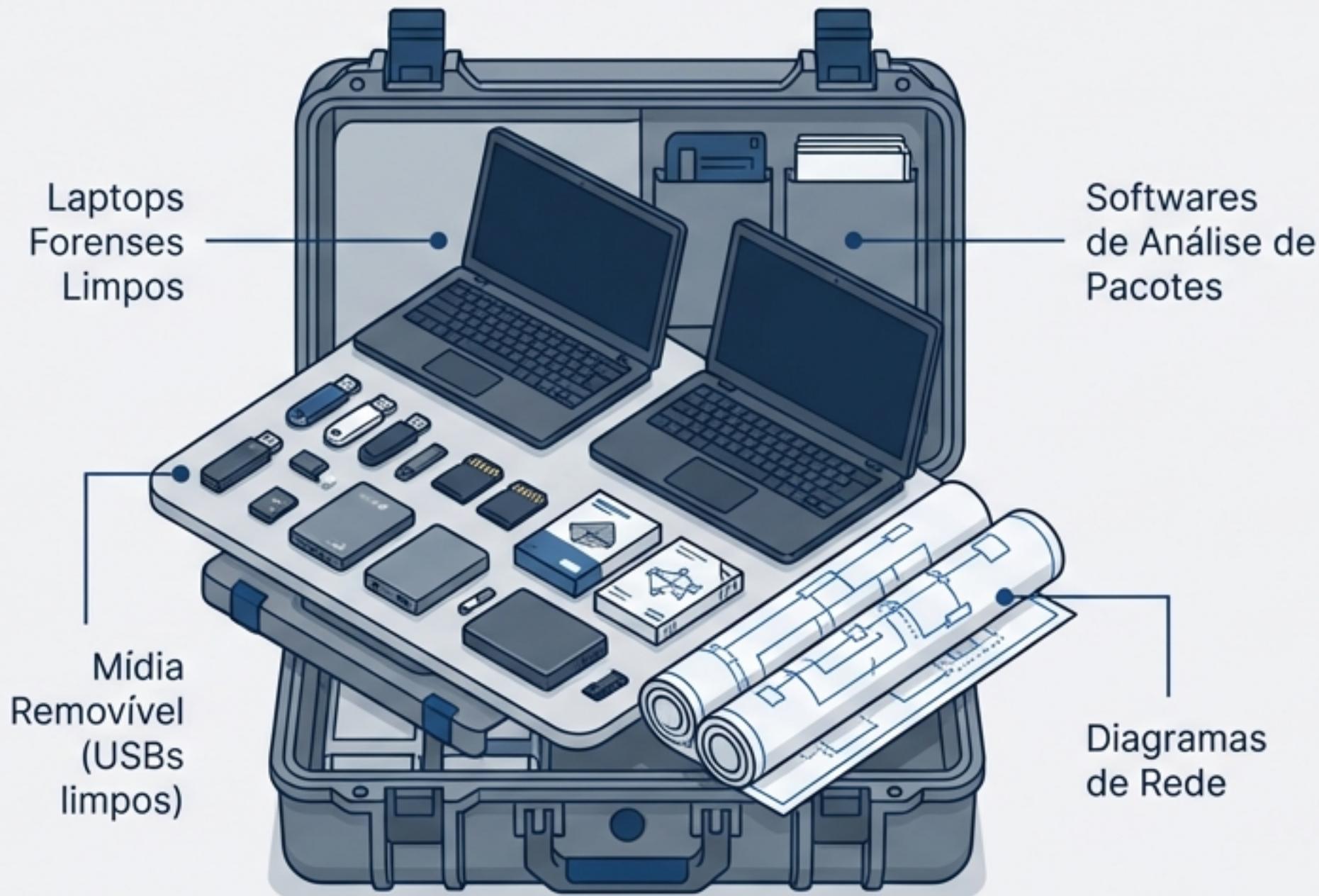
Passos técnicos detalhados (SOPs).

O Ciclo de Vida de Resposta a Incidentes



Esta estrutura circular garante melhoria contínua. A atividade pós-incidente alimenta a preparação para o próximo ciclo.

Preparação: Ferramentas e Comunicação



Infraestrutura Crítica

- **War Room:** Espaço central de coordenação.
- **Comunicação Segura:** Smartphones e encriptação (**FIPS-validated**).
- Lista de Contatos de Emergência.



Prevenção: Endurecimento de Sistemas (Hardening)

Reduzindo a Superfície de Ataque

- **Princípio do Menor Privilégio:** Apenas permissões essenciais.
Evitar serviços como **root**.
 - **Gestão de Patches:** Aplicação crítica e regular de atualizações.
 - **Autenticação Forte:** Chaves SSH e políticas de senha robustas.
 - **Serviços Mínimos:** Desabilitar serviços desnecessários e fechar portas.
 - **SELinux:** Controle de acesso obrigatório ativado.



O Desafio da Detecção: Precursors vs. Indicadores

Precursors (Sinais de Futuro)	Indicadores (Sinais Presentes)
<p>Sinais de que um incidente PODE ocorrer.</p> <ul style="list-style-type: none">- Logs de scanner de vulnerabilidade- Ameaças de grupos hackers- Anúncios de novos exploits	<p>Sinais de que um incidente OCORREU ou ESTÁ ocorrendo.</p> <ul style="list-style-type: none">- Alerta de antivírus/IDPS- Falha de servidor- Alterações de arquivos críticos

Insight: A automação (SIEM) filtra o ruído, mas a análise humana valida a precisão.



Detecção e
Análise

Vetores de Ataque e Vulnerabilidades Web

Vetores de Ataque Comuns

- 🌐 Web: Ataques via websites/aplicações.
- ✉️ Email: Phishing e anexos maliciosos.
- USB Mídia Removível: Infecção via USB.
- 🛡️ Atrição: DDoS e Força Bruta.
- 👤 Impersonation: Spoofing e Man-in-the-Middle.

Technical Callout



Ferramenta em Foco: OWASP ZAP

O scanner de aplicações web mais usado no mundo.
Identificação proativa de **SQL Injection** e **XSS**.



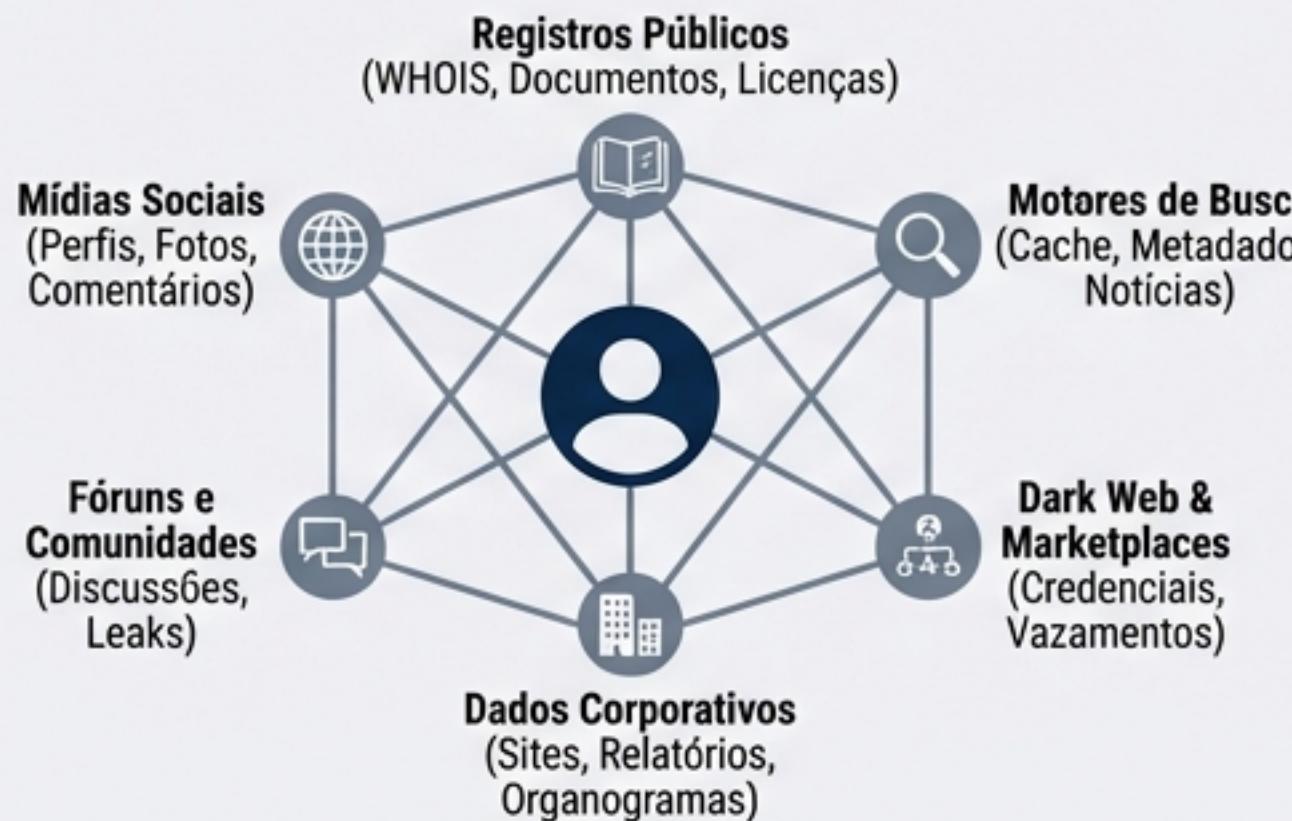
Detecção e
Análise

Reconhecimento e Inteligência (OSINT & Scanning)

```
nmap -sV -O 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-26 18:00
Nmap scan report for 192.168.1.1
Host is up (0.0828s latency).
Not shown: 596 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
443/tcp   open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:11:22:33:44:55 (Manufacturer Inc.)
Device type: general purpose
Running: Linux S.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.4 - 5.11
```

Scanning Ativo

Ferramenta: Nmap. Padrão para descoberta de rede, portas abertas e fingerprinting de SO.



OSINT (Inteligência de Fontes Abertas)

- Coleta Passiva:** Informação pública sem engajamento direto.
- Coleta Ativa:** Engajamento com o alvo (**risco de detecção**).

Análise e Priorização do Incidente



Detecção e
Análise

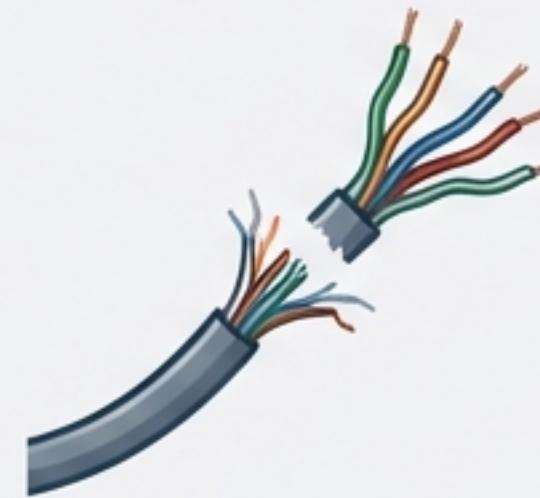
Impacto Funcional	Impacto na Informação	Esforço de Recuperação
		
Nenhum		Regular
		
Baixo	Violação de Privacidade	Suplementado
		
Médio	Proprietária	Estendido
		
Alto (Serviços Críticos Parados)	Perda de Integridade	Irrecuperável

A documentação rigorosa (Logbook) deve começar imediatamente.

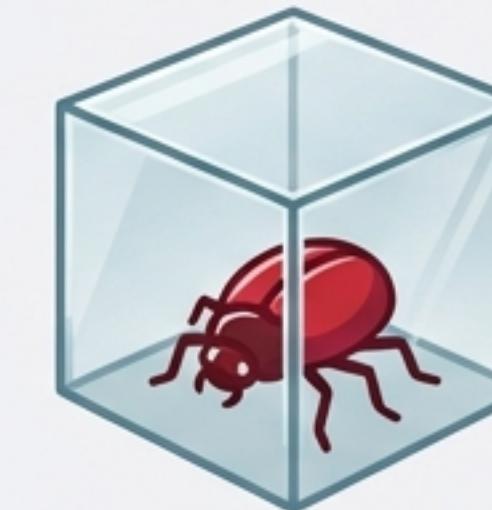


Contenção,
Erradicação e
Recuperação

Contenção: Estancando a Sangria



Previne danos imediatos.
Risco: Perda de evidências voláteis na RAM.



Coleta inteligência sobre o atacante.
Risco: Danos contínuos permitidos.

IMPORTANTE: Adquirir evidências antes de alterar o estado do sistema (Cadeia de Custódia).



Contenção,
Erradicação e
Recuperação

Erradicação e Recuperação

Erradicação (Limpar)

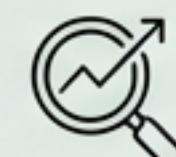
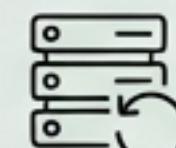
- Remover malware
- Eliminar contas violadas
- Patching de vulnerabilidades



Se novos hosts afetados surgirem, retornar à Detecção.

Recuperação (Restaurar)

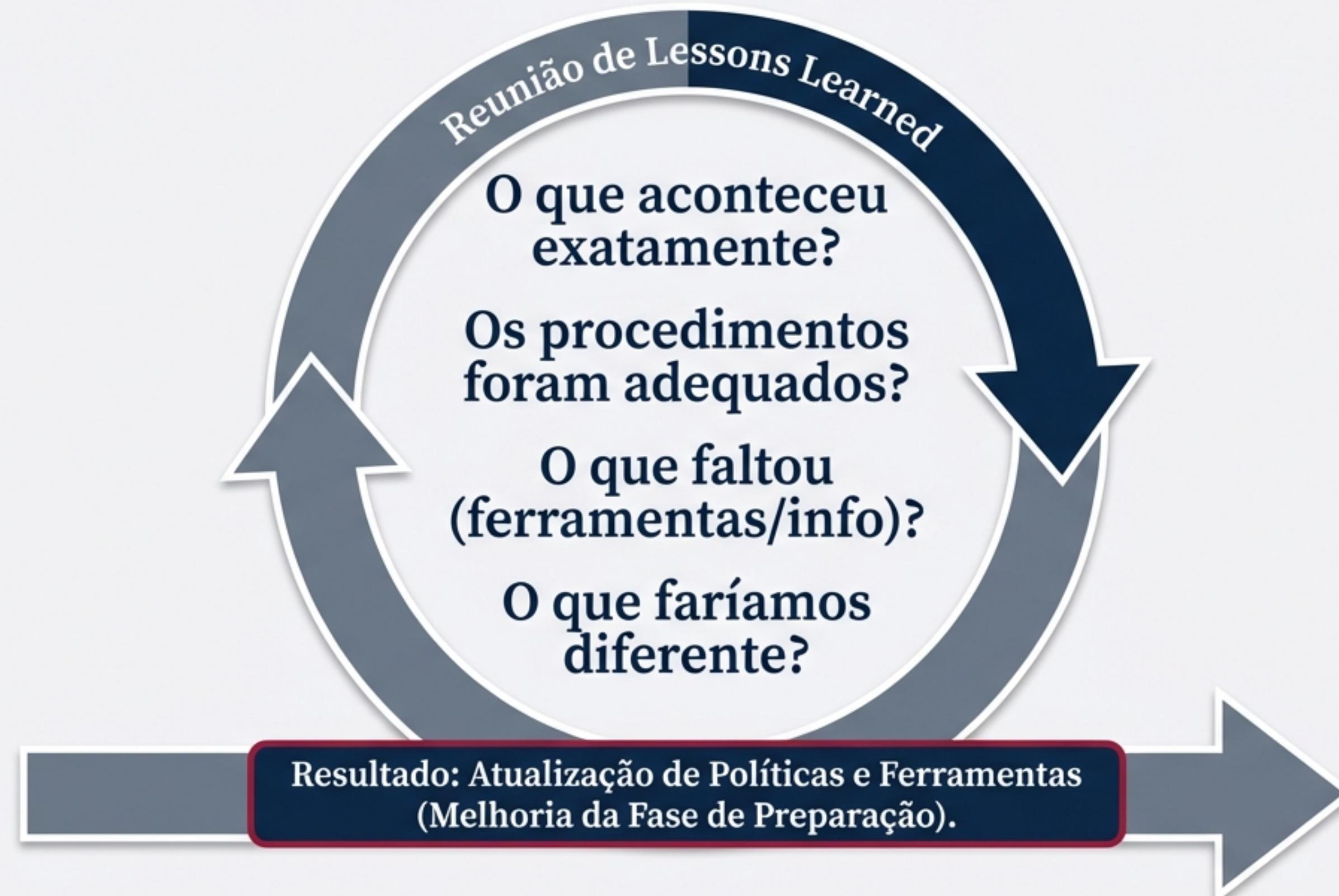
- Restaurar de backups limpos e confiáveis
- Reconstrução do zero
- Monitoramento elevado pós-incidente



Priorizar correções de alto valor primeiro.



Atividade Pós-Incidente: Lições Aprendidas



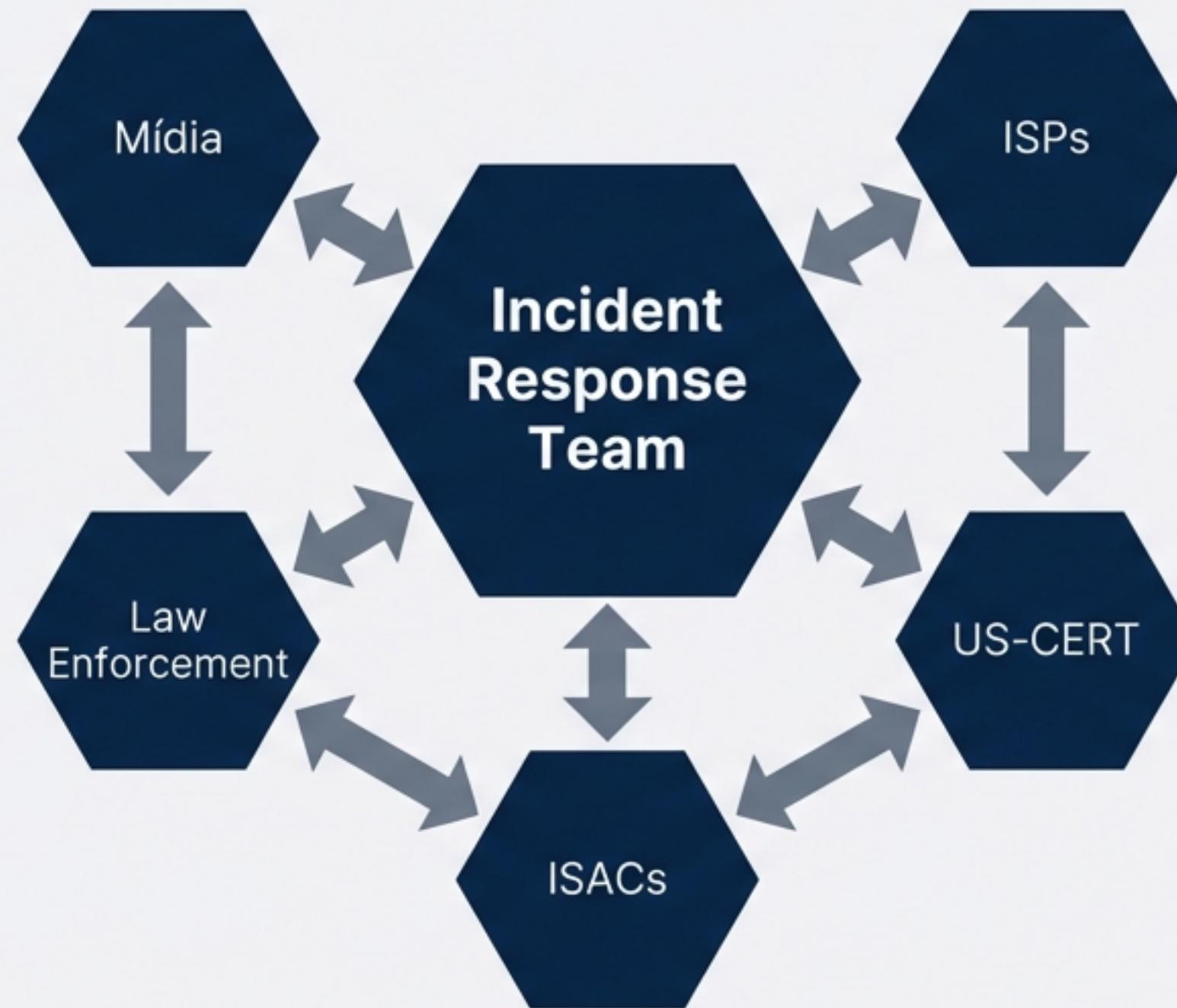


Coordenação e
Comunicação

Coordenação e Compartilhamento de Informações

Stakeholders Externos

- Mídia
- Law Enforcement
- ISPs
- US-CERT
- ISACs



Compartilhamento Granular

- Info de Impacto de Negócios: Apenas para gestão.
- Info Técnica (IoCs): Compartilhar para defesa coletiva.
- Sanitização: Remover dados sensíveis antes de enviar.



Conclusão e Métricas de Sucesso

Tempo



Tempo de Detecção até Contenção.

Medição do tempo desde a identificação inicial do incidente até a neutralização efetiva da ameaça.

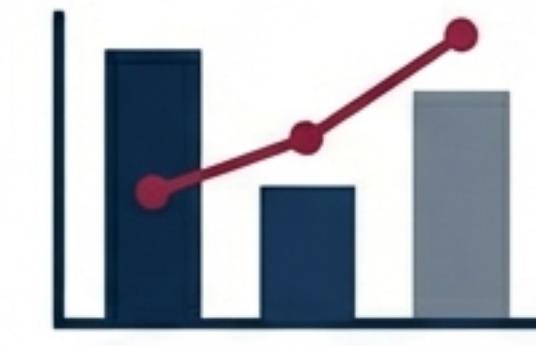
Custo



Horas de trabalho e danos diretos.

Cálculo dos recursos humanos, tecnológicos e financeiros consumidos, além do impacto financeiro do incidente.

Volume



Número de incidentes por categoria.

Análise quantitativa da frequência e tipo de incidentes registrados.

Qualidade



Objetiva

Subjetiva

Avaliação objetiva vs. subjetiva.

Comparação entre métricas quantificáveis e feedback qualitativo das partes interessadas.

A segurança cibernética não é um destino, mas um processo contínuo de adaptação, aprendizado e resiliência.