CSIRT FROM SCRATCH

A Never Ending Story

Jacson Querubin
Itaipu Binacional


CSIRT

Protagonista

BASTIÃO

- Analista de TI
- Proativo/ Dedicado
- Trabalha 24x7
- Instala desde impressora com db25 até compaq deskpro 6000 com windows nt

Internet

O Inicio

A internet ataca

- Aumento dos ataques
- Ataques mais elaborados (phishing, MFA Fatigue, Jobshing?)
- Vida digital (footprint e "superfície Digital") cada vez maiores
- Impacto economico

Forum de CSIRTS

Inicio

O chamado da aventura

- Entendendo O Cenário De Ameaças

Qual negocio da empresa?

Qual ramo da empresa?

Quais ameaças mais comuns?

Inicio

O chamado da aventura

- Entendendo O Cenário De Ameaças
- Definir O Escopo Do Csirt

Qual papel do CSIRT?

Quantas pessoas?

Quem irá atender/apoiar?

Inicio

O chamado da aventura

- Entendendo O Cenário De Ameaças
- Definir O Escopo Do Csirt
- Definir Os Objetivos Do Csirt

Operativo ou Coordenaçao?

Quais serviços vai oferecer?

Inicio

O chamado da aventura

- Entendendo O Cenário De Ameaças
- Definir O Escopo Do Csirt
- Definir Os Objetivos Do Csirt
- Envolver Todo Mundo

Equipes que irao interagir com o CSIRT

Diretoria, gerencias

Montar a Equipe

ESTRUTURA

ARREGIMENTANDO A EQUIPE

- IDENTIFICAR OS PAPÉIS

NOC

Analista de Segurança

FIRST CSIRT Roles and Competences

ESTRUTURA

ARREGIMENTANDO A EQUIPE

- IDENTIFICAR OS PAPÉIS
- ESTABELECER AS RESPONSABILIDADES E AUTORIDADE

Documento oficial da empresa/instiuiçao formalizando o CSIRT

ESTRUTURA

ARREGIMENTANDO A EQUIPE

- IDENTIFICAR OS PAPÉIS
- ESTABELECER AS RESPONSABILIDADES E AUTORIDADE
- DEFINIR OS RELATÓRIOS
- CRIAR O TIME (E PROMOVER A COESÃO)

Importante pensar na

pressao e como

Reunião

Organizando a equipe

- Estabelecer o protocolo de comunicação
- Definir os canais internos de comunicação (backups também)
- Definir e coordenar com entidades externas
- Plano de comunicação claro e objetivo

Principalmente para equipes que nao sao da TI

Alianças

Formando alianças estratégicas

- Identificar parceiros para colaboração (internos e externos)
- Estabelecer acordos de cooperação (externos)
- Participar de redes de troca de informações (comunidades/MISP)
- Promover a cultura da colaboração

Colaboraçao ocorre entre

PESSOAS e CONFIANÇA

Ação

PLANO

ESCREVER O PLANO DE AÇAO

- DESENVOLVER AS POLÍTICAS DE RESPOSTA A INCIDENTES
- CRIAR O PLANO (PROCESSO) DE RESPOSTA A INCIDENTES
- DEFINIR AS FASES: PREPARAÇÃO, DETECÇÃO, ANALISE, CONTENÇÃO, ERRADICAÇÃO, RECUPERAÇÃO
- REVISAR E ATUALIZAR

Equipamentos

Equipando os heróis

- Identificar ferramentas essenciais
  - Tickets, documentação, siem, threat intel, etc..
- Implementar e configurar ferramentas
- Treinar a equipe para uso das ferramentas

ENCONTRO

O PRIMEIRO ENCONTRO

- Implementar ferramentas de monitoramento
- Definir os mecanismos de detecção
- Conduzir análise de incidente
- Gerenciamento de logs e registros

Classificação

Entendendo o impacto

- Desenvolver um critério de classificação
- Definir os níveis de severidade
- Priorizar incidentes baseado no impacto
- Comunicar as prioridades

Contenção

A luta contra o desconhecido

- Definir as estratégias de contenção
- Planificar a erradicação
- Criar plano de desastre e recuperação (backup!)
- Testar e refinar (PDCA)

Reportar

Contando a Jornada

- Definir o que deve constar nos relatórios
- Desenvolver modelos (templates) [post mortem]
- Garantir a acurácia e integridade de evidencias (Cadeia de custódia)
- Revisar e melhorar (inclui apresentar para alta gerencia)

Serviços

Quais ferramentas dispomos

- Definir quais serviços de resposta a incidentes podemos prestar
- Verificar a possibilidade de oferecer o gerenciamento de vulnerabilidades
- Prover dfir/preservação de evidências
- Serviços de inteligência situacional (threat intel)

Preparação

Antes da batalha

- Desenvolver programa de treinamento para a equipe
- Conduzir testes de mesa e simulações
- Promover conscientização (desafio enorme)
- Avaliar efetividade dos treinamentos/conscientização (teste de phishing)

Oráculo

Prevendo o Futuro

- Coletar informações de inteligência (threat intel)
- Analisar dados
- Integrar threat intel com o processo de incidentes
- Compartilhar inteligência com envolvidos

Aprendizagem

Tomo do conhecimento

- Conduzir revisões pós incidente - post mortem
- Identificar lições aprendidas
- Implementar as melhorias
- Monitorar a efetividade

Legal

Consultando o oráculo

- Identificar leis e regulamentações pertinentes
- Garantir o compliance da LGPD
- Consultar corpo jurídico
- Documentar tudo

Maturidade

Cada vez mais forte

- Definindo e coletar indicadores (KPI)
- Analisar e reportar a performance do csirt
- Avaliar o estado de maturidade
- Identificar os gaps de capacidade (treinamento, ferramentas, pessoal)
- Desenvolver um plano de melhorias
- Re-Avaliações regulares

Crises

Garantindo a resiliência

- Criar o plano de continuidade
- Integrar processo de resposta a incidentes com plano de continuidade
- Conduzir testes e exercícios
- Revisar e atualizar o plano (PDCA SEMPRE)

O Maior Inimigo

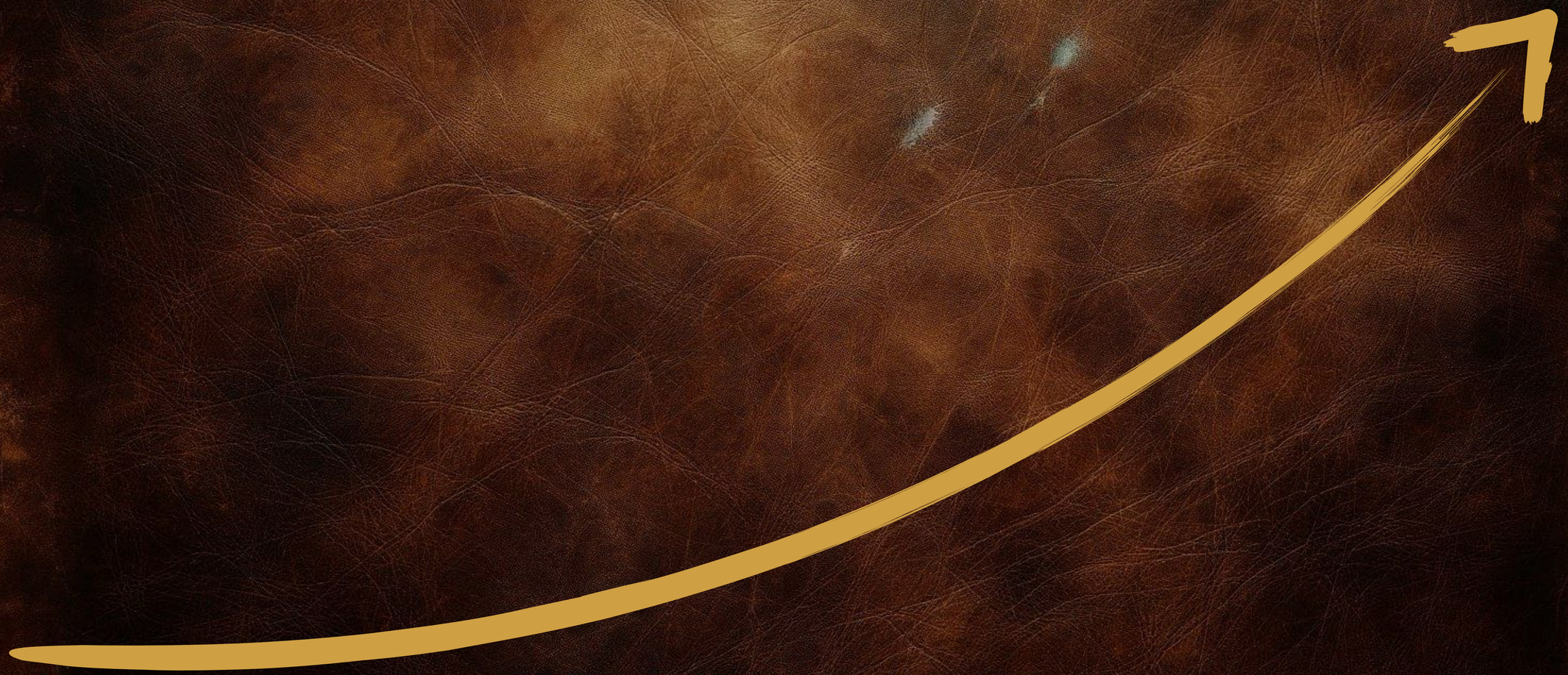
O NADA

Fazer nada é uma escolha

- Uma não ação é uma escolha
- Cada dia pode acarretar em Maior “Débito técnico”
- Riscos e ataques são dinâmicos

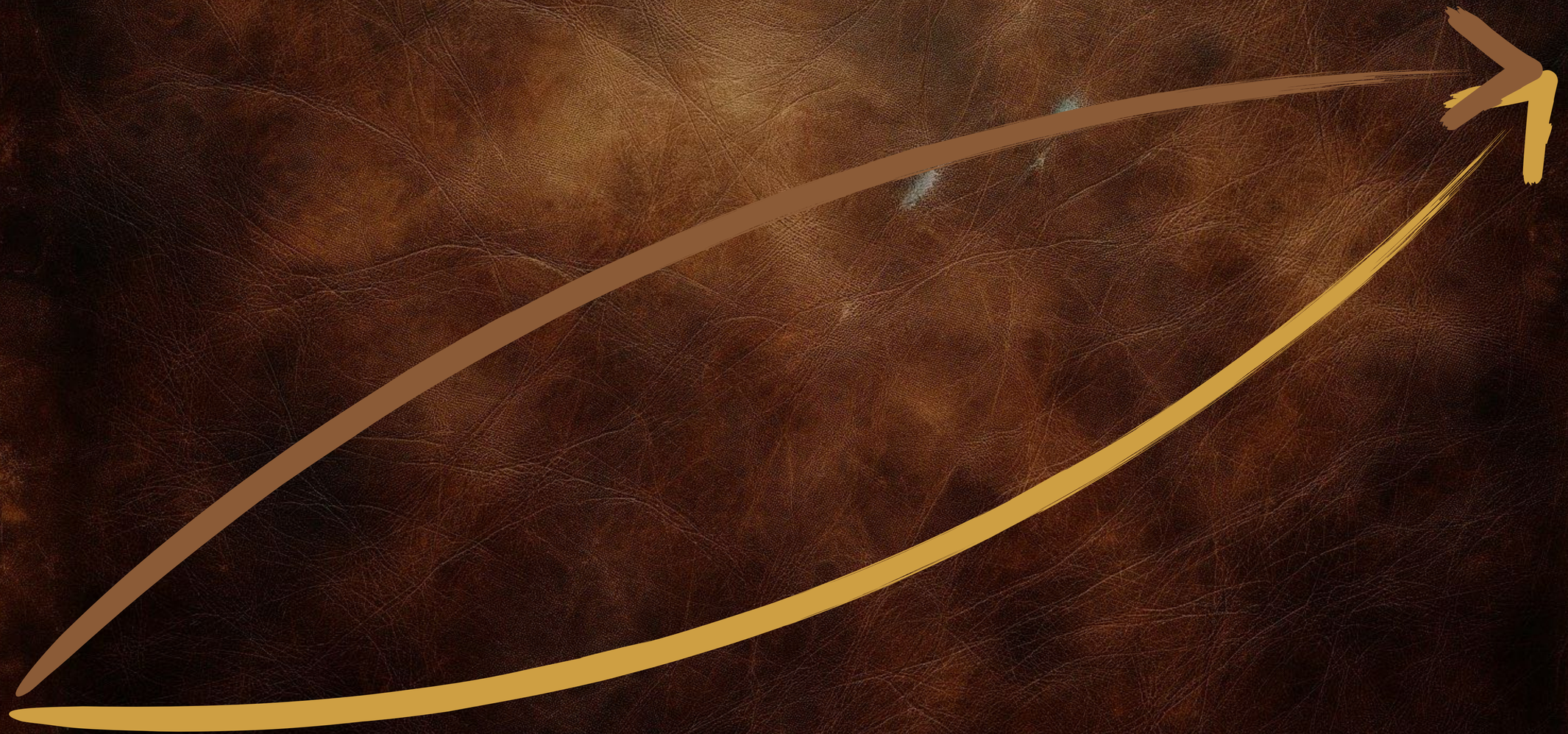
Finalizando

Aprendizado contínuo



TLP:CLEAR

Aprendizado contínuo



TLP:CLEAR

Aprendizado contínuo

TLP:CLEAR

Recapitulando

Passos

1. Definir escopo e equipe
2. Ter aprovação e regimento/documentação
3. Listar ferramentas e serviços/processos
4. Priorizar ações (quick wins ou pareto)
5. Exercitar (pdca)

Tomos da sabedoria

1. https://cert.br/csirts/
2. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework
3. https://sim3-check.opencsirt.org/
4. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
5. https://www.cisecurity.org/controls
6. NIST CFS e NBR ISO/IEC 27000

Depois disso tudo, vem auditoria, briga de orçamento, mais pessoal ..

Mas isso é outra historia


CSIRT