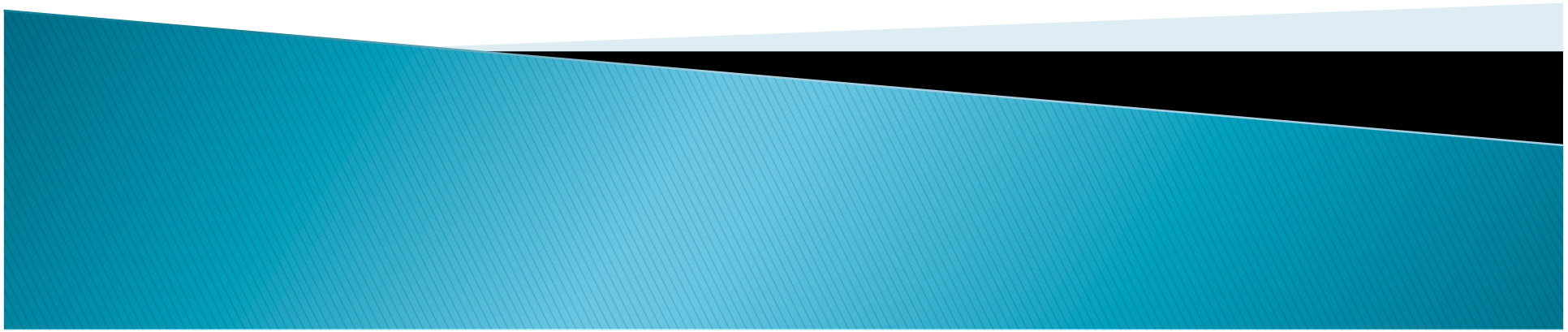
Desafios na criação de um CSIRT Distribuído

Karina Morato Queiroz



- Estabelecimento
- Interfaces
- Processos
- Comunicação
- Planos de Ação
- Documentações

Estabelecimento »

"...chefe, sabemos que gerenciamento de incidentes de segurança é parte da ISO27K ,ISO20K ,PCI, ...certo ? ...só que chefe, vou te mostrar cenários ruins, com incidentes horríveis , muitos, acontecendo todos os dias em nossa infra-estrutura... ...mas.....não se preocupe, estamos aqui para salvá-lo ."

Estabelecimento

Definição de escopo de serviço

- Que serviços de tratamento e resposta a incidentes de segurança poderia prover com a infra-estrutura de TI atual da empresa ?

Definição de escopo de atendimento

- Identificação de cenários de risco e/ou infra-estrutura crítica para o negócio até o nível dos ativos

Adequação interna

- Criação de políticas de segurança da informação e gerenciamento de incidentes de segurança
- Criação de contas de mail e identificação de meios de comunicação internos (intranet, mural, campanhas, e-learning, treinamento)

Interfaces »

"...carta da PF ? hum... É melhor ligar no jurídico e dizer a eles que estamos fazendo um DoS no IP x.x.x.x e que fomos acionados imediatamente para explicar , ufa, acho que resolve..."

Interfaces

Mapeamento de interfaces

- Identificação de interfaces operacionais, administrativas e de engenharia que poderão servir de apoio para o estabelecimento dos novos processos
- Reuniões, fóruns, treinamentos, pontos de contato do CSIRT

Estabelecimento de compromissos

- Desenvolvimento e comprometimento no estabelecimento de uma matriz de responsabilidade de Segurança da informação na organização que inclua atividades do CSIRT

Processos

- Alinhamento dos processos do CSIRT com os processos administrativos e técnicos utilizados atualmente

Processos »

"... CSIRT ?
...é uma área ?
..tem
organograma ? ..quem
faz parte desse time ?
...distribuído ?
hã ? ...precisamos dos
processos
estabelecidos, não sei
como reagir em situação
alguma...
...nem sei quem são..."

Processos

Políticas de segurança da informação

- Políticas de uso aceitável de ativos – softwares, hardwares e sites proibidos
- Padrão de gestão de incidentes de segurança com base na política segurança
- Política de sanção disciplinar (RH) – sempre aplicáveis para incidentes corporativos
- Política de controle de acesso lógico e físico – a tudo !
- Código de Conduta para especialistas do CSIRT
- Matriz de responsabilidades de prevenção e tratamento de incidentes
- Fluxo por serviço do CSIRT – análise de artefato, gestão de vulnerabilidades, incidentes, patch, projetos de prevenção e melhoria contínua, etc.
- Alertas de violação de políticas – alerta de vulnerabilidades, incidentes

Infra-estrutura existente

- Utilização de infra-estrutura de processo já desenhada – HelpDesk, suporte técnico, field service, engenharia, SOC, NOC, RH, entre outras.
- Uso de infra-estrutura de monitoração e controles de redes e sistemas atuais para o estabelecimento de escopo de atendimento e serviços do CSIRT

Comunicação

“”Nossa, alguém usou minha conta de mail ?
E agora ?
....”Disque: CSIRT”, é o que diz na Intranet, no mural, no bottom, no mouse pad, na tela de proteção, no e-learning, no e-mail , ...”

Comunicação

Acordos e parcerias

- Reuniões periódicas de alinhamento do processo de resposta a incidentes com as áreas operacionais e administrativas – compromissos que mudarão o modo de trabalhar das áreas envolvidas.

Fóruns

- Fóruns e reuniões de trabalho técnico para desenvolvimento de expertise no processo de prevenção e tratamento
- Fóruns específicos – TI, RH, jurídico, finanças, recepção, segurança física.
- Canal de comunicação interno (intranet, ramal, mails exclusivos (abuse, csirt, security)

Processos estabelecidos

- Adequação do padrão de comunicação que será adotado durante e após o tratamento do incidente – O código de conduta ou a política de segurança pode limitar a comunicação externa a área de marketing.

Planos de Ação »

"....ouvi falar que além do SLA agressivo de tratamento de incidente, ainda teremos que aplicar patch mensalmente em todos os servidores windows ?
...isso só pode ser brincadeira..."

Planos de Ação

Ações preventivas e corretivas

- Tratamento de erros conhecidos gerados por todos os processos do CSIRT
- Endereçamento das sanções disciplinares
- Instruções de apoio às áreas operacionais para coleta e guarda de evidências
- Apoio às áreas administrativas durante o tratamento de incidentes

Gestão do processo

- Estabelecimento de SLA com todas as áreas de apoio
- Identificação de meios de endereçamento de problemas internamente – mail, sistema de service desk
- Consolidação de indicadores de gestão de incidentes e vulnerabilidades
- Estabelecimento de métricas para o CSIRT
- Identificação de falhas nos processos do CSIRT
- Levantamento de indicadores e medição de eficácia periodicamente junto às áreas

OBRIGADA

Karina Queiroz
Especialista em segurança da informação
Karina.qrz@gmail.com