■ Relatório de Crise

Prioridade: Crítico

Relatório de Crise: Ataque Cibernetico

Evento: Ataque Cibernetico

Origem: Externa, DDoS

Detalhes:

- **Sistema afetado:** Servidor Auth

- **Erro ocorrido:** Não consigo acessar o servidor.

- **Impacto:** Usuários não conseguem fazer login.

Resposta Reativa:

* Ataque detectado! Acionando time de segurança e bloqueando tráfego suspeito.

Plano de Ação:

1. **Isolar sistemas afetados**: Isolar o servidor auth e outros sistemas afetados para minimizar a perda de dados e prevenir a propagação do ataque.

2. **Analisar logs**: Analisar os logs do sistema para identificar as origens do ataque, a natureza do ataque (DDoS) e quaisquer detalhes adicionais que possam ser úteis para entender melhor o cenário de segurança atual.

3. **Comunicar stakeholders**: Comunicar imediatamente com os stakeholders relevantes (gerentes, administradores de TI, clientes afetados, etc.) sobre a natureza do ataque e as medidas corretivas tomadas, garantindo que todos estejam alinhados e informados sobre o plano de ação.

Prioridade: Crítico

Observações:

* A prioridade de "Crítico" reflete a gravidade da situação, pois o ataque afeta diretamente os usuários que tentam fazer login no servidor auth.

* É crucial agir rapidamente para minimizar os danos e garantir que os sistemas estejam restaurados o mais rápido possível.

Monitoramento:

O plano de ação estará em vigor até que as medidas corretivas sejam completadas, monitorando regularmente a situação para garantir que os sistemas estejam funcionando corretamente.