Dicas Básicas sobre Incidentes de Cibersegurança

Hoje quero falar aqui umas dicas básicas sobre seis tipos de incidentes de cibersegurança comuns e o que fazer em cada um.

Ataque de Phishing

Uma tecnica de engenharia social que engana usuários para roubar dados ou acessos.

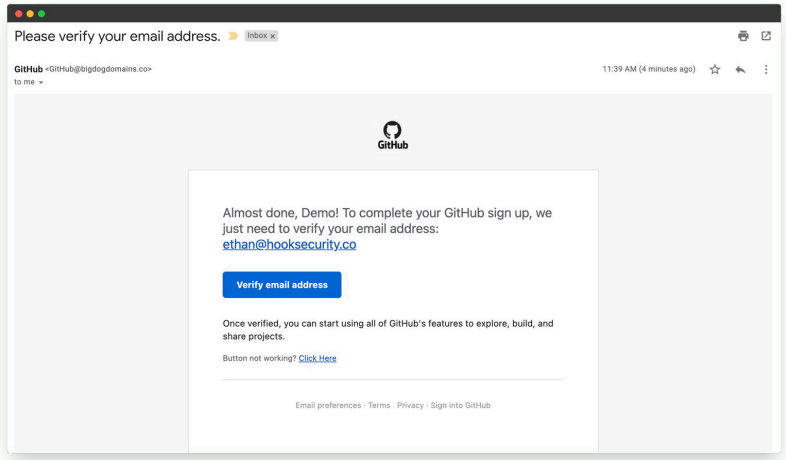
O que fazer?

Isolar contas afetadas.

Forçar a troca de senha.

Revogar acessos concedidos.

Notificar o time de segurança.



Dica: Treinamento contínuo de usuários é o melhor antídoto.

Ataques DDoS

São ataques que sobrecarregam sistemas com excesso de tráfego, provocando quedas desses sistemas.

Ativar serviço de mitigação

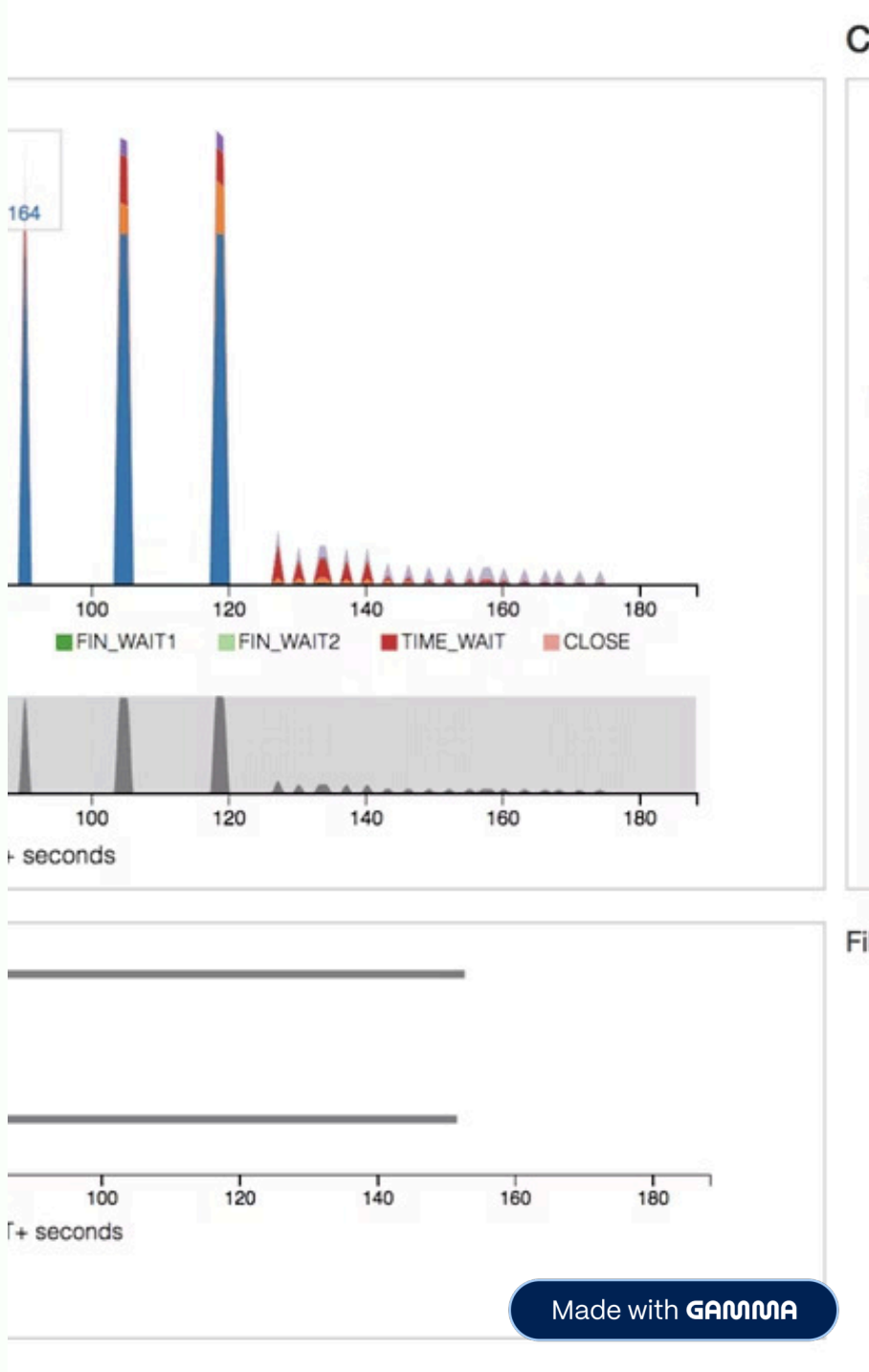
CDN, WAF

Ajustar politicas de Firewall

Isolar os pontos críticos

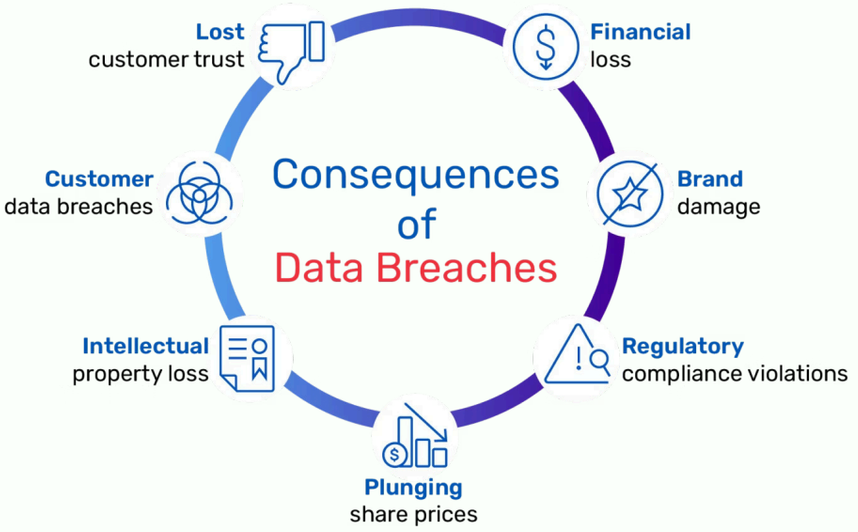
Monitorar tráfego em tempo real

> **Dica:** Sempre tenha uma estratégia de redundância.



Vazamento de Dados

È o vazamento de informações sensíveis, causado por falhas ou ataques intencionais.



O que fazer?

1. **Identificar o que foi exposto**
2. **Notificar times internos e jurídicos**
3. **Avaliar riscos de impacto**
4. **Comunicar conforme a LGPD**

⚠ **Dica:** Você não deve esconder um vazamento. Deve agir com transparência e rapidez.

Malware / Ransomware

È um software malicioso que compromete, rouba ou bloqueia dados (geralmente por resgate).

Desconectar o dispositivo da rede

Isole imediatamente para evitar propagação

Identificar o ponto de entrada

Determine como o malware entrou no sistema

Restaurar backup seguro

Utilize backups não comprometidos

Realizar varredura por IOCs

Busque indicadores de comprometimento

> **Dica:** Fazer backup ofline e atualizado será sua melhor defesa.

Comprometimento de Conta Privilegiada

É quando invasores obtêm acesso a contas com permissões elevadas.

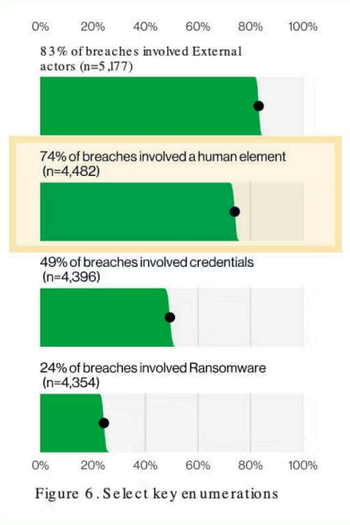


Figure 6. Select key enumerations

O que fazer?

Revogar acessos imediatamente

Trocar senhas forçadamente

Auditar logs da conta

Ativar autenticação multifator (MFA)

Dica: Menos é mais: conceda privilégios mínimos sempre.

Exploração de Vulnerabilidade

É a exploração de uma falha antes que ela seja corrigida.

Aplicar a patch de segurança

Monitorar comportamento pós-correção

Validar se houve movimentação lateral

Auditar logs de forma proativa

> **Dica:** Patch rápido é mais seguro do que patch perfeito.

Obrigado!

È isso!

Não esquece de se inscrever no nosso canal da Fenix Shield para receber notificação de videos novos.

E visitem nosso blog: https://fenixcyberblog.com.br

Sigam também nosso querido Professor João Alkimin la no linkedin.

Um abraço!