***Medidas de Detecção e Prevenção de Ataques***

1. ***Implementação de IDS/IPS:*** Instalar sistemas de detecção e prevenção de intrusões para monitorar tráfego em tempo real e bloquear atividades suspeitas.
2. ***Análise de Logs:*** Configurar a coleta e análise de logs de eventos de sistemas e aplicativos para identificar padrões anômalos.
3. ***Segmentação de Rede:*** Dividir a rede em segmentos para limitar a propagação de ataques e facilitar a detecção.
4. ***Firewall Avançado:*** Utilizar firewalls de próxima geração que ofereçam funcionalidades de inspeção profunda de pacotes.
5. ***Regras de Detecção Customizadas:*** Criar regras específicas para identificar comportamentos e padrões conhecidos de ataque na sua infraestrutura.
6. ***Atualizações Regulares de Assinaturas:*** Manter as assinaturas de detecção atualizadas para garantir a proteção contra novas ameaças.
7. ***Monitoramento de Atividades Suspeitas****:* Estabelecer alertas automáticos para atividades anômalas, como tentativas de login falhadas ou acessos em horários não usuais.
8. ***Treinamento em Segurança****:* Capacitar a equipe em práticas de segurança e identificação de potenciais ameaças, como phishing.
9. ***Análise de Vulnerabilidades****:* Realizar varreduras periódicas para identificar e corrigir vulnerabilidades nos sistemas.
10. ***Respostas a Incidentes:*** Estabelecer um plano de resposta a incidentes que inclua procedimentos para isolar e mitigar ataques detectados.