Insper

Roteiro 4

Data de entrega: 14/05

Este roteiro tem como objetivo guiar os alunos na configuração de medidas de segurança em um ambiente de nuvem, utilizando ferramentas como Zabbix, Telegram, CloudWatch e Wazuh. Os principais pontos abordados serão a configuração do chat bot do Telegram para enviar alertas do Zabbix, a integração do CloudWatch para monitorar e alertar sobre logs do servidor Wazuh, e a configuração de alertas por e-mail no Zabbix.

Passo 1: Configuração do Chat Bot do Telegram com Zabbix

1.1. Criar um bot no Telegram utilizando o BotFather.

1.2. Obter o token de acesso do bot gerado pelo BotFather.

1.3. Configurar a integração do Telegram no Zabbix Server.

1.4. Criar ação no Zabbix para enviar alertas para o bot do Telegram.

Passo 2: Configuração do CloudWatch para Monitoramento de Logs

2.1. Configurar o agente do CloudWatch para enviar logs para o Wazuh.

2.2. Criar uma role no IAM com permissões necessárias para acessar o CloudWatch.

2.3. Configurar o CloudWatch Logs Agent para enviar logs do servidor Wazuh.

2.4. Criar métricas e filtros no CloudWatch para identificar tentativas de autenticação SSH (sucesso ou falha).

2.5. Configurar um alarme no CloudWatch para alertar sobre tentativas de autenticação SSH.

Passo 3: Configuração de Alertas por E-mail no Zabbix

Insper

3.1. Configurar o servidor de e-mail no Zabbix Server.

3.2. Criar um media type para envio de e-mails.

3.3. Configurar um usuário no Zabbix com o endereço de e-mail válido.

3.4. Associar o media type de e-mail ao usuário.

3.5. Criar ação no Zabbix para enviar alertas por e-mail em casos específicos.