**Regras de segurança:**  É muito importante considerar a qualidade das regras de segurança, cada fornecedor dessas regras tem um procedimento a ser seguido, e esses procedimentos podem ou não ser uteis. Sempre que um alerta de inteligência de ameaças é acionado, é importante avaliar a precisão dos fornecedores que fornecem essas listas. Devemos identificar quais fornecedores são mais confiáveis e quais precisam ser melhorados, ajudando na gestão de riscos.

**Fontes de alertas e suas diferenças:** Além de analisar a qualidade, devemos diferenciar os tipos de fontes, algumas são focadas em detecção de riscos enquanto outras já são focadas na prevenção dos riscos. Devemos ajustar as necessidades com cada tipo de fonte, para não gerar falsos positivos.

**Classificação de alertas em segurança:** Regras de alertas podem se dividir em duas categorias principais sendo elas indicando algo ruim ou que sinalizam anomalias. É crucial distinguir entre elas ao analisar alertas, anomalias podem gerar falsos positivos como também ataques desconhecidos. Alertas de anomalias são mais propensos a falsos positivos, para melhor identificação contamos com um sistema de pontuação que pode ajudar a avaliar a confiabilidade dos alertas e a reputação das fontes de informação.