# O processamento de triagem

Nesta leitura, você explorará o processo de triagem e seus Benefícios. Como analista de segurança, você será responsável por analisar os alertas de segurança. É importante ter as habilidades necessárias para fazer uma triagem eficaz, pois isso lhe permite abordar e resolver os alertas de segurança com eficiência.

## Processo de triagem

Os incidentes podem ter o potencial de causar danos significativos a uma organização. As Equipes de segurança devem responder de forma rápida e eficiente para evitar ou LIMITAR o impacto de um incidente antes que seja tarde demais. **A triagem** é a priorização de incidentes de acordo com seu nível de importância ou urgência. O processamento de triagem ajuda as equipes de segurança a avaliar e priorizar os alertas de segurança e a alocar recursos de forma eficaz para que os problemas mais críticos sejam tratados primeiro.

O processo de triagem consiste em três etapas:

1. Receber e avaliar
2. Atribuir prioridade
3. Coletar e analisar

### ****Receber e avaliar****

Durante essa primeira etapa do processo de triagem, um analista de segurança recebe um alerta de um sistema de alerta, como um **Sistema de detecção de intrusão** (IDS). Talvez você se lembre de que um IDS é um aplicativo que monitora a atividade do sistema e alerta sobre possíveis intrusões. Em seguida, o analista analisa o alerta para verificar sua Validade e garantir que ele tenha uma compreensão completa do alerta.

Isso envolve reunir o máximo possível de informações sobre o alerta, inclusive detalhes sobre a atividade que o acionou, os sistemas e recursos envolvidos e muito mais. Aqui estão algumas perguntas a serem consideradas ao verificar a Validade de um alerta:

* **O alerta é um Falso positivo?** Os analistas de segurança devem determinar se o alerta é uma preocupação genuína de segurança ou um **Falso positivo**, ou seja, um alerta que detecta incorretamente a presença de uma ameaça.
* **Esse alerta foi acionado no passado?** Em caso afirmativo, como ele foi resolvido? O histórico de um alerta pode ajudar a determinar se o alerta é um problema novo ou recorrente.
* **O alerta é acionado por uma vulnerabilidade conhecida?** Se um alerta for acionado por uma vulnerabilidade conhecida, os analistas de segurança poderão aproveitar o Conhecimento existente para determinar uma resposta apropriada e minimizar o impacto da vulnerabilidade.
* **Qual é o grau de gravidade do alerta?** A gravidade de um alerta pode ajudar a determinar a prioridade da resposta para que os problemas críticos sejam rapidamente encaminhados.

### ****Atribua prioridade****

Depois que o alerta tiver sido devidamente avaliado e verificado como um problema de segurança genuíno, ele precisa ser priorizado de acordo. Os incidentes diferem em seu impacto, tamanho e escopo, o que afeta os esforços de resposta. Para gerenciar o tempo e os recursos, as equipes de segurança devem priorizar a forma de responder a vários incidentes, pois nem todos são iguais. Aqui estão alguns fatores a serem considerados ao determinar a prioridade de um incidente:

* **Impacto funcional:** Os incidentes de segurança que têm como alvo os sistemas de tecnologia da informação impactam o serviço que esses sistemas fornecem aos usuários. Por exemplo, um incidente de ransomware pode afetar gravemente a confidencialidade, a disponibilidade e a integridade dos sistemas. Os dados podem ser criptografados ou excluídos, tornando-os completamente inacessíveis aos usuários. Considere como um incidente impacta a funcionalidade comercial existente do sistema afetado.
* **Impacto nas informações:** Os incidentes podem afetar a confidencialidade, a integridade e a disponibilidade dos dados e das informações de uma organização. Em um ataque de exfiltração de dados, agentes mal-intencionados podem roubar dados confidenciais. Esses dados podem pertencer a usuários ou organizações de terceiros. Considere os efeitos que o comprometimento das informações pode ter além da organização.
* **Confiabilidade:** a forma como uma organização se recupera de um incidente depende do tamanho e do Escopo do incidente e da quantidade de recursos disponíveis. Em alguns casos, a recuperação pode não ser possível, como quando um agente mal-intencionado rouba com sucesso dados proprietários e os compartilha publicamente. Gastar tempo, esforço e recursos em um incidente sem recuperabilidade pode ser um desperdício. É importante considerar se a recuperação é possível e se vale a pena o tempo e o custo.

**Observação**: os alertas de segurança geralmente vêm com um nível de prioridade ou gravidade atribuído que classifica a Urgência do alerta com base em um nível de priorização.

### ****Coletar e analisar****

A etapa final do processamento de triagem envolve o analista de segurança que realiza uma análise abrangente do incidente. A análise envolve a coleta de evidências de diferentes fontes, a realização de pesquisas externas e a documentação do processamento investigativo. O objetivo dessa etapa é reunir informações suficientes para tomar uma decisão informada sobre o incidente. Dependências da gravidade do incidente, pode ser necessário o encaminhamento para um analista de nível dois ou para um gerente. Os analistas e gerentes de nível dois podem ter mais conhecimento sobre o uso de técnicas avançadas para resolver o incidente.

## Benefícios da triagem

Ao priorizar os incidentes com base em seu impacto potencial, você pode reduzir o escopo do impacto para a organização, garantindo uma resposta oportuna. Aqui estão alguns Benefícios que a triagem traz para as equipes de segurança:

* **Gerenciamento de recursos:** A triagem de alertas permite que as equipes de segurança concentrem seus recursos nas ameaças que exigem atenção urgente. Isso ajuda os Membros da equipe a evitar dedicar tempo e recursos a tarefas de prioridade mais baixa e também pode reduzir o tempo de resposta.
* **Abordagem padronizada:** A triagem oferece uma abordagem padronizada para o tratamento de incidentes. A documentação do processo, como os manuais, ajuda a mover os alertas por um processo iterativo para garantir que os alertas sejam avaliados e validados adequadamente. Isso garante que apenas os alertas válidos sejam transferidos para investigação.

## Principais conclusões

A triagem permite que as equipes de segurança priorizem os incidentes de acordo com seu nível de importância ou urgência. O processamento de triagem é importante para garantir que uma organização atinja suas metas de resposta a incidentes. Como profissional de segurança, você provavelmente utilizará a triagem para responder e resolver incidentes de segurança com eficácia.