**Logs e sua importância:** Os logs são registros digitais que ajudam a investigar atividades em sistemas. Um bom exemplo é quando equipes de segurança precisam analisar eventos que identifiquem ataques, a equipe através dos logs captura tanto ações normais quanto maliciosas.

**Caso de uso:** Existem diversas aplicações para uso de logs, alguns como monitoramento de segurança, investigação de incidentes, solução de problemas, monitoramento de desempenho e auditoria e entre outros. Em tempo real conseguimos detectar qualquer tipo de comportamento seja normal ou anormal através de informações detalhadas sobre eventos passados de comportamentos.

**Tipos e Análise de Logs:** Existem muitos tipos de logs por exemplo, logs de rede ou logs de segurança que registram eventos específicos. São aplicadas técnicas manuais e automatizadas para extrair informações valiosas.

**Logs em Windows:** Logs em windows são organizados por categorias que facilitam a analise com informações detalhadas sobre atividades. O event viewer permite filtrar e visualizar esses logs categorizados.

**Análise de logs de acesso web:** A análise de logs é fundamental para entender o comportamento dos usuários e detectar suspeitas. Através da análise podemos ver os registros de todas as solicitações feitas a um site, incluindo IP e tipo de requisição.