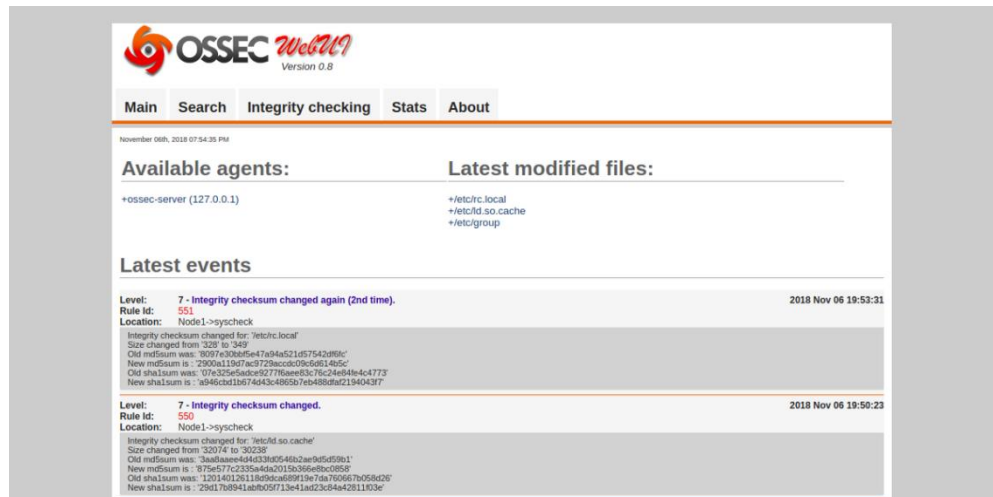


# Declaração de Intenções do Projeto

Neste projeto vamos explorar a ferramenta OSSEC, que é um sistema de deteção de intrusão baseado em host livre e aberto. Serve também para analisar o tráfego num ambiente computacional.



## Com o OSSEC iremos fazer:

- Análise de integridade dos logs;
- Review da integridade dos ficheiros – Caso algum ficheiro seja alterado, o administrador é notificado pelo OSSEC no momento;
- Deteção de Rootkit – O OSSEC mantém uma base de dados atualizada sobre diversos tipos de rootkits e malwares, para prevenir ataques;
- Alertas em tempo real de intrusões – Caso o OSSEC encontre algum problema, o administrador é logo notificado;
- Suporte GeoIP – serve para fazer mapeamento de um IP para um país ou cidade;

Por fim, OSSEC é uma ferramenta poderosa que serve para garantir a segurança da informação em ambientes de redes.

## Realizado por:

Luís Oliveira, nº24833, ERSC

Bruno Rodrigues, nº23683, ERSC

