EMVENCI™
CYBERSECURITY CLOUD

BIGDATA CORRELATION AND ALERT NOTIFICATION

A EBS (Emvenci Business Services) desenvolve uma plataforma SaaS de cibersegurança com diversos módulos, desde um simulador de phishing, a formação em cibersegurança (elearning), um gestor de políticas de segurança, plataforma de registo dos requisitos do RGPD (Regulamento Geral de Proteção de Dados), um gestor de vulnerabilidades e uma plataforma de centralização e gestão de logs.

Os logs são uma parte importante da nossa aplicação e, do ponto de vista da segurança, críticos para identificar ameaças. Mais do que a capacidade de guardar logs, é necessário ler os logs regularmente, identificar eventos e padrões maliciosos e agir sobre eles.

A nossa plataforma está constantemente a gerar logs e a guardá-los. Estes logs são ao dia de hoje guardados numa solução de bigdata, o que permite guardar e analisar grandes quantidades de dados em tempo real. Este projeto assenta em criar um software que comunique com a solução bigdata para analisar os eventos e padrões de modo a poder agir em conformidade. O tipo de evento ou padrão que se vai procurar e as respetivas ações, são previamente criadas e definidas através de regras de correlação, ou de desvios do padrão normal. As regras e desvios a identificar devem ser suficientemente flexíveis e configuráveis sempre via API.

Objetivos

- Analisar a arquitetura existente e os requisitos funcionais da solução;
- Desenhar e definir o plano de implementação;
- Implementar, testar e concluir.

Plano de Trabalhos

Análise

- Conhecer e analisar a plataforma existente no que toca à gestão de logs;
- Analisar requisitos funcionais.

Desenho

- Definir arquitetura e soluções para o problema;
- Estruturar e desenhar as soluções;
- Definir tarefas e nível de esforço de modo a planear e organizar em Sprints de desenvolvimento.

Implementação

- Executar o desenho e planeamento definido;
- Participar ativamente no código desenvolvido pela equipa de desenvolvimento, na forma de reuniões e code reviews.

Testes

- Testar funcionalidades e desempenho;
- Efetuar melhorias necessárias assentes no feedback tanto dos desenvolvedores como da equipa de testes;
- Concluir melhorias na segurança da plataforma.