Sistema de Gestão de Ciberincidentes e Respostas de Segurança

Trabalho Prático - Turno: PL4
Programação I
Engenharia Informática
Ano letivo 2024/2025

Luís Brito*
britoluis@estg.ipvc.pt

*Escola Superior de Tecnologia e Gestão, IPVC

Resumo: Desenvolver uma aplicação em linguagem C que permita registar e gerir ciberincidentes numa organização. O sistema deve tratar diferentes tipos de incidentes, associar responsáveis, acompanhar o estado e tempo de resposta, e gerar relatórios. O projeto deve utilizar listas ligadas, alocação dinâmica de memória, algoritmos de ordenação e pesquisa, e persistência de dados em ficheiros binários e de texto.
Palavras-chave: ciberincidentes, cibersegurança, respostas de segurança

---

1. Descrição da aplicação

Cada incidente deve conter: ID único, tipo (phishing, malware, acesso não autorizado, etc.), data e hora do evento, descrição, nível de severidade, estado atual (por tratar, em análise, resolvido) e técnico responsável.

O sistema deve permitir o registo de novos incidentes, a atualização do seu estado, a atribuição de técnicos e a produção de relatórios periódicos com os incidentes registados e resolvidos. Deve ainda manter um histórico com as ações tomadas para cada incidente.

No arranque, o programa deve pedir a identificação (user e password) ao utilizador. Se um user não existir, o programa deve perguntar se se pretende registar. Se sim, deve proceder ao registo. De origem, existe um user `admin` com perfil de Administrador e com password `admin`. No primeiro login (e apenas no primeiro), o programa deve forçar a alteração da password do Administrador.

2. Funcionalidades por tipo de utilizador

O sistema terá dois tipos de utilizadores: Administrador de Segurança e Técnico de Resposta.
Como Administrador de Segurança, o programa deve permitir:

- Validar os Técnicos de Resposta que se tenham registado.

- Adicionar e remover incidentes.
- Consultar e listar todos os incidentes filtrados por estado, severidade ou tipo.
- Ordenar incidentes por data, severidade ou técnico responsável.
- Gerar relatórios semanais/mensais com estatísticas (ficheiro de texto).
- Ver o histórico de ações de cada incidente.
- Ver tempo médio de resolução por técnico.
- Filtrar incidentes por intervalo de datas.

Como Técnico de Resposta, o programa deve permitir:

- Indicar tempo estimado para resolução ao aceitar um novo incidente.
- Visualizar incidentes atribuídos.
- Atualizar o estado de um incidente (ex: em análise, resolvido).
- Adicionar comentários e ações realizadas.
- Consultar o histórico dos seus incidentes resolvidos.
- Delegar incidente para outro técnico (com motivo).
- Registar uso de ferramentas na análise (ex: antivírus, scanner de rede, etc.).

3. Gestão de Dados

- Utilizar ficheiros binários para armazenar dados de incidentes, técnicos e históricos de ações.
- Utilizar ficheiros de texto para gerar relatórios e logs de auditoria.
- Utilizar listas ligadas para manipular os dados em memória.
- Aplicar algoritmos de ordenação e pesquisa para análise rápida e eficaz dos registos.

A aplicação deve ser desenvolvida com boas práticas de programação em C (nomeadamente código devidamente comentado), com uma interface de linha de comandos simples e clara.

NOTA: As regras e os requisitos do trabalho podem ser ajustados mediante justificação no relatório final.

Luís Brito