

Projeto Semestral: Desenvolvimento de um Sistema de Monitoramento e Resposta a Incidentes Cibernéticos

Objetivo: Desenvolver um sistema integrado de monitoramento e resposta a incidentes cibernéticos para uma organização fictícia, visando aprimorar a segurança de seus ativos de informação.

Etapas do Projeto:

1. **Levantamento de Requisitos:** Identificação dos ativos críticos da organização, suas vulnerabilidades, e as ameaças cibernéticas mais relevantes.
2. **Desenho da Arquitetura:** Projeto da arquitetura do sistema, incluindo componentes de detecção de ameaças, análise de logs, resposta a incidentes, e recuperação de desastres.
3. **Implementação de Ferramentas de Monitoramento:** Configuração de ferramentas de SIEM (Security Information and Event Management) para coleta, normalização, e análise de logs de diferentes fontes.
4. **Desenvolvimento de Planos de Resposta a Incidentes:** Criação de procedimentos detalhados para resposta a incidentes específicos, baseados em cenários reais e potenciais.
5. **Simulação de Ataques e Testes de Penetração:** Realização de simulações controladas de ataques para testar a eficácia do sistema em detectar e responder a ameaças.
6. **Treinamento e Conscientização:** Desenvolvimento de um programa de treinamento para a equipe de segurança e demais funcionários da organização, focando na prevenção de incidentes e na resposta eficaz.
7. **Avaliação e Melhoria Contínua:** Implementação de um ciclo PDCA (Plan-Do-Check-Act) para avaliação contínua do sistema, identificação de melhorias e atualização de procedimentos e ferramentas.

Documentação:

- **Documento de Projeto:** Descrição detalhada do projeto, incluindo objetivos, metodologia, arquitetura do sistema, planos de implementação e testes, e procedimentos de resposta a incidentes.
- **Relatórios de Simulação:** Análise dos resultados das simulações de ataques e testes de penetração, incluindo recomendações para fortalecimento da segurança.
- **Manual de Treinamento:** Material de apoio para o programa de treinamento e conscientização em segurança cibernética.

Acompanhamento pelo Jira:

O projeto será gerenciado e acompanhado utilizando a ferramenta Jira, permitindo a criação de tarefas, alocação de responsáveis, definição de prazos e monitoramento do progresso de cada etapa do projeto.