Hand-on-Labs: SIEM and SOAR

Tecnologias de Informação - Segurança

- **Nível:**
- **Duração:** h

Sobre o curso

Neste curso os formandos vão trabalhar num conjunto de exercícios para proporcionar uma compreensão abrangente dos Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) e Resposta Orquestrada a Ameaças e Automatizada (SOAR).

Através de exercícios práticos, os formandos irão configurar, integrar e utilizar estas tecnologias para fortalecer a postura de segurança.

Destinatários

- Profissionais de cibersegurança interessados em aprofundar competências em SIEM e SOAR.
- Administradores de sistemas e redes que procuram implementar e integrar eficazmente soluções de SIEM e SOAR.

Objetivos

- Compreender os fundamentos dos Sistemas de Informação e Gestão de Eventos de Segurança (SIEM).
- Realizar configurações básicas de SIEM para uma compreensão prática.
- Integrar e utilizar ferramentas de Resposta Orquestrada a Ameaças e Automatizada (SOAR).
- Realizar análises avançadas usando SIEM para detectar e responder a ameaças.
- Implementar automação de resposta em ambientes de segurança usando SOAR.
- Explorar as melhores práticas e casos de estudo no campo de SIEM e SOAR.

Pré-requisitos

- Familiaridade com conceitos de segurança da informação
- Conhecimentos em redes e sistemas
- Experiência prática com configuração de redes e sistemas

Programa

- SIEM Overview
- Basic SIEM Configuration
- Hands-on Lab: Initial SIEM Setup
- Advanced Analysis with SIEM
- Introduction to SOAR
- Hands-on Lab: SIEM and SOAR Integration
- Automated Response with SOAR
- Best Practices and Case Studies