



FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA



OFFCYBEREMY



Nível E

Recolha e Análise Forense de Dados - Edição 29-09-2025 | 2 ECTS

Universidade do Algarve

35 horas / B-Learning / 50€

Sinopse

Esta formação destina-se a todas as pessoas, portadoras de bases bem consolidadas em cibersegurança, que ambicionam ingressar numa carreira profissional em equipas Computer Security Incident Response Team (CSIRT) ou Security Operations Centre (SOC). Os formandos terão oportunidade de desenvolver as seguintes competências:

1. pensamento crítico e criativo;
2. gestão de risco;
3. deteção de ameaças; e
4. análise de vulnerabilidades.

Depois de frequentar este curso o Analista Forense ganhará conhecimentos:

1. Para dissecar um ataque ou incidente de um ponto de vista forense
2. Sobre as técnicas e procedimentos necessários para preservar a prova
3. Sobre as obrigações e trâmites durante todo o processo de análise forense.

Short bio do Formador

Júlio Botequilha Fernandes é bacharel em Engenharia Elétrica e Eletrónica Ramo de Telecomunicações e licenciado em Informática Ramo de Sistemas, ambos pela Universidade do Algarve. Atualmente é assistente convidado na Faculdade de Ciências da UAlg onde leciona na Pós-Graduação de Cibersegurança. Assegura também a nomeação de Encarregado de Proteção de Dados da UAlg, assim como a coordenação da equipa de resposta a incidentes de informática (CSIRT) da UAlg e também a nomeação de responsável pela segurança de informação da Universidade do Algarve. Foi recentemente nomeado coordenador pelo membro UAlg do Centro de Competência em Cibersegurança do Algarve do Projeto C-Network do CNCS, formador e coordenador do programa C-Academy do CNCS na Universidade do Algarve.

Conteúdos Programáticos

- 1) A atividade e o contexto da investigação forense
- 2) O ambiente em que opera a investigação forense (Hard Disks & File Systems)
- 3) A importância da recolha e preservação das evidências, e da analítica em tempo real (agregação de logs, SIEM, endpoints, MDM e SOC)
- 4) Recolha de dados e duplicação para efeitos de investigação e prova
- 5) Investigação forense nos diversos sistemas operativos (Windows, Linux e Mac)
- 6) Investigação forense em redes de comunicação
- 7) Investigação forense em bases de dados e em ambientes cloud
- 8) Investigação forense em equipamentos móveis e IOT
- 9) Análise de malware
- 10) Investigação forense fora do perímetro da organização (darkweb, OSINT e redes sociais)
- 11) Desenho e conteúdo de relatórios forenses

Avaliação e Certificado

Os resultados de aprendizagem são avaliados individualmente através de 1 exame escrito (restantes 70% da nota). Assim a nota final será 70% exame + 30% participação.

Pré-requisitos para quem vai frequentar a formação:

Bases bem consolidadas em cibersegurança.

Observações: Não aplicável.

Calendário

Local	Dia	Horário	Formato
	29/9/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	30/9/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	2/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	3/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	6/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	7/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	9/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	13/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de

			participar remotamente)
	14/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)
	16/10/2025	17:30-21:00	B-Learning (presencial com possibilidade de participar remotamente)