UNIVERSIDADE ABERTA
www.uab.pt

MICROCREDENCIAL EM ANALISTA DE CIBERSEGURANÇA

alv Aprendizagem ao Longo da Vida

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

["Conhece o teu inimigo e conhece-te a ti próprio

e em cem batalhas nunca serás derrotado.

Se não conheces o teu inimigo e apenas te conheces a ti mesmo,

por cada vitória sofrerás uma derrota.

Se não conheces o teu inimigo nem te conheces a ti mesmo

serás derrotado em todas as batalhas."

SunTzu, A Arte da Guerra, 400 a.c.]

ÍNDICE

MICROCREDENCIAIS

Segundo com a Comissão Europeia, “microcredenciais” são qualificações que certificam resultados de aprendizagens resultantes de cursos curtos ou de módulos, tendo em vista a requalificação e atualização profissional de cada um. Estas qualificações podem ser obtidas pelos cidadãos com diversas modalidades de aprendizagem, presencial, a distância online ou mista.

Seja qual for o regime ou forma como são obtidas as qualificações, a Comissão Europeia vê nas microcredenciais uma oportunidade de aprendizagem flexível e inclusiva, no contexto dos sistemas de ensino e formação europeus e uma nova forma de acreditação adequada a diferentes necessidades.

Estas qualificações, por norma de curta duração, serão essencialmente úteis para quem pretende complementar o seu conhecimento e competências ou para quem pretende requalificar-se, procurando novas oportunidades no mercado de trabalho.

Na sua essência as microcredenciais assentam e dão resposta ao conceito e à prática de uma “aprendizagem ao longo da vida”.

ENQUADRAMENTO

O ciberespaço é um ambiente complexo, materializado por redes e sistemas de informação que permitem a sociedade em rede e criam novas oportunidades, potenciando as organizações e as suas atividades. A cibersegurança compreende as medidas e ações de prevenção e monitorização que visam cumprir os requisitos de autenticidade, confidencialidade, integridade, disponibilidade e não repúdio da informação contida no ciberespaço. A crescente dependência da sociedade nas tecnologias assentes no ciberespaço, cria vulnerabilidades e oportunidades de serem exploradas, por hackers em nome individual, pelo crime organizado, por extremistas ideológicos e políticos e mesmo por Estados.

As vulnerabilidades dos sistemas ou software, são exploradas por atores maliciosos que procuram lucro ou vantagem estratégica ao nível político, militar ou organizacional. Verifica-se que a evolução tecnológica aumenta a complexidade do ciberespaço e não tem foco na segurança, fazendo as vulnerabilidades prevalecerem porque os protocolos, arquiteturas das redes de computadores, o software e hardware são inseguros. A

severidade do impacto de uma vulnerabilidade explorada por um ator mal-intencionado (a ameaça), constitui assim um risco que é fundamental mitigar ou eliminar.

O sucesso da cibersegurança está assente na necessidade de uma monitorização contínua em vez de assentar numa postura reativa e passiva. Muitas vezes essa postura tradicional, pressupõe a implementação de uma solução de segurança na expectativa que seja a solução infalível para o problema. Contudo, esta abordagem não é suficiente para as ameaças atuais, sendo necessário adotar uma postura proativa, orientada à deteção de ameaças ou anomalias, partindo da premissa de que o sistema possa já ter sido comprometido. Até mesmo os mais recentes sistemas de deteção de intrusão e outros sistemas de segurança, são suscetíveis a falhas e a ataques avançados e direcionados. É essencial apostar na capacitação da componente humana para configurar adequadamente as redes, *endpoints* e dispositivos de segurança, e para monitorizar os sistemas de forma sistematizada, tendo em conta as novas ameaças e formas de atuação dos agentes maliciosos. A enorme quantidade de dados que é gerada nos sistemas de uma organização, pode e deve ser potenciada para detetar potenciais ameaças, num processo designado *Threat Hunting*.

Este curso titulado por uma Microcredencial* é direcionado para quem pretender aprofundar as suas competências de cibersegurança e especificamente para analistas de segurança que poderão desempenhar funções num Centro de Operações de Segurança (SOC). O curso prepara os formandos para analisarem e interpretarem de forma eficiente, os dados recolhidos na rede de uma organização, permitindo a deteção de anomalias e possíveis comprometimentos aos sistemas, bem como a consequente atualização e implementação de políticas de segurança segundo as boas práticas das normativas internacionais.

O presente curso desenvolve-se em regime de formação teórica e prática à distância, online (também dito e-learning), com uma componente de avaliação final baseada na elaboração de um projeto prático, a depositar na plataforma informática para análise, correção e classificação pelos professores até à data-hora estabelecida. O curso, de cariz eminentemente prático, inclui o enquadramento e conceitos de base, a modelação das ciberameaças, arquiteturas de rede seguras, operações de segurança, implementação e utilização eficiente de um SIEM, notas práticas de um SOC, monitorização de segurança contínua, análise de eventos de rede e de *endpoint*, configurações seguras, *Threat*

* Certificação digital adquirida em cursos de curta duração ou em módulos.

Intelligence, *Threat Hunting*, inteligência artificial na deteção de intrusões, desafios futuros e muito mais.

OBJETIVOS

O objetivo do curso é proporcionar conhecimentos e competências que permitam aos formandos zelar pela autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação numa organização. Assim, no final, os participantes saberão:

- Configurar e utilizar diversos dispositivos de segurança;
- Avaliar os pontos fortes e fracos dos dispositivos de segurança perante diversos cenários de ataque;
- Analisar e usar diferentes formas de deteção de ameaças e rastreamento de Indicadores de Comprometimento;
- Reconhecer e implementar controlos de segurança críticos;
- Explicar a estrutura e funcionamento de um Centro de Operações de Segurança (SOC) e discutir os desafios que se colocam.
- Explicar a importância da *Threat Intelligence* e praticar a sua utilização no processo de monitorização contínua;
- Adotar uma abordagem proativa de *Threat Hunting*;
- Avaliar o impacto da inteligência artificial na cibersegurança e reconhecer as novas técnicas de deteção de intrusões.

COMPETÊNCIAS

No final da ação os participantes ficarão habilitados com um conjunto de competências tecnológicas e procedimentais que lhes permitirão tomar ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Deste modo os participantes irão adquirir as seguintes competências que lhes serão creditadas nesta Microcredencial:

- Reconhecer o contexto atual da cibersegurança ao nível organizacional e perceber os elementos estruturantes das tecnologias e sistemas de informação;
- Adotar uma postura proativa na monitorização de cibersegurança;
- Entender como os sistemas e dispositivos de segurança funcionam, quais as suas capacidades e os seus papéis na monitorização contínua;
- Perceber como e porquê usar determinadas ferramentas de monitorização (de rede e *endpoint*) de acordo com os diversos cenários de ataque;
- Analisar e gerir vulnerabilidades;
- Usar a auditoria de configuração de uma *baseline* e *patching* para tornar os *endpoints* mais resilientes;
- Implementar controlos de segurança;
- Saber a constituição e organização de um SOC e qual o papel do analista;
- Adotar uma abordagem correta na triagem de alarmes de um SIEM;
- Perceber o papel do analista no reporte de problemas e no processo de resposta a incidentes;
- Reconhecer a importância do SIEM e os princípios gerais para uma implementação de sucesso;
- Utilizar a *Threat Intelligence* como suporte à segurança organizacional;
- Saber tirar proveito da *Cyber Kill Chain*, *Mittre Att&ck framework* e o *Diamond Model*, no âmbito do processo de *Threat Hunting*;
- Compreender os conceitos de Inteligência Artificial e Machine Learning e fazer a associação com a cibersegurança e com os desafios futuros;

Este curso permitirá ainda aos formandos adquirir diferentes competências ditas para a empregabilidade, designadamente competências:

- Para aprender continuamente e em regime de autoaprendizagem;
- De orientação para resultados;
- De intercomunicação online e de *networking*;
- De trabalho em equipa;
- Na utilização de tecnologias informáticas;
- Na autogestão do tempo e das atividades.

PROGRAMA E CONTEÚDOS

Este curso de cibersegurança está estruturado em 8 módulos, com a duração de uma semana cada, que se desenvolvem sequencialmente. Estes módulos são precedidos de um módulo de ambientação ao contexto online do curso e de integração dos participantes, designado módulo 0 ou pré-curso.

O curso tem a duração de 104 horas a que corresponde um crédito de 4 ECTS** da UAb e realiza-se em regime de formação a distância online (e-learning) ao longo das 9 semanas.

Na Internet o curso é suportado pela plataforma informática Moodle (PlataformAbERTA) em utilização na UAb e adaptada ao seu Modelo Pedagógico Virtual.

MÓDULOS	DESCRIÇÃO
0. Ambientação ao contexto online	Pretende socializar os participantes, criar de "um grupo" de trabalho online e familiarizar com a utilização do software de gestão do curso (o Learning Management System PlataformAbERTA) para uma exploração eficaz de todas as suas funcionalidades.
1. Fundamentos e enquadramento	Cibersegurança em contexto organizacional, utilização de máquinas virtuais e prática em ambiente Linux.
2. Arquiteturas de segurança em rede	Cenários de ataques modernos. Identificação e descrição diferentes tipos de dispositivos de segurança. Configurar e utilizar dos dispositivos de segurança avaliando seus pontos fortes e fracos.
3. Monitorização de segurança em rede	Conceito de Monitorização de Segurança Contínuo (MSC). Ferramentas de MSR. Analisar e usar diferentes formas de deteção de ameaças e rastreamento de Indicadores de Comprometimento (IOC).
4. Arquitetura de segurança nos dispositivos endpoint e monitorização de segurança contínua	Controlos de segurança críticos, patching, whitelisting de aplicações, configuração de baseline segura e monitorização de aplicações. Uso de ferramentas de proteção no host. Emprego e uso de técnicas de monitorização de segurança contínua em ambiente Windows.

** O ECTS (Sistema Europeu de Transferência de Créditos) foi desenvolvido pela Comissão Europeia. Os créditos ECTS representam o volume de trabalho que o estudante/formando deve produzir. Na UAb 1 ECTS equivale a 26 horas de trabalho do formando

5. Notas práticas de um Centro de Operações de Segurança (SOC)	Estrutura e funcionamento de um SOC. Desafios que se colocam ao analista. Debater o papel do SIEM num SOC e explicar os passos fundamentais para a sua implementação com sucesso. Principais atividades na resposta a incidentes. Contributo do analista de segurança.
6. Threat intelligence e Threat Hunting	Importância da Threat Intelligence, o conhecimento das ameaças e a análise dos dados sobre as mesmas. Abordagem proativa de Threat Hunting.
7. Inteligência artificial e deteção de intrusões	Conceitos fundamentais relacionados com a Inteligência Artificial. Demonstrar a utilização de algoritmos de Machine Learning na deteção de intrusões. Análise prospetiva dos desafios futuros relacionados com o impacto da Inteligência Artificial na cibersegurança.
8. Exercício final	Realização de um conjunto de exercícios sobre as diversas temáticas abordadas no decorrer do curso. Análise de um cenário que representa um sistema de rede que apresenta indícios de comprometimento, através de logs e ficheiros de captura de pacotes de rede.

MÓDULO 0: AMBIENTAÇÃO AO CONTEXTO ONLINE

[Duração: 13 horas | 1 semana]

1. A plataforma informática de ensino/aprendizagem da UAb, PlataformAbERTA
2. Treino na exploração das ferramentas e recursos da PlataformAbERTA

Objetivos do módulo

Este módulo tem por objetivos a socialização dos participantes e a criação de "um grupo" de trabalho online, a familiarização com a utilização do software de gestão do curso (o *Learning Management System* PlataformAbERTA) por forma a adquirirem as competências necessárias à exploração eficaz de todas as suas funcionalidades de intercomunicação, em especial as assíncronas por força do Modelo Pedagógico Virtual da UAb.

Competências a adquirir

No final deste módulo, pretende-se que os formandos sejam capazes de:

- Interagir e comunicar com os colegas, com os formadores e com a interface de aprendizagem no sentido de conseguir resolver problemas básicos de interação, de comunicação;

- Explorar com eficácia todas as ferramentas e possibilidades da PlataformAbERTA, com o estatuto de formando;
- Pesquisar, selecionar e organizar informação a partir da Web para a transformar em conhecimento mobilizável;
- Pesquisar, organizar, tratar e produzir informação em função das necessidades, problemas a resolver e das situações.

MÓDULO 1: FUNDAMENTOS E ENQUADRAMENTO

[Duração: 13 horas teórico-práticas | 1 semana]

1. A cibersegurança
2. Conceitos fundamentais
3. Máquinas virtuais
4. Ambiente Linux
5. Monitorização da cibersegurança (desafios e motivação)
6. Prática em contexto de formação

Objetivos do módulo

Enquadrar a cibersegurança no contexto organizacional.

Explicar os conceitos estruturantes das tecnologias e sistemas de informação. Demonstrar a utilização das máquinas virtuais e usar o Virtual Box em apoio ao ambiente virtual para o curso.

Praticar comandos em ambiente Linux.

Discutir os desafios relativos à monitorização da cibersegurança e motivar para os restantes módulos.

Competências a adquirir

- Identificar as principais ameaças no ciberespaço;
- Reconhecer o contexto atual da cibersegurança ao nível organizacional;
- Perceber os elementos estruturantes das tecnologias e sistemas de informação;
- Instalar e utilizar um sistema operativo numa máquina virtual;
- Utilizar os principais comandos em ambiente Linux;
- Adotar uma postura proativa na monitorização de cibersegurança.

MÓDULO 2: ARQUITETURAS DE SEGURANÇA EM REDE

[Duração: 13 horas teórico-práticas | 1 semana]

1. Cenários do adversário moderno
2. Dispositivos de segurança
3. Análise dos dispositivos de segurança face aos diferentes cenários de ataque
4. Prática em contexto de formação

Objetivos do módulo

Apresentar diferentes tipos de cenários de ataques modernos.

Identificar e descrever diferentes tipos de dispositivos de segurança.

Praticar a configuração e utilização dos dispositivos de segurança.

Avaliar os pontos fortes e fracos destes dispositivos de segurança perante os cenários anteriormente apresentados.

Competências a adquirir

- Diferenciar entre técnicas de ataques tradicionais e modernos;
- Demonstrar entendimento de como sistemas de firewall e de deteção/prevenção de intrusões funcionam, quais as suas capacidades e os seus papéis na monitorização contínua;
- Demonstrar e aplicar entendimento de como e porquê usar um conjunto de ferramentas de monitorização na rede para melhorar a capacidade de deteção de intrusões na rede;
- Demonstrar compreensão de como os proxies e SIEMs funcionam, quais são as suas capacidades e as funções que desempenham na monitorização contínua;
- Demonstrar capacidade de identificar pontos de acesso ao perímetro e dispositivos de rede que podem ser usados para proteger o perímetro.

MÓDULO 3: MONITORIZAÇÃO DE SEGURANÇA EM REDE

[Duração: 13 horas teórico-práticas | 1 semana]

1. Monitorização da segurança contínua
2. Ferramentas de monitorização de segurança em rede
3. Formas de deteção de ameaças e de rastreamento de indicadores de comprometimento
4. Prática em contexto de formação

Objetivos do módulo

Apresentar o conceito de Monitorização de Segurança Contínuo (MSC), distinguir MSC

de Monitorização de Segurança de Rede (MSR) e apresentar um caso de estudo real. Descrever e aplicar um conjunto de ferramentas de MSR. Analisar e usar diferentes formas de deteção de ameaças e rastreamento de Indicadores de Comprometimento (IOC).

Competências a adquirir

- Demonstrar entendimento dos princípios de defesa tradicional e moderna;
- Demonstrar entendimento das ferramentas e técnicas usadas para levantamento de dispositivos de rede e hosts e de análise de vulnerabilidades;
- Aplicar métodos e princípios de análise de tráfego em rede para deteção de explorações e estar apto a rapidamente encontrar intrusões na rede;
- Aplicar os princípios de deteção de uma exploração para identificar intrusões cifradas na rede;
- Demonstrar entendimento de como e porquê usar um conjunto de ferramentas de monitorização na rede para melhorar a capacidade de deteção de intrusões na rede.

MÓDULO 4: ARQUITETURA DE SEGURANÇA NOS DISPOSITIVOS *ENDPOINT* E MONITORIZAÇÃO DE SEGURANÇA CONTÍNUA

[Duração: 13 horas teórico-práticas | 1 semana]

1. Controlos de segurança críticos
2. Ferramentas de proteção no *host*
3. Monitorização de segurança contínua
4. Prática em contexto de formação

Objetivos do módulo

Descrever e explicar os controlos de segurança críticos, nomeadamente *patching*, *whitelisting* de aplicações, configuração de *baseline* segura e monitorização de aplicações.

Identificar e demonstrar o uso de ferramentas de proteção no *host*.

Enunciar e empregar o uso de técnicas de monitorização de segurança contínua através da realização de diversos exemplos práticos maioritariamente em ambiente Windows

Competências a adquirir

- Demonstrar habilidade para controlar os níveis de privilégios de contas e aplicações;

- Demonstrar entendimento das ferramentas e técnicas usadas para a monitorização de alteração de configurações;
- Demonstrar entendimento das ferramentas e técnicas usadas para levantamento de dispositivos de rede e *hosts* e de análise de vulnerabilidades;
- Compreender como usar a auditoria de configuração de uma *baseline* e *patching* para tornar os *endpoints* mais resilientes;
- Demonstrar compreensão das estruturas de arquitetura de segurança tradicionais e modernas e qual o papel dos SOCs;
- Demonstrar compreensão dos benefícios de manter inventários de software e listas de permissões.

MÓDULO 5: NOTAS PRÁTICAS DE UM CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

[Duração: 13 horas teórico-práticas | 1 semana]

1. O Centro de Operações de Segurança (SOC)
2. Dia-a-dia do analista de segurança SOC
3. O SIEM e gestão de eventos
4. Contributos para a resposta a incidentes
5. Prática em contexto de formação

Objetivos do módulo

Explicar a estrutura e funcionamento de um SOC, focando os aspetos mais pertinentes para um analista.

Discutir os desafios que se colocam ao analista no âmbito das suas funções.

Debater o papel do SIEM num SOC e explicar os passos fundamentais para a sua implementação com sucesso.

Diferenciar as principais atividades na resposta a incidentes e o contributo do analista de segurança.

Competências a adquirir

- Saber a constituição e organização de um SOC e qual o papel do analista;
- Ser capaz de adotar uma abordagem correta na triagem de alarmes;
- Perceber o papel do analista no reporte de problemas e no processo de resposta a incidentes;
- Reconhecer a importância do SIEM e os princípios gerais para uma implementação de sucesso.

MÓDULO 6: *THREAT INTELLIGENCE* E *THREAT HUNTING*

[Duração: 13 horas teórico-práticas | 1 semana]

1. *Threat Intelligence*
2. *Threat Hunting*
3. Exemplos de *Threat Hunting*
4. Prática em contexto de formação

Objetivos do módulo

Explicar a importância da *Threat Intelligence*, o conhecimento das ameaças e a análise dos dados sobre as mesmas.

Demonstrar e exemplificar a importância de uma abordagem proativa de *Threat Hunting*.

Competências a adquirir

- Utilizar a *Threat Intelligence* como suporte à segurança organizacional;
- Identificar as fontes de informação que são relevantes para o processo de *Threat Intelligence* vocacionado para a organização;
- Compreender como é realizada a partilha de *Threat Intelligence*;
- Saber tirar proveito da *Cyber Kill Chain*, *Mittre Att&ck Framework* e o *Diamond Model*, no âmbito do processo de *Threat Hunting*;
- Conseguir exemplificar a utilização de *Threat Hunting*, identificando indicadores de comprometimento típicos nos cenários de ataque mais populares.

MÓDULO 7: INTELIGÊNCIA ARTIFICIAL E DETEÇÃO DE INTRUSÕES

[Duração: 13 horas teórico-práticas | 1 semana]

1. Conceitos fundamentais e machine learning
2. Deteção de intrusões com machine learning
3. Desafios futuros da IA na cibersegurança
4. Prática em contexto de formação

Objetivos do módulo

Explicar os conceitos fundamentais relacionados com a Inteligência Artificial.

Demonstrar a utilização de algoritmos de *Machine Learning* na deteção de intrusões.

Debater, em análise prospetiva, os desafios futuros relacionados com o impacto da Inteligência Artificial na cibersegurança.

Competências a adquirir

- Compreender os conceitos de Inteligência Artificial e *Machine Learning*;
- Perceber os conceitos fundamentais relacionados com *Machine Learning*;

- Reconhecer as limitações dos sistemas de deteção de intrusões tradicionais;
- Conseguir fazer a aplicação prática de algoritmos baseados em métodos não supervisionados, na deteção de intrusões;
- Discutir os desafios futuros e o impacto da inteligência artificial na cibersegurança.

MÓDULO 8: EXERCÍCIO FINAL

[Duração: 13 horas teórico-práticas | 1 semana]

1. Exercícios temáticos
2. Análise de cenário
3. Elaboração de relatório

O exercício final consiste na realização de um conjunto de pequenos exercícios sobre as diversas temáticas abordadas no decorrer do curso, e numa análise de um cenário que representa um sistema de rede que apresenta indícios de comprometimento, através de logs e ficheiros de captura de pacotes de rede. Os formandos deverão responder às questões previamente elencadas pelos formadores, sob a forma de um relatório a ser submetido online, para poder ser visualizado, analisado, avaliado e classificado pelos formadores. Este trabalho tem por objetivo a aplicação dos conhecimentos e competências adquiridas ao longo de todo o curso.

O trabalho final é de realização obrigatória. A sua não realização implica a não aprovação no curso. O trabalho final escrito é objeto de classificação quantitativa e, para aprovação no curso, a classificação deste trabalho deve ser igual ou superior a 9,5 valores, numa escala de 0 a 20.

DESTINATÁRIOS

São destinatários potenciais desta microcredencial:

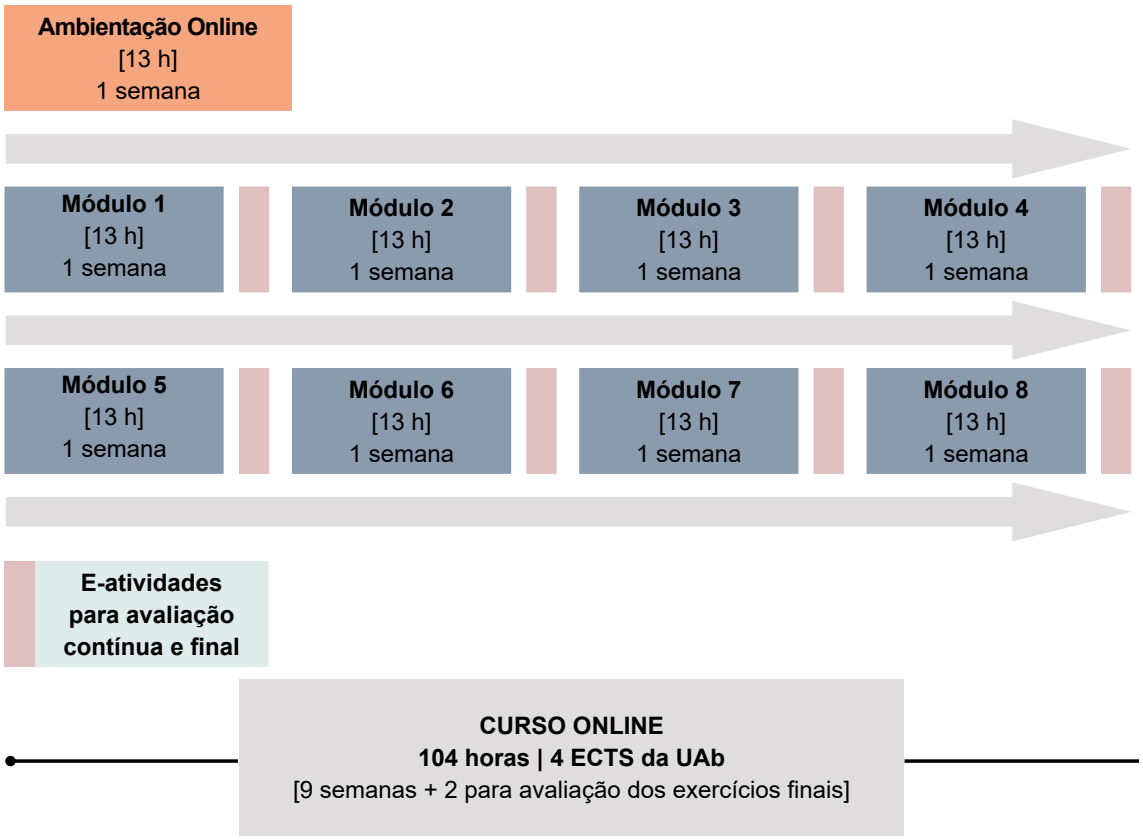
- Todos os profissionais que trabalham na área de IT ou cibersegurança das empresas/organizações e desejem aprofundar os conhecimentos na área da análise de eventos de segurança, gestão de vulnerabilidades e ameaças;
- Todos os profissionais que pretendam iniciar-se na resposta a incidentes de cibersegurança;
- Indivíduos que desejem especializar-se em operações de cibersegurança e análise de eventos de segurança para poderem desempenhar a função de analistas de cibersegurança nas organizações/empresas;

Além da motivação e ou interesse os formandos devem ter:

- Habilitações mínimas ao nível do 12.º ano ou equivalente;
- Computador com pelo menos 8GB de memória RAM e 50 GB de espaço em disco disponível;
- Conhecimentos e prática de informática como utilizadores;
- Prática de utilização de browsers de navegação na Web;
- Uma conta de correio eletrónico ativa e prática na sua utilização;
- Disponibilidade de tempo mínima para o curso de 13 horas por semana.

ESTRUTURA

A duração total da microcredencial é de 104 horas, estruturadas em 8 módulos de realização sequencial, precedidos de um módulo de Ambientação.



METODOLOGIA

O curso segue um modelo no qual é a instituição formadora que define os objetivos, conteúdos, percursos de aprendizagem e meios e métodos de avaliação. Este modelo

pressupõe a existência de canais de comunicação fáceis e disponíveis em permanência, entre a instituição e os formandos e entre estes e os formadores(es), canais esses integrados na PlataformAbERTA a utilizar.

A metodologia seguida neste curso é a estabelecida no Modelo Pedagógico Virtual da UAb para ações de aprendizagem ao longo da vida a desenvolver em regime de e-learning e adota o modelo de ensino/aprendizagem de 5 níveis de que nos fala Gilly Salmon (2000).

A forma de trabalho utilizada neste curso compreende (1) a leitura e reflexão individuais dos conteúdos disponibilizados ou de outros sobre os mesmos temas obtidos pelos formandos, (2) a partilha da reflexão e do estudo com os colegas, assim como também (3) o esclarecimento de dúvidas nos fóruns moderados pelo formador e a (4) realização das e-atividades propostas.

A leitura e a reflexão individuais devem acontecer ao longo de todo o processo de aprendizagem e sem elas o formando fica muito limitado na sua participação nos fóruns previstos, assim como também dificilmente poderá realizar com sucesso as atividades programadas.

A aprendizagem está estruturada por tópicos que correspondem a módulos do curso. Em cada tópico será criado um fórum moderado pelo formador para esclarecimento das dúvidas e ultrapassagem das dificuldades sentidas e apresentadas pelos formandos, proporcionando assim uma possibilidade de interação permanente dos formandos entre si e com o formador. Todos os fóruns decorridos permanecerão abertos ao longo de todo o curso, possibilitando assim a consulta a todo o tempo das mensagens trocadas. No entanto, quaisquer mensagens enviadas depois de terminado o módulo em que o fórum de discussão decorreu não serão consideradas pelos professores para efeitos de classificação da participação nesse fórum.

No módulo 0 e de acordo com o modelo de ensino/aprendizagem de Salmon cumprem se os níveis 1 e 2, respetivamente “acesso e motivação” e a “socialização online”; dependendo do grupo concreto de formandos iniciar-se-á ou não o nível 3 de “processamento de conteúdos” onde a tutoria se consubstancia no apoio na utilização de materiais pedagógicos e nas tarefas, nesta fase apenas em relação ao modo como fazer pesquisa orientada em WWW.

Nos módulos seguintes cumprem-se todos os restantes níveis do modelo de Gilly

Salmon, “processamento de conteúdos” centrado na interação com os materiais de aprendizagem e com os restantes participantes do curso (colegas e formadores), “construção do conhecimento” onde é natural que o papel do formador se dilua e “exploração”, nível onde o suporte técnico disponibiliza novas fontes de informação e a tutoria dá apoio e resposta a questões.

Em dados momentos do curso os formadores enviam aos formandos as e-atividades que devem realizar no prazo previsto, e enviar ao formador para avaliação até a data e hora limite indicadas.

Dada a natureza do tipo de trabalho a realizar pelos participantes, o acompanhamento dos mesmos exige grande disponibilidade por parte dos formadores, pelo que cada turma virtual não deve ter um número muito elevado de e-formandos.

Nesta ação de formação os formandos terão, sequencialmente, acesso aos conteúdos dos diversos módulos, para o seu estudo e para a execução das atividades solicitadas, em situações on e offline. O acesso offline possibilita a leitura/estudo dos conteúdos dos módulos por parte dos formandos sem necessidade de ligação à Internet.

A tutoria a prestar pelos formadores será ativa e permanente e far-se-á preferencialmente através dos fóruns de discussão abertos nos diversos tópicos (correspondentes aos módulos da estrutura do curso) na PlataformAbERTA.

Podem realizar-se sessões síncronas de discussão online (chats), em datas, horários e locais (Tópicos) a comunicar antecipadamente pelos formadores.

RECURSOS DE APRENDIZAGEM

Recursos pedagógicos

Os materiais técnico-pedagógicos a fornecer aos formandos para utilização no curso são:

- Textos base sobre os temas a abordar, colocados online no curso criado na PlataformAbERTA e/ou na Web em servidor a indicar aos participantes para procederem o seu download;
- Apresentações multimédia diversas concebidas pelos formadores para situações de aprendizagem específicas;
- Tutorial sobre a forma de utilizar a PlataformAbERTA na situação de e-formando;

- Tutorial “Como Fazer para…”, documento orientador dos procedimentos para aceder ao curso alojado na PlataformAbERTA;
- Guia da Microcredencial;
- Guia do Formando Online.

Recursos técnicos

Plataforma informática Moodle (V 2.4), em https://elearning.uab.pt/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

AVALIAÇÃO E CLASSIFICAÇÃO

A avaliação em formação online tem uma importância acrescida em relação à avaliação em regime presencial em virtude da natureza particular do contexto de ensino-aprendizagem.

Avaliação nos Módulos

Os módulos 1 a 7 do curso são sujeitos a avaliação. A avaliação nos módulos 1 a 7 integra:

- Uma componente contínua ao longo do módulo (participação nos fóruns) de discussão e eventual realização de e-atividades intermédias);
- Uma componente final do módulo baseada na realização de uma e-atividade final que pode revestir qualquer forma (trabalho, teste, projeto, etc.).

Os instrumentos de avaliação de um módulo têm o mesmo peso e, por isso, a avaliação final do módulo é dada pela média simples das 2 ou 3 provas realizadas, numa escala de 0 a 20 valores.

A média final da avaliação dos módulos traduz a sua classificação final.

Na avaliação da participação dos alunos num fórum de discussão têm-se em atenção os seguintes fatores:

- A qualidade e a quantidade de mensagens com conteúdo significativo para o(s) assunto(s) em discussão;
- A relevância das mensagens para os temas em discussão;
- A clareza e objetividade das mensagens;
- A redação das mensagens (pontuação, erros de ortografia, etc.);

- A oportunidade do envio das mensagens, privilegiando-se a distribuição destas ao longo de todo o período de discussão em fórum.

Todas as mensagens enviadas para os fóruns de módulos já terminados **não são consideradas** para efeitos de avaliação.

As e-atividades a realizar em cada um dos módulos (tanto as intermédias como a final) podem revestir qualquer tipo – teste tradicional, trabalho offline, trabalho online, síntese, pesquisa, relatório, etc. – ficando a sua escolha ao critério do formador do respetivo módulo.

É obrigatória a realização de todas as e-atividades de avaliação dos módulos que contam para a classificação final do curso. A não realização de uma e-atividade é contabilizada com 0 valores para efeitos de obtenção da média. A não participação num fórum de discussão traduz-se numa classificação de 0 valores nesse fórum.

Todas as e-atividades de avaliação final dos diversos módulos realizam-se numa só data e num período de 24 a 48 horas. **Excecionalmente**, e apenas por razões de doença ou de inoperacionalidade da plataforma, ambas devidamente comprovadas, se admite a realização das e-atividades para avaliação numa data de **segunda oportunidade**.

Classificação Final no curso

A classificação final no curso (CFC) é obtida pela aplicação da fórmula:

$$\mathrm{CFC} = \left(\frac{\mathrm{AFM1} + \mathrm{AFM2} + \mathrm{AFM3} + \mathrm{AFM4} + \mathrm{AFM5} + \mathrm{AFM6} + \mathrm{AFM7}}{7}\right) \times 0{,}6 + \mathrm{AFM8} \times 0{,}4$$

onde AFMx representa a Avaliação Final do Módulo x.

Consideram-se com aproveitamento no curso os formandos que obtiverem classificação Final no Curso **igual ou superior 10 valores**, numa escala de 0 a 20 e, cumulativamente, tenham uma avaliação final em todos os módulos 1 a 7 igual ou superior a 8 valores.

Para efeitos de aproveitamento e de inscrição no Certificado as classificações finais com décimas de 0,5 a 0,9 são arredondadas para o valor inteiro superior e as de 0,1 a 0,4 para o valor inteiro inferior.

A todos os formandos com aproveitamento é entregue um **Certificado de Formação** que será enviado para a morada que consta no formulário de inscrição no curso.

A todos os formandos que realizaram integralmente o curso e o terminaram sem aproveitamento, de acordo com o Regulamento do Curso e a seu pedido expresso, será entregue um **Certificado de Frequência**.

EQUIPA DOCENTE

FORMADORES	MÓDULOS
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
Luís Dias André Calvinho	1. Fundamentos e enquadramento
André Calvinho	2. Arquiteturas de segurança em rede
André Calvinho	3. Monitorização de segurança em rede
André Calvinho	4. Arquitetura de segurança nos dispositivos *Endpoint* e Monitorização de Segurança Contínua
Luís Dias	5. Notas práticas de um SOC
Luís Dias	6. Threat intelligence e Threat Hunting
Luís Dias	7. Inteligência artificial e deteção de intrusões
Luís Dias André Calvinho	8. Exercício Final – Ambiente Virtual
Luís Dias André Calvinho	Análise, avaliação e classificação dos trabalhos finais

LUÍS FILIPE XAVIER CAVACO DE MENDONÇA DIAS é Major Engenheiro da Arma de Transmissões do Exército Português, especializado em Segurança da Informação e Docente na Academia Militar. É Doutorado em Segurança de Informação pelo Instituto Superior Técnico, Mestre em Engenharia Eletrotécnica Militar (Especialidade de Transmissões) pela Academia Militar, e está ainda habilitado com o Curso de Estado-Maior Conjunto das Forças Armadas. Detém várias certificações da Indústria (SANS GCFE, EC-Council E CSA e ENSA, etc.) e é membro do GIAC advisory board.
Atualmente e desde 2016, é docente de “Segurança Informação, Sistemas de Informação e Ciberdefesa” (entre outras Unidades Curriculares) na Academia Militar.

Desempenhou funções na componente operacional de ciberdefesa do Exército, entre 2010 e 2015. Participou como "jogador" em diversas edições de exercícios de ciberdefesa Nacionais e Internacionais (Ciber Perseu, Cyber Coalition da NATO). Em 2018 e 2019 foi organizador dos Exercícios Nacionais de Ciberdefesa (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

É membro investigador do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento (INESC-ID) e do Centro de Investigação da Academia Militar (CINAMIL). Desenvolve investigação no âmbito da aprendizagem automática de ameaças no ciberespaço através da análise de dados de segurança, com recurso a algoritmos de aprendizagem não supervisionada. É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2019.

ANDRÉ VICENTE CALVINHO é Capitão Engenheiro da Arma de Transmissões do Exército Português, especializado na área da Ciberdefesa e Segurança da Informação. Possui 7 anos de experiência na área da cibersegurança. É engenheiro de cibersegurança, investigador na área da segurança e penetration tester. É mestre em Engenharia Eletrotécnica e de Computadores na Academia Militar e Instituto Superior Técnico.

Possui diversas certificações da indústria, tais como: Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) e GIAC Certified Intrusion Analyst (GCIA). Possui ainda a certificação em GIAC Continuous Monitoring Certification (GMON), é membro do GIAC Advisory Board e detentor de inúmeros cursos na área dos sistemas de informação entre os quais o CCNA-Exploration da Cisco e IBM Security QRadar.

Possui ainda experiência nas áreas de Information Assurance, Vulnerability Assessment, Penetration Testing, Forensics, Configurations Analysis, Security Analysis, Hardening e Incident Response. Desenvolveu vários projetos na área, entre os quais a criação da ferramenta EmailAnalyzer, disponível na plataforma GitHub. Destaque ainda para a sua participação nos seguintes exercícios internacionais: NATO Cyber Coalition (2014, 2015, 2016 e 2019), NATO Locked Shields (2018, 2019 e 2021), CrossedSwords (2020), BRAZIL – CyberSecurity Brazilian Army Course e Ibero-Armerican Exercise of Cyber Defense (2018).


UNIVERSIDADE
ABERTA
www.uab.pt