Certified Cybersecurity Operations Analyst™ (CCOA™)

ISACA

- **Nível:**
- **Duração:** 25h

Sobre o curso

A certificação CCOA Certified Cybersecurity Operations Analyst, capacita profissionais com as competências técnicas necessárias para avaliar ameaças, identificar vulnerabilidades e desenvolver contramedidas para proteger ecossistemas digitais. À medida que as tecnologias emergentes, como a automação com recurso a AI, continuam a evoluir, a procura por analistas de cibersegurança qualificados é crítica para salvaguardar as organizações.

Neste curso os formandos vão desenvolver competências analíticas e de investigação necessárias para detetar, responder e mitigar incidentes de cibersegurança. Assim como explorar os fundamentos da tecnologia, táticas e procedimentos adversariais, deteção e resposta a incidentes, e segurança de ativos através de cenários práticos e aprendizagem aplicada.

Ao desenvolver a capacidade de identificar padrões, anomalias e indicadores de comprometimento, os participantes irão reforçar o seu papel como componente vital da defesa de cibersegurança da sua organização.

Destinatários

- Analistas de cibersegurança e profissionais de operações
- Analistas de SOC e responsáveis pela resposta a incidentes
- Administradores de IT e de redes que pretendem desenvolver especialização em segurança
- Profissionais responsáveis pela governação, compliance e gestão de risco em cibersegurança
- Profissionais em início ou meio de carreira que pretendem reforçar competências técnicas e operacionais

---

Objetivos

- Identificar os principais componentes das redes informáticas e cloud, bases de dados e ambientes virtualizados
- Compreender a governação da cibersegurança e alinhar a estratégia de segurança com os objetivos empresariais
- Analisar táticas, técnicas e procedimentos adversariais para detetar e responder a ameaças de forma

eficaz
- Aplicar técnicas de deteção e resposta a incidentes, incluindo análise forense e análise de malware
- Reconhecer a importância da preparação e planeamento proativos de incidentes
- Conceber e recomendar contramedidas para proteger ativos digitais em vários setores
- Implementar práticas de gestão de identidade, acessos e vulnerabilidades
- Aplicar boas práticas, frameworks e normas para reforçar as operações de cibersegurança

---

Condições

- Inclui respetivo exame de certificação

Pré-requisitos

A certificação CCOA é recomendada para profissionais de cibersegurança com 2 a 3 anos de experiência prática que pretendam expandir as suas competências técnicas e responder de forma mais eficaz à evolução das ciberameaças.

Metodologia

Este curso tem uma duração aproximada de 25 horas assíncronas e é acedido através da plataforma da ISACA. Os formandos após a conclusão do curso obterão 30 CPE. Os conteúdos estão disponíveis em Inglês.

Programa

- Fundamentos da tecnologia
- Princípios de cibersegurança
- Táticas, técnicas e procedimentos adversariais (TTPs)
- Deteção e resposta a incidentes
- Proteção de ativos

Domínio 1: Fundamentos da tecnologia

- Fundamentos de redes informáticas e cloud
- Bases de dados, virtualização e contentorização
- Interfaces de linha de comandos
- APIs: objetivo, benefícios e utilização
- Princípios de DevOps, SecDevOps e pipelines de CI/CD
- Fundamentos de programação e scripting

Domínio 2: Princípios de cibersegurança

- Governação da cibersegurança e alinhamento com os impulsionadores do negócio
- Definição de estratégia com base nos objetivos empresariais
- Comunicação transversal à organização para a cibersegurança
- Papéis e responsabilidades nas iniciativas
- Métricas para avaliar o desempenho do programa
- Envolvimento das partes interessadas e planeamento de investimento
- Processos de gestão de risco e requisitos de compliance
- Documentação do risco nas operações empresariais

Domínio 3: Táticas, técnicas e procedimentos adversariais (TTPs)

- Táticas, técnicas e procedimentos adversariais comuns
- Desenvolvimento do pensamento crítico e criativo para deteção de ameaças
- Diferenciação entre eventos de dashboard e insights de atacantes
- Deteções de baseline para comportamentos anómalos
- Capacidades reativas e proativas de deteção de ameaças
- Threat hunting e utilização de fontes de intelligence
- Vetores de ataque, agentes de ameaça e motivações
- Análise de técnicas de exploit e fases de ataque
- Papel dos testes de segurança na deteção e resiliência

Domínio 4: Deteção e resposta a incidentes

- Preparação para incidentes e importância da deteção precoce
- Componentes e técnicas de deteção (analytics, logs, alertas)
- Desenvolvimento de use cases de deteção e reconhecimento de indicadores de comprometimento
- Ferramentas e tecnologias para monitorização eficaz
- Fundamentos da resposta a incidentes: contenção e tratamento
- Técnicas de análise forense, malware, tráfego de rede e pacotes
- Análise de ameaças e processos estruturados de resposta

Domínio 5: Proteção de ativos

- Conceção de contramedidas para proteção de ativos digitais
- Abordagens iterativas e holísticas à segurança de sistemas
- Necessidades de proteção de ativos específicas da indústria e tolerância ao risco
- Influência dos objetivos de negócio e das avaliações de risco nos controlos de segurança
- Planeamento de contingência e continuidade de negócio
- Técnicas de controlo para proteção de ativos
- Princípios e práticas de gestão de identidade e acessos
- Boas práticas, frameworks e normas para segurança de ativos
- Avaliação de vulnerabilidades, remediação e mitigação de risco