ISEIG
Institut Suisse d'Enseignement de l'Informatique de Gestion

ISEIG Depuis 1982 | Plus de 40 ans d'excellence … … pas mal !

CompTIA Advanced Security Practitioner

Certification CASP+

Introduction

CASP+ (CompTIA Advanced Security Practitioner) est une certification destinée aux praticiens de la sécurité et non aux gestionnaires de la sécurité. Les gestionnaires de la cybersécurité aident à identifier les politiques et cadres de cybersécurité à mettre en œuvre. Les professionnels praticiens certifiés CASP+ ont des compétences avancées dans la cybersécurité. Ils déterminent comment mettre en œuvre des solutions dans le cadre des politiques et des cadres définis par les gestionnaires de la sécurité.

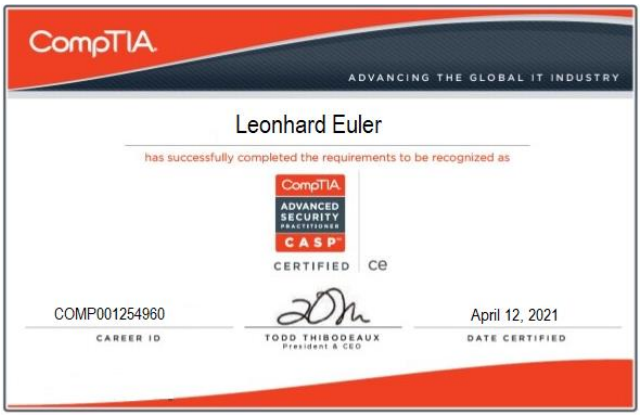
CASP+ est la certification idéale pour les professionnels techniques qui souhaitent rester immergés dans la technologie, par opposition à une gestion stricte.

Les thèmes traités dans cette formation sont pour la plupart génériques. Ils peuvent s'appliquer à de nombreux dispositifs et technologies de sécurité, quel que soit le fournisseur. Bien que l'examen CASP+ soit neutre par rapport aux fournisseurs, les dispositifs et les technologies sont mis en œuvre par de multiples vendeurs indépendants.

L'examen de certification, d'une durée de 165 minutes, est en anglais. Il comprend au maximum 90 questions à choix multiple adaptatives, c'est-à-dire que les questions dépendent des questions et réponses précédentes. Il se déroule à l'ISEIG un jeudi à convenir.

Pour qui

- professionnels de la cybersécurité souhaitant rester immergés dans la technologie plutôt que de gérer la politique et les cadres de cybersécurité.



Objectifs

- savoir évaluer les politiques et les procédures de sécurité et de confidentialité en fonction des besoins de l'organisation
- savoir mettre en œuvre des stratégies et des contrôles d'atténuation des risques sur la base d'un scénario
- savoir analyser des scénarios de mesure des risques pour sécuriser l'entreprise
- savoir identifier et gérer les risques liés à la sécurité des informations pour assurer les objectifs métiers
- savoir analyser un scénario et intégrer les composants, concepts et architectures de réseau et de sécurité pour répondre aux exigences de sécurité
- savoir analyser un scénario et intégrer les contrôles de sécurité pour les dispositifs hôtes afin de répondre aux exigences
- savoir sélectionner les contrôles de sécurité appropriés compte tenu de scénarios de vulnérabilité logicielle
- savoir évaluer la sécurité en utilisant les méthodes appropriées sur la base d'un scénario
- savoir analyser un scénario ou un résultat, et sélectionner l'outil approprié pour une évaluation de sécurité
- savoir mettre en œuvre des procédures de réponse aux incidents et de récupération sur la base d'un scénario
- savoir intégrer les hôtes, le stockage, les réseaux et les applications dans une architecture sécurisée
- savoir intégrer les technologies cloud computing et de virtualisation dans une architecture d'entreprise sécurisée sur la base d'un scénario
- savoir intégrer et dépanner les technologies avancées d'authentification et d'autorisation afin de soutenir l'architecture d'entreprise sur la base d'un scénario
- savoir mettre en œuvre des techniques cryptographiques sur la base d'un scénario
- savoir sélectionner le contrôle approprié pour sécuriser les solutions de communication et de collaboration
- savoir appliquer des méthodes de recherche pour déterminer les tendances du secteur et leur impact sur l'entreprise
- savoir mettre en œuvre des activités de sécurité tout au long du cycle de vie de la technologie
- savoir expliquer l'importance de l'interaction entre les diverses unités d'affaires pour atteindre les objectifs de sécurité.

Prérequis

- minimum 10 ans d'expérience dans l'administration IT dont au moins 5 ans dans la mise en place technique de la sécurité
- anglais technique écrit, la documentation pédagogique et les examens étant en anglais

CASP

Programme

1. **Business and Industry Influences and Associated Security Risks**
   - Risk Management of New Products, Technologies, Users
   - New or Changing Business Models/Strategies
   - Security Concerns of Integrating Diverse Industries
   - Internal and External Influences
   - Impact of De-perimeterization
2. **Security, Privacy Policies, and Procedures**
   - Policy and Process Life Cycle Management
   - Support Legal Compliance and Advocacy
   - Common Business Documents to Support Security
   - Security Requirements for Contracts
   - General Privacy Principles for Sensitive Information
   - Support the Development of Policies of Security Practices
3. **Risk Mitigation Strategies and Controls**
   - Categorize Data Types by Impact Levels Based on CIA
   - Select and Implement Controls Based on CIA Requirements and Organizational Policies
   - Extreme Scenario Planning/Worst-Case Scenario
   - Conduct System-Specific Risk Analysis
   - Make Risk Determination Based upon Known Metrics
   - Translate Technical Risks in Business Terms
   - Chose which Strategy Should Be Applied Based on Risk Appetite
   - Risk Management Processes
   - Continuous Improvement/Monitoring
   - Business Continuity Planning
   - IT Governance and Enterprise Resilience
4. **Risk Metric Scenarios to Secure the Enterprise**
   - Review Effectiveness of Existing Security Controls
   - Reverse Engineer/Deconstruct Existing Solutions
   - Creation, Collection, and Analysis of Metrics
   - Prototype and Test Multiple Solutions
   - Create Benchmarks and Compare to Baselines
   - Analyze Trend Data to Anticipate Cyber Defense Needs
   - Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs
   - Use Judgment to Solve Problems Where the Most Secure Solution Is Not
5. **Network and Security Components, Concepts, and Architectures**
   - Physical and Virtual Network and Security Devices
   - Application and Protocol-Aware Technologies
   - Advanced Network Design (Wired/Wireless)
   - Complex Network Security Solutions for Data Flow
   - Secure Configuration and Baselining of Networking and Security
   - Software-Defined Networking
   - Network Management and Monitoring Tools
   - Advanced Configuration of Routers, Switches, and Other Devices
   - Security Zones
   - Network Access Control and Network-Enabled Devices
6. **Security Controls for Host Devices**
   - Trusted OS (e.g., How and When to Use It)
   - Endpoint Security Software
   - Host Hardening and Boot Loader Protections
   - Vulnerabilities Associated with Hardware
   - Terminal Services/Application Delivery Services
7. **Security Controls for Mobile and Small Form Factor Devices**
   - Enterprise Mobility Management
   - Security Implications/Privacy Concerns
   - Wearable Technology
8. **Software Vulnerability Security Controls**
   - Application Security Design Considerations
   - Specific Application Issues and Application Sandboxing
   - Secure Encrypted Enclaves and Database Activity Monitor
   - Web Application Firewalls
   - Client-Side Processing vs. Server-Side Processing
   - Operating System and Firmware Vulnerabilities
9. **Security Assessments**
   - Methods and Test Types
10. **Select the Appropriate Security Assessment Tool**
    - Network Tool Types and Host Tool Types
    - Physical Security Tools
11. **Incident Response and Recovery**
    - E-Discovery and Data Breach
    - Facilitate Incident Detection and Response
    - Incident and Emergency Response
    - Incident Response Support Tools
    - Severity of Incident or Breach
    - Post-incident Response
12. **Host, Storage, Network, and Application Integration**
    - Adapt Data Flow Security to Meet Changing Business Needs
    - Interoperability Issues and Resilience Issues
    - Data Security Considerations
    - Resources Provisioning and Deprovisioning
    - Design Considerations During Mergers, Acquisitions and Demergers/Divestitures
    - Network Secure Segmentation and Delegation
    - Logical Deployment Diagram and Corresponding Physical Deployment Diagram of All Relevant Devices
    - Security and Privacy Considerations of Storage Integration
    - Security Implications of Integrating Enterprise Applications
13. **Cloud and Virtualization Technology Integration**
    - Technical Deployment Models (Outsourcing/Insourcing/Managed Services/Partnership)
    - Security Advantages and Disadvantages of Virtualization
    - Cloud Augmented Security Services
    - Vulnerabilities Associated with Comingling of Hosts with Different Security Requirements
    - Data Security Considerations
    - Resources Provisioning and Deprovisioning
14. **Authentication and Authorization Technology Integration**
    - Authentication and Authorization
    - Attestation and Identity Propagation
    - Federation and Trust Models
15. **Cryptographic Techniques**
    - Techniques and Implementations
16. **Secure Communication and Collaboration**
    - Remote Access and Unified Collaboration Tools
17. **Industry Trends and Their Impact to the Enterprise**
    - Perform Ongoing Research and Threat Intelligence
    - Research Security Implications of Emerging Business Tools
    - Global IA Industry/Community
18. **Security Activities in the Technology Life Cycle**
    - Systems and Software Development Life Cycle
    - Adapt Solutions and Asset Management (Inventory Control)
19. **Business Unit Interaction**
    - Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines
    - Provide Objective Guidance and Impartial Recommendations to Staff and Management on Security Processes and Controls
    - Establish Effective Collaboration Within Teams to Implement Secure Solutions
    - Governance, Risk, and Compliance Committee
20. **Exam Preparation**

Durée, prix :

Formation	Jours	Prix	Prix/j
CompTIA Advanced Security Practitioner, certification CASP+	5	3'750.-	750.-

Selon conditions générales. Le prix comprend toute la documentation distribuée.
Le prix de l'examen de EUR 466.- (tarif 2021) n'est pas compris.
Les cours se déroulent de 09:00 à 12:00 et de 13:30 à 17:00