

# Préparation à la certification officielle Cisco Certified CyberOps Associate // #3049

 84 h

## Public

Les professionnels du secteur informatique, opérateurs, techniciens, ingénieurs, consultants, responsables informatiques et gestionnaires de réseaux informatiques ou toute personne souhaitant orienter sa carrière dans ce domaine.

## Objectifs

Le programme "Cisco Certified CyberOps Associate" fournit une première étape dans l'acquisition des connaissances et des compétences nécessaires pour travailler avec une équipe en charge des opérations de sécurité informatique, et peut être un élément précieux pour commencer une carrière dans ce domaine. Le cours est fourni via l'environnement d'apprentissage Cisco NetAcad.com.

Cette formation est agréée Chèques-Formation sous le numéro 3049 : en voici le lien direct : [fiche agréée chèque-formation. \(https://www.leforem.be/catalogue-des-formations/formations/b607382d-5449-4d35-84bd-693f863de087\)](https://www.leforem.be/catalogue-des-formations/formations/b607382d-5449-4d35-84bd-693f863de087) Cette fiche se retrouve dans le [Catalogue wallon des formations \(https://www.leforem.be/catalogue-des-formations\)](https://www.leforem.be/catalogue-des-formations) et vous pouvez aussi utiliser le numéro d'agrément dans la recherche par mot-clé. Le titre de la formation peut varier d'un catalogue à l'autre, sans incidence sur la validité du numéro d'agrément.

Le cours est fourni via l'environnement d'apprentissage Cisco NetAcad.com. Plus d'informations [https://www.cisco.com/c/dam/en\\_us/training-events/certifications/shared/docs/cyber-ops-at-a-glance.pdf](https://www.cisco.com/c/dam/en_us/training-events/certifications/shared/docs/cyber-ops-at-a-glance.pdf) ([https://www.cisco.com/c/dam/en\\_us/training-events/certifications/shared/docs/cyber-ops-at-a-glance.pdf](https://www.cisco.com/c/dam/en_us/training-events/certifications/shared/docs/cyber-ops-at-a-glance.pdf))

- Cybersécurité et centre des opérations de sécurité
- Système d'exploitation Windows
- Système d'exploitation Linux
- Protocoles et services réseaux
- Infrastructure réseaux
- Principes de la sécurité des réseaux
- Attaques de réseaux
- Protéger les réseaux
- Cryptographie et infrastructure
- Sécurité et analyse des terminaux
- Surveillance de la sécurité
- Analyse des données d'intrusion
- Réponse et traitement des incidents

## Version anglaise détaillée:

### Chapter 1. Cybersecurity and the Security Operations Center

- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain why networks and data are attacked.
- Explain how to prepare for a career in Cybersecurity operations.

## Chapter 2. Windows Operating System

- Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
- Explain the operation of the Windows Operating System.
- Explain how to secure Windows endpoints.

## Chapter 3. Linux Operating System

- Explain the features and characteristics of the Linux Operating System.
- Perform basic operations in the Linux shell.
- Perform basic Linux administration tasks.

## Chapter 4. Network Protocols and Services

- Analyze the operation of network protocols and services.
- Explain how the Ethernet and IP protocols support network communications and operations
- Explain how network services enable network functionality.

## Chapter 5. Network Infrastructure

- Explain network topologies and the operation of the network infrastructure.
- Explain how network devices
- Explain how devices and services are used to enhance network security.

## Chapter 6. Principles of Network Security

- Classify the various types of network attacks.
- Explain how networks are attacked.
- Explain the various types of threats and attacks.

## Chapter 7. Network Attacks: A Deeper Look

- Use network monitoring tools to identify attacks against network protocols and services.
- Explain network traffic monitoring.
- Explain how TCP/IP vulnerabilities enable network attacks.
- Explain how common network applications and services are vulnerable to attack.

## Chapter 8. Protecting the Network

- Use various methods to prevent malicious access to computer networks, hosts, and data.
- Explain approaches to network security defense.
- Use various intelligence sources to locate current security threats.

## Chapter 9. Cryptography and the Public Key Infrastructure

- Explain the impacts of cryptography on network security monitoring.
- Use tools to encrypt and decrypt data.
- Explain how the public key infrastructure (PKI) supports network security

## Chapter 10. Endpoint Security and Analysis

- Explain endpoint vulnerabilities and attacks investigation process.
- Use tools to generate a malware analysis report.
- Classify endpoint vulnerability assessment information.

## Chapter 11. Security Monitoring

- Evaluate network security alerts.

- Explain how security technologies affect security monitoring.
- Explain the types of log files used in security monitoring.

#### Chapter 12. Intrusion Data Analysis

- Analyze network intrusion data to identify compromised hosts and vulnerabilities
- Explain how security-related data is collected.
- Analyze intrusion data to determine the source of an attack.

#### Chapter 13. Incident Response and Handling

- Explain how network security incidents are handled by CSIRTs.
- Apply incident response models, such as NIST 800-61r2 to a security incident.
- Use a set of logs to isolate threat actors and recommend an incident response plan.

*Cette formation sera animée par Guillaume DAMSIN, Consultant Senior en Réseaux et Sécurité IT, ainsi qu'Instructeur Cisco NetAcad.*

*Notre formateur est expérimenté et détient de nombreuses certifications, notamment : Cisco CCNP Enterprise, CCNP Security, CyberOps Associate, CCNA, Wireshark WCNA, Fortinet FCSS in Security Operations, Security Operations 6.7 Architect, FCP in Security Operations, Microsoft MCSA & ITIL Foundation.*

*Pour en savoir plus, visitez son profil Credly: <https://www.credly.com/users/guillaumedamsin> (<https://www.credly.com/users/guillaumedamsin>)*

© 2018 Cisco and/or its affiliates

## Informations pratiques

### > Droit d'inscription

- ✓ Cette formation est agréée "chèques formation".

### > Certificat - Attestation

Attestation de participation.

### > Aides sectorielles à la formation

Pouvez-vous bénéficier d'une aide sectorielle ? Pour en savoir plus, consultez l'onglet **Fonds sectoriels de formation** (<http://www.formation-continue.be/vpage-1195-2-Fonds-sectoriels-de-formation>)

### > Reconnaissance

Le Centre IFAPME Liège-Huy-Verviers est reconnu comme Académie CISCO officielle.  
Plus d'informations sur les académies CISCO sur **Netacad**.



