Programme de formation

Cybersecurité • promo 2023

des codeuses_

Networking Academy

Programme de formation

Cybersecurité • promo 2023

des codeuses_

Networking Academy

Table des matières

1

Présentation de la formation

1.1. Descriptif de la formation

Le programme de formation en cybersécurité de DESCODEUSES prépare les apprenantes à des opportunités d'apprentissage en tant que non professionnelles de la cybersécurité. Développé avec le soutien de la Cisco Networking Academy, ce programme permet aux apprenantes d'acquérir les connaissances et compétences tactiques requises pour intégrer des équipes de Centre Opérationnel de Sécurité (SOC) afin de détecter et répondre aux menaces de cybersécurité. Il prépare également les apprenantes à la certification Cisco CyberOps Associate, qui valide leur expertise dans ce domaine.

Les objectifs et résultats du programme de cybersécurité sont conformes à la mission de DESCODEUSES, qui vise à offrir des programmes professionnels entièrement accrédités et compétitifs au niveau national pour les licences et les cycles supérieurs. Les diplômées peuvent ainsi bénéficier d'une employabilité immédiate après l'obtention de leur diplôme, ainsi que de la possibilité de poursuivre des études de niveau avancé dans des disciplines connexes.

1.2. La durée, le rythme et la modalité

- 6 mois de formation
- 100% en Présentiel
- 6 mois de stage en entreprise
- Effectifs par groupe : 16 apprenantes.

1.3. Principale méthode pédagogique appliquée

Learning by doing

Learning by doing (L'apprentissage par l'action) est une approche éducative qui met l'accent sur l'importance de l'expérience pratique dans le processus d'apprentissage. Cette approche suggère que les individus peuvent acquérir des connaissances et des compétences plus efficacement en s'engageant activement dans des tâches pratiques plutôt qu'en consommant simplement passivement des informations.

Cette approche est basée sur l'idée que les gens apprennent mieux lorsqu'ils sont activement impliqués dans le processus d'apprentissage, plutôt que de simplement observer ou écouter quelqu'un d'autre leur expliquer les choses. En faisant réellement quelque chose, les apprenants peuvent acquérir une compréhension plus profonde de la matière, développer des compétences en résolution de problèmes et renforcer leur confiance en leurs capacités.

Dans l'ensemble, l'apprentissage par l'action encourage les apprenants à prendre un rôle actif dans leur propre éducation, à expérimenter et à explorer, et à apprendre de leurs erreurs alors qu'ils acquièrent de nouvelles connaissances et compétences.

1.4. Méthodes d'évaluation

En amont

L'analyse préalable des connaissances et des besoins des apprenantes lors des entretiens permet :

- D'optimiser le temps de formation et de définir un contenu approprié aux besoins spécifiques individuels et collectifs
- D'identifier les attentes et définir les objectifs visés,
- D'identifier le profil du groupe pour développer des exercices et des études de cas adaptés à l'environnement de chacun

Durant la formation

- Points d'étapes réguliers tous les deux mois sur la compréhension des stagiaires, leurs attentes et leurs demandes
- Rétrospective en fin de projet pour ajustements éventuels de la suite du parcours
- Fiche de suivi des compétences indiquant les acquis à la fin de chaque projet module
- Journal de bord des apprenantes.

Soutenance pour le titre professionnel

La réalisation d'un projet individuel répondant aux attentes du titre professionnel d'Analyste SOC.

L'évaluation consiste en une soutenance devant le jury constitué de 3 membres minimum :

- 1 jury habilité par le ministère de l'Éducation nationale
- 1 jury responsable DesCodeuses
- jury professionnel du secteur avec 5 ans d'expérience minimum.

Sera aussi évalué en amont de la soutenance votre dossier professionnel regroupant la description de toutes vos activités liées aux blocs de compétences du titre professionnel visé.

1.5. L'accompagnement pédagogique & socio-professionnel

L'accompagnement pédagogique

DESCODEUSES fournit un accompagnement complet aux stagiaires pour les engager et éviter les abandons, notamment en offrant un soutien pédagogique comprenant des encouragements à la solidarité de groupe et à la cohésion d'équipe, ainsi qu'un mentorat collectif et individuel pour aider les apprenantes à progresser dans leur apprentissage.

L'accompagnement socio-professionnel

L'équipe DesCodeuses s'investit dans le domaine social en proposant diverses initiatives :

- Un accompagnement personnalisé permettant de réorienter les apprenantes vers les services d'accompagnement sociaux appropriés en fonction de leurs besoins.
- Des ateliers de coaching, dirigés par la communauté et l'équipe, sont organisés pour renforcer la confiance en soi.
- En outre, des simulations d'entretiens professionnels avec des entreprises partenaires sont proposées pour faciliter l'entrée sur le marché du travail, ainsi que la mise en pratique de techniques de recherche d'emploi et de stage.

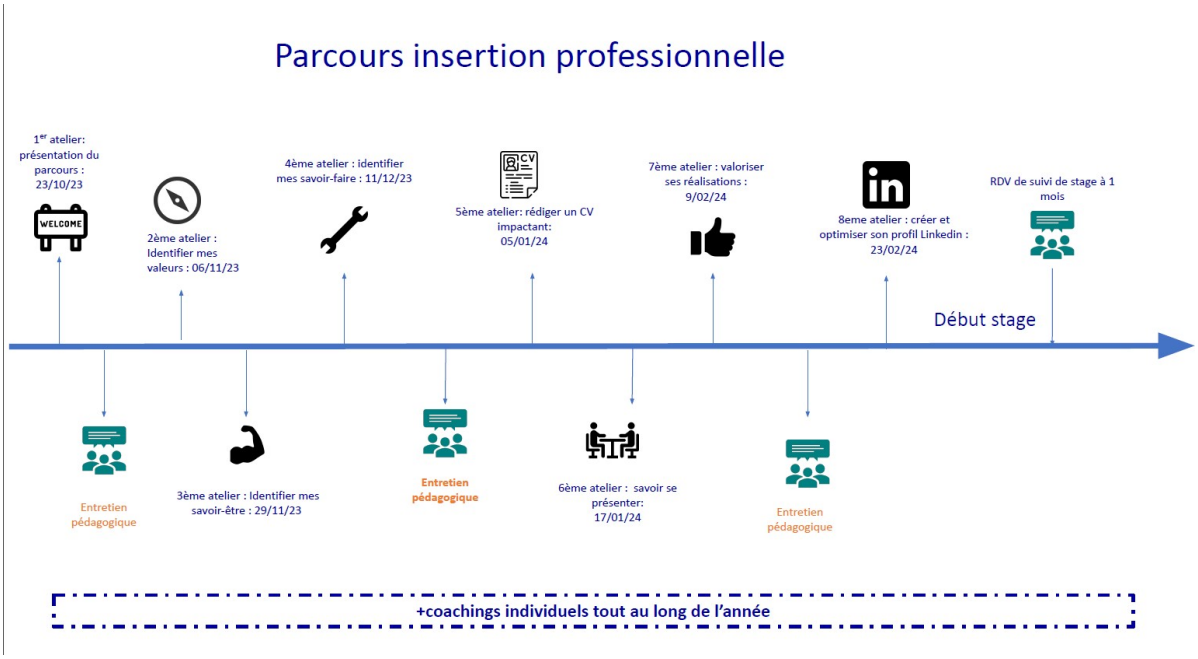

Figure 1.1 – Planning du parcours d'insertion professionnelle

1.6. Calendrier et organisation de la formation

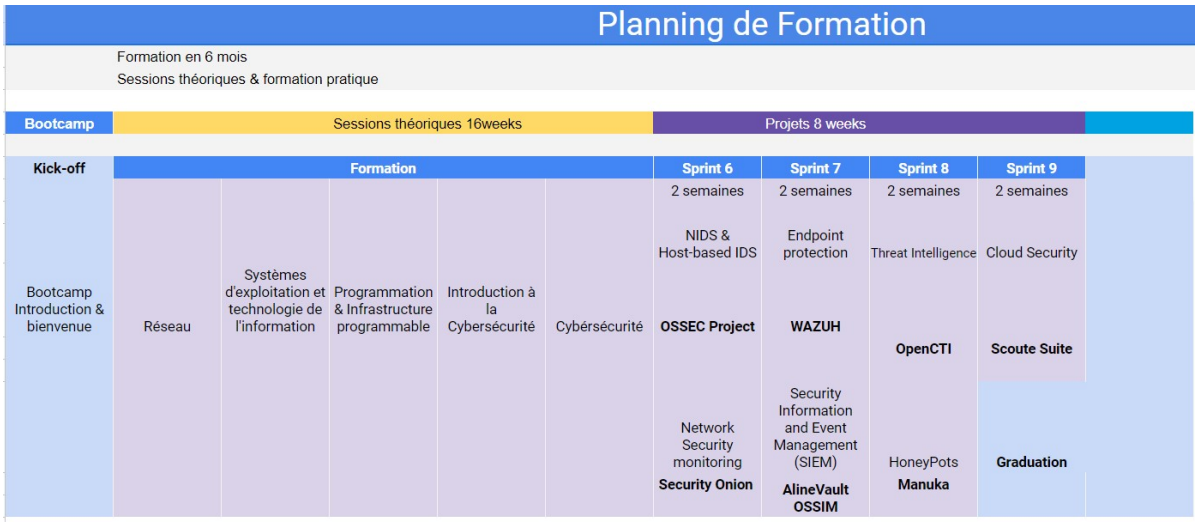

Figure 1.2 – Planning du parcours

- Lieu : 124 Rue des Rosiers, 93400 St-Ouen-sur-Seine
- Ouverture des inscriptions : 12/06/2023
- Lancement Préqualifications (place limitée à 30) : 09/10/2023
- Début de formation : 27/11/2023

Inscription et modalités d'accès :

- S'inscrire sur le formulaire : descodeuses.org/inscription/
- Recevoir un parcours de présélection à Compléter dans délais qui vous sera communiqué par mail.

- Passer un entretien avant le début de la préqualification.
- Participer au parcours de pré-qualifications.
- Passer un entretien d'admission 3 semaines avant le début de formation.

Tarifs

- Formation gratuite intégralement financée
- Rémunérée pour les demandeuses d'emploi ((financement Pôle Emploi)

Méthodes mobilisées

- Apprentissage par projets professionnels
- Des cours et apports théoriques
- Les mise en situation et les études de cas
- L'assimilation en autonomie sur la Cisco Networking Academy, la plateforme de formation de Cisco
- Accompagnement sur mesure pour l'insertion professionnelle.

Accessibilité

- Accessibilité DesCodeuses met un point d'honneur à proposer des formations inclusives et est en capacité d' accueillir les personnes reconnues RQTH et d'adapter les conditions matérielles. Notre référente handicap est l'interlocutrice privilégiée du public apprenant en situation de handicap afin d'identifier les aménagements nécessaires à mettre en place.

2

Objectifs et Débouchés

2.1. Découverte du métier et débouchés

En tant qu'analyste SOC, vous serez responsable de la surveillance et de l'analyse des activités de sécurité informatique pour protéger les systèmes et les données de votre organisation contre les cyberattaques. Les analystes SOC surveillent les journaux d'événements de sécurité et les alertes pour identifier les menaces potentielles et évaluent la gravité des incidents de sécurité. Les analystes SOC sont très recherchés en France en raison de la croissance de la cybercriminalité, offrant ainsi de bonnes perspectives d'emploi dans le marché de la sécurité informatique qui devrait continuer à croître dans les prochaines années. Les analystes SOC sont l'une des fonctions les plus demandées dans le domaine de la sécurité informatique en France, avec une augmentation de la demande de 29% par rapport à l'année précédente, offrant ainsi des salaires moyens attractifs en fonction de l'expérience et des compétences.

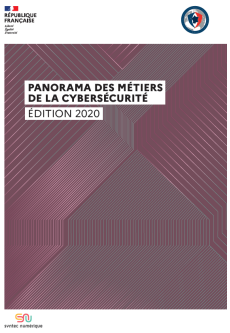

Figure 2.1 – Panorama des métiers de la cybersécurité

2.2. Les besoins du marché

Selon différentes études et analyses de l'écosystème de la cybersécurité en France, il existe une forte demande pour les analystes SOC en raison de la croissance continue des cybermenaces et de la nécessité pour les entreprises de protéger leurs données sensibles. Voici quelques chiffres pour étayer cette affirmation :

- Selon le Baromètre de la cybersécurité en France 2020, réalisé par OpinionWay pour le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), 83% des entreprises françaises ont subi au moins une cyberattaque en 2019. Cela souligne la nécessité d'avoir des professionnels de la sécurité qualifiés pour protéger les réseaux et les données.
- Selon une étude de Gartner, le marché mondial des services de sécurité informatique devrait atteindre 170 milliards de dollars d'ici 2022, ce qui montre la croissance rapide de la demande pour les services de cybersécurité.
- Le rapport sur l'emploi dans la cybersécurité en France publié en 2020 par le cabinet de recrutement Robert Walters montre que les postes les plus demandés en cybersécurité sont les analystes SOC, les ingénieurs de sécurité et les experts en gestion des risques. Selon le rapport, les analystes SOC sont en tête de liste avec une forte demande de la part des employeurs.
- Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il y a eu une augmentation de 60% du nombre d'incidents de sécurité informatique en France entre 2018 et 2019. Cette augmentation souligne la nécessité pour les entreprises de renforcer leur sécurité et de recruter des professionnels de la cybersécurité qualifiés.
- Le marché ouvert comptait plus de 15 000 offres d'emploi dans le domaine de la cybersécurité en 2019, selon une étude publiée par l'ANSSI. Ce chiffre est en constante évolution en raison de la pénurie de talents en cybersécurité et de la croissance du nombre des cyberattaques.

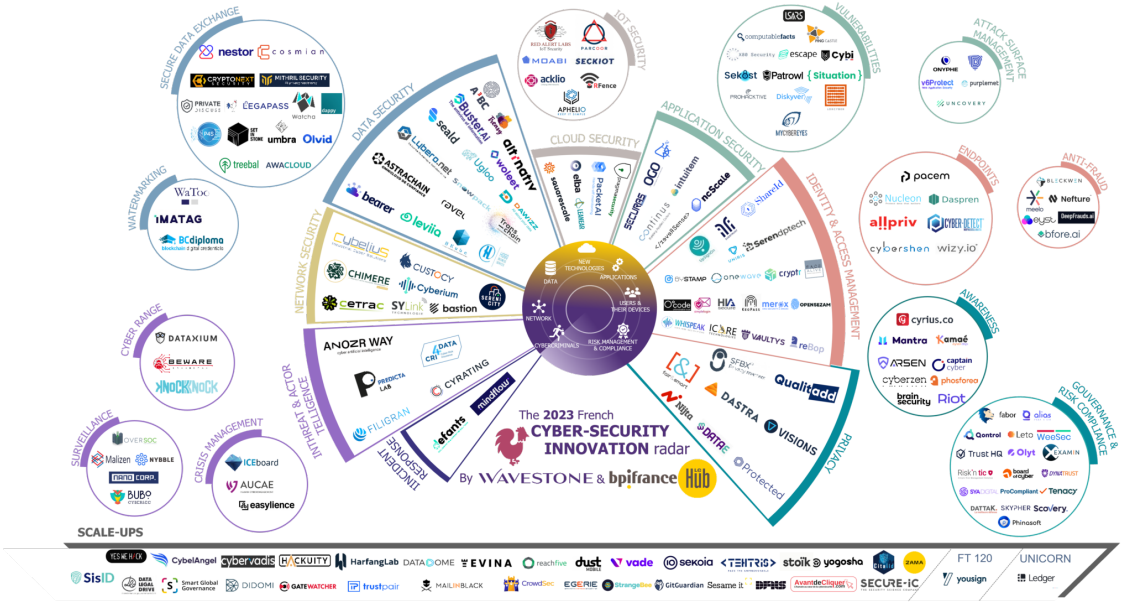

Figure 2.2 – L'écosystème des startups cybersécurité française 2023

Lecture > 166 startups, 24 scale-ups, 1 licorne cyber et 630M€ de fonds levés : tels sont les chiffres de l'édition 2023 du radar Wavestone des startups cybersécurité françaises.
Source > Radar des startups cybersécurité française 2023 - Wavestone.

Une étude réalisée par la Bpifrance, France Digitale, le Campus Cyber, le Secrétariat Général pour l'Investissement et Wavestone démontrent un développement considérable de l'écosystème d'innovation cybersécurité [1].

2.3. Les qualités et compétences requises

Pour réussir en tant qu'analyste en cybersécurité, il est crucial d'avoir à la fois des compétences techniques solides et une compréhension approfondie des projets. Les qualités essentielles pour ce poste incluent :

- Connaissances techniques : un analyste SOC doit avoir une solide compréhension des réseaux informatiques, des protocoles de sécurité, des systèmes d'exploitation, des logiciels malveillants, des outils de détection et de réponse aux incidents, des pare-feux, des serveurs de journaux, des bases de données, des environnements virtuels, et des technologies cloud. Il doit également être capable de comprendre et d'analyser les journaux et les alertes de sécurité.
- Compétences en résolution de problèmes : un analyste SOC doit être capable de résoudre rapidement et efficacement les incidents de sécurité. Il doit être en mesure d'identifier les causes profondes des incidents et de prendre des mesures pour les résoudre.
- Aptitude à la communication : un analyste SOC doit être en mesure de communiquer efficacement avec les membres de l'équipe, les parties prenantes externes, et les clients. Il doit être capable de fournir des rapports clairs et précis sur les incidents de sécurité.
- Esprit d'équipe : un analyste SOC travaille en étroite collaboration avec les membres de l'équipe de sécurité, les administrateurs système, les ingénieurs réseau, et les autres parties prenantes. Il doit être capable de travailler en équipe et de collaborer avec les autres membres de l'équipe pour résoudre les incidents de sécurité.
- Compétences en veille technologique : un analyste SOC doit être à jour sur les dernières tendances en matière de sécurité informatique et les menaces émergentes. Il doit être en mesure

1. (*Radar des startups cybersécurité française 2022*. url : https://www.wavestone.com/fr/insight/radar-startups-cybersecurite-2022/)

de surveiller les sites de sécurité, les forums de discussion, les blogs et les réseaux sociaux pour détecter les nouvelles menaces et les vulnérabilités.
- Capacité à travailler sous pression : un analyste SOC doit être en mesure de travailler sous pression, car les incidents de sécurité peuvent survenir à tout moment et nécessitent une réponse rapide.

2.4. Le salaire d'un analyste SOC

Le salaire d'un analyste SOC en France varie selon plusieurs facteurs tels que l'expérience, le niveau de responsabilité, la localisation géographique, la taille de l'entreprise, etc. Les débutants peuvent s'attendre à un salaire brut annuel de 30 000 € à 40 000 €, tandis que les plus expérimentés peuvent gagner 60 000 € à 80 000 € ou plus s'ils ont des responsabilités de gestion d'équipe. Cependant, ces chiffres sont des indications générales et peuvent varier selon chaque entreprise et chaque individu.

2.5. Pourquoi ce former au métier ?

Les entreprises sont de plus en plus conscientes de l'importance de la sécurité informatique et de la nécessité d'avoir une équipe dédiée pour surveiller, détecter et prévenir les cyberattaques.

Quelques raisons pour lesquelles il est important de se former au métier d'analyste SOC en France :

- Forte demande : Selon une étude récente de Pôle emploi, le nombre d'offres d'emploi pour les analystes SOC a augmenté de 98 % en France en 2020 par rapport à l'année précédente. Il y a donc une forte demande pour les professionnels de la sécurité informatique, en particulier ceux qui ont une expérience en matière d'analyse SOC.
- Salaire attractif. Ce dernier est généralement plus élevé que celui d'autres professions dans le domaine de la sécurité informatique.
- Évolution de carrière : Avec de l'expérience, un analyste SOC peut évoluer vers des postes de direction ou de gestion de la sécurité informatique, tels que chef de SOC ou responsable de la sécurité informatique. Cela offre une opportunité d'évolution de carrière intéressante pour les professionnels de la sécurité informatique.
- Importance de la sécurité informatique : Les cyberattaques et les cybermenaces sont de plus en plus fréquentes et sophistiquées. Les entreprises ont donc besoin de professionnels qualifiés pour surveiller leur système d'information, détecter les menaces et prendre des mesures pour les prévenir.

Les femmes sont peu représentées dans le domaine

- Les femmes sont en effet peu représentées dans les métiers de la cybersécurité. Selon une étude menée par l'ISC2 en 2021 sur la diversité dans la cybersécurité, seulement 24% des professionnels de la cybersécurité sont des femmes.
- De plus, une enquête menée par l'agence européenne pour la sécurité des réseaux et de l'information (ENISA) a révélé que seulement 7% des professionnels de la cybersécurité en Europe étaient des femmes.
- Il est important de noter que cette sous-représentation des femmes n'est pas due à un manque d'intérêt pour le domaine de la cybersécurité. En effet, une étude menée par l'ISC2 en 2019 a révélé que 51% des femmes interrogées ont déclaré être intéressées par une carrière dans la cybersécurité, contre 39% des hommes.ans ce domaine.

3

Contenu Pédagogique

3.1. Réseau

3.1.1. Notions de base sur le réseau

Présentation du cours

Le cours suivant aborde l'ensemble des notions basiques du réseau informatique, des équipement réseau, supports et protocoles. Les apprenantes auront acquis à travers ce cours le savoir nécessaire permettant d'effectuer une configuration de base des équipements pour une connexion au réseau.

Prérequis :
aucun

Durée du cours :
25H

Objectifs
- Configuration d'un retour et hôte sans fils pour une connexion à internet.
- Une compréhension des protocoles, équipements et autres supports permettant d'établir une communication réseaux Ethernet.
- Créer un LAN simple.
- Une compréhension de la communication assurée par les adresses IP.

3.1.2. Équipements réseau et Configuration de base

Présentation du cours

Ce cours enseigne les compétences et les connaissances de niveau intermédiaire en matière de réseau en détaillant les concepts et les compétences fondamentales requises pour établir un réseau pour domicile ou pour un petit bureau.

Prérequis :
aucun

Durée du cours :
25H

Objectifs
- Acquérir une connaissance pratique de l'utilisation de l'Ethernet dans un réseau commuté.
- Comprendre comment les routeurs utilisent les protocoles et les services de la couche réseau pour transmettre des données.
- Explorer comment le protocole TCP (Transmission Control Protocol) assure la distribution fiable des données sur un réseau.
- Mettre en place un réseau informatique de base avec des équipements Cisco en utilisant les connaissances acquises.

3.1.3. Premiers pas avec Cisco Packet Tracer

Présentation du cours

Le cours d'initiation vise à familiariser les apprenants avec Cisco Packet Tracer, un outil de simulation et de visualisation de réseau novateur. Les objectifs sont de comprendre comment télécharger l'outil, de se familiariser avec son interface et d'apprendre à créer un réseau en utilisant des exemples concrets pour s'entraîner.

Prérequis :
aucun

Durée du cours :
5H

Objectifs
- Apprendre à télécharger et installer Cisco Packet Tracer, un outil de simulation et de visualisation de réseau performant.
- Utiliser Cisco Packet Tracer pour appliquer ses compétences en réseau, cybersécurité et IoT en créant et en simulant des exemples concrets.

3.1.4. Exploration d'un réseau avec Cisco Packet Tracer

Présentation du cours

Dans ce cours, les étudiants apprennent à créer et à gérer un petit réseau de bureau en utilisant Cisco Packet Tracer. Ils acquièrent des compétences pour connecter et configurer différents équipements de réseau, y compris les périphériques sans fil, et pour surveiller et gérer efficacement le réseau. Le cours fournit également des conseils précieux pour mettre en pratique les compétences acquises avec Cisco Packet Tracer.

Prérequis :
aucun

Durée du cours :
5H

Objectifs
- Acquérir les compétences pour configurer et connecter les équipements d'un réseau de petit bureau à l'aide de Packet Tracer
- Comprendre le fonctionnement des paquets sur un réseau grâce au mode de simulation disponible dans Packet Tracer
- Explorer l'utilisation d'un contrôleur réseau pour la gestion et la configuration d'un réseau.

3.1.5. Les notions fondamentales du réseau

Présentation du cours

Ce cours aborde le domaine des réseaux dans des contextes courants tels que les petites entreprises ou les bureaux à domicile, afin de fournir aux étudiants une expérience immersive et autonome. Les étudiants pourront utiliser une simulation Packet Tracer, des exercices interactifs et même des équipements disponibles chez eux pour renforcer leurs compétences.

Prérequis :
aucun

Durée du cours :
60H

Objectifs
- Pour les développeurs, les spécialistes de la cybersécurité, les analystes commerciaux ou les autres professionnels : acquérir des connaissances de base sur les réseaux
- Pour les étudiants : un point de départ pour diverses carrières, de la cybersécurité au développement logiciel, en passant par le commerce.

3.2. Systèmes d'exploitation et technologie de l'information

3.2.1. Les Fondamentaux de l'IT

Présentation du cours

IT Essentials est axé sur l'enseignement des compétences informatiques et professionnelles fondamentales requises pour des postes débutants dans le domaine de l'informatique. Les étudiants auront l'opportunité de développer leurs compétences en apprenant les procédures nécessaires pour installer, configurer et dépanner des ordinateurs, des appareils mobiles et des logiciels.

Prérequis :
aucun

Durée du cours :
30H

Objectifs
- Acquérir les compétences requises pour les postes d'assistant technique de niveau débutant dans le domaine de la technologie
- Se préparer efficacement à l'examen de certification CompTIA A+ pour renforcer ses compétences techniques
- Acquérir les connaissances de base nécessaires pour poursuivre des cours de niveau CCNA en matière de réseau.

3.2.2. Le système d'exploitation Linux

Présentation du cours

Ce cours aborde les connaissances essentielles relatives au système d'exploitation back-end. Il permet d'apprendre les bases de l'installation et de la configuration de Linux ainsi que l'utilisation de la ligne de commande Linux. Les principes fondamentaux du système d'exploitation, de la ligne de commande et des concepts de programmation open source de Linux sont également présentés dans ce cours.

Prérequis :
aucun

Durée du cours :
60H

Objectifs

- Découvrir Linux et évaluer votre intérêt à en apprendre davantage
- Acquérir des connaissances de base en informatique
- Explorer les opportunités de carrière associées à ces compétences
- Développer des compétences de base en systèmes d'exploitation pour des postes IT débutants
- Se préparer à l'examen de certification LPI Satisfaire les prérequis pour approfondir vos compétences en informatique et en réseau.

3.3. Programmation

3.3.1. Python I

Présentation du cours

Ce cours enseigne des compétences très recherchées dans le domaine de l'informatique, telles que la conception, le développement et l'amélioration de programmes en utilisant le langage de programmation Python.

Prérequis :
aucun

Durée du cours :
30H

Objectifs

- Découvrir le domaine de la programmation informatique et les métiers qui y sont associés.
- Acquérir des compétences en codage grâce à Python.
- Apprendre les fondamentaux tels que les types de données, les variables, les entrées/sorties, le contrôle de flux et d'autres fonctions essentielles.

3.4. Infrastructure programmable

3.4.1. Introduction à l'IoT et aux transformations digitales

Présentation du cours

Ce cours fournit une perspective générale sur l'Internet des objets (IoT) et explique comment la transformation numérique affecte les entreprises, les administrations publiques, les différents secteurs d'activité ainsi que notre vie quotidienne.

Prérequis :
aucun

Durée du cours :
8H

Objectifs

- Acquérir des connaissances numériques fondamentales
- Explorer les opportunités de carrière dans le domaine des technologies émergentes

3.5. Cybersécurité

3.5.1. Introduction à la cybersécurité

Présentation du cours

Dans ce cours, sont abordées les tendances actuelles en matière de cybersécurité, les menaces qui pèsent sur les données personnelles et professionnelles, ainsi que les solutions de protection correspondantes.

Prérequis :
aucun

Durée du cours :
6H

Objectifs
- Rendre la cybersécurité accessible à tous pour une meilleure protection de la vie numérique.
- Explorer les différentes opportunités de carrière dans le domaine de la cybersécurité.

3.5.2. Les concepts fondamentaux de la cybersécurité

Présentation du cours

Dans ce cours, vous acquerrez les connaissances essentielles dans les domaines de la cybersécurité, notamment la sécurité des informations, des systèmes et du réseau, l'éthique et les lois, ainsi que les techniques de protection et de réduction des risques dans une entreprise.

Prérequis :
aucun

Durée du cours :
30H

Objectifs
- Acquérir les connaissances fondamentales en matière de cybersécurité.
- Découvrir les différentes possibilités de carrière offertes par le domaine de la cybersécurité.
- Orienter les apprenants entre une carrière en réseau et une carrière en cybersécurité.

3.5.3. Sécurité des terminaux

Présentation du cours

Dans ce cours, vous apprendrez comment évaluer les vulnérabilités du réseau, des systèmes d'exploitation et des terminaux, ainsi que les méthodes pour sécuriser le réseau. Il couvre également les compétences nécessaires pour préserver l'intégrité, la confidentialité et la disponibilité du réseau et des données.

Prérequis :
aucun

Durée du cours :
40H

Objectifs

- Acquérir les connaissances fondamentales de la cybersécurité
- Découvrir les diverses opportunités de carrière dans le domaine de la cybersécurité
- Développer des compétences pour sécuriser un réseau de bout en bout, y compris le matériel, les logiciels et les supports

3.5.4. Défense du réseau

Présentation du cours

Dans ce cours, plusieurs méthodes de surveillance du réseau et d'analyse des alertes de sécurité sont décrites. Vous apprendrez également les outils et les techniques utilisés pour protéger le réseau, y compris les contrôles d'accès, les pare-feu, la sécurité du cloud et le chiffrement.

Prérequis :
aucun

Durée du cours :
40H

Objectifs

- Acquérir les bases de la cybersécurité
- Explorer les différentes voies professionnelles offertes par le domaine de la cybersécurité
- Développer les compétences nécessaires pour élaborer une stratégie de cybersécurité efficace à plusieurs niveaux

3.5.5. Gestion des Cybermenaces

Présentation du cours

Dans ce cours, vous découvrirez la gouvernance de la cybersécurité et la gestion des menaces. Vous apprendrez à développer des politiques et à vous assurer que votre entreprise respecte les normes éthiques ainsi que les cadres juridiques et réglementaires.

Prérequis :
aucun

Durée du cours :
20H

Objectifs

- Acquérir des connaissances fondamentales en cybersécurité.
- Explorer les différentes opportunités de carrière dans le domaine de la cybersécurité.
- Développer des compétences en gestion des menaces, notamment en évaluant les vulnérabilités du réseau, en gérant les risques et en répondant aux incidents de sécurité.

4

Projets

4.1. Host-based Analysis

Le projet OSSEC (Open Source HIDS SECurity) est une solution open source de détection d'intrusions basée sur l'hôte, conçue pour aider les administrateurs à surveiller les activités de sécurité des serveurs, des postes de travail et des applications.

- Le projet OSSEC utilise un agent installé sur chaque machine à surveiller, qui collecte des informations de sécurité telles que les journaux d'événements, les fichiers de configuration, les modifications de fichiers et les activités réseau. Les informations collectées sont envoyées à un serveur centralisé pour analyse et stockage.
- OSSEC est capable de détecter les intrusions, les attaques par déni de service, les tentatives d'exploitation de vulnérabilités et les comportements malveillants. Il fournit également une surveillance de l'intégrité des fichiers, de la conformité réglementaire et des activités d'utilisateurs.
- OSSEC est hautement personnalisable, avec des règles de détection configurables, des notifications d'alerte et des options de réponse automatisées. Il prend également en charge l'intégration avec des outils tiers tels que Nagios, Splunk et OpenVAS.
- Le projet OSSEC-HIDS est une extension d'OSSEC qui fournit une fonctionnalité supplémentaire pour la détection d'intrusion sur les serveurs de production. Cette extension inclut des règles spécifiques pour la détection d'attaques connues sur des applications web populaires telles que Apache, IIS et Tomcat, ainsi que des règles pour la surveillance des journaux de base de données.

4.2. Network Security monitoring

Security Onion est une distribution Linux spécifiquement conçue pour détecter les intrusions dans les réseaux. Elle intègre plusieurs outils populaires de sécurité réseau tels que Snort, Suricata, Zeek, Bro, Sguil, Squert, ELSA, Xplico, et bien d'autres encore.

- Installer Security Onion sur une machine dédiée : Vous pouvez télécharger l'image ISO de Security Onion à partir du site web officiel et l'installer sur une machine dédiée. Vous pouvez également utiliser des machines virtuelles pour tester la solution.
- Configurer le réseau : Une fois que Security Onion est installé, vous devez configurer le réseau pour permettre la surveillance de tous les flux de trafic réseau. Vous pouvez configurer un switch pour copier tout le trafic vers le port sur lequel la machine Security Onion est connectée ou utiliser un hub pour connecter tous les périphériques au réseau.
- Configurer les règles de détection d'intrusion : Security Onion utilise des outils de détection d'intrusion tels que Snort et Suricata pour analyser les paquets réseau en temps réel. Vous devez configurer ces outils pour qu'ils utilisent les règles appropriées pour détecter les attaques connues et inconnues.
- Configurer Zeek pour l'analyse de protocole : Zeek (anciennement appelé Bro) est un outil d'analyse de protocole réseau qui peut être utilisé pour détecter les anomalies de réseau. Vous devez configurer Zeek pour qu'il analyse les flux de trafic réseau et génère des journaux pour une analyse ultérieure.
- Configurer Wazuh pour la surveillance des hôtes : Wazuh est un système de détection de menaces et de réponse (TDR) qui peut être utilisé pour surveiller les hôtes du réseau. Vous pouvez installer l'agent Wazuh sur tous les hôtes et configurer le serveur Wazuh pour collecter les journaux de tous les agents et détecter les menaces potentielles.
- Utiliser Kibana pour visualiser les données de sécurité : Kibana est une interface web qui peut être utilisée pour visualiser et analyser les données de sécurité collectées par Security Onion. Vous pouvez utiliser Kibana pour créer des tableaux de bord et des graphiques pour une meilleure compréhension des menaces potentielles.

4.3. Endpoint protection

Wazuh est un système open source qui permet de détecter et répondre aux menaces de sécurité sur les endpoints tels que les ordinateurs de bureau, les serveurs et les appareils mobiles. Pour mettre en place une solution de détection et de réponse avec Wazuh, voici les étapes à suivre :

- Installer les agents Wazuh sur les endpoints : Les agents Wazuh doivent être installés sur tous les endpoints à surveiller pour collecter les données sur les événements système et les activités des utilisateurs.
- Configurer la surveillance des endpoints : Wazuh surveille en temps réel l'activité des endpoints pour détecter les comportements malveillants. Vous pouvez configurer les règles de surveillance pour détecter des activités suspectes telles que la modification de fichiers système, l'accès à des fichiers sensibles, l'installation de logiciels malveillants, etc.
- Analyser les alertes générées par Wazuh : Les alertes générées peuvent être consultées dans l'interface utilisateur de Wazuh ou envoyées à un système SIEM. Elles contiennent des informations détaillées sur l'activité suspecte détectée, notamment les fichiers impliqués, les processus, les utilisateurs et les adresses IP.
- Effectuer une analyse de réponse à l'incident : En cas d'alerte, il est important de comprendre l'étendue de l'attaque et de prendre les mesures nécessaires pour y remédier. Wazuh fournit des outils pour aider les équipes de sécurité à enquêter sur les alertes et à effectuer une analyse de réponse à l'incident.

4.4. Security Information and Event Management (SIEM)

AlienVault OSSIM (Open Source Security Information and Event Management) est une plateforme open source de gestion des informations et des événements de sécurité conçue pour aider les entreprises à surveiller et protéger leur réseau contre les menaces de sécurité. Voici les étapes pour utiliser OSSIM :

- Installation d'OSSIM : OSSIM peut être installé sur une machine physique ou virtuelle sous Linux. La dernière version d'OSSIM peut être téléchargée sur le site Web d'AlienVault. OSSIM nécessite une interface réseau pour capturer les données réseau, et vous pouvez configurer une interface spécifique pour OSSIM à l'aide d'outils système Linux.
- Collecte de données de sécurité : OSSIM collecte des données de sécurité à partir de différents sources telles que les journaux système, les journaux d'événements réseau, les logs d'application, etc. OSSIM prend en charge de nombreux protocoles tels que Syslog, SNMP et WMI.
- Analyse des événements : OSSIM utilise un moteur de corrélation pour analyser les événements et identifier les menaces potentielles. Il prend en charge plus de 5000 règles de corrélation pour détecter les menaces courantes.
- Génération d'alertes : Lorsqu'OSSIM détecte une menace potentielle, il génère des alertes pour avertir les administrateurs de la sécurité du réseau. Les alertes peuvent être envoyées par courrier électronique, Slack ou tout autre système de messagerie.
- Interface utilisateur : OSSIM dispose d'une interface web pour visualiser les données capturées et les alertes générées. L'interface permet également de rechercher des événements spécifiques et de filtrer les résultats en fonction de critères spécifiques.
- Gestion des vulnérabilités : OSSIM dispose également d'un module de gestion des vulnérabilités pour détecter les vulnérabilités de sécurité dans les systèmes et les applications et aider les administrateurs à les corriger.

4.5. Analyse de la cybermenace (Threat intelligence)

Le projet OpenCTI (Open Cyber Threat Intelligence), développé en collaboration entre l'ANSSI et le CERT-EU, est un outil qui vise à gérer et partager les connaissances en matière d'analyse de la cybermenace (Threat Intelligence). À l'origine, l'outil était conçu pour structurer les informations de l'ANSSI concernant les menaces informatiques, mais il facilite également les échanges entre l'ANSSI et ses partenaires. OpenCTI est entièrement open source et disponible pour tous les acteurs de la "threat intelligence". Cette application leur permet de stocker, organiser, visualiser et partager leurs propres connaissances dans ce domaine.

- Pour installer OpenCTI, suivez les instructions fournies par l'ANSSI, disponibles sur le site officiel d'OpenCTI ou dans la documentation du projet sur GitHub.

- Pour configurer OpenCTI, créez un compte administrateur et configurez des éléments tels que la langue et le fuseau horaire lors de la configuration initiale de l'outil.
- Collecte de données : Rassemblez des données provenant de diverses sources, telles que des flux de renseignements sur les menaces, des journaux de sécurité, des rapports d'incidents, etc. Importez ces données dans OpenCTI pour les utiliser lors de vos analyses.
- Utilisez OpenCTI pour créer des entités qui représentent les différents éléments de votre système d'information, tels que des actifs, des attaquants, des vulnérabilités, des indicateurs de compromission, et bien d'autres.
- Lors de l'analyse des relations dans OpenCTI, vous pouvez lier les entités pour visualiser et analyser leurs interactions. Par exemple, vous pouvez associer une menace spécifique à un actif vulnérable ou à une technique d'attaque connue. Cette approche vous permet de mieux comprendre l'impact des menaces sur votre environnement en identifiant les connexions pertinentes entre les entités.
- Utilisation des graphiques : Exploitez les fonctionnalités de visualisation graphique d'OpenCTI pour observer les relations entre les entités et détecter des schémas, des tendances et des comportements malveillants. Appliquez des filtres pour affiner votre analyse.
- Enrichissement des données : Améliorez les données en ajoutant des informations provenant de sources externes, telles que des bases de données de renseignements sur les menaces ou des services de réputation IP. Cela renforce votre analyse en fournissant des informations contextuelles supplémentaires.
- Partage des résultats : Utilisez les fonctionnalités de partage d'OpenCTI pour partager les résultats de vos analyses avec d'autres utilisateurs ou équipes. Vous pouvez générer des rapports personnalisés, exporter des données ou collaborer avec d'autres analystes de cybermenaces.

4.6. Honeypots

Manuka est un outil open source de déploiement et de gestion de honeypots, qui permet de surveiller les activités des attaquants en simulant des cibles vulnérables fictives. Voici comment utiliser Manuka pour mettre en place des honeypots :

- Manuka peut être installé sur un serveur Linux dédié en suivant les instructions d'installation disponibles sur le site web du projet.
- Une fois installé, Manuka permet de configurer et de déployer des honeypots sur le réseau. Les honeypots peuvent être configurés pour simuler différents services et protocoles, tels que SSH, FTP, HTTP, etc.
- Les honeypots peuvent être configurés pour simuler des vulnérabilités connues, en utilisant des logiciels obsolètes ou des versions dépassées des systèmes d'exploitation.
- Les honeypots de Manuka enregistrent les activités des attaquants, telles que les tentatives de connexion, les scans de ports et les tentatives d'exploitation de vulnérabilités.
- Les données collectées par Manuka peuvent être analysées pour identifier les tendances et les modèles de comportement des attaquants. Les informations collectées peuvent aider à comprendre les menaces potentielles et à renforcer la sécurité du réseau.
- Génération d'alertes : Lorsqu'une activité suspecte est détectée, Manuka peut générer des alertes pour informer les administrateurs de sécurité. Les alertes peuvent être envoyées par e-mail, Slack ou tout autre système de messagerie.

4.7. Cloud platform security

Scout Suite est un outil open source de sécurité conçu pour les environnements cloud qui permet d'analyser les configurations de sécurité des plates-formes cloud telles qu'AWS, Azure et Google Cloud Platform. Voici les étapes à suivre pour utiliser Scout Suite pour améliorer la sécurité de votre plate-forme cloud :

- Installation de Scout Suite : Pour installer Scout Suite, vous pouvez suivre les instructions d'installation fournies sur le site web du projet. L'outil peut être installé localement ou sur un serveur dédié.

- Configuration des informations d'identification : Pour effectuer des scans sur une plate-forme cloud, Scout Suite doit être configuré avec les informations d'identification appropriées pour accéder à la plate-forme. Les informations d'identification peuvent inclure des clés d'accès, des identifiants de compte ou des jetons d'accès spécifiques à la plate-forme cloud.
- Lancement des scans : Une fois que les informations d'identification ont été configurées, les scans peuvent être lancés pour analyser les configurations de sécurité de la plate-forme cloud. Scout Suite permet de scanner l'ensemble de la plate-forme cloud ou des parties spécifiques, telles que les instances EC2, les groupes de sécurité, les buckets S3, etc.
- Analyse des résultats : Après l'analyse, Scout Suite génère des rapports détaillés sur les configurations de sécurité de la plate-forme cloud. Ces rapports contiennent des informations sur les vulnérabilités et les erreurs de configuration, ainsi que des recommandations pour améliorer la sécurité de la plate-forme.
- Intégration avec d'autres outils de sécurité : Pour une gestion plus facile des alertes et des incidents, Scout Suite peut être intégré à d'autres outils de sécurité tels que Splunk, ElasticSearch et Jira.

5

Préparation à l'examen de certification Cisco CyberOps Associate

5.1. CyberOps Associate

Présentation du cours

Ce cours propose d'acquérir les compétences et les concepts essentiels en matière de sécurité, pour être capable de surveiller, détecter et analyser les menaces de cybercriminalité, de cyberespionnage, les menaces internes, les menaces avancées persistantes, les exigences réglementaires et autres problématiques liées à la cybersécurité auxquelles les entreprises sont confrontées, tout en proposant des solutions adaptées.

Prérequis :
aucun

Durée du cours :
80H

Objectifs

- Acquérir les compétences requises pour devenir technicien de sécurité débutant.
- Se préparer à l'examen de certification DevNet CyberOps.
- S'orienter vers une carrière passionnante dans le domaine de la cybersécurité, un secteur en constante évolution et en forte croissance qui englobe tous les secteurs d'activité.

Contenu et déroulement du cours CyberOps Associate (CA) v1.0

Dernière mise à jour le 20 décembre 2020

Introduction

Les entreprises d'aujourd'hui se doivent de détecter rapidement les failles de cybersécurité et de répondre efficacement aux incidents. Les centres opérationnels de sécurité (SOC) surveillent étroitement les systèmes de sécurité et protègent les entreprises en détectant et en éliminant les exploits et les menaces. Le cours CyberOps Associate prépare les candidats à travailler en tant qu'analystes dans les centres opérationnels de sécurité.

Profil des participants

Le cours CyberOps Associate est destiné aux élèves de la Cisco Networking Academy® qui veulent développer des compétences professionnelles basiques d'analystes de la sécurité. Les profils visés incluent les étudiants dans le domaine des technologies et les professionnels IT qui souhaitent poursuivre leur carrière dans un centre opérationnel de sécurité (SOC). Pendant ce cours, les étudiants développeront toutes les connaissances fondamentales nécessaires pour détecter et analyser les menaces de cybersécurité de base, et les transmettre aux personnes les plus à même de les traiter, à l'aide d'outils Open Source.

Connaissances préalables requises

Les élèves du cours CyberOps Associate doivent posséder les compétences et les connaissances suivantes :

- Compétences en matière de navigation sur PC et sur Internet
- Notions de base sur les systèmes Windows et Linux
- Notions de base sur les réseaux informatiques (niveau CCNA ITN)
- Compréhension du système binaire et hexadécimal
- Maîtrise de Cisco Packet Tracer

Certifications visées

Ce cours s'aligne sur la certification Cisco Certified CyberOps Associate (CBROPS). Les candidats doivent passer l'examen CBROPS 200-201 pour obtenir la certification Cisco Certified CyberOps Associate. L'examen CBROPS teste les connaissances et les compétences d'un candidat en matière de sécurité, de surveillance, d'analyse basée sur l'hôte, d'analyse des intrusions réseau et des politiques et procédures de sécurité.

Description du cours

Le cours comporte de nombreuses fonctionnalités pour aider les élèves à maîtriser ces concepts :

- Le cours comprend vingt-huit (28) modules. Chaque module est composé de rubriques.
- Les modules mettent l'accent sur l'esprit critique, la résolution des problèmes, la collaboration et l'application pratique des compétences.

- Chaque module propose une mise en pratique et une évaluation de la compréhension de l'élève, comme un travail pratique ou une activité Packet Tracer. Ces activités dans chaque module s'accompagnent de commentaires qui indiquent à l'élève s'il maîtrise les compétences requises. Les élèves peuvent vérifier leur niveau de compréhension avant de passer un questionnaire noté ou un examen.
- Chaque rubrique fait l'objet d'un questionnaire interactif ou d'un autre type d'évaluation de la bonne compréhension des élèves, comme des travaux pratiques ou une session Packet Tracer. Ces évaluations sont conçues pour que les élèves sachent s'ils ont une bonne compréhension du sujet ou s'ils doivent réviser avant de poursuivre. Ils peuvent vérifier leur niveau de compréhension avant de passer un questionnaire noté ou un examen. Les questionnaires de vérification de la compréhension des élèves n'ont aucun impact sur la note globale.
- Les contenus multimédias riches, notamment des activités interactives, des vidéos et des questionnaires, s'adaptent à de nombreux styles de formation pour favoriser l'assimilation des connaissances.
- Des environnements virtuels simulent des scénarios de cyberattaque concrets et permettent de s'entraîner à la surveillance, à l'analyse et à la résolution de problèmes de sécurité.
- Les exercices pratiques aident les étudiants à développer leur capacité à résoudre les problèmes complexes et leur esprit critique.
- Grâce aux évaluations innovantes, les élèves reçoivent des commentaires instantanés de la part de l'instructeur pour mieux évaluer le niveau de connaissances et de compétences atteint.
- Les concepts techniques sont présentés dans un langage adapté aux élèves de tous niveaux, et des activités interactives intégrées au cours interrompent la lecture du contenu et aident à améliorer la compréhension.
- Le cursus encourage les étudiants à envisager une formation supplémentaire en informatique, mais met aussi l'accent sur les compétences mises en œuvre et l'expérience pratique.
- Les exercices Cisco Packet Tracer sont conçus pour Packet Tracer 7.3.0 ou version ultérieure.

Objectifs du cours

Le cours CyberOps Associate v1.0 vous permet d'acquérir les connaissances et les compétences nécessaires pour prendre en charge les tâches et les responsabilités d'un analyste de cybersécurité débutant travaillant dans un centre opérationnel de sécurité (SOC).

À l'issue du cours *CyberOps Associate v1.0*, les élèves seront en mesure d'effectuer les tâches suivantes :

- Installer des machines virtuelles afin de créer un environnement sécurisé pour la mise en œuvre et l'analyse des incidents de cybersécurité.
- Expliquer le rôle de l'analyste de cybersécurité dans l'entreprise.
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Windows nécessaires pour renforcer les analyses de cybersécurité.
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Linux.
- Analyser le fonctionnement des services et des protocoles réseau.
- Expliquer le fonctionnement de l'infrastructure de réseau.
- Classer les divers types d'attaques réseau.
- Utiliser des outils de surveillance du réseau pour identifier les attaques contre les services et les protocoles réseau.

- Expliquer comment empêcher un accès malveillant aux réseaux informatiques, aux hôtes et aux données.
- Expliquer les effets de la cryptographie sur la surveillance de la sécurité du réseau.
- Expliquer comment enquêter sur les attaques et les vulnérabilités des terminaux.
- Évaluer les alertes de sécurité du réseau.
- Analyser les données liées aux intrusions réseau afin d'identifier les hôtes compromis.
- Appliquer des modèles de gestion des incidents liés à la sécurité du réseau.

Conditions requises pour les équipements utilisés lors des travaux pratiques

Ce cours ne nécessite aucun équipement physique autre que le PC destiné aux travaux pratiques. Il utilise plusieurs machines virtuelles pour créer une expérience pratique.

Bundle d'équipements de base :

- Configuration système minimale requise pour les PC
  - CPU : Intel Pentium 4, 2,53 GHz ou équivalent avec prise en charge de la virtualisation
  - Systèmes d'exploitation, tels que Microsoft Windows, Linux et Mac OS
  - Processeur 64 bits
  - RAM : 8 Go
  - Stockage : 40 Go d'espace disque disponible
  - Résolution d'affichage : 1 024 x 768
  - Polices de langue prenant en charge le codage Unicode (en cas d'affichage dans des langues autres que l'anglais)
  - Derniers pilotes de cartes vidéo et mises à jour du système d'exploitation
- Connexion Internet pour les ordinateurs des étudiants et ceux des ateliers pratiques

Logiciels sur le PC de l'élève :

- Machine virtuelle Oracle VirtualBox Manager (version 6.1 ou ultérieure)
- Poste de travail virtuel CyberOps
  - Téléchargeable à partir du cours
  - Nécessite 1 Go de RAM et 20 Go d'espace disque
- Machine virtuelle Security Onion
  - Téléchargeable à partir du cours
  - Nécessite 4 Go de RAM (minimum), 8 Go de RAM (fortement recommandé) et 20 Go d'espace disque

Description du cours CyberOps Associate

Vous trouverez ci-dessous l'ensemble des modules et les compétences associées présentés dans ce cours. Chaque module constitue une unité d'apprentissage intégrée, se composant de contenus, d'activités et d'évaluations qui ciblent un ensemble spécifique de compétences. La taille du module dépend du niveau de connaissances et d'aptitudes nécessaires pour maîtriser la compétence. Certains modules sont considérés comme fondamentaux, étant donné que les éléments présentés, bien qu'ils ne soient pas évalués, traitent de concepts qui sont couverts lors de l'examen de certification CBROPS.

Tableau 1. Description du cours CyberOps Associate v1.0

Contenu et déroulement du cours CyberOps Associate (CA) v1.0

Module/rubriques	Objectifs
Module 1. Le danger	**Expliquer pourquoi les réseaux et les données sont la cible d'attaques.**
1.0 Introduction	Une brève introduction au cours et au premier module.
1.1 Histoires de guerre	Décrire les spécificités des incidents de cybersécurité.
1.2 Hackers	Expliquer les raisons qui motivent les hackers à l'origine d'incidents de sécurité spécifiques.
1.3 Impact des menaces	Expliquer l'impact potentiel des attaques du réseau.
1.4 Résumé : les dangers	Un résumé et le questionnaire du module.
Module 2. Les combattants de la guerre contre la cybercriminalité	**Expliquer comment se préparer à une carrière dans les opérations de cybersécurité.**
2.0 Introduction	Une introduction au module.
2.1 Le centre opérationnel de sécurité moderne	Expliquer la mission du centre opérationnel de sécurité (SOC).
2.2 Devenir un acteur de la protection	Décrire les ressources disponibles pour se préparer à une carrière dans les opérations de cybersécurité.
2.3 Résumé : les combattants de la guerre contre la cybercriminalité	Un résumé et le questionnaire du module.
Module 3. Le système d'exploitation Windows	**Présenter les fonctionnalités de sécurité du système d'exploitation Windows.**
3.0 Introduction	Une introduction au module.
3.1 L'histoire de Windows	Décrire l'histoire du système d'exploitation Windows.
3.2 Architecture et fonctionnement de Windows	Expliquer l'architecture de Windows et son fonctionnement.
3.3 Configuration et surveillance de Windows	Expliquer comment configurer et surveiller Windows.
3.4 La sécurité Windows	Expliquer comment Windows peut être sécurisé.
3.5 Résumé : le système d'exploitation Windows	Un résumé et le questionnaire du module.
Module 4. Présentation de Linux	**Mettre en œuvre la sécurité Linux de base.**
4.0 Introduction	Une introduction au module.
4.1 Notions de base sur Linux	Expliquer pourquoi les compétences Linux sont essentielles pour la surveillance de la sécurité du réseau et l'investigation.
4.2 Utilisation du shell Linux	Utiliser le shell Linux pour manipuler des fichiers texte.
4.3 Serveurs et clients Linux	Expliquer le fonctionnement des réseaux client-serveur.
4.4 Administration de base du serveur	Expliquer comment un administrateur Linux localise et manipule les fichiers journaux de sécurité.

Module/rubriques	Objectifs
4.5 Le système de fichiers Linux	Gérer le système de fichiers Linux et les autorisations.
4.6 Utiliser l'interface graphique Linux	Expliquer les composants de base de l'interface graphique Linux.
4.7 Utiliser un hôte Linux	Utiliser les outils pour détecter les malwares sur un hôte Linux.
4.8 Résumé : les principes de base de Linux	Un résumé et le questionnaire du module.
Module 5. Protocoles réseau	**Expliquer comment les protocoles permettent d'exploiter le réseau.**
5.0 Introduction	Une introduction au module.
5.1 Processus de communication du réseau	Expliquer le fonctionnement de base des communications de données en réseau.
5.2 Les protocoles de communication	Expliquer comment les protocoles permettent d'exploiter le réseau.
5.3 L'encapsulation des données	Expliquer comment l'encapsulation de données permet la transmission des données sur le réseau.
5.4 Résumé : les protocoles réseau	Un résumé et le questionnaire du module.
Module 6. Ethernet et protocole IP	**Expliquer comment les protocoles Ethernet et IP assurent la communication réseau.**
6.0 Introduction	Une introduction au module.
6.1 Ethernet	Expliquer comment Ethernet prend en charge la communication réseau.
6.2 IPv4	Expliquer comment le protocole IPv4 prend en charge la communication réseau.
6.3 Notions de base sur l'adressage IP	Expliquer comment les adresses IP assurent la communication réseau.
6.4 Les types d'adresses IPv4	Présenter les types d'adresses IPv4 qui permettent la communication réseau.
6.5 La passerelle par défaut	Expliquer comment la passerelle par défaut assure la communication réseau.
6.6 Longueur du préfixe IPv6	Expliquer comment le protocole IPv6 assure la communication réseau.
6.7 Résumé : les protocoles Ethernet et IP	Un résumé et le questionnaire du module.
Module 7. Principes de sécurité du réseau	**Vérification de la connectivité.**
7.0 Introduction	Une introduction au module.
7.1 ICMP	Expliquer comment le protocole ICMP sert à tester la connectivité du réseau.
7.2 Utilitaires ping et Traceroute	Utiliser les outils Windows, ping et Traceroute pour vérifier la connectivité du réseau.

Module/rubriques	Objectifs
7.3 Résumé : la vérification de la connectivité	Un résumé et le questionnaire du module.
Module 8. Protocole ARP (Address Resolution Protocol)	**Analyser les unités de données du protocole ARP sur un réseau.**
8.0 Introduction	Une introduction au module.
8.1 Les adresses MAC et IP	Comparer les rôles de l'adresse MAC et de l'adresse IP.
8.2 ARP	Analyser ARP en examinant les trames Ethernet.
8.3 Les problèmes liés à ARP	Expliquer l'impact qu'ont les requêtes ARP sur le réseau et les performances des hôtes.
8.4 Résumé : le protocole ARP (Address Resolution Protocol)	Un résumé et le questionnaire du module.
Module 9. La couche de transport	**Expliquer comment les protocoles de la couche de transport prennent en charge la fonctionnalité du réseau.**
9.0 Introduction	Une introduction au module.
9.1 Les caractéristiques de la couche de transport	Expliquer comment les protocoles de la couche de transport prennent en charge les communications réseau.
9.2 Établissement de sessions dans la couche de transport	Expliquer comment la couche de transport établit des sessions de communication.
9.3 Fiabilité de la couche de transport	Expliquer comment la couche de transport établit des communications fiables.
9.4 Résumé de la couche de transport	Un résumé et le questionnaire du module.
Module 10. Services réseau	**Expliquer comment les services réseau assurent la fonctionnalité du réseau.**
10.0 Introduction	Une introduction au module.
10.1 DHCP	Expliquer comment les services DHCP assurent la fonctionnalité du réseau.
10.2 DNS	Expliquer comment les services DNS assurent la fonctionnalité du réseau.
10.3 NAT	Expliquer comment les services NAT assurent la fonctionnalité du réseau.
10.4 Les services de transfert et de partage des fichiers	Expliquer comment les services de transfert des fichiers assurent la fonctionnalité du réseau.
10.5 Les e-mails	Expliquer comment les services de messagerie assurent la fonctionnalité du réseau.
10.6 HTTP	Expliquer comment les services HTTP assurent la fonctionnalité du réseau.
10.7 Résumé : les services réseau	Un résumé et le questionnaire du module.

Module/rubriques	Objectifs
Module 11. Les périphériques de communication réseau	**Expliquer comment les périphériques réseau assurent les communications réseau filaires et sans fil.**
11.0 Introduction	Une introduction au module.
11.1 Les périphériques réseau	Expliquer comment les périphériques réseau assurent les communications réseau.
11.2 Les communications sans fil	Expliquer comment les périphériques sans fil assurent les communications réseau.
11.3 Résumé : les appareils de communication réseau	Un résumé et le questionnaire du module.
Module 12. L'infrastructure de sécurité du réseau	**Expliquer comment les périphériques et les services renforcent la sécurité du réseau.**
12.0 Introduction	Une introduction au module.
12.1 Les topologies du réseau	Expliquer comment les conceptions de réseau influent sur le flux de trafic transitant via le réseau.
12.2 Les périphériques de sécurité	Expliquer comment les périphériques spécialisés renforcent la sécurité du réseau.
12.3 Les services de sécurité	Expliquer comment les services renforcent la sécurité du réseau.
12.4 Résumé : l'infrastructure de sécurité du réseau	Un résumé de ce module.
Module 13. Les hackers et leurs outils	**Expliquer comment les réseaux sont attaqués.**
13.0 Introduction	Une introduction au module.
13.1 Qui attaque notre réseau ?	Expliquer l'évolution des menaces ciblant le réseau.
13.2 Outils des hackers	Décrire les différents types d'outils d'attaque utilisés par les hackers.
13.3 Résumé : les hackers et leurs outils	Un résumé et le questionnaire du module.
Module 14. Les attaques et les menaces fréquentes	**Expliquer les divers types de menaces et d'attaques.**
14.0 Introduction	Une introduction au module.
14.1 Les malwares	Décrire les types de programmes malveillants.
14.2 Les attaques réseau courantes : reconnaissance, accès et ingénierie sociale	Expliquer les attaques de reconnaissance, d'accès et d'ingénierie sociale.
14.3 Les attaques réseau : déni de service, dépassement de la mémoire tampon et contournement	Expliquer les attaques par déni de service, dépassement de la mémoire tampon et contournement.
14.4 Résumé : les menaces et les attaques courantes	Un résumé et le questionnaire du module.
Module 15. Observation du fonctionnement du réseau	**Expliquer la surveillance du trafic réseau.**
15.0 Introduction	Une introduction au module.

Module/rubriques	Objectifs
15.1 Présentation de la surveillance du réseau	Expliquer l'importance de la surveillance du réseau.
15.2 Présentation des outils de surveillance du réseau	Expliquer comment la surveillance de réseau est effectuée.
15.3 Résumé : les outils et la surveillance du réseau	Un résumé et le questionnaire du module.
Module 16. Attaques ciblant les fondements du réseau	**Expliquer comment les vulnérabilités TCP/IP favorisent les attaques réseau.**
16.0 Introduction	Une introduction au module.
16.1 Informations sur les unités de données de l'adresse IP	Expliquer la structure de l'en-tête des adresses IPv4 et IPv6.
16.2 Les vulnérabilités IP	Expliquer comment les vulnérabilités IP favorisent les attaques réseau.
16.3 Les vulnérabilités TCP et UDP	Expliquer comment les vulnérabilités TCP et UDP favorisent les attaques réseau.
16.4 Résumé : les attaques ciblant les fondements du réseau	Un résumé et le questionnaire du module.
Module 17. Attaques ciblant les activités	**Expliquer pourquoi les applications et les services réseau fréquemment utilisés sont vulnérables face aux attaques.**
17.0 Introduction	Une introduction au module.
17.1 Les services IP	Expliquer les vulnérabilités des services IP.
17.2 Les services d'entreprise	Expliquer comment les vulnérabilités des applications réseau favorisent les attaques réseau.
17.3 Résumé : les attaques ciblant les activités	Un résumé et le questionnaire du module.
Module 18. Comprendre les mécanismes de défense	**Expliquer les approches en matière de protection du réseau.**
18.0 Introduction	Une introduction au module.
18.1 Une défense en profondeur	Expliquer comment la stratégie de défense approfondie protège les réseaux.
18.2 Les politiques de sécurité, les réglementations et les standards	Présenter les standards, les réglementations et les politiques de sécurité en vigueur.
18.3 Résumé : comprendre la défense	Un résumé et le questionnaire du module.
Module 19. Contrôle d'accès	**Expliquer comment le contrôle d'accès protège un réseau.**
19.0 Introduction	Une introduction au module.
19.1 Les concepts de contrôle d'accès	Expliquer comment le contrôle d'accès protège les données du réseau.
19.2 Utilisation et fonctionnement du modèle AAA	Expliquer comment le modèle AAA contrôle l'accès au réseau.
19.3 Résumé : le contrôle d'accès	Un résumé et le questionnaire du module.
Module 20. Threat Intelligence	**Utiliser diverses sources d'informations pour localiser les**

Module/rubriques	Objectifs
	menaces actuelles.
20.0 Introduction	Une introduction au module.
20.1 Sources d'informations	Décrire les sources d'information utilisées pour indiquer les nouvelles menaces de sécurité du réseau.
20.2 Les services de Threat Intelligence	Décrire les divers services de Threat Intelligence.
20.3 Résumé : la Threat Intelligence	Un résumé et le questionnaire du module.
Module 21. Cryptographie	**Expliquer comment l'infrastructure à clé publique assure la sécurité du réseau.**
21.0 Introduction	Une introduction au module.
21.1 Intégrité et authenticité	Expliquer le rôle de la cryptographie pour garantir l'intégrité et l'authenticité des données.
21.2 La confidentialité	Expliquer comment les méthodes cryptographiques améliorent la confidentialité des données.
21.3 La cryptographie à clé publique	Expliquer la cryptographie à clé publique.
21.4 Les autorités et le système d'infrastructure à clé publique	Expliquer comment l'infrastructure à clé publique fonctionne.
21.5 Les utilisations et les effets de la cryptographie	Expliquer comment l'utilisation de la cryptographie a un impact sur les opérations de cybersécurité.
21.6 Résumé : la cryptographie	Un résumé de ce module.
Module 22. La protection des terminaux	**Expliquer comment un site web d'analyse des malwares génère un rapport.**
22.0 Introduction	Une introduction au module.
22.1 Protection antimalware	Expliquer les méthodes de protection contre les malwares.
22.2 La prévention des intrusions basée sur l'hôte	Expliquer les entrées de journal IPS/IDS basées sur l'hôte.
22.3 La sécurité des applications	Expliquer comment la fonction de sandboxing permet d'analyser les programmes malveillants.
22.4 Résumé : la protection des terminaux	Un résumé et le questionnaire du module.
Module 23. Évaluation des vulnérabilités des terminaux	**Expliquer comment les vulnérabilités des terminaux sont évaluées et gérées.**
23.0 Introduction	Une introduction au module.
23.1 Profilage du réseau et du serveur	Expliquer l'intérêt du profilage du réseau et des serveurs.
23.2 Le système d'évaluation des vulnérabilités (CVSS)	Expliquer comment les rapports CVSS permettent de décrire les vulnérabilités de sécurité.
23.3 Gestion sécurisée des périphériques	Expliquer comment les techniques de gestion sécurisée des

Module/rubriques	Objectifs
	périphériques protègent les données et les ressources.
23.4 Les systèmes de gestion de la sécurité de l'information (ISMS)	Expliquer comment les systèmes de gestion de la sécurité de l'information sont utilisés pour protéger les ressources.
23.5 Résumé : évaluation des vulnérabilités des terminaux	Un résumé et le questionnaire du module.
Module 24. Les technologies et les protocoles	**Expliquer l'incidence des technologies de protection sur la surveillance de la sécurité.**
24.0 Introduction	Une introduction au module.
24.1 Les protocoles courants en surveillance	Expliquer le comportement des protocoles réseau courants dans le cadre de la surveillance de la sécurité.
24.2 Les technologies de sécurité	Expliquer comment les technologies de sécurité affectent la surveillance des protocoles réseau courants.
24.3 Résumé : les technologies et protocoles	Un résumé et le questionnaire du module.
Module 25. Les données sur la sécurité du réseau	**Expliquer les types de données sur la sécurité du réseau que vous utilisez pour surveiller la sécurité.**
25.0 Introduction	Une introduction au module.
25.1 Les types de données de sécurité	Décrire les types de données utilisées pour surveiller la sécurité.
25.2 Les journaux des terminaux	Décrire les éléments du fichier journal d'un terminal.
25.3 Les journaux du réseau	Décrire les éléments du fichier journal d'un périphérique réseau.
25.4 Résumé : les données de sécurité réseau	Un résumé et le questionnaire du module.
Module 26. L'évaluation des alertes	**Expliquer le processus d'évaluation des alertes.**
26.0 Introduction	Une introduction au module.
26.1 Les sources d'alertes	Identifier la structure des alertes.
26.2 Présentation de l'évaluation des alertes	Expliquer comment les alertes sont classées.
26.3 Résumé : évaluation des alertes	Un résumé et le questionnaire du module.
Module 27. L'utilisation des données sur la sécurité du réseau	**Interpréter les données afin de déterminer la source d'une alerte.**
27.0 Introduction	Une introduction au module.
27.1 Une plate-forme de données commune	Expliquer comment les données sont préparées pour une utilisation dans un système de surveillance de la sécurité du réseau (NSM).
27.2 Examiner les données du réseau	Utiliser les outils Security Onion pour examiner les événements de sécurité du réseau.
27.3 Améliorer le travail des analystes en cybersécurité	Décrire les outils de surveillance du réseau qui améliorent la gestion du workflow.

Module/rubriques	Objectifs
27.4 Résumé : l'utilisation des données sur la sécurité du réseau	Un résumé et le questionnaire du module.
Module 28. Analyse et réponse aux incidents numériques	**Expliquer comment CyberOps Associate répond aux incidents de cybersécurité.**
28.0 Introduction	Une introduction au module.
28.1 La gestion des preuves et l'attribution des attaques	Expliquer le rôle des processus d'analyse numérique.
28.2 La chaîne de frappe	Identifier les étapes de la chaîne de frappe.
28.3 Analyse du modèle d'intrusion en diamant	Classer un événement d'intrusion à l'aide du modèle en diamant.
28.4 La réponse aux incidents	Appliquer les procédures de gestion des incidents 800-61r2 du NIST par rapport à un scénario donné.
28.5 Résumé : enquêtes techniques et analyse et réponse aux incidents	Un résumé de ce module.
28.6 Préparez-vous à votre examen et lancez votre carrière !	Préparation à la certification, bons de réduction et autres ressources professionnelles.

Webographie

Radar des startups cybersécurité française 2022. url : https://www.wavestone.com/fr/insight/radar-startups-cybersecurite-2022/.