Mise en pratique du SIEM

Formation Informatique / Bureautique / Sécurité

Grâce à des mises en situation réelles, vous serez à mêmes de comprendre pourquoi et comment utiliser les différents outils, méthodologies, et services externes dont vous disposerez, en tant qu'analyste, au sein d'un SOC. Vous vous entrainerez et passerez la certification QRadar.

OBJECTIFS

- Maîtriser la chaîne méthodologique d'usage des principaux outils à la disposition d'un analyste SOC
- S'entrainer à concevoir des propositions de remédiation
- Appréhender les perspectives d'évolution des outils de SIEM
- Connaître l'ensemble des services et organisations spécialisés en matière de cyber sécurité
- S'entrainer et passer la certification QRadar

PUBLIC

Administrateur Systèmes et réseaux, analystes de sécurité, les architectes techniques « sécurité », les gestionnaires d'infractions

PRE-REQUIS

- Connaissances des architectures logicielles Linux et Windows
- Avoir suivi le module « Les outils de l'analyste SOC »

PROGRAMME

Mises en situation

- Le cas « Target », 110 Millions d'enregistrements dérobés : analyse d'une attaque de points de vente en plein Black Friday.
- Discussion ouverte et travail collectif : propositions d'amélioration pour donner suite à l'analyse du cas Target.
- Présentation par les étudiants d'un cas de hack et analyse collective.
- Le SIEM, extensions et perspectives ?
- La réponse à incident
- L'analyse de binaires / L'étude forensique
- Les procédures itératives d'amélioration continue
- Le Threat Hunting
- Le rôle de L'ANSSI, du SANS Institute, les CERTs/CSIRTs
- L'écosystème des CERTs et des CSIRTs privés, commerciaux et publics
- Les métiers de la cyber sécurité, les certifications reconnues

Préparation et passage de la certification Analyste QRadar

- Rappel des notions et références utiles
- Examen blanc
- Passage de la certification

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

A retenir

Durée : **3 jours** soit 21h.
Réf. **SOCP**

01 42 93 52 72

Dates des sessions

Paris
09/05/2023
10/07/2023
04/12/2023

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

Mise en pratique du SIEM

Formation Informatique / Bureautique / Sécurité

CERTyou est certifié Qualiopi

CERTyou a été reconnu par le BUREAU VERITAS pour la qualité de ces procédures et lui a décerné la certification Qualiopi Formation Professionnelle. La certification de services Qualiopi Formation Professionnelle répond aux exigences qualité décrites dans l'article 1 du décret n°2015-790 du 30 juin 2015.

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

Retrouvez cette formation sur notre site :
Mise en pratique du SIEM

CERTYOU, 37 rue des Mathurins, 75008 PARIS
Tél : +33 1 42 93 52 72 - contact@certyou.com - www.certyou.com
RCS de Paris n° 804 509 461 - TVA intracommunautaire FR03 804509461 - APE 8559A
Déclaration d'activité enregistrée sous le N° 11 75 52524 75 auprès du préfet de région d'Ile-de-France