INTITULE DE LA FORMATION :

IBM QRadar SIEM Advanced Topics

REF. COURS : BQ203

***CETTE FORMATION EST ÉLIGIBLE AU CPF*.**

DUREE : 2 JOURS (14H)

- Formation inter-entreprise ou intra-entreprise
- Formation en présentiel ou distanciel
- Horaires : 9h-12h30 – 14h-17h30

PRIX PUBLIC INTERENTREPRISES : 1580€ HT / PERS

DESCRIPTION :

QRadar SIEM est une plate-forme de gestion de sécurité des réseaux conçue pour détecter les anomalies, identifier les menaces et filtrer les faux positifs (des erreurs de jugement conduisant à lancer des alertes sans qu'il n'y ait lieu de le faire). Pour y parvenir, QRadar SIEM consolide les données des évènements historisés et des flux réseaux avant de les analyser pour détecter les éventuelles infractions à la sécurité nécessitant des enquêtes. Les participants à cette formation avancée apprendront à tirer parti de l'ensemble des possibilités offertes par la plate-forme pour sécuriser encore davantage leurs réseaux.

OBJECTIFS PEDAGOGIQUE :

- Comprendre comment créer des sources de journal personnalisées pour utiliser des événements provenant de sources inhabituelles
- Apprendre à créer, gérer et utiliser des collections de données de référence
- Savoir développer et gérer des règles personnalisées pour détecter une activité inhabituelle dans votre réseau
- Être en mesure de développer et gérer des scripts d'action personnalisés pour une réponse automatique aux règles
- Apprendre à développer et gérer des règles de détection d'anomalies pour détecter les situations de trafic réseau inhabituelles

COMPETENCE VISEE :

PUBLIC :

Administrateurs de sécurité

Architectes techniques de sécurité

Gestionnaires des infractions

Services professionnels utilisant QRadar SIEM

Administrateurs QRadar SIEM

PRE-REQUIS :

Connaissances de l'infrastructure informatique, des principes fondamentaux de la sécurité informatique, de Linux, Microsoft Windows, de la mise en réseau TCP/IP, des fichiers de journaux et des événements et des flux réseau

Vous devez également avoir suivi la formation "IBM QRadar SIEM - Les bases".

PROGRAMME :

- CRÉATION DE TYPES DE SOURCE DE JOURNAL
- EXPLOITATION DES COLLECTIONS DE DONNÉES DE RÉFÉRENCE
- DÉVELOPPEMENT DE RÈGLES PERSONNALISÉES
- CRÉATION DE SCRIPTS D'ACTION PERSONNALISÉS
- DÉVELOPPEMENT DE RÈGLES DE DÉTECTION DES ANOMALIES

TEST AND CERTIFICATION :

EVALUATION DE LA FORMATION :

- Avant la formation : Auto-positionnement du stagiaire selon les prérequis
- Pendant la formation (démarche formative) : évaluation continue des connaissances, travaux pratiques.
- À l'issue de la formation (démarche sommative) : questionnaire de satisfaction du stagiaire,
- A 6 mois : évaluation différée

INTERVENANT :

- Consultant/ Formateur habilité et certifié IBM

LIEU ET DELAI D'ACCES

- Lieu en présentiel : **38 rue Victor Hugo – 92400 COURBEVOIE ou autre site préciser dans la convocation**
- **Présentiel** : groupe de 4 participants minimum et 12 participants maximum
- **Distanciel** : groupe de 4 participants minimum et 10 participants maximum
- **Le délai estimé** entre la demande du bénéficiaire et le début de la prestation est estimé entre 3 mois et 1 jour (financement CPF).

METHODES MOBILISEES EN DISTANCIEL

ARROW ECS Education adapte ses modules en distanciel avec l'outil TEAMS (autre selon contraintes techniques), autour de l'organisation et des principes pédagogiques suivants:

- Un référent technique adresse en amont aux participants les informations techniques nécessaire et un tuto pour suivre la formation à distance avec l'outil TEAMS. Il valide avec chacun le bon fonctionnement des connections audio et vidéo lors d'un RV technique collectif. Il pose également les règles du jeu d'un fonctionnement en virtuel et gère d'éventuelles problématiques techniques.

  Par ailleurs il est disponible la première demi-journée de formation en cas de soucis technique des participants, pour gérer individuellement d'éventuels ajustements liés à l'outil « en ligne ».
- Des documents sont envoyés en amont (par mail) : questionnaire, supports bénéficiaires, auto-tests éventuels, boite à outils …
- La « classe virtuelle » permet aux participants d'avoir accès aux mêmes ressources techniques qu'en présentiel. Chaque participant aura accès à un support de cours et un environnement technique accessible via le Cloud. Cette démarche vise à renforcer la dimension opérationnelle des sessions à distance, tout en gardant la richesse du partage en intelligence collective.

  Au-delà de l'animation en plénière, l'outil en ligne permet l'organisation de sous-groupes virtuels de travail dans le déroulé de la formation et le formateur passe d'un groupe à l'autre en soutien. De même les mises en situation sont maintenues.
  Une messagerie (chat) permet aux participants d'interagir par écrit, au-delà des échanges interactifs.

MOYENS PEDAGOGIQUES ET TECHNIQUES

- Supports en Anglais : les participants recevront le support de la formation en format numérisé. Un lien d'accès à une plateforme de téléchargement dédiée leur sera adressé avant la formation, leur permettant de télécharger l'ensemble des supports, documentations et outils de la formation.
- Matériel nécessaire pour la formation en présentiel :

✓ Une salle dont la taille est compatible avec le plan gouvernemental de lutte contre l'épidémie de COVID-19 en vigueur au moment de la formation
✓ Un vidéo projecteur et la possibilité de sonorisation
✓ 1 paperboard
✓ Une connexion internet

- ✓ Un PC

- Matériel nécessaire pour la formation en distanciel :

  - ✓ Un ordinateur comprenant un micro, une enceinte et si possible un double écran.
  - ✓ Une connexion Internet.

MODALITES DE SUIVI

- La convocation et le livret d'accueil sont envoyés à l'apprenant 10 jours avant le début de la formation.
- L'intervenant ou ARROW ECS Education remet le règlement intérieur, signe et fait signer la feuille d'émargement au stagiaire par demi-journées.
- L'attestation de formation est remise au stagiaire à la fin de la formation.
- Le livret d'accueil et le règlement intérieur sont consultables sur notre site https://edu.arrow.com/fr/ rubrique « ressources ».

- Suivi post formation : le participant envoie sa demande au formateur par écrit à l'adresse mail suivante : training.ecs.fr@arrow.com . Le formateur lui répond par retour de mail, sous 3 jours en fonction de ses disponibilités. Selon le niveau de complexité de la demande, il peut également lui proposer un rendez-vous téléphonique dans les cinq jours pour approfondir la question et solutionner sa problématique. Cette assistance est mise en place durant trois mois, à partir de la fin de la session.

ACCESSIBILITE ET PRISE EN COMPTE DES SITUATIONS DE HANDICAP

- Pour nos formations, nous faisons une étude préalable à la formation pour adapter nos locaux, nos modalités pédagogiques et d'animation en fonction de la situation de handicap portée à notre connaissance. En fonction des besoins spécifiques, nous mettrons tout en œuvre avec nos partenaires spécialisés pour être en capacité de réaliser la prestation.
- Pour toute demande, merci de bien vouloir contacter notre référent handicap Cédric BOUTROS par mail : cedric.boutros@arrow.com

MOYENS D'ENCADREMENT

- **Assistance pédagogique** : Thierry DESOUCHE – thierry.desouche@arrow.com – 06 85 34 81 53 - du lundi au vendredi (9h30-13h, 14h-17h30)
- **Assistance technique :** Jean Yves BORG – jean-yves.borg@arrow.com - – 06 76 98 76 61 - du lundi. au vend.(9h30-13h,14h-17h30)
- **Intervenant** : (préciser son nom) training.ecs.fr@arrow.com – 01 49 97 49 51 du lundi au vendredi (9h30-13h, 14h-17h30)
- **Référent handicap** : Cédric. BOUTROS – cedric.boutros@arrow.com – 06 38 14 03 69 (9h30-13h, 14h-17h30)

DEBOUCHES ET SUITE DU PARCOURS

En France et dans l'OCDE les mutations économiques, technologiques mais aussi sociétales s'accélèrent depuis ces dernières années et incitent les entreprises à modifier en profondeur leur organisation du travail, pour anticiper les changements et de s'y adapter. Dans ce contexte, le développement et l'adaptation des compétences à ces évolutions prend une dimension primordiale, pour permettre aux équipes d'être en adéquation avec la mutation technologique en perpétuelle évolution et des nouvelles compétences techniques nécessaires.

L'accompagnement des équipes dans un environnement apprenant est devenu aujourd'hui un enjeu majeur pour permettre aux structures de déployer et réussir la transformation, mais aussi pour donner la capacité aux individus à maintenir leur employabilité ou à intégrer le marché du travail.

Cette formation vous permet de développer vos compétences et les participants à cette formation avancée apprendront à tirer parti de l'ensemble des possibilités offertes par la plate-forme pour sécuriser encore davantage leurs réseaux.