Formation Cyber Sécurité

OBJECTIFS :

1. **Compréhension des concepts de sécurité** : Maîtriser les principes de la triade de la CIA (confidentialité, intégrité, disponibilité) et explorer les stratégies de défense en profondeur.
2. **Surveillance de la sécurité** : Identifier les surfaces d'attaque et analyser les différentes menaces réseau et applicatives.
3. **Analyse basée sur l'hôte** : Utiliser des technologies de point de terminaison pour détecter des anomalies et interpréter les journaux de sécurité.
4. **Analyse des intrusions dans le réseau** : Évaluer les événements de sécurité avec des outils comme Wireshark et comprendre les alertes d'intrusion.
5. **Politiques et procédures de sécurité** : Développer des plans de réponse aux incidents et évaluer les métriques de sécurité.

*** Laboratoires pratiques**

Population cible :

Cette formation s'adresse aux : **Étudiants**, **Responsables IT, Techniciens**, **Analystes, ingénieurs de réseau et sécurité et Administrateur système…**

G2C, Avenue Hedi Nouira, Résidence Yassine App AM2 à la Mezzanine, à coté de MG Ennasr2
Tél/Fax : 70 621 226 ; GSM : 27 519 739 – 50 911 280
E-mail : gccformation2@gmail.com, commercial@gc-inter.com

G2C
Coaching&Consulting

Programme :

Les fondamentaux des opérations de cybersécurité de Cisco

1 : les concepts de sécurité

- Présentation du concept de triade de la CIA (confidentialité, intégrité, disponibilité).
- Comparaison entre plusieurs types de déploiement de sécurité.
- Explication des termes relatifs à la sécurité.
- Comparaison entre différents concepts de sécurité.
- Présentation des principes de la stratégie de défense en profondeur.
- Comparaison entre plusieurs modèles de contrôle d'accès.
- Explication des termes employés dans la norme de sécurité CVSS.
- Identification des défis liés à la visibilité des données (réseau, hôte et Cloud) au moment de la détection.
- Identification des pertes de données potentielles en fonction des profils de trafic fournis.
- Interprétation de la méthode du 5-tuple afin d'isoler un hôte compromis dans un ensemble groupé de journaux.
- Comparaison entre la détection basée sur des règles et la détection comportementale ou statistique.

2 : la surveillance de la sécurité

- Comparaison entre une surface d'attaque et une surface de vulnérabilité.
- Identification des types de données fournies par ces technologies.
- Explication de l'utilisation de ces types de données dans la surveillance de la sécurité.
- Présentation des attaques réseau (attaques basées sur le protocole, attaques par déni de service, attaques par déni de service distribué et attaques de type Man in the middle).
- Présentation des attaques contre les applications web (attaques par injection SQL, attaques par injection de commandes, attaques par scripts intersites, etc.).
- Présentation d'une attaque d'ingénierie sociale.
- Explication des attaques basées sur les points de terminaison (débordements de mémoire tampon, commande et contrôle, logiciels malveillants et ransomwares).

G2C, Avenue Hedi Nouira, Résidence Yassine App AM2 à la Mezzanine, à coté de MG Ennasr2
Tél/Fax : 70 621 226 ; GSM : 27 519 739 – 50 911 280
E-mail : gccformation2@gmail.com, commercial@gc-inter.com

- Présentation des techniques de contournement et d'obscurcissement (tunneling, cryptage et proxy).
- Explication des impacts des certificats sur la sécurité incluant la PKI, la traversée des réseaux publics et privés, l'asymétrie et la symétrie).
- Identification des composants des certificats dans un scénario particulier.

3 : l'analyse basée sur l'hôte

- Présentation des technologies de point de terminaison en matière de surveillance de la sécurité.
- Identification des composants sur Windows et Linux dans une situation spécifique.
- Explication du rôle de l'attribution dans une investigation.
- Identification des types de preuves apportées sur la base des journaux fournis.
- Comparaison d'images de disques modifiées et non modifiées
- Interprétation des journaux du système d'exploitation, de l'application ou de la ligne de commande pour identifier un évènement.
- Interprétation du rapport de sortie d'un outil d'analyse de logiciels malveillants comme la chambre de détonation ou le bac à sable).

4 : l'analyse des intrusions dans le réseau

- Mettre en correspondance les évènements fournis et les technologies sources.
- Comparaison de l'impact et de l'absence d'impact pour ces éléments.
- Comparaison de l'inspection approfondie des paquets avec le filtrage des paquets et le fonctionnement d'un pare-feu dynamique.
- Comparaison de l'interrogation du trafic en ligne avec les écoutes ou la surveillance du trafic.
- Comparaison des caractéristiques des données obtenues à partir des écoutes ou de la surveillance du trafic et des données transactionnelles (NetFlow) dans le cadre de l'analyse.
- Extraction de fichiers à partir d'un flux TCP lorsque vous recevez un fichier PCAP et Wireshark.
- Identification des éléments clés d'une intrusion à partir d'un fichier PCAP spécifique.
- Interprétation des champs d'entête de protocole dans le cadre de l'analyse des intrusions.
- Interprétation des éléments d'artéfact communs d'un évènement afin d'identifier une alerte.
- Interprétation des expressions régulières de base.

5 : les politiques et les procédures de sécurité

- Présentation des différents concepts de gestion.
- Description des éléments d'un plan de réponse aux incidents selon la norme NIST.SP800-61.
- Application du processus de gestion des incidents pour un évènement.
- Identification des éléments utilisés pour le profilage du réseau et des serveurs.
- Identification des données protégées dans un réseau.
- Classification des événements d'intrusion dans les catégories décrites dans le modèle de sécurité, notamment le modèle Cyber Kill Chain et le modèle Diamond d'intrusion.
- Description de la relation entre les métriques SOC et l'analyse de la portée (temps de détection, temps de confinement, temps de réponse et temps de contrôle).

Laboratoires pratiques :

- Utiliser les outils NSM pour analyser les catégories de données.
- Explorer les technologies cryptographiques.
- Explorer les attaques TCP/IP.
- Explorer la sécurité des points finaux.
- Étudier la méthodologie des pirates informatiques.
- Chasse au trafic malveillant.
- Corréler les journaux d'événements, les captures de paquets (PCAP) et les alertes d'une attaque.
- Étudier les attaques par navigateur.
- Analyser les activités suspectes du système de noms de domaine (DNS).
- Explorer les données de sécurité à des fins d'analyse.
- Enquêter sur les menaces persistantes avancées.
- Explorer le système d'exploitation Windows et Linux.

La direction Technique

G2C coaching & consulting

G2C, Avenue Hedi Nouira, Résidence Yassine App AM2 à la Mezzanine, à coté de MG Ennasr2
Tél/Fax : 70 621 226 ; GSM : 27 519 739 – 50 911 280
E-mail : gccformation2@gmail.com, commercial@gc-inter.com