SETC Training Corporate Logo

Formation sécurité informatique: Intelligence cybernétique (CYBERTFR, 4 jours)

Description

La formation Formation sécurité informatique : Intelligence cybernétique est une exploration complète des principes et de l'application de la mise en œuvre d'un programme de Cyber Threat Intelligence au sein de votre organisation. En commençant par l'anatomie d'une attaque et les indications de compromission, le cours explore la chaîne de mise à mort des cybermenaces ainsi que le cycle de cyberintelligence, la collecte et l'analyse des données ainsi que l'analyse des menaces et l'utilisation des réseaux et des partenaires.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Principes de base du renseignement sur les cybermenaces

- Types de renseignements sur les cybermenaces
- Principales caractéristiques des services de renseignement sur les menaces
- Avantages de la veille sur les cybermenaces
- Exploiter l'intelligence du réseau pour identifier les dispositifs infectés
- Le cycle du renseignement sur les cybermenaces (CTI)
- Avantages du CTI
- Avantages du CTI stratégique
- Aperçu des groupes APT

Indicateurs de compromission

- La nature des menaces persistantes avancées (APT)
- Trafic réseau sortant inhabituel
- Anomalies dans l'activité des comptes d'utilisateurs privilégiés
- Irrégularités géographiques
- Autres drapeaux rouges de connexion
- Augmentation des volumes de lecture de données
- Des réponses HTML de grande taille
- Grand nombre de demandes pour le même fichier
- Trafic port-application non concordant
- Modifications suspectes du registre
- Anomalies dans les requêtes DNS
- Mise à jour inattendue des systèmes
- Modifications du profil des dispositifs mobiles
- Des paquets de données au mauvais endroit
- Un trafic Web au comportement surhumain
- Signes d'une activité DDoS

CTI : adoption et utilisateurs

- Caractéristiques principales des CTI
- Le processus CTI : Vue d'ensemble
- Considérations clés : Orienté vers le processus, ajusté au risque et basé sur les adversaires
- Assurer la protection et la prévention
- Partage des cybermenaces et connaissance de la situation

Sensibilité de l'information et exigences légales
A propos de la cyber-guerre : Types et stratégies
Exigences en matière de renseignement sur les cybermenaces
Autres exigences clés de la CTI
Aperçu des outils essentiels : 7 outils indispensables

La chaîne du crime cybernétique

Les 7 phases de la chaîne meurtrière du cyberespace
Reconnaissance
Armement
Livraison
Exploitation
Installation
Commandement et contrôle
Actions sur les objectifs

Le cycle du cyber renseignement

CTI tactique, opérationnel et stratégique
Aperçu du cycle du renseignement sur les menaces
Planification et orientation
Collection
Traitement
Analyse
Diffusion
Tout mettre en place

Collecte et communication des renseignements sur les menaces

Aperçu de la collecte et des rapports
Agrégation
Normalisation et analyse syntaxique
Collecte de renseignements sur les menaces
Collecte de renseignements sur les menaces stratégiques
Collecte de renseignements sur les menaces opérationnelles
Collecte de renseignements sur les menaces tactiques
Composants de la collecte de renseignements sur les menaces

En savoir plus sur la collecte

Aperçu des sources de données
Choisir une source de données : Dispositifs, IP, phishing et autres
Catégories d'informations sur les menaces
Statistiques et rapports sur les cybermenaces
Collecte d'informations CTI : Collecte passive, active et hybride
Open Source Intelligence
L'intelligence humaine
Signals Intelligence
Intelligence de l'imagerie
Mesures et Signatures Intelligence

Analyse de la menace

Composantes de l'analyse des informations sur les cybermenaces
Analyse du CTI
Analyse du renseignement stratégique sur les menaces
Analyse du renseignement sur les menaces opérationnelles
Analyse tactique du renseignement sur les menaces
Analyse des renseignements sur les menaces techniques

Évaluation de la CTI

Élaboration de plans d'action pour la prévention des attaques futures

Programme CTI et partenaires

Planification d'un programme CTI

Les composantes d'un programme CTI réussi

Recommandations

Aperçu des composantes opérationnelles

Mise en œuvre d'un programme de renseignement sur les menaces

Partenaires CTI

Principaux cas d'utilisation

Meilleures pratiques et défis