SOC Analyst (CSA)

OBJECTIFS

- **Après avoir terminé ce cours, vous devriez être capable de :**
  - Articuler les processus, procédures, technologies et flux de travail SOC.
  - Comprendre et sécuriser les menaces, les attaques, les vulnérabilités, les comportements des attaquants, la cyber kill chain, etc.
  - Reconnaître les outils, tactiques et procédures des attaquants pour identifier les indicateurs de compromission (IOC) qui peuvent être utilisés lors des enquêtes actives et futures.
  - Surveillez et analysez les journaux et les alertes provenant d'une variété de technologies différentes sur plusieurs plates-formes (IDS/IPS, protection des points finaux, serveurs et postes de travail).
  - Appliquez les processus de gestion centralisée des journaux (CLM).
  - Effectuer des événements de sécurité et collecter, surveiller et analyser des journaux.
  - Comprendre la gestion des informations de sécurité et des événements.
  - Administrer les solutions SIEM (Splunk/AlienVault/OSSIM/ELK).
  - Comprendre l'architecture, la mise en œuvre et la mise au point des solutions SIEM (Splunk/AlienVault/OSSIM/ELK).
  - Acquérez une expérience pratique sur le processus de développement de cas d'utilisation SIEM.
  - Développer des cas de menaces (règles de corrélation), créer des rapports, etc.
  - Identifiez les cas d'utilisation largement utilisés dans le déploiement SIEM.
  - Planifiez, organisez et effectuez une surveillance et une analyse des menaces dans l'entreprise.
  - Surveillez les modèles de menaces émergentes et effectuez une analyse des menaces de sécurité.
  - Acquérez une expérience pratique du processus de tri des alertes.
  - Transférer les incidents aux équipes appropriées pour obtenir une assistance supplémentaire.
  - Utilisez un système de tickets Service Desk.
  - Préparer des briefings et des rapports sur la méthodologie d'analyse et les résultats.
  - Intégrez les renseignements sur les menaces dans SIEM pour améliorer la détection et la réponse aux incidents.
  - Exploitez des informations sur les menaces variées, disparates et en constante évolution.
  - Articuler la connaissance du processus de réponse aux incidents.
  - Comprendre la collaboration SOC et IRT pour une meilleure réponse aux incidents.

Prérequis

Les participants doivent remplir les conditions préalables suivantes :
Expérience en administration de réseau ou dans le domaine de la sécurité

PROGRAMME

Concepts essentiels du SOC

- Fondamentaux des réseaux informatiques
- Suite de protocoles TCP/IP
- Protocoles de couche application
- Protocoles de couche transport
- Protocoles de couche Internet
- Protocoles de couche liaison
- Adressage IP et numéros de port
- Contrôles de sécurité du réseau
- Dispositifs de sécurité réseau
- Sécurité Windows
- Sécurité Unix/Linux
- Fondamentaux des applications Web
- Normes, lois et actes relatifs à la sécurité de l'information

Opérations et gestion de la sécurité

- Gestion de la sécurité
- Opérations de sécurité
- Centre des opérations de sécurité (SOC)
- Besoin de SOC
- Capacités SOC
- Opérations SOC
- Flux de travail SOC
- Composantes du SOC : personnes, processus et technologie
- Personnes
- Technologie
- Processus
- Types de modèles SOC
- Modèles de maturité SOC
- Générations SOC
- Mise en œuvre du SOC
- Indicateurs de performance clés du SOC
- Défis liés à la mise en œuvre du SOC
- Meilleures pratiques pour exécuter SOC
- SOC contre CNO

Comprendre les cybermenaces, les IoC et la méthodologie d'attaque

- Cybermenaces
- Intention-Motif-Objectif
- Tactiques-Techniques-Procédures (TTP)
- Opportunité-Vulnérabilité-Faiblesse
- Attaques au niveau du réseau
- Attaques au niveau de l'hôte
- Attaques au niveau des applications
- Menaces de sécurité des e-mails

- Comprendre les indicateurs de compromis
- Comprendre la méthodologie de piratage de l'attaquant

Incidents, événements et journalisation

- Incident
- Événement
- Enregistrer
- Sources de journaux typiques
- Besoin de journal
- Exigences de journalisation
- Format de journal typique
- Approches de journalisation
- Journalisation locale
- Journalisation centralisée

Détection des incidents avec gestion des informations et des événements de sécurité (SIEM)

- Gestion des informations et des événements de sécurité (SIEM)
- Analyse de sécurité
- Besoin de SIEM
- Capacités SIEM typiques
- Architecture SIEM et ses composants
- Solutions SIEM
- Déploiement SIEM
- Détection d'incidents avec SIEM
- Exemples de cas d'utilisation couramment utilisés dans tous les déploiements SIEM
- Gestion du tri et de l'analyse des alertes

Détection améliorée des incidents grâce à la Threat Intelligence

- Comprendre les renseignements sur les cybermenaces
- Pourquoi un SOC basé sur les renseignements sur les menaces ?

Réponse aux incidents

- Réponse aux incidents
- Équipe de réponse aux incidents (IRT)
- Quelle est la place de l'IRT dans l'organisation
- Collaboration SOC et IRT
- Présentation du processus de réponse aux incidents (RI)
- Étape 1 : Préparation à la réponse aux incidents
- Étape 2 : Enregistrement et attribution des incidents
- Étape 3 : Triage des incidents
- Étape 4 : Notification
- Étape 5 : Confinement
- Étape 6 : Collecte de preuves et analyse médico-légale
- Étape 7 : Éradication
- Étape 8 : Récupération

- Étape 9 : Activités post-incident
- Répondre aux incidents de sécurité du réseau
- Répondre aux incidents de sécurité des applications
- Répondre aux incidents de sécurité de messagerie
- Répondre aux incidents internes
- Répondre aux incidents de logiciels malveillants