03 20 61 95 06
formation@access-it.fr

Formation Analyste SOC - Security Operation Center

Durée de la formation : 8 jour(s)

OBJECTIFS

A l'issue de la formation le participant sera capable de :
Expliquer l'état de l'art du SOC (Security Operation Center)
Répondre aux besoins des enjeux cybers et des menaces par le métier d'analyste SOC.

PREREQUIS

Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux…) et d'adapter le contenu de la formation si besoin.
Avoir des connaissances générales en sécurité offensive et défensive et des notions sur le fonctionnement des systèmes d'exploitation.

PUBLIC

Administrateurs système et/ou réseaux, consultants en sécurité de l'information

03 20 61 95 06
formation@access-it.fr

Formation Analyste SOC - Security Operation Center

Durée de la formation : 8 jour(s)

PROGRAMME

SOC et métier d'analyste

Etat de l'art du Security Operation Center
Définition du SOC
Les avantages, l'évolution du SOC
Les services intégrés au SOC, les données collectées, playbook
Le modèle de gouvernance du SOC (approche SSI, type de SOC, CERT, CSIRT)
PDIS (Prestataires de Détection d'Incidents de Sécurité) de l'ANSSI
Prérequis et rôles d'un analyste SOC (techniques, soft skills, rôles, modèles)
Les référentiels (ATT&CK, DeTT&CT, Sigma, MISP)
Exemple de démonstration : utilisation du Framework ATT&CK via Navigator (attaque et défense)

Découverte et mise en place du SIEM

Focus sur l'analyste SOC
Quel travail au quotidien ?
Triage des alertes
Révision et état de sécurité
Identification et rapport
Threat Hunting
Exemple de démonstration : utilisation de l'outil Sysmon

Threat Hunting

Les sources de données à monitorer
Indicateur Windows (processus, firewall...)
Service Web (serveur, WAF, activité)
IDS / IPS
EDR, XDR
USB
DHCP, DNS
Antivirus, EPP
DLP, whitelist
Email
Exemple de travaux pratiques (à titre indicatif) :
Cas d'usage et ligne de défense

Analyse, Logstash, Elasticsearch

Tour d'horizon du SIEM
Contexte du SIEM
Solution existante
Principe de fonctionnement d'un SIEM
Les objectifs d'un SIEM
Solution de SIEM

Présentation de la suite Elastic

Formation Analyste SOC - Security Operation Center

Durée de la formation : 8 jour(s)

Les agents BEATS et Sysmon
Découverte de Logstash
Découverte d'Elasticsearch
Découverte de Kibana
Exemple de travaux pratiques (à titre indicatif) :
Mise en place d'ELK et première remontée de log

Logstash (ETL)

Fonctionnement de Logstash
Les fichiers Input et Output
Enrichissement : les filtres Groks et sources externes

Elasticsearch

Terminologie
Syntax Lucene
Alerte avec ElastAlert et Sigma
Exemple de démonstration : utilisation d'ElastAlert et Sigma
Exemple de travaux pratiques (à titre indicatif)
Création d'alertes, alarmes

Kibana

Recherche d'événements
Visualisation des données
Exemple de démonstration :
Création d'un filtre sur Kibana
Ajout de règles de détection, IoC
Allez plus loin dans l'architecture ELK avec HELK

Cyber-entraînement et rapport

Mise en situation
L'analyste SOC est en situation et doit identifier plusieurs scénarios d'attaque lancés par le formateur
Exemple de travaux pratiques (à titre indicatif) :
Configurer un SIEM et l'exploiter

Travaux Pratiques

Détecter une cyber attaque simple
Détecter une cyber attaque complexe (APT MITRE ATT&CK)

Rapport

L'analyste SOC doit rapporter les attaques, détecter et identifier les menaces, impacts et vérifier si son système d'information est touché
Exemple de travaux pratiques (à titre indicatif) /
Créer un rapport des attaques interceptées et évaluer l'impact

03 20 61 95 06
formation@access-it.fr

Formation Analyste SOC - Security Operation Center

Durée de la formation : 8 jour(s)

Initiation à la gestion des incidents

Réponse aux incidents
Etat de l'art de la réponse aux incidents (CSIRT, CERT, FIRST, CERT-FR)
Les différents métiers du CSIRT
Quelle méthode, quel framework pour un CSIRT ?
PRIS (Prestataires de Réponse aux Incidents de Sécurité) de l'ANSSI
Communication avec le CSIRT
Alerter le CSIRT lors d'une détection
Comment le CSIRT procède lors d'une crise et quelle réponse apporte-t-il aux incidents ?

Synthèse

Echange autour des différents travaux / rapport des stagiaires lors de la formation : points positifs / points négatifs
Quelle conclusion pour la méthodologie d'un analyse SOC

03 20 61 95 06
formation@access-it.fr

Formation Analyste SOC - Security Operation Center

Durée de la formation : 8 jour(s)

Prise en compte du handicap
Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre
Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).
Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.
Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.
La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).
Durant la formation, le formateur prévoit :
Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;
Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;
Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;
Le formateur valide les connaissances acquises après chaque TP ;
Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.
A la demande, il sera délivré un certificat de réalisation.

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action
Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis
Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.
La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).
A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.
Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation
Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en oeuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen
Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation
Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques
Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.
À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).
Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.
Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.
Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.
Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.
Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants
Se former depuis leur lieu de travail ou leur domicile,
Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.
Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques...
Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise
Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.
Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).
Limiter les temps de déplacement.
Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.
Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances