Cybersécurité : structurer et piloter sa veille

Repérer les signaux utiles, évaluer leur pertinence et ajuster ses pratiques pour anticiper les nouvelles menaces

Séminaire en présentiel
Sécurité

Code :
CYSPV

Durée :
1 jour(s) (7,00 heures)

Exposés : **50 %**
Cas pratiques : **25 %**
Echanges d'expérience : **25 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 120,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Les cybermenaces évoluent chaque jour, tout comme les technologies qui les accompagnent. Pour rester pertinent et réactif, il ne suffit plus de surveiller l'actualité : il faut savoir identifier les signaux faibles, distinguer l'essentiel de l'accessoire et transformer l'information en décisions utiles.

Cette formation vous apporte une méthode concrète pour mettre en place une veille cybersécurité efficace, sélectionner les sources les plus pertinentes, prioriser les informations à forte valeur ajoutée et partager les connaissances au sein de votre organisation.

Vous développerez ainsi une capacité durable à anticiper les risques, suivre les tendances émergentes et renforcer votre posture de sécurité

OBJECTIFS PEDAGOGIQUES

- Mettre en œuvre une démarche pérenne de veille et de maintien des connaissances en cybersécurité
- Structurer et industrialiser ses activités de veille, à l'échelle individuelle comme collective
- Identifier, analyser et exploiter les informations pertinentes pour éclairer les décisions, les projets et la gestion des risques
- Organiser le partage et la capitalisation des connaissances afin d'ancrer durablement les pratiques de veille au sein de l'organisation

PUBLIC CIBLE

- Expert IT, cybersécurité et digital
- Architecte et responsable sécurité
- Responsable innovation
- Manager technique
- Référent métier et expert fonctionnel

PRE-REQUIS

Connaissances de base en informatique (IT) et en sécurité des systèmes d'information (SSI) recommandées.

Une première expérience dans le domaine de la cybersécurité est

également souhaitable.

METHODE PEDAGOGIQUE

- Apports méthodologiques et retours d'expérience
- Études de cas et mises en situation
- Ateliers collaboratifs et échanges entre pairs

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

STRUCTURER ET MAÎTRISER LA VEILLE CYBERSÉCURITÉ

- Enjeux et fondamentaux de la veille technologique
  - Définir la veille et distinguer ses grandes familles : veille stratégique et concurrentielle, veille réglementaire, veille technologique, veille cyber et géopolitique
  - Situer la veille comme dispositif d'anticipation et d'aide à la décision, et clarifier ce qu'elle n'est pas (collecte sans finalité, simple revue de presse)

Identifier les besoins de veille à partir des missions, des enjeux et du contexte de l'organisation, et les lier à des objectifs concrets

- Méthodologies de veille
  - Comprendre et appliquer le cycle du renseignement (orientation, collecte, traitement, analyse, diffusion et retour d'expérience) afin de structurer une démarche de

veille efficace et adaptée aux enjeux de cybersécurité
    - Formuler des besoins de veille exploitables (questions de renseignement prioritaires - PIR) à partir d'objectifs concrets
    - Distinguer veille permanente, veille ponctuelle et alerte, et choisir le rythme adapté à chaque besoin

Définir un périmètre de surveillance (technologies, menaces, secteurs, acteurs, zones géographiques) et cadrer le passage de la donnée brute au livrable utile

- Sources d'information et fiabilité
    - Cartographier les familles de sources : presse et médias spécialisés, sources institutionnelles et académiques, bases de données et registres, réseaux sociaux, sources humaines, OSINT
    - Évaluer la fiabilité d'une source et la crédibilité d'une information à l'aide d'une grille de cotation (type source / information) et des réflexes de sourcing journalistique
    - Identifier les biais cognitifs, les mécanismes de désinformation et les tentatives de manipulation, puis mettre en œuvre une démarche rigoureuse de vérification de l'information (fact-checking)

Recouper, dater et tracer la provenance des informations retenues pour distinguer fait établi, hypothèse et rumeur, et garantir l'auditabilité

- Outils et dispositifs de veille
    - Construire une chaîne d'outils cohérente : agrégateurs et flux RSS (Feedly, Inoreader), alertes (Google Alerts), newsletters, réseaux sociaux, plateformes de veille
    - Exploiter les techniques de recherche avancée et les outils OSINT généralistes (Dorks, archives web, recherche d'image, registres ouverts)
    - Mettre en place un dispositif personnel de capitalisation (notes, tags, classement) et doser automatisation et curation humaine selon les ressources
- Ateliers pratiques
    - Travail en sous-groupes sur un cas défini
    - Présentation d'un contexte
    - Application guidée :
        - Formulation des besoins et des axes de veille
        - Sélection et cotation des sources
        - Configuration d'un dispositif de collecte
        - Vérification et qualification de quelques informations
    - Restitution et échanges

Jour 2

MAINTENIR L'ÉTAT DE L'ART DANS LA DURÉE

- Du suivi de l'information à l'exploitation opérationnelle
  - Transformer une information de veille en action ou en recommandation pour le bon destinataire
  - Hiérarchiser l'information selon sa pertinence, son impact et son degré d'urgence
  - Rédiger un livrable adapté au lecteur (brève, bulletin de veille, note de synthèse, flash alerte) avec un angle clair
- Maintien à l'état de l'art au niveau individuel
  - Organiser une routine de veille personnelle tenable dans la durée (rythme, temps dédié, tri, capitalisation)

Évaluer régulièrement ses besoins de montée en compétences au regard de l'évolution du domaine, et mobiliser les communautés, réseaux professionnels et événements spécialisés comme leviers de maintien à l'état de l'art

- Organisation collective et gouvernance
  - Définir et répartir les rôles et responsabilités au sein d'un dispositif de veille collective afin d'assurer une collecte, une analyse et une diffusion efficaces de l'information
  - Formaliser les processus : circuits de diffusion, niveaux d'alerte, articulation avec les instances de décision
  - Organiser le partage et la mutualisation (capitalisation collective, communautés, et réseaux)
- Pérennisation et pilotage
  - Définir des indicateurs de pilotage (KPI)
  - Démontrer la valeur de la veille auprès des clients
  - Organiser son amélioration continue : revue périodique des besoins et des sources
- Ateliers pratiques
  - Travail en sous-groupes, poursuite du cas du Jour 1
  - Application guidée :
    - Hiérarchisation et sélection des informations
    - Production d'un livrable de synthèse et d'une recommandation client
    - Définition des rôles et du circuit de diffusion
  - Sélection de 3 à 5 indicateurs clés de pilotage de la veille
  - Restitution des travaux, échanges et retours d'expérience entre participants
- Conclusion
  - Synthèse de la journée
  - Rappel des messages clés
  - Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com