MODALITÉ DE FORMATION CYBERSÉCURITÉ

SOMMAIRE

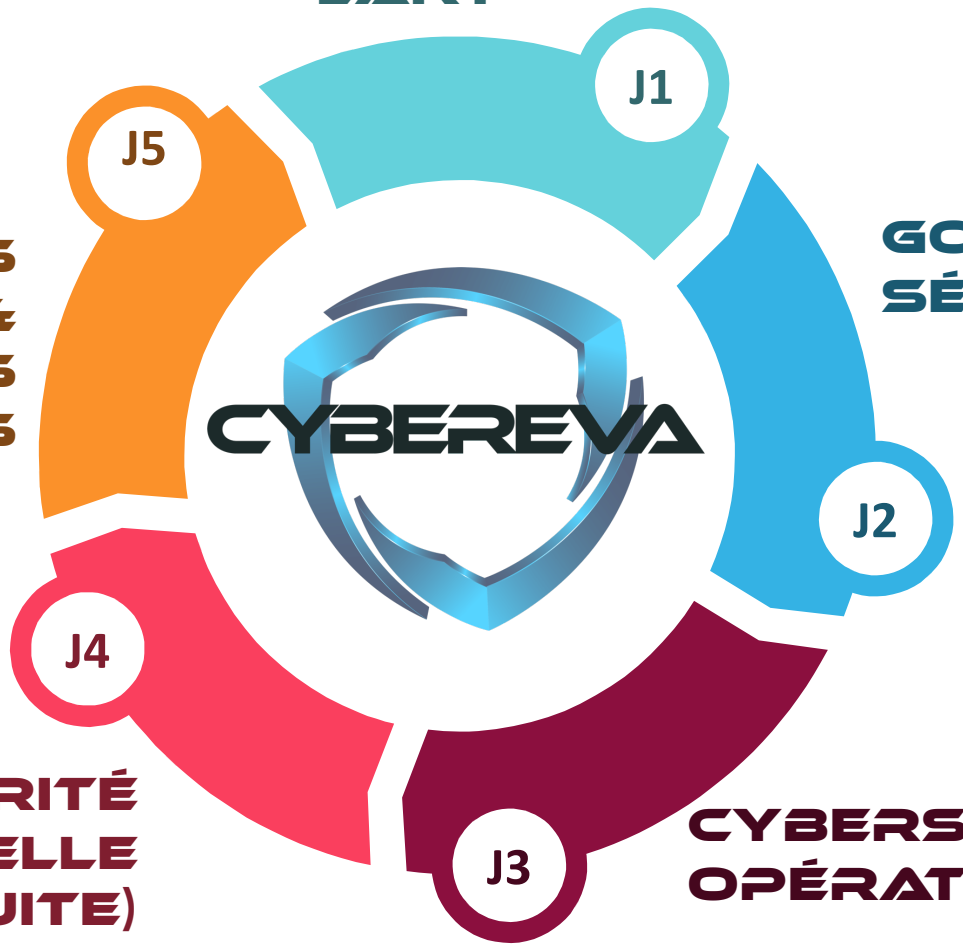
J1 GÉNÉRALITÉ SUR LA CYBERSÉCURITÉ : ÉTAT DE L'ART

J2 GOUVERNANCE DE LA SÉCURITÉ DES SI

J3 CYBERSÉCURITÉ OPÉRATIONNELLE

J4 CYBERSÉCURITÉ OPÉRATIONNELLE (SUITE)

J5 LA GESTION DES CRISES CYBER & VALIDATION DES ACQUIS



PARCOURS INTRODUCTIF À LA CYBERSÉCURITÉ

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue
Domaine : Cybersécurité – Sécurité informatique

Filière : Fondamentaux de la cybersécurité
Rubrique : Fondamentaux

LIEUX DE LA FORMATION

Sur site : Entreprises ou Campus universitaires
À distance : Via les outils de visioconférence tels que Zoom ou Microsoft Teams

* Formation accessible aux personnes en situation d'handicap

HORAIRES ET MODALITÉS

Durée : 5 jours soit 35 heures au total
Modalités :
- 9h00 à 12h30 et 14h00 à 17h30 soit 7h / jour
- Intra et inter-campus.

Coût : à partir de 15.000 € pour 10 stagiaires

*Pour les groupes inférieurs à 10 personnes : tarifs sur devis

PRÉSENTATION

Objectifs et compétences

Cette formation a pour objectif d'apporter une vision générale sur le domaine de la cybersécurité dans le contexte des enjeux technologiques, économiques et sociaux mondial.
À l'issue de cette formation, les participants seront capables de :

- ❑ Découvrir les grands référentiels et normes qui encadrent la cybersécurité au niveau national et international ;
- ❑ Comprendre les obligations juridiques et les responsabilités des organisations en matière de sécurité numérique ;
- ❑ Identifier les menaces et les vulnérabilités pesant sur les systèmes d'information, et évaluer les risques associés ;
- ❑ Mettre en place des mesures de protection concrètes pour anticiper, atténuer et répondre efficacement aux incidents de sécurité ;
- ❑ Adopter les bonnes pratiques en matière de sécurité informatique au quotidien, tant au niveau personnel que professionnel ;
- ❑ Se familiariser avec les outils clés de la cybersécurité, utilisés par les professionnels pour sécuriser les infrastructures et les données.

Prérequis

Avoir des connaissances générales dans les systèmes d'information.

PARCOURS INTRODUCTIF À LA CYBERSÉCURITÉ

MODALITÉS

Modalités
En présentiel, en distenciel ou mixte

Pédagogie :
Cette formation est essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique.
Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques
- ❑ Support de formation au format PDF et/ou Power Point;
- ❑ Ordinateur;
- ❑ Vidéoprojecteur;
- ❑ Tableau blanc;
- ❑ Visioconférence (Zoom, MS Teams);

Pendant la formation :
Mises en situation, cas d'usage, travail individuel ou collaboratifs sur des cas réels.

Après la formation :
- ❑ Enquête de satisfaction dans le cadre d'une amélioration continue
- ❑ Validation des acquis par un test de connaissance à l'issue des jours de formation

Contact : training@cybereva.com

PROGRAMME DE FORMATION – JOUR 1 [MATIN]

I. GÉNÉRALITÉ SUR LA CYBERSÉCURITÉ – ÉTAT DE L'ART

Présentation de cursus et Biographie formateur

- ❑ Présentation générale de la formation cybersécurité
- ❑ Présentation formateur (orateur)

Chapitre 1. Introduction à la Cybersécurité

- ❑ Définition Cybersécurité & Hacking
- ❑ DICP et les critères de sécurité
- ❑ Différentes catégories de Hackers

Chapitre 2: Les tendances de la cybercriminalité

- ❑ L'évolution de la cybercriminalité en France, en Afrique et dans le reste du monde
- ❑ L'impact économique de la cybercriminalité
- ❑ Le modèle économique "hacking as a service"
- ❑ Caractéristiques, coûts, usages
- ❑ Mini sondage - Word cloud

Chapitre 3 : Les métiers autour de la cybersécurité

- ❑ 6. Métiers pouvant se spécialiser en cybersécurité
- ❑ 5. Métiers contribuant à la démarche cybersécurité
- ❑ 4. Conseil, service et recherches
- ❑ 3. Gestion des incidents et crises
- ❑ 2. Conception et maintien
- ❑ 1. Gestion et pilotage

PROGRAMME DE FORMATION – JOUR 1 [APRÈS-MIDI]

I. Généralité sur la cybersécurité – État de l'art

Chapitre 4 : Parcours Cybersécurité

- ❑ Parcours académique, certifications et autodidacte
- ❑ Cartographie de parcours
- ❑ Connaissances à acquérir

Chapitre 5 : Les différentes familles d'équipes cybersécurité

- ❑ Blue Team (méthodes et outils)
- ❑ Red Team (méthodes et outils)
- ❑ Purple Team (organisation)

Chapitre 6 : Les ressources et certifications

- ❑ Ressources éducatives des opérations cybersécurité
- ❑ Certifications en Cybersécurité

Chapitre 7 : Identifier les acteurs de la lutte contre la cybercriminalité

- ❑ Cyber-délits en France et Europe : quel dispositif ?
- ❑ Les services spécialisés du ministère de l'Intérieur
- ❑ OCLCTIC, BEFTI, IRCGN, BFMP, DGSI, etc.
- ❑ CISA, NSA, DOJ, DHS, Cyber US Command
- ❑ La cybersécurité et le continent Africain

Chapitre 8 : Les bonnes pratiques

- ❑ Gouvernance de la cybersécurité
- ❑ Défense en profondeur
- ❑ Gestion des incidents de cybersécurité

PROGRAMME DE FORMATION – JOUR 2 [MATIN]

II. Gouvernance de la sécurité des systèmes d'information

Chapitre 9 : Normes & Référentiels

- ❑ ISO 27001 : Norme internationale
- ❑ CIS controls : Cadre international
- ❑ RGPD / DORA : normes Européennes
- ❑ PCI DSS, HIPAA, NIST
- ❑ Autres référentiels : ITIL, FISMA, COBIT etc…
- ❑ **TP #1 : Cas pratique élaboration d'une PSSI**

Chapitre 10 : DevSecOps

- ❑ Modèle de sécurisation des applications
- ❑ Framework OWASP & MITRE
- ❑ SSDLC et STRIDE
- ❑ Les différents outils
- ❑ **TD #01 - Démo Audit d'une application Web**

PROGRAMME DE FORMATION – JOUR 2 [APRÈS-MIDI]

II. Gouvernance de la sécurité des systèmes d'information

Chapitre 11 : Gestion de risques

- ❑ Focus sur l'objectif ultime : la donnée
- ❑ Analyse de risque Méthode EBIOS-RM
- ❑ **TP #2: À l'aide d'une étude de cas, estimer les scénarios de risques et cartographier les risques cyber sur une entreprise fictive.**

PROGRAMME DE FORMATION – JOUR 3 [MATIN]

III. Cybersécurité Opérationnelle

Chapitre 12 : Introduction au test de pénétration et d'intrusion

- ❑ Les différentes phases du Hacking
- ❑ Les différentes phases d'un test d'intrusion
- ❑ Aspects légaux et réglementaires liés aux tests d'intrusion
- ❑ Méthodes et Framework pour un test d'intrusion
- ❑ **TD #02 - Démo Framework (référentiel) Pentest CYBEREVA**
- ❑ **TP #3: Constitution de plusieurs équipes**
- ❑ **TP #4: Questionnaire du pré-engagement**
- ❑ **TP #5: Rédaction d'un contrat de pré-engagement.**

Chapitre 13 : Préparation du test d'intrusion

- ❑ Préparation de machines pour effectuer un test d'intrusion
- ❑ **TD #03 - Démo Utilisation de gadgets Geek**
- ❑ **TP #6: Elaboration d'une matrice de suivi de test d'intrusion**

PROGRAMME DE FORMATION – JOUR 3 [APRÈS-MIDI]

III. Cybersécurité Opérationnelle

Chapitre 14: Collecte d'informations

- ❑ Ingénierie des sources publiques (OSINT)
- ❑ Relevé passif et actif d'informations sur l'organisation cible
- ❑ **TD #04 - Présentation des outils d'OSINT**
- ❑ **TP #7: Relevé d'informations & Reconnaissance**

Chapitre 15 : Énumération de l'infrastructure

- ❑ Énumération du périmètre
- ❑ Evasion sur infrastructure sécurisée Enumération des protocoles
- ❑ **TD #05 - Présentations des outils d'énumération**
- ❑ **TP #8 : Enumération de l'infrastructure**

PROGRAMME DE FORMATION – JOUR 4 [MATIN]

III. Cybersécurité Opérationnelle

Chapitre 16 : Analyse des vulnérabilités

- ❑ Scan de vulnérabilités
- ❑ Présentation des différents outils
- ❑ **TD #06 - Présentation OpenVAS et/ou Nmap**
- ❑ Les vulnérabilités connues
- ❑ **TP #9 : Identification des vulnérabilités**

Chapitre 17 : Exploitation

- ❑ Recherche d'Exploits
- ❑ Présentation des outils/Framework d'attaques
- ❑ **TD #07 - Présentation Metasploit**
- ❑ Déploiement et exécution de charges
- ❑ Écoute passive et active des infrastructures
- ❑ Bruteforcing
- ❑ Mouvements latéraux et pivoting
- ❑ Élévation de privilèges (Méthodes, outils, vulnérabilités Linux, …)
- ❑ **TP #10 : Exploitation des vulnérabilités**

PROGRAMME DE FORMATION – JOUR 4 [APRÈS-MIDI]

III. Cybersécurité Opérationnelle

Chapitre 18 : Post-Exploitation

- ❑ Désactivation des éléments de traçabilité
- ❑ Etude des persistances (ADS, base de registre, planificateur de tâches, services)
- ❑ Nettoyage des traces
- ❑ **TP #11 : Présentation de la matrice de suivi de test d'intrusion (élaborée au TP #5)**
- ❑ **TP #12 : Présentation d'un rapport de test d'intrusion (chaque équipe constituée)**

PROGRAMME DE FORMATION - JOUR 5 [MATIN]

IV. La gestion des crises cyber

Chapitre 19 : La gestion des incidents cybersécurité

- ❑ Actualité sur les crises cybersécurité
- ❑ Définition des incidents ou crises cyber
- ❑ Communication et objectifs autour des la gestion des incidents
- ❑ Communication autour des la gestion des incidents
- ❑ Difficultés rencontrées
- ❑ Etapes d'une crise cyber

Chapitre 20 : Forensics ou investigations numériques

- ❑ Etapes d'une investigation numérique
- ❑ **TD #08 - Présentation d'un cas de crise cyber**
- ❑ Les outils Digital Forensics
- ❑ Collecte des données physiques et virtualisation
- ❑ **TD #09 - Présentation d'un cas pratique via un Lab**
- ❑ **TP #13 : Mission Forensics d'une entreprise victime de cyberattaque**

PROGRAMME DE FORMATION - JOUR 5 [APRÈS-MIDI]

V. Validation des acquis

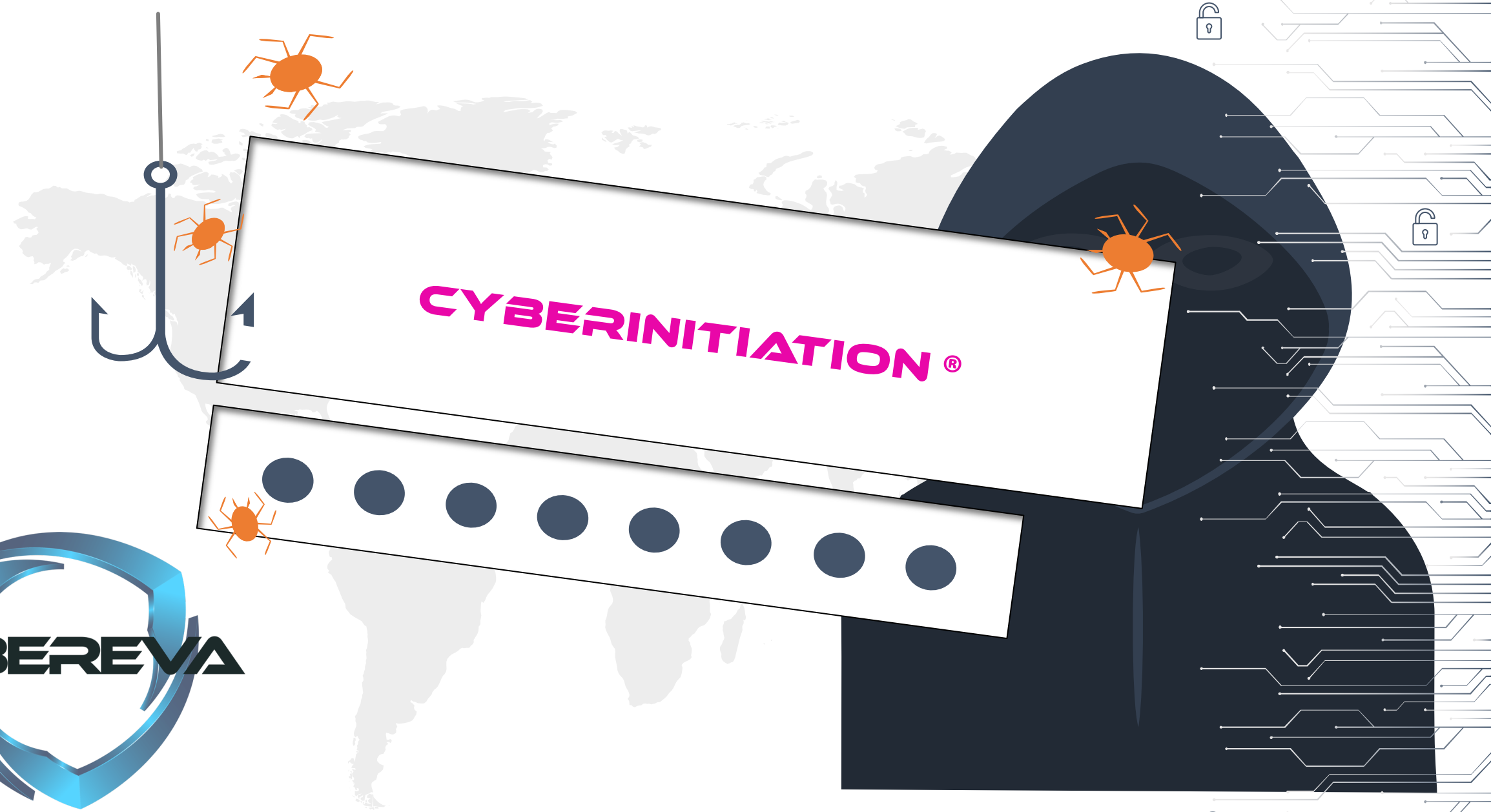
Sondage et test

- ❑ Enquête de satisfaction pour la Qualité et l'Amélioration Continue
- ❑ Validation des connaissances acquises

VI. Extra

Bonus : Dark Web

- ❑ Définition Dark Web
- ❑ Dark Web et les différentes strates d'internet
- ❑ Les entreprises face au Dark Web
- ❑ **TD #10 - Démonstration d'un accès sécurisé vers la fausse des Mariannes**



CYBEREVA