Date de publication : 29/08/2025

Formation : Red Team, Blue Team : comprendre les méthodes de ses équipes

Une vision claire des méthodes offensives (Red Team) et défensives (Blue Team)

Cours de synthèse - 1j - 7h00 - Réf. RTB

Prix : 630 CHF H.T.

NEW

Cette formation d'une journée offre aux managers et responsables IT une vision claire des méthodes offensives (Red Team) et défensives (Blue Team). À travers des démonstrations concrètes et des cas pratiques, vous découvrirez comment vos équipes identifient, mènent et contrent des attaques pour mieux piloter vos projets de cybersécurité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre le rôle des équipes Red Team et Blue Team dans la cybersécurité
- Acquérir une vue d'ensemble des méthodologies et des outils utilisés par chaque équipe
- Apprendre à communiquer efficacement avec ces équipes et à évaluer leurs performances
- Intégrer les pratiques Red Team et Blue Team dans le cadre de la gestion de projet et la gestion des risques IT

Public concerné

Managers, responsables IT, chefs de projet, responsables sécurité, décideurs souhaitant mieux comprendre le travail de leurs équipes techniques.

Prérequis

Aucune connaissance particulière.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

PARTICIPANTS

Managers, responsables IT, chefs de projet, responsables sécurité, décideurs souhaitant mieux comprendre le travail de leurs équipes techniques.

PRÉREQUIS

Aucune connaissance particulière.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Pourquoi Red Team et Blue Team ?

- Principes de sécurité : défense en profondeur, modélisation du risque Cyber.
- Risques associés à l'intrusion, aux attaques, et à la protection des systèmes.
- Pourquoi deux équipes distinctes ? Les Red Teams (attaque) et Blue Teams (défense).
- _1_ Le rôle de la Red Team : comprendre l'attaque :
- Introduction aux tests d'intrusion (pentests).
- Les étapes de l'attaque : reconnaissance, exploitation, post-exploitation.
- Outils utilisés par les Red Teams (ex : Kali Linux, Metasploit, nmap).
- Scénarios d'attaque et objectifs de la Red Team : évaluation de la sécurité du réseau et des systèmes.
- _2_ Le rôle de la Blue Team : comprendre la défense :
- Introduction à la détection d'intrusion, à la surveillance et à la gestion des incidents.
- Les étapes de la réponse à incident : détection, analyse, containment, eradication.
- Outils utilisés par les Blue Teams (SIEM, firewalls, systèmes IDS/IPS).
- Rôle clé des Blue Teams dans la prévention et la gestion de crise.

2 La collaboration entre Red Team et Blue Team : Simulation et confrontation

- Comment les retours de la Red Team aident à améliorer les défenses de la Blue Team et vice versa.
- Le rôle du management dans la gestion de ces interactions.

Démonstration

Exemples d'exercices de "Red Team vs Blue Team" (Purple Teaming).

3 Comprendre les méthodologies et les rapports

- Que recherchent les Red Teams dans leurs rapports ? (points faibles, vulnérabilités exploitées, résultats des tests).
- Comment une Blue Team analyse un incident et rédige un rapport de gestion de crise.
- Que doivent retenir les managers dans les rapports techniques pour prendre des décisions stratégiques ?

4 Gérer les risques et intégrer les équipes Red et Blue dans les projets IT

- L'importance des tests de sécurité dans le cycle de développement logiciel (DevSecOps).
- Comment intégrer les résultats des Red et Blue Teams dans le processus de gestion des risques.
- Préparer des projets IT en tenant compte des tests de pénétration et de la défense proactive.

Dates et lieux

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

CLASSE À DISTANCE
2026 : 19 juin, 18 sep., 11 déc.