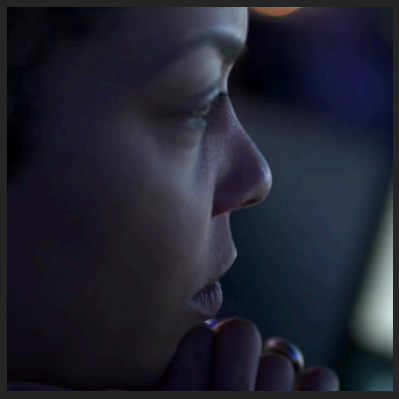
X-Force Command

Votre entreprise est attaquée. Déployez maintenant une réponse à cette attaque.

Entraînez-vous avec une équipe d'élite composée de cyber-intervenants spécialisés dans la première réponse dans un centre d'entraînement à la sécurité haut de gamme. Bénéficiez de l'expérience IBM X-Force Command.

IBM **Security**



Il s'agit de la première expérience de formation en matière de cyber-sécurité. Où les meilleure agences militaires et agences de renseignement, banques et entreprises du domaine de l'énergie du monde dépêchent leurs équipes en vue de se préparer à l'imprévisible et à réagir aux situations du tout pour le tout qui surviennent après une faille de sécurité. IBM® X-Force Command Experience vous aide à vous préparer au pire des scénarios avec des exercices ludiques et intenses basés sur des attaques survenant dans le monde réel et dirigés par des experts de X-Force Command qui possèdent des connaissances de première main sur les lignes de front.

Ces expériences uniques, adaptées à votre organisation et à votre secteur, sont organisées dans des installations de nouvelle génération conçues avec style et précision qui visent à répondre aux besoins des clients. Les caractéristiques globales d'IBM X-Force Command incluent les suivantes :

- **La portée virtuelle de IBM X-Force Command :** La toute première installation à usage commercial immergeant le personnel de la sécurité et les chefs d'entreprise dans un environnement simulé qui est basé sur un centre d'opérations de sécurité (SOC)
- **Centre d'opérations tactique et virtuel IBM X-Force Command (C-TOC) :** Une expérience virtuelle pratique qui peut être configurée comme une gamme virtuelle ou un environnement stérile pour mener des cyber-enquêtes ou une surveillance sur site pour des événements de sécurité à caractère spécial
- **Centres de briefing exécutif IBM X-Force Command :** Rencontrez des intervenants, des testeurs d'intrusion, des experts dans la pensée du design expérimentés, mais aussi des cadres d'IBM pour élaborer et perfectionner votre stratégie de cyber-sécurité et de réponse aux incidents.

Entraînez-vous pour le pire jour que rencontrera votre entreprise

Tous les membres de votre organisation (le SOC, les cadres supérieurs, le conseil d'administration, les métiers des ressources humaines aux relations publiques, ainsi que les opérateurs de clavier situés au rez-de-chaussée) ont un rôle à jouer dans la réponse à une attaque. Votre équipe est-elle prête ? Testez vos compétences et acquérez celles dont vous avez besoin dans divers scénarios basés sur des attaques réelles.

Raisonner rapidement dans un environnement sous pression

- Réagissez aux scénarios de cyber-attaques du monde réel et injectez-les dans un centre d'opérations de sécurité réaliste
- Entraînez-vous dans des situations ludifiées et sous haute pression, dirigées par des personnes se trouvant en première ligne
- Observez les impacts générés par des équipes non formées et un plan d'intervention n'ayant pas été préparé.

Comprenez comment les solutions de sécurité fonctionnent en synergie

- Employez de multiples outils pour enquêter sur un cyber-incident
- Bénéficiez de ressources de pointe, telles que l'intelligence artificielle et les solutions de réponse aux incidents automatisées et la manière de les appliquer aux enquêtes modernes
- Utilisez de véritables outils de piratage et logiciels malveillants pour créer des attaques sous forme de jeu de rôles dans un environnement sécurisé et isolé.

Découvrez comment vos équipes doivent travailler ensemble.

- Collaborez avec vos cyber-analystes, juristes, relations publiques et cadres lors d'un incident
- Passez en revue la tactique de votre entreprise et les guides de communication en situation de crise
- Testez des équipes n'ayant pas de capacités techniques et évaluez l'état de préparation de vos médias.

Des défis stimulants basés sur des scénarios du monde réel

Défi de réponse Ox

Collaborez dans un environnement de centre d'équipe Fusion afin de maintenir votre entreprise à l'écart des grands titres de l'actualité. Déterminez comment réagir en équipe dans toutes les dimensions des réponses que vous devrez apporter dans les domaines techniques, juridiques et des relations publiques.

Objectifs d'apprentissage

1. Faites l'expérience d'un cyber incident en tant que réponse d'entreprise interfonctionnelle
2. Découvrez les lacunes que comporte votre plan de réponse
3. Apprenez les meilleures pratiques en matière de leadership et de réponse numérique techniques.

Les personnes qui devraient y assister

- Dirigeants de SOC, directeurs, chefs d'équipe
- Cadres supérieurs : Responsable de la Sécurité Informatique (RSI), DPI, Responsable des ressources (RS), Directeur des opérations (DO), Président Directeur Général (PDG)
- Équipes de soutien : juridique, RH, relations publiques et risque.

Jeu de guerre virtuel

Ce défi d'ordre consultatif est un exercice conduit par l'utilisateur autour d'un cyber incident. Votre équipe est informée. Cependant, lorsque vous entrez dans le SOC, la réponse de votre équipe dépend de vous. Soudain, la première attaque survient. Y avez-vous répondu correctement ? Les conseillers de X-Force Command surveilleront et noteront les indicateurs de performance clés pour établir un feedback précis.

Objectifs d'apprentissage

1. Utilisez des outils du monde réel pour découvrir la nature du problème et répondre à la menace
2. Testez votre capacité de résolution de problèmes et voyez si vous pouvez résoudre le casse-tête
3. Découvrez comment des équipes stratégiques et techniques peuvent travailler ensemble.

Les personnes qui devraient y assister

- Dirigeants de SOC, directeurs, chefs d'équipe, responsables
- Membres de l'équipe stratégique et technique
- Équipes de soutien et analystes techniques.

OpRedEscape

Pour combattre les pirates, vous devez penser comme un pirate. Mettez-vous à la place d'un cyber-criminel tout en occupant une place dans une équipe de piratage informatique ayant pour objectif de voler des données sur le réseau d'une victime. L'événement se termine par une salle d'évasion de bâtiment où vous pourrez mettre en pratique vos nouvelles compétences. Le contenu est personnalisé afin de correspondre aux compétences définies dans la pièce.

Objectifs d'apprentissage

1. Comprenez les outils utilisés par les pirates pour compromettre un réseau et voler des données
2. Développez vos connaissances sur des sujets liés à la cyber-criminalité tels que le Web caché et les logiciels de rançonnage en crypto-monnaies
3. Découvrez votre « côté obscur » en prenant part à un événement important dans une salle d'évasion.

Les personnes qui devraient y assister

- Dirigeants de SOC, directeurs, chefs d'équipe, responsables
- Cadres supérieurs RSI, DPI, RS, DO, PDG
- Membres du conseil, investisseurs et autres dirigeants.

Une expérience conçue pour vous

- Une expérience de sécurité totalement immersive qui vise à tester les compétences, les processus et les compétences en matière de leadership
- Scénarios d'une journée et d'une demi-journée composés de pratique, de temps d'évaluation et de réflexion
- Utilisez votre propre manuel si vous en avez un
- Un enseignement sur mesure spécifique à votre secteur d'activité et à votre localisation géographique
- Réseautez avec des responsables de la sécurité gérée et de la réponse aux incidents IBM Security.

Testez vos compétences. Apprenez celles dont vous avez besoin.