KASPERSKY lab

Programmes de formation et de sensibilisation Kaspersky Industrial CyberSecurity

www.kaspersky.fr/enterprise-security/industrial

Kaspersky Lab vous fait bénéficier de son expérience, de ses connaissances et de ses informations concernant les menaces en matière de cybersécurité industrielle grâce à ces programmes pédagogiques innovants.

Environ 80 % des incidents de cybersécurité sont dus à une erreur humaine. Dans les cas où ces incidents peuvent entraîner des pannes de systèmes critiques ou arrêter complètement des processus industriels, l'erreur humaine s'avère très coûteuse et potentiellement mortelle.

Dans un environnement où le paysage de menaces est en constante évolution et où les attaques ciblées fondées sur la faiblesse humaine augmentent chaque jour, l'une de vos meilleures défenses est un personnel informatique pour lequel les pratiques de travail sécurisées sont automatiques et instinctives.

C'est pourquoi tous vos employés doivent être sensibilisés aux dangers et aux méthodes pour s'en protéger. Les membres du personnel directement impliqués dans la cybersécurité informatique et technologique doivent également disposer des compétences indispensables à la gestion et à la réduction des menaces, ainsi qu'à leur prévention et à leur détection.

Les formations techniques et de sensibilisation Kaspersky Industrial CyberSecurity sont spécifiquement conçues pour permettre aux opérateurs d'infrastructures critiques, aux fournisseurs de services et aux industries manufacturières de mieux protéger leur environnement industriel contre les perturbations et les dégâts liés aux cyberincidents et aux cyberattaques.

LES FORMATIONS

(Toutes les formations sont proposées en anglais)

<table>
<tr><th>Sensibilisation à la cybersécurité</th><th colspan="2">Développement des compétences et formation en matière de cybersécurité</th></tr>
<tr><td>Pour les ingénieurs/ouvriers :</td><td>Pour les responsables de la sécurité informatique et des responsables sécurité des technologies opérationnelles (OT security managers)</td><td>Pour les professionnels de la sécurité informatique et technologique :</td></tr>
<tr><td>Cybersécurité de base</td><td rowspan="4">Cybersécurité industrielle avancée en pratique</td><td>Tests de pénétration des ICS (systèmes de contrôle industriel) pour professionnels</td></tr>
<tr><td>Pour les responsables :</td><td rowspan="3">Cyberdiagnostic des ICS pour professionnels</td></tr>
<tr><td>Jeux de rôles autour de la cybersécurité industrielle</td></tr>
</table>

SENSIBILISATION À LA CYBERSECURITÉ INDUSTRIELLE

Modules de formation interactifs sur site et en ligne et formation sous forme de jeux autour de la cybersécurité pour tous les employés qui manipulent des systèmes informatisés (production, salles de contrôle et back-office), ainsi que pour leurs responsables.

Les entreprises dépensent des millions en programmes de sensibilisation à la cybersécurité, mais rares sont les RSSI (cadres supérieurs et responsables de la sécurité des systèmes d'information) vraiment satisfaits des résultats. Quel est le problème ?
La plupart des formations de sensibilisation à la cybersécurité sont trop générales, trop longues, trop techniques et foncièrement négatives. Elles n'exploitent pas les principaux points forts des participants, à savoir leurs capacités en matière de prise de décision et d'apprentissage, ce qui les rend parfois inefficaces. De plus, elles ont tendance à ne pas refléter les véritables défis de la cybersécurité spécifiques à l'industrie.

C'est pourquoi les entreprises cherchent des approches comportementales plus élaborées (par exemple, le développement de la culture d'entreprise), qui se focalisent sur des questions spécifiques à leur environnement de travail et offrent un retour sur investissement à la fois mesurable et concret.

Les formations de sensibilisation à la cyberSécurité de Kaspersky Lab reposent sur les points suivants :

- L'évolution des comportements : inciter l'employé à travailler de façon sûre et responsable et promouvoir un environnement d'entreprise dans lequel il peut dire : « je me préoccupe de la cybersécurité, parce que c'est le cas de tout le monde ici ; ça fait partie de notre travail ».
- La combinaison d'une approche qui repose sur la motivation avec des techniques d'apprentissage ludiques, des simulations d'attaques inspirées de situations industrielles réelles et une formation interactive approfondie aux techniques de cybersécurité.

DESCRIPTION DÉTAILLÉE

Exhaustivité en toute simplicité : la formation couvre un large éventail de questions relatives à la sécurité, qui vont des règles de bases de la cyberhygiène aux attaques de programmes malveillants, en passant par les fuites de données et l'utilisation sécurisée des réseaux sociaux, par le biais d'une série d'exercices simples. Nos techniques d'apprentissage exploitent la dynamique de groupe, des modules interactifs et des jeux de rôles inspirés de scénarios industriels réels pour rendre le processus d'apprentissage stimulant et pertinent.

Accessibilité : la formation de sensibilisation à la cybersécurité d'une journée peut être dispensée sur site ou dans tout autre lieu, alors que notre programme de jeux de rôles sur la CyberSécurité industrielle, Kaspersky Industrial Protection Simulation (KIPS), est conçu pour que les employés y participent en ligne ou en face-à-face, selon leurs préférences. KIPS se décline en plusieurs versions adaptées à différents secteurs industriels tels que le traitement de l'eau ou la production et le transport d'électricité, pour assurer l'immersion des employés dans un environnement d'apprentissage réel.

Motivation en toutes circonstances : nous créons des moments propices à l'enseignement à travers l'apprentissage ludique et des compétitions, puis nous renforçons ces périodes de formation tout au long de l'année par des exercices de simulation d'attaque en ligne, des sessions d'évaluation et des campagnes de formation.

Évolution des mentalités : les employés prennent conscience de l'importance de leur rôle dans la protection contre des menaces spécifiques ; ils découvrent comment ils peuvent éviter de devenir des victimes des différents dangers et attaques, de s'y exposer ou d'y exposer leur lieu de travail.

Développement dans l'entreprise d'une culture de la cybersécurité : nous formons les dirigeants à devenir des ambassadeurs de la sécurité ; il est impossible d'instaurer une culture où la cybersécurité est une préoccupation naturelle en l'imposant simplement, mais cela devient bien plus facile lorsque la direction s'implique et montre l'exemple.

Positivité et collaboration : nous démontrons dans quelle mesure la cybersécurité contribue à améliorer l'efficacité et la productivité opérationnelles en général et encourageons une coopération plus efficace avec d'autres services internes, dont l'équipe de sécurité informatique et technologique.

Mesurabilité : nous fournissons des outils pour mesurer les compétences des employés et évaluons l'ensemble de l'entreprise à partir d'une analyse de l'attitude du personnel face à la cybersécurité dans le travail au quotidien.

DÉVELOPPEMENT DES COMPÉTENCES ET FORMATION EN MATIÈRE DE CYBERSÉCURITÉ

Nos formations incluent un large choix de sujets et de techniques liés à la cybersécurité, destinées aux personnes qui sont déjà directement impliquées dans la sécurité des systèmes et technologies industriels, ou le seront à l'avenir. Toutes les formations sont dispensées soit dans les bureaux de Kaspersky Lab, soit directement chez le client, au choix.

Les participants auront l'occasion de collaborer avec nos experts mondiaux, qui partageront avec eux leur expérience très pointue de la prédiction, de la prévention et de la détection du cybercrime, ainsi que des réponses à y apporter.

Les formations se composent de sessions théoriques et d'ateliers pratiques. À l'issue de chaque formation, les participants sont invités à passer un examen de validation des connaissances.

DÉVELOPPEMENT DE L'EXPERTISE DE VOTRE ENTREPRISE

Ces formations permettent aux entreprises d'approfondir leurs connaissances en matière de cybersécurité dans trois domaines principaux :

- Connaissance de base concernant la cybersécurité des systèmes de contrôle industriel
- Tests de pénétration des ICS
- Cyberdiagnostic des ICS

Cybersécurité industrielle avancée
Ces formations proposent aux responsables de la sécurité informatique et aux responsables sécurité des technologies opérationnelles une nouvelle compréhension du paysage des menaces et des vecteurs d'attaque qui prennent votre environnement industriel pour cible. Elles leurs fournissent les outils nécessaires à l'élaboration d'un plan de réponse basique en cas d'incident.

Tests de pénétration des ICS (systèmes de contrôle industriel) pour professionnels
Cette formation apprend aux responsables de la sécurité informatique et aux responsables sécurité des technologies opérationnelles à mener des tests de pénétration complets et approfondis dans différents environnements industriels et à prendre des décisions éclairées quant aux mesures correctives adaptées.

Cyberdiagnostic des ICS pour professionnels
Dans le cadre de cette formation, les responsables de la sécurité informatique et les responsables sécurité des technologies opérationnelles apprendront à établir des cyberdiagnostics réussis dans différents environnements industriels, pour proposer des analyses et recommandations très pointues.

DÉTAIL DES FORMATIONS

Sujets	Durée	Résultats/compétences acquises
Cybersécurité industrielle avancée		
• Aperçu du paysage des menaces actuelles, des problèmes de sécurité, des facteurs humains et des attaques réseau ICS • Sécurité des réseaux dans le domaine informatique et les environnements de systèmes de contrôle industriel : considérations particulières • Étude de cas : démonstration de l'utilisation des techniques de prévention, de détection et de réduction des risques • Conformité à la législation et aux normes industrielles • Topologies des réseaux et fonctionnement des technologies de sécurité des réseaux • Rôles en matière de cybersécurité et structure des équipes • Erreurs de sécurité fréquentes.	1 à 2 jours	• Compréhension des menaces industrielles actuelles et apprentissage des méthodes de défense contre les cyberincidents qui visent votre industrie ou votre entreprise • Détection et identification des incidents liés à la sécurité • Réalisation d'enquêtes simples • Élaboration et mise en œuvre d'un plan de réponse efficace en cas d'incident. Cette formation comprend des éléments hautement personnalisables et peut être planifié sur 1 ou 2 jours, selon vos préférences. La formation débouche sur la délivrance d'un diplôme.
Tests de pénétration des ICS (systèmes de contrôle industriel) pour professionnels		
• Introduction aux éléments, aux architectures et au déploiement des ICS, dans les différents secteurs industriels tels que : – La production et la distribution d'électricité – Le secteur pétrolier et gazier – Le transport • Techniques pratiques de tests de pénétration des ICS appliquées aux environnements susmentionnés et à d'autres environnements de systèmes de contrôle industriel • Création d'un plan de tests de pénétration des ICS : considérations et contraintes • Collecte de données • Analyses des vulnérabilités des systèmes SCADA et PLC • Analyse des résultats et rapports • Ateliers pratiques.	5 jours	• Compréhension et analyse des vulnérabilités des systèmes de contrôle industriel • Création d'un plan efficace de tests de pénétration des ICS • Réalisation de tests de pénétration sûrs sur les systèmes SCADA, PLC et d'autres composantes des ICS • Élaboration de recommandations éclairées quant aux mesures correctives. La formation débouche sur la délivrance d'un diplôme.
Cyberdiagnostic des ICS pour professionnels		
• Introduction aux éléments, aux architectures et au déploiement des ICS, dans les différents domaines industriels tels que : – La production et la distribution d'électricité – Le secteur pétrolier et gazier – Le transport • Prise en compte des défis et contraintes liés aux ICS • Techniques de cyberdiagnostic appliquées aux environnements de systèmes de contrôle industriel • Création d'un plan de cyberdiagnostic des ICS • Collecte et conservation manuelles des données de diagnostic : travailler avec les protocoles en matière d'ICS et de RTOS • Analyse des artefacts et vérification des anomalies • Rapports • Ateliers pratiques.	4 jours	• Réalisation d'enquêtes scientifiques fructueuses dans les environnements de systèmes de contrôle industriel • Création d'un plan de cyberdiagnostic efficace pour les ICS • Recueil de preuves physiques et numériques et traitement adéquat de celles-ci • Mise en œuvre des outils et des instruments de cyberdiagnostic dans le cadre des systèmes SCADA et PLC • Détection de traces d'intrusion fondée sur les artefacts découverts • Reconstruction des incidents et utilisation des données d'horodatage • Élaboration de rapports éclairés et de recommandations exploitables La formation débouche sur la délivrance d'un diplôme.

Livre blanc sur les formations KICS, décembre 2016