

FORMATION

Cybersécurité des Systèmes Industriels



Les grandes entreprises ainsi que les PME sont de plus en plus les cibles de cyberattaques qui entravent voire paralysent le fonctionnement des sites de production et infectent les parcs informatiques. Cela entraîne des risques sur la sécurité des biens et des personnes, et expose les entreprises aux tentatives d'extorsion de fonds ou de rançonnement avec des conséquences négatives aussi bien sur le plan financier que sur l'image de marque.

Aussi, les attaques des systèmes informatiques ont montré que les systèmes automatisés sont impactés de façon significative. En effet, la frontière entre l'informatique de gestion et l'informatique industrielle est devenue très mince, voire inexistante. Il est par conséquent important de se former afin de s'engager dans une démarche de sécurisation de l'informatique industrielle de façon générale : automates, télétransmetteurs, réseaux informatiques, SCADA / IHM, usages, ...

LA SOLUTION

Prosyst – Spécialiste de la performance des systèmes automatisés et Serval – Expert en sécurité informatique, unissent leurs savoir-faire pour proposer des parcours de formation en cybersécurité industrielle au personnel des entreprises. Nos formateurs sont des experts reconnus dans leurs domaines et travaillent depuis plus de deux décennies sur des projets de performance et de cybersécurité industrielle.

Les différents parcours de formation répondent, par gradations théoriques et techniques en fonction des interlocuteurs de l'entreprise, aux exigences particulières de la cybersécurité des systèmes industriels :

- sensibiliser,
- proposer des méthodes de prévention / protection, de conception des installations, de surveillance,
- se confronter à des problématiques et des solutions industrielles,
- acquérir un esprit critique afin d'améliorer les installations existantes et concevoir les installations futures.

TEMOIGNAGE



« Jacques a su nous transmettre la bonne parole. Le but est atteint et Prosyst/Serval ont réussi à sensibiliser les participants sur l'importance de la sécurité dans la conception d'un système informatique industriel. La démonstration sur plateforme a su bien illustrer les possibilités d'interceptions et corruptions des échanges entre automates. »

Rémy SCOTTO LA CHIANCE
Chargé de projet Radio et Informatique industrielle chez VNF

Les formations s'adressent à tous les interlocuteurs de l'entreprise, en fonction de leur acquis et de leurs responsabilités en matière de sécurité des systèmes industriels au sein des organisations. Les parcours de formation alternent théorie et travaux pratiques sur plateforme matérielle.

	CYBERSENS Formation (1jour)	CYBERFORM Formation (3jours)	CYBERPRO Formation (5jours)
Personnel d'entreprise	✓		
Expert Automatismes & Informatique	✓	✓	
Ingénierie projets & DSI <small>(Direction des Systèmes d'Information)</small>		✓	✓

Formation à la carte :

En fonction de vos demandes spécifiques, nous pouvons vous proposer un parcours de formation adapté à vos besoins (aussi bien en matière de contenu que de durée de formation). Vous désirez consacrer plus de temps aux cas pratiques ou bénéficier d'une plateforme matérielle conforme à vos contrôle-commande réels ; nous consulter.

CYBERSENS*

L'objectif de la formation CYBERSENS est d'apporter aux auditeurs les connaissances et compétences suivantes :

- comprendre les risques et les enjeux de la cybermenace,
- intégrer les règles de bonnes pratiques de cybersécurité des systèmes industriels.

CYBERFORM & CYBERPRO *

L'objectif des formations CYBERFORM & CYBERPRO est d'apporter aux auditeurs les connaissances et compétences suivantes :

- avoir une vision globale de la cyberdéfense,
- appréhender les problématiques de sécurité des systèmes d'information et systèmes industriels,
- être en mesure de comprendre et mettre en œuvre des attaques concrètes sur des systèmes industriels afin de mieux cerner les mécanismes de défense à déployer,
- mettre en œuvre des outils de surveillance et de défense sur des systèmes industriels.

La formation sur 5 jours CYBERPRO permet d'aborder plus en détail les démonstrations d'interception et de corruption des échanges entre systèmes automatisés et de déployer des cas pratiques plus nombreux.

Pour l'ensemble des formations, vous bénéficiez d'une plateforme matérielle permettant des démonstrations réelles, des exercices et travaux pratiques (tests de pénétrations et de vulnérabilité, mises en œuvre d'attaques, exercices de script,...) en immersion sur un système automatisé 100% simulé.

*Formation basée sur le référentiel ANSSI :

«Guide pour une formation sur la cybersécurité des systèmes industriels»

