

Plan du cours

Security Center : Certification Renforcement du système	
Code	SC-SHC-001
Niveau	Intermédiaire
Durée	2 heures (auto-formation en ligne)
Public cible	Techniciens, administrateurs et professionnels de l'informatique
Conditions préalables	Certification SC-OTC-001, SC-STC-001, SC-AFC-001 ou SC-AMP-001
Objectifs	<ul style="list-style-type: none">• Comprendre les risques croissants liés au monde interconnecté• Comprendre l'impact et les risques pour les systèmes de sécurité• Comprendre l'approche de Genetec en matière de sécurité des systèmes• Effectuer une analyse pratique en prenant le contrôle d'accès comme exemple• Utiliser les outils de renforcement intégrés à Security Center• Appliquer les bonnes pratiques générales à un système Security Center• Comprendre la direction à emprunter pour la suite des événements
Certification	Oui. Questionnaire(s) en ligne

Sujet	Description
Module 0 : <i>Introduction</i>	<ul style="list-style-type: none"> • Introduction • Qu'attendre de cette formation
Module 1 : <i>Les risques croissants liés à notre monde interconnecté</i>	<ul style="list-style-type: none"> • Le prix de l'interconnexion • Le coût des cybermenaces • Événements et statistiques récents en matière de cybercriminalité
Module 2 : <i>En quoi cela me concerne ?</i>	<ul style="list-style-type: none"> • Quels sont les risques pour les systèmes de vidéosurveillance ? • Attaques via l'Internet des objets • Appareils non fiables • Mouvement latéral • Quels sont les risques pour les systèmes de contrôle d'accès ?
Module 3 : <i>Approche de renforcement des systèmes</i>	<ul style="list-style-type: none"> • Sécurité de votre système de sécurité <ul style="list-style-type: none"> ○ Authentification ○ Autorisation ○ Chiffrement
Module 4 : <i>Analyse de renforcement pratique</i>	<ul style="list-style-type: none"> • Analyse pratique (contrôle d'accès) • Architecture • Identifiants • Wiegand vs OSDP • TLS • Architecture sécurisée
Module 5 : <i>Renforcement de Security Center</i>	<ul style="list-style-type: none"> • Widget Score de sécurité • Coffre-fort des micrologiciels • Outil de diagnostic des privilèges • 11 « bonnes pratiques »
Module 6 : <i>Étapes suivantes</i>	<ul style="list-style-type: none"> • Choisir des solutions certifiées • La cybersécurité est l'affaire de tous, pas seulement du service informatique • L'éducation des utilisateurs est essentielle • Informations / documents de référence
Test de certification SC-SHC-001	<ul style="list-style-type: none"> • Chaque module de formation est suivi d'un petit examen en ligne de 5 questions (à l'exception du <i>Module 0</i>) • Le score cumulé de l'ensemble des questionnaires <u>constitue</u> l'examen de certification. • Une note d'au moins 80 % est requise pour obtenir la certification.