

Solutions sécurisées SEL



Les spécialistes et les solutions SEL vous aident à sécuriser votre infrastructure essentielle

- Créez une base de référence de votre système de technologie opérationnelle (TO) actuel et déterminez les vulnérabilités potentielles.
- Comblez les lacunes grâce à des solutions réseau sécurisées et assurez la conformité avec les normes en interrompant au minimum le déroulement des opérations.
- Simplifiez les initiatives en matière de conformité grâce à la gestion centralisée des ressources, aux mises à jour logicielles et micrologicielles, aux journaux d'événements et à la rotation des mots de passe.
- Détectez les événements relatifs à la cybersécurité et assurez une réponse efficace et une restauration rapide du système.



Points à prendre en considération pour déceler les lacunes en matière de cybersécurité

RESSOURCES

Comment votre équipe de cybersécurité est-elle structurée ?

Les systèmes TI et TO ont différentes exigences en matière de performances. Nous pouvons vous aider à mettre en œuvre des stratégies de cybersécurité qui réduisent les perturbations au minimum dans les environnements TO.

Qui gère vos systèmes de communication TO ?

Les opérations quotidiennes nécessitent des compétences spécialisées. Notre personnel compétent et nos ressources vous accompagnent dans chaque aspect de la propriété du système TO.

Qui surveille la sécurité de votre système ?

Une conception appropriée des systèmes de notification des événements est essentielle à la connaissance de la situation. Nous vous aidons à concevoir et à mettre en œuvre des solutions de surveillance de la sécurité clé en main, et notre centre des opérations de sécurité propose des services de surveillance 24 h/24, 7 j/7 et 365 j/an.

CADRE

Disposez-vous d'un cadre de cybersécurité TO ?

Les solutions de sécurité SEL sont conçues sur la base du cadre de cybersécurité du NIST (National Institute of Standards and Technology), qui permet la conformité avec d'autres cadres de sécurité, tels que les normes CIP de la NERC et la norme CEI 62351. Nous pouvons vous aider à élaborer une feuille de route pour la mise en œuvre de ces solutions et fournir une surveillance constante du système.

Êtes-vous tenu de respecter les normes de cybersécurité ?

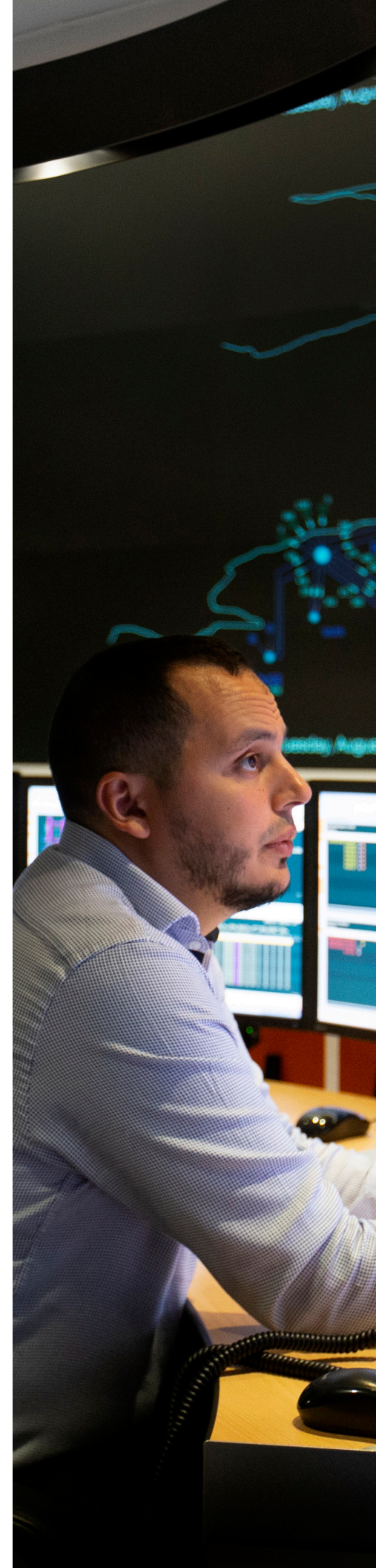
Nous proposons des services d'évaluation qui confirment la conformité avec les normes de cybersécurité, et nous pouvons fournir des guides de renforcement de la cybersécurité pour les ordinateurs, les relais et les contrôleurs.

La sécurité physique est-elle intégrée à votre cadre de cybersécurité ?

La sécurité physique fait partie de l'approche de défense en profondeur de la cybersécurité. Les solutions SEL prennent en compte la sécurité physique, ainsi que les catastrophes naturelles et environnementales, pour offrir une vue globale des risques de cybersécurité.

La sécurité de la chaîne d'approvisionnement des fournisseurs est-elle l'une de vos considérations actuelles ?

Chez SEL, nous comprenons l'importance de sécuriser notre chaîne d'approvisionnement et nous suivons des processus internes et externes rigoureux pour la sécurité de nos produits et de nos applications. Nous sommes propriétaires de chaque ligne de code de nos logiciels et micrologiciels. Ce code est signé numériquement, jamais partagé en dehors de SEL et il est surveillé en permanence pour détecter les nouvelles menaces. Lorsque vous choisissez une solution SEL, vous pouvez être sûr qu'elle est sécurisée.





CONCEPTION DE RÉSEAU

Quand avez-vous effectué un audit de réseau tiers pour la dernière fois ?

Nous proposons des évaluations sur site et des audits de conformité pour répondre à vos besoins.

Comment sécurisez-vous les liaisons réseau pour l'accès à distance ?

Nous proposons des services de conception, de conseil et de mise en œuvre de solutions d'accès à distance sécurisées et chiffrées.

Vos appareils TO ont-ils été éprouvés ?

Nous proposons des solutions de mise en réseau qui utilisent la technologie SDN (mise en réseau pilotée par logiciel, Software-Defined Networking) pour mettre en liste blanche les flux réseau autorisés, désactiver les ports et services inutilisés et éliminer plusieurs vecteurs d'attaque des réseaux locaux traditionnels.

PROCESSUS DE MAINTIEN DE LA SÉCURITÉ

Quel est le processus de gestion des ressources sur vos systèmes TO ?

La gestion des ressources pour les systèmes de grande taille peut être une tâche difficile. Le logiciel de gestion des ressources de SEL peut contribuer à réduire le coût des opérations et à simplifier les processus de mise à jour pour la gestion des correctifs.

Comment les comptes utilisateur sont-ils gérés pour vos dispositifs TO ?

Les réseaux TO possèdent de nombreux dispositifs comportant plusieurs niveaux d'autorisation. Les mots de passe doivent faire l'objet d'une rotation sécurisée et les autorisations utilisateur doivent être attribuées de manière adéquate. Nous proposons une gestion centralisée des comptes utilisateur pour simplifier les opérations et la maintenance de ces comptes.

Comment gérez-vous le contrôle de version des paramètres système ?

La création et la maintenance d'une base de référence des paramètres du système sont des éléments cruciaux de la propriété du système. Nous pouvons fournir un logiciel de gestion des ressources qui simplifie l'établissement d'une référence pour le système et le contrôle de version.

Comment abordez-vous la gestion des correctifs ?

Il peut être difficile de comprendre quels correctifs sont applicables et comment installer les mises à jour en toute sécurité. Nous proposons des services de gestion des correctifs qui surveillent les avis de vulnérabilité et nous fournissons un plan d'atténuation des menaces qui a fait l'objet d'essais.

DÉTECTION ET RÉPONSE

Êtes-vous prêt à détecter les événements relatifs à la cybersécurité sur votre système ?

Il existe de nombreux indicateurs d'atteinte à la sécurité des systèmes qui révèlent une activité potentiellement malveillante et montrent les tactiques connues utilisées par les attaquants. Les solutions sécurisées SEL détectent les intrusions et nous fournissons des guides pour les procédures d'intervention.

Passez-vous en revue les procédures de reprise au moyen d'exercices de simulation ?

Les règlements et les procédures sont les plus bénéfiques lorsque le personnel est correctement formé. Nous proposons des exercices de simulation pour tester les connaissances du personnel et l'efficacité des procédures d'intervention. Des services tels que la sauvegarde automatique des paramètres peuvent faciliter le processus de reprise.

Pourquoi choisir SEL ?

Grâce à notre expertise confirmée en matière de cybersécurité et de TO, nous élaborons des solutions clé en main efficaces qui améliorent la cybersécurité et rationalisent la gestion des ressources et les initiatives de conformité. Une solution sécurisée SEL sera prête à protéger votre système contre les vulnérabilités et à les prévenir, et n'aura aucun effet négatif au regard des autres exigences du système TO. SEL offre un large éventail de solutions, et un grand nombre de spécialistes SEL sont à votre disposition, selon les besoins.

Étapes suivantes

Contactez SEL à l'adresse secure@selinc.com pour communiquer avec notre équipe de spécialistes en cybersécurité TO.



Services d'ingénierie SEL
+1.509.332.1890 | secure@selinc.com | selinc.com

© 2019 par Schweitzer Engineering Laboratories, Inc.
20191003