SecurityST* pour la génération d'énergie

Dans un univers complexe de technologies qui ne cessent d'évoluer, GE s'est rendu compte qu'il était essentiel d'avoir un partenaire expérimenté pour aider à instaurer une bonne sécurité a. En tant que leader mondial des contrôles industriels, GE est particulièrement bien équipée pour aider ses clients à améliorer leurs positions en matière de sécurité et à soutenir leurs efforts de conformité. Nos produits sont construits dans un souci de sécurité et ils s'intègrent facilement à des systèmes de centrales et des architectures IT plus étendues.

La solution de gestion de la sécurité centralisée SecurityST de GE joue un rôle essentiel dans le système de défense en profondeur des environnements de contrôles des générateurs, des centrales et des turbines. Par l'emploi de technologies et de services de défense modulaires, ce système centralisé donne aux entreprises l'avantage unique de pouvoir observer le statut de leur sécurité Internet, de pouvoir mettre en œuvre des stratégies et des politiques proactives pour protéger le système de contrôle critique et ses réseaux associés, outre de fournir une capacité centralisée de création de rapports permettant de gérer les risques Internet. Cette solution permet d'atténuer les vulnérabilités d'Internet au niveau du réseau, du point limite et des contrôleurs.

La solution SecurityST Mark* VIe et les services de mise en service sont agréés Achilles® - niveau Bronze - ce qui indique que la solution est instaurée selon les meilleures pratiques de l'industrie en matière de sécurité Internet, ce qui prouve aux clients que leurs systèmes sont mis au point et instaurés en toute sécurité. La solution SecurityST et ses services associés sont conçus pour soutenir l'effort de conformité des centrales aux normes et directives de cybersécurité incluant NERC CIP, NEI 08-09 et ISA99/CEI 62443.

Directives types de cybersécurité

- Le système de contrôle doit être protégé contre les menaces internes et externes.
- Le réseau du système de contrôle doit être séparé des autres réseaux.
- Les points d'accès au réseau doivent être protégés et surveillés ; les menaces potentielles doivent être journalisées et les notifications appropriées doivent être envoyées aux personnes pertinentes.
- Tous les appareils et utilisateurs doivent être authentifiés et autorisés avec le moins de privilèges nécessaires possibles.
- Toutes les interfaces et l'équipement des systèmes de contrôle doivent être renforcés pour être conformes aux normes et aux meilleures pratiques de l'industrie.
- Le système doit être constamment contrôlé pour déceler toute activité anormale à son propos et toutes les signatures de cyberattaques connues.
- Les mises à jour logicielles de sécurité validées et approuvées doivent être appliquées aux composants du système de contrôle le cas échéant.
- Plusieurs mesures de détection et de défense doivent être intégrées à la solution.
- Sécurité intégrée – l'échec des fonctions de sécurité n'aura pas d'impact sur les opérations du système.
- La mise en œuvre, la fonction et le transfert doivent se faire en toute sécurité.
- Les Points d'accès externes (PAE) doivent être sécurisés.

Les systèmes de prévention et de détection d'intrusion réseau

Cette option de sécurité du réseau personnalisable donne la possibilité de surveiller et de bloquer les attaques et les activités malicieuses.

- Elle fournit une visibilité continue de l'activité inhabituelle et des menaces potentielles susceptibles d'affecter le réseau du système de contrôle.
- Elle capture les journaux de trafic et permet d'analyser le réseau en continu, aussi bien au niveau local qu'au niveau de l'entreprise.
- Protection actualisée améliorée par des mises à jour de signatures IDS/IPS fournies par GE conçues pour détecter les menaces connues ou se protéger contre elles
- Elle promeut un contrôle plus fort sur les protocoles d'application OT, qui appliquent les règles d'autorisation/d'interdiction sur le réseau du système de contrôle.

Contrôle de l'accès basé sur le rôle

Cette fonction fournit une gestion et un contrôle centralisés avec des alertes spécifiques à l'environnement des contrôles, à savoir, qui peut accéder au système de contrôle industriel et quelles permissions sont données.

Les avantages incluent :

- • une facilité de paramétrage par l'utilisation de rôles prédéfinis de la centrale, créés à l'aide des pratiques d'excellence de l'industrie ;
- un impact du risque réduit par la limitation de l'accès à l'infrastructure critique ;
- une visibilité accrue des niveaux d'accès de l'utilisateur avec la possibilité immédiate de donner ou de retirer l'accès afin de rationaliser les besoins de tiers ou des employés ;
- une capacité de mode sécurisé à deux facteurs du contrôleur qui réduit l'accès et améliore la protection ;
- l'instauration d'une gestion centralisée par mot de passe qui permet au client de mettre en place et de gérer aisément une politique de mot de passe avec des options disponibles définies par le client ou définies au préalable.

Gestion des évènements et informations de sécurité

Nous proposons une solution extensible avec des vues en temps réel et de l'historique de l'activité Internet (par ex. changement des configurations de commutateur, échecs de tentatives de connexion, accès non autorisé à un port et utilisation USB).

Les avantages incluent :

- une fonction centralisée avec un affichage des évènements et un tableau de bord visuel du statut de la sécurité en temps réel, qui offre une visibilité complète de votre équipement et qui vous avertit des menaces potentielles ;
- un enregistrement et un stockage des journaux pour tous les composants du système, ce qui vous donne la possibilité de récupérer l'activité passée et d'associer les évènements aux alertes d'incidents et aux rapports réglementaires. Les journaux peuvent être transférés à l'équipe de l'entreprise pour une assistance supplémentaire.

Sécurité de l'accès à distance

Nous faisons appel aux pratiques d'excellence pour aider à la sécurité de l'accès à distance sur la base des normes et des besoins des clients. Les options de notre solution incluent l'authentification de plusieurs facteurs, un boîtier de sécurité, un réseau unidirectionnel, un RPV, une prévention de l'intrusion et un accès à lecture seule. Nous vous aidons à contrôler l'identité des personnes pouvant accéder à vos équipements critiques et les informations auxquelles elles ont accès.

Les avantages incluent :

- un accès aux segments à l'aide de zone d'instauration claires entre les réseaux interne et externe, qui vous aide à satisfaire les exigences en matière de conformité et qui empêche un accès non autorisé au système de contrôle ;
- la définition et le regroupement des systèmes et des utilisateurs autorisés avec lesquels ils ont le droit d'avoir une interface avec les environnements de clients ;
- la surveillance et l'inspection du trafic entre les organisations pour déceler les comportements inhabituels et capturer les activités des utilisateurs et des dispositifs.

Secours et reprise

- Secours centralisé, automatique et reprise du domaine de contrôle du processus, qui économise du temps et de l'argent grâce à la garantie d'un plan antisinistre avec temps d'indisponibilité minime.
- Toutes les activités de secours sont journalisées et sont aisément accessibles pour la création de rapports afin d'aider aux exigences en matière de génération de rapports.

Pour de plus amples informations, veuillez contacter :
GE Oil & Gas
Amérique du Nord +1-888-943-2272 ; +1-540-387-8726
Amérique latine (Brésil) : +55-11-3958-0098
Europe (France) : +33-2-72-249901
Asie/Chine (Singapour) : +65-6622 1623
Afrique/Inde/Moyen-Orient (E.A.U) : +971-2-699 7119

Email : ControlsConnect@ge.com
Portail client : ge-controlsconnect.com

1800 Nelson Road
Longmont, CO, USA 80501
https://www.gemeasurement.com/machinery-control

Service de mise à jour du correctif

La souscription à la cyberprotection de l'équipement fournit des mises à jour mensuelles de vos IHM, historiens, commutateurs, pare-feux, OSM et RSG. Les mises à jour logicielles incluent notamment :

- Le système d'exploitation Windows®
- GE Cimplicity (spécifique ICS-CERT)
- Signatures de détection d'intrusion
- Signatures anti-virus
- Mises à jour des commutations
- System 1*
- Microsoft® Excel et Microsoft® Word
- Adobe

Les avantages incluent :

- un déploiement centralisé du service de souscription GE de gestion des correctifs, ce qui fait économiser 4 heures par IHM, pouvant engendrer entre 10 000 à 20 000 USD d'économies mensuelles pour une centrale type ;
- l'amélioration de votre position en matière de sécurité grâce à la protection, sur une base mensuelle, de vos équipements critiques contre les vulnérabilités connues ;
- des mises à jour au déploiement aisé qui sont cumulatives et qui peuvent être automatisées ou programmées en fonction des besoins de la centrale ;
- la réception d'un rapport sur l'applicabilité qui définit la criticité, le temps requis à la mise à jour et la nécessité d'un réamorçage, ce qui donne des renseignements qui vous permettent de prendre des décisions informées pour vos opérations.

Protection du point limite

La protection du point limite permet de protéger l'intégrité de vos données et les systèmes qui exploitent vos équipements. Elle contrôle les activités malicieuses par l'intermédiaire de points d'accès (USB, CD/DVD, ports Ethernet, etc.) et elle bloque l'accès interdit.

Avec la nouvelle option de création d'une liste blanche des applications, les dispositifs basés Windows® se trouvent mieux protégés grâce à une réduction des risques et des coûts associés aux programmes malveillants ce qui améliore la fiabilité et la stabilité du réseau. Cette fonction identifie automatiquement les logiciels de confiance qui sont autorisés à l'exploitation sur des IHM de système de commande tout en bloquant les logiciels inconnus ou indésirables.

Chaîne de contrôle et mise en œuvre sécurisée

En qualité de vendeur, la sécurité commence avec nous. Alors que nous construisons et préparons chaque SecurityST, une attention particulière est donnée à la sécurité numérique et physique par l'utilisation de périmètres physiques, un contrôle de l'accès avec surveillance vidéo et un transfert de la garde sécurisé. Notre siège social à Longmont, dans l'état du Colorado aux États-Unis, est certifié comme satisfaisant les exigences des clients dans la génération d'énergie, le nucléaire, outre le pétrole et le gaz, par le strict respect des normes appliquées par NEI 08-09, NERC-CIP et CEI 62443.

GEA31245C-FR (06/2016)