

### Siemens et le CCD COE de l'OTAN renforcent leur coopération en matière de cybersécurité pour les infrastructures critiques

- **La formation contre les cyberattaques est essentielle pour protéger les réseaux électriques intelligents**
- **De précieuses informations sur les attaques et les points vulnérables permettent de créer des solutions innovantes et des produits plus sûrs**

Siemens Smart Infrastructure et le Centre d'excellence de cybersécurité coopérative de l'OTAN (CCD COE) ont signé un protocole d'accord pour poursuivre la coopération en matière de cybersécurité pour les infrastructures critiques. Le CCD COE a organisé l'exercice « Locked Shields », son exercice annuel de cybersécurité, qui constitue un pilier pour l'amélioration des capacités de défense communes. Ce nouvel accord va permettre aux parties de renforcer leur coopération existante en matière de formation à la cybersécurité des réseaux électriques. Dans le cadre de son expérimentation avec le logiciel de contrôle du réseau électrique Spectrum Power, Siemens recueille de précieuses informations sur les vecteurs d'attaque potentiels et peut tester de manière exhaustive de nouvelles fonctions ou de nouveaux protocoles de sécurité pour ses produits et solutions.

L'exploitation et la gestion des réseaux électriques ont radicalement changé au cours des dernières années avec l'intégration de sources d'énergie plus renouvelables et décentralisées. Le besoin d'optimisation des réseaux et d'interaction entre prosommateurs, ainsi que le nombre de nouveaux arrivants sur le marché ont augmenté de manière significative. Les technologies d'information et de communication se sont fait une place au sein des réseaux de transmission et de distribution. Ces interconnexions croissantes offrent davantage de vecteurs d'attaque potentiels sur les réseaux électriques. C'est pourquoi, la cybersécurité est une priorité absolue pour les exploitants de réseaux électriques et les organismes gouvernementaux.

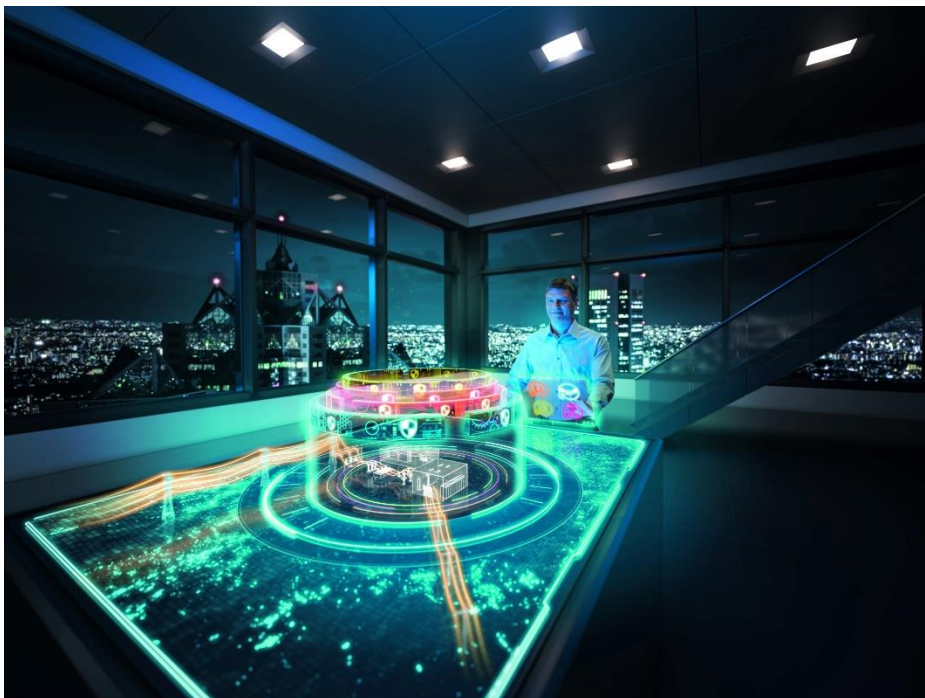
Lancé en 2010, Locked Shields est un exercice annuel de cyberdéfense organisé par le CCD COE de l'OTAN qui vise à former des équipes d'intervention en cyberdéfense pour lutter contre des cyberattaques de grande ampleur. Siemens collabore avec le CCD COE de l'OTAN depuis 2017 pour intégrer des scénarios d'attaque de réseaux électriques à l'exercice de défense, qui s'appuie sur des systèmes et des produits, tels que le logiciel Spectrum Power et les terminaux distants Sicam A8000 de Siemens. Ces solutions permettent de répondre à des configurations de réseaux électriques complexes impliquant des centres de contrôle et des stations secondaires qui sont interconnectés et interdépendants. Dans le cadre de cet exercice, les équipes de défense doivent mettre en place les lignes de défense d'une infrastructure complexe pourvue de différents systèmes et applications et devant être capables de résister à des cyberattaques d'envergure lancées par un grand nombre de pirates informatiques. Les experts en cybersécurité ont notamment dû s'atteler à la lourde tâche de traquer les menaces, de signaler les attaques et de rétablir le système tout en garantissant le maintien du réseau. Locked Shields constitue une opportunité d'apprendre au travers d'exercices, de formations et de coopérations dans le domaine des opérations de cyberdéfense.

Robert Klaffus, PDG de Digital Grid chez Siemens a affirmé : « Les réseaux électriques et tous les éléments qui y sont connectés forment la colonne vertébrale des sociétés modernes et sont, de ce fait, des cibles de choix pour les pirates informatiques. Les connaissances et l'expérience acquises grâce à l'exercice Locked Shields jouent un rôle clé dans la sécurisation et la protection des réseaux électriques. La coopération renforcée avec le CCD COE de l'OTAN va permettre à Siemens de recueillir de précieuses informations sur de nouvelles formes d'attaques et sur la façon de traiter les défis de cybersécurité en pleine évolution liés aux réseaux électriques intelligents. Ces informations seront réutilisées dans le cadre de futurs développements de notre portefeuille. »

Le protocole de communication standard ouvert OPC UA PUB/SUB à la base de nombreuses applications d'IoT constitue un exemple de test de nouvelles fonctions dans le cadre de cette coopération.

Le colonel Jaak Tarien, directeur du CCD COE de l'OTAN a déclaré : « Notre longue coopération avec Siemens dans la formation d'experts en cybersécurité pour protéger les infrastructures critiques en général et les réseaux électriques en particulier représente un atout majeur pour les exercices techniques de cyberdéfense du CCD COE de l'OTAN. Visant à renforcer les interactions entre les différentes parties prenantes de la cyberdéfense, ainsi que la collaboration et les échanges de meilleures pratiques, cet accord va donner une nouvelle dimension à notre coopération. Nos sociétés s'appuient sur des infrastructures solides et résilientes. Par conséquent, nous avons tout intérêt à faire avancer la

cybersécurité ensemble avec les principaux partenaires du secteur, comme Siemens Smart Infrastructure. »



Vous trouverez ce communiqué ainsi que des visuels d'illustrations à l'adresse :

<https://sie.ag/2CHJEsP>

Pour plus d'informations sur le CCD COE de l'OTAN, rendez-vous sur [www.ccdcoe.org](http://www.ccdcoe.org)

#### **Contacts presse :**

CLC Communications

Jérôme Saczewski, Christelle Grelou, Ingrid Jaunet, Orlin Nzuzi

Téléphone : 01 42 93 04 04

E-mails : [c.grelou@clccom.com](mailto:c.grelou@clccom.com), [i.jaunet@clccom.com](mailto:i.jaunet@clccom.com), [o.nzuzi@clccom.com](mailto:o.nzuzi@clccom.com)

**Siemens Smart Infrastructure (SI)** développe des infrastructures intelligentes et évolutives pour le monde d'aujourd'hui et de demain. SI répond aux défis de l'urbanisation et du changement climatique en connectant les systèmes d'énergie, les bâtiments et les sites industriels grâce à un portefeuille complet et unique de produits, systèmes, solutions et services, de la production jusqu'à la consommation d'énergie. Dans un monde toujours plus digital, SI accompagne ses clients dans leur développement et participe au progrès de la société tout en contribuant à la protection de la planète : « SI creates environments that care ». Siemens Smart Infrastructure, dont le siège est localisé à Zoug (Suisse), compte 72 000 salariés dans le monde.

**Siemens France Holding** est une filiale de Siemens AG, groupe technologique de dimension mondiale. Depuis près de 170 ans en France, le nom de Siemens est synonyme de performance technique, d'innovation, de qualité et de fiabilité. Siemens opère dans les domaines de la production et de la distribution d'énergie, des infrastructures intelligentes pour les bâtiments et la production d'énergie décentralisée, de l'automatisation et de la digitalisation dans l'industrie manufacturière et l'industrie des procédés. Par ailleurs, Siemens Mobility, une société du groupe bénéficiant d'une autonomie de gestion de ses activités, est un fournisseur majeur de solutions de mobilité intelligente pour le transport de passagers et de marchandises. Avec sa filiale cotée en bourse Siemens Healthineers AG, l'entreprise est également un fournisseur de premier plan de solutions et de services destinés au secteur de la santé. Également filiale cotée en bourse, Siemens Gamesa Renewable Energy propose des solutions durables pour l'éolien terrestre et en mer. Avec 7 100 collaborateurs, 11 sites industriels et 19 sites de R&D et d'ingénierie,

Siemens France s'engage activement dans les filières stratégiques pour l'industrie française. Au 30 septembre 2019, date de clôture du dernier exercice, Siemens France a enregistré, au titre de ses activités poursuivies, un chiffre d'affaires de 2,35 milliards d'euros dont 28 % réalisés à l'export. **Suivez-nous sur Twitter @Siemens\_France**

**Le CCD COE** est un centre de cyberdéfense accrédité par l'OTAN spécialisé dans la recherche, la formation et les exercices. Il représente une communauté de 25 nations qui apportent une vision globale de la cyberdéfense et bénéficient d'une expertise dans les domaines de la technologie, de la stratégie, des opérations et du droit.

Le centre est pourvu en personnel et financé par ses nations membres, à savoir l'Allemagne, l'Autriche, la Belgique, la Bulgarie, le Danemark, l'Espagne, l'Estonie, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Italie, la Lettonie, la Lituanie, la Norvège, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie, la Suède et la Turquie. Le Canada, le Japon, la Croatie, l'Australie, le Luxembourg, l'Irlande, le Monténégro, la Slovénie, la Suisse et la Corée du Sud sont également en passe de rejoindre le Centre.