ICARE
CYBER SECURITY

Cyber Sécurité

Services de Sécurité info-gérés
Pour les Systèmes de Contrôle Industriels

ICARE
CYBER SECURITY

Sécuriser vos systèmes opérationnels pour une fraction du cout d'une interruption de service.

En 2014 le **risque cybernétique** est entré pour la première fois dans **la liste des 10 risques majeurs** du Baromètre de l'Allianz Group. Il est considéré comme **3eme plus gros risque**. Plus de **50% des attaques** cybernétiques sont conduites sur les **infrastructures critiques** des pays comme l'Eau, le Gaz et l'Electricité et **75% sur les sites industriels**. La plupart de ces infrastructures ont été conçus pour de la résilience mais pas pour se prémunir des risques cybernétiques.

Des composants informatiques sont souvent rajoutés aux systèmes SCADA (Supervisory Control And Data Acquisition) et PLC (Programmable Logic Controllers) ainsi que des connections Internet les rendant vulnérables aux attaques.

Le coût moyen d'un temps d'arrêt toutes industries confondues est de € 5,600 par minute.
Le coût d'un temps d'arrêt dans l'industrie est plus élevé autour de € 22'000 per minute
La moyenne de durée d'un incident est de 90 minutes coutant au moins € 500'000 par incident

D'après le dernier rapport d'ICS-CERT, les secteurs de l'Energie et l'Industrie ont rapporté le plus grand nombre d'incidents dus au faible niveau de sécurité des systèmes SCADA

LA SITUATION EST DEVENUE TRES CRITIQUE

- Ces attaques causent de graves interruptions.
- Avec d'importants dommages physiques et économiques.
- Les assureurs sont de plus en plus réticents à assurer ce type de risque
- La vulnérabilité de ces systèmes vieillissants est exposée à Internet

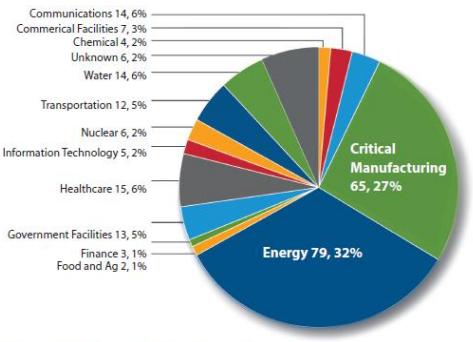


Figure 1. FY 2014 incidents reported by sector (245 total).

COMMENT POUVONS-NOUS VOUS AIDER?

ICARE est une société d'ingénierie et de services dans les domaines du Pétrole, Gaz, et Energie. Nous avons complémenté nos compétences dans ce domaine en forgeant des partenariats avec les plus grands acteurs de la Cyber Sécurité industrielle afin de fournir la solution la plus complète que possible

UNE SOLUTION SIMPLE A UN PROBLEME COMPLEXE

ICARE Cyber Security, est une Division du groupe ICARE basée en **Suisse** qui a comme but d'aider les entreprises industrielles à se **Protéger** et à se **Prémunir** des attaques Cybernétiques. Le but principal étant de réduire le risque en minimisant la vulnérabilité des infrastructures industrielles et de fournir aux employés une formation, une sensibilisation ainsi que des compétences techniques et opérationnelles.

Le **Services de Sécurité info-gérés** d'ICARE est une solution de Cyber Sécurité complète pour un déploiement rapide, incluant du Monitoring, de la détection, de l'investigation, la mise à disposition d'un laboratoire d'analyse, ainsi que de la formation et des exercices pratiques. Si vous n'arrivez pas à voir ce qui se passe sur votre réseau, vous ne serez pas en mesure de comprendre et d'adresser les problèmes

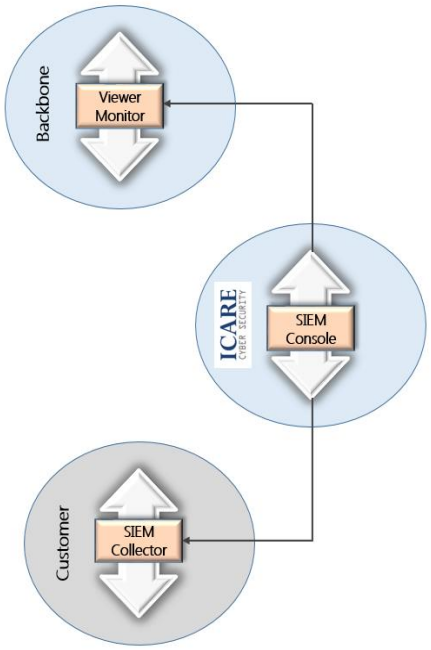
La solution n'est pas juste **Technologique** – Elle inclut de la **Formation et du travail comportemental** ainsi que des **Processus d'Urgences** pour monter en maturité et se protéger efficacement.

Construire un COS requière de gros investissements et beaucoup d'expertise.

NOTRE APPROACHE

En 2 semaines nous vous fournissons une **Analyse de Risque** afin de définir précisément la topologie des réseaux SCADA ainsi que la maturité des **Employés,** des **Processus & Procédures** et de la **Technologie** utilisés.

Notre solution **Non-Intrusive** connecte nos clients par le Biais du SIEM Event Collector/Processor à notre centre de monitoring et à l'infrastructure permanente.



SERVICES FOURNIS: LA SUITE DE VISIBILITE

La première étape d'une démarche de Cyber Sécurité commence par vous rendre votre visibilité sur les évènements de votre réseau. Cette approche **Non-Intrusive** vous permet de rapidement comprendre les comportements suspectes dans votre réseau industriel, de rapidement détecter les intrusions, assurer la traçabilité des foyers d'attaques et de prendre les mesures appropriées pour minimiser le danger.

Nous fournissons les divers services de protections par le biais de l'infrastructure permanente, et prenons nos clients étape par étape à travers les mesures nécessaires pour sécuriser leurs infrastructures critiques.

LA SUITE DE VISIBILITE INCLUS:

- COS Opération, Monitoring 24 x 7 et centre d'appels
- Monitoring jusqu'a 100 évènements/sec
- Corrélation de comportement aux attaques déjà répertoriées
- Rapports hebdomadaires; Alertes immédiates
- Formation de base pour 5 personnes
- Investigation et disponibilité du Laboratoire d'Analyse
- Service Delivery Manager
- Connection sécurisée avec le l'infrastructure permanente

RETROUVEZ VOTRE VISIBILITÉ.
ON NE PEUT PAS GÉRER CE QUI EST INVISIBLE

SUITE DE SECURITE

CENTRE des OPERATION de SECURITE (COS)

Le COS protège les entreprises des attaques cybernétiques, en utilisant des technologies innovantes de type command and control, intelligence and monitoring capable d'assurer le bon déroulement des opérations de nos clients sans interruption de leurs activités. C'est un investissement important en personnes et Technologies d'où l'importance de le mutualiser pour sa rentabilité.

INTELLIGENCE ET INVESTIGATION

Pour ce type de services nous avons forgé un partenariat avec des sociétés spécialisées dans l'analyse et l'intelligence ayant la capacité de corréler les diverses sources d'informations : Medias, Réseaux Sociaux, Sites Professionnels et Dark Web. Grace à ça nous sommes capables de mener une investigation poussée et fournir un rapport d'activité détaillé.

SECURITE DES FOURNISSEURS

Quels risques sont liés à vos fournisseurs et lesquels posent le plus grand risque à votre entreprise? Notre équipe est capable d'évaluer vos fournisseurs et d'identifier ceux dont les produits et services ont besoins d'un traitement spécialisé. En partenariat avec vous nous établirons les règles de sécurité pour vos fournisseurs existants ainsi que des fiches de qualifications pour vos futurs fournisseurs.

SENSIBILISATION

Le module de Sensibilisation se décline en fonction des différents aspects de la Cyber Sécurité comme le développement, investigation, la Contre-Attaque et en fonction des différents types d'intervenants : Managers, Operateur, Superviseur etc...

EXERCICES ET FORMATION

Notre équipe peut vous fournir un vaste choix de courses de formations couvrant les différents aspects de la cyber sécurité. Nous vous fournissons aussi divers exercices de simulations très proches de la réalité. Chaque cas peut simuler les différents types de dangers et évaluer le niveau de maturité de vos collaborateurs. Les scenarios sont coordonnés avec nos clients et utilisent divers outils de piratage et de simulation afin de répliquer une attaque dans un environnement contrôlé.

Contacte

Pour plus de détails, contactez-nous:

info@icare-cybersecurity.com

+41 22 960 7602

icare-cybersecurity.com