Construire un Bouclier de Protection Intégrale

Construire un Bouclier de Protection Intégrale

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.

Par exemple, Le Virus **Stuxnet a détruit 20% de la capacité d'enrichissement d'Uranium de l'Iran en 2010**. Cette attaque fut conduite sans que les opérateurs ne réalisent quoi que ce soit.

On constate une nette augmentation des attaques cybernétiques de divers niveaux de sophistication au fur et à mesure que la vulnérabilité des systèmes SCADA systèmes est mise à nue.

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

Il N'Y A PAS DE SOLUTION SIMPLE

Une mise à jour ou un emplacement de ces systèmes n'est pas envisageable. Premièrement ils sont éparpillés sur de larges sites industriels – Deuxièmement leurs remplacement ou maintenance engendrent une interruption de service, causant des répercussions sur l'activité de l'entreprise et suivi de lourds investissements.

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.

VOTRE ORGANISATION EST ELLE PRETE?

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.

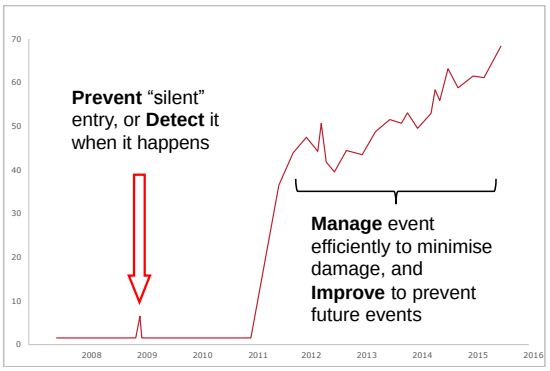
ICARE Cyber Security, est une Division du groupe ICARE basée en **Suisse** qui a comme but d'aider les entreprises industrielles à se **Protéger** et à se **Prémunir** des attaques Cybernétiques.
Nos Technologies, Processus et Formations ont été conçus autour de : **La Prévention, Détection, Prise en charge et l'Amélioration** – pour aider nos clients à faire face à cette nouvelle donne.

ETRE PRET …

Nos solutions couvrent la formation de votre personnel informatique, la mise en place de processus & procédures de sécurité, et les outils informatiques pour vous prémunir contre les attaques cybernétiques, a vous aider à identifier le plus tôt possible pour minimiser la contagion et les risques associés et identifier les domaines d'amélioration à apporter.

Nos solutions adressent trois points cruciaux:

- **Formation:** Apprendre à détecter une attaque le plus tôt possible afin de la contenir et réduire son impact sur l'entreprise
- **Processus & Procédures:** Création et implémentation de Processus et Procédures au niveau de l'organisation
- **Systèmes & Technologie:** Monitoring actif, contrôle et gestion des évènements, Analyse en temps réel et corrélation entre les différentes sources d'information



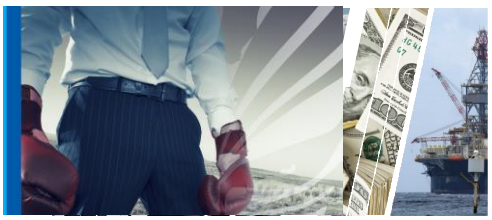
NOTRE DEMARCHE

Nous commençons chaque engagement par une **Analyse de Risques et d'Ecarts** pour définir le niveau de maturité de nos clients autour des axes suivants : **Personnes, Processus & Procédures** et **Systèmes & Technologie**.

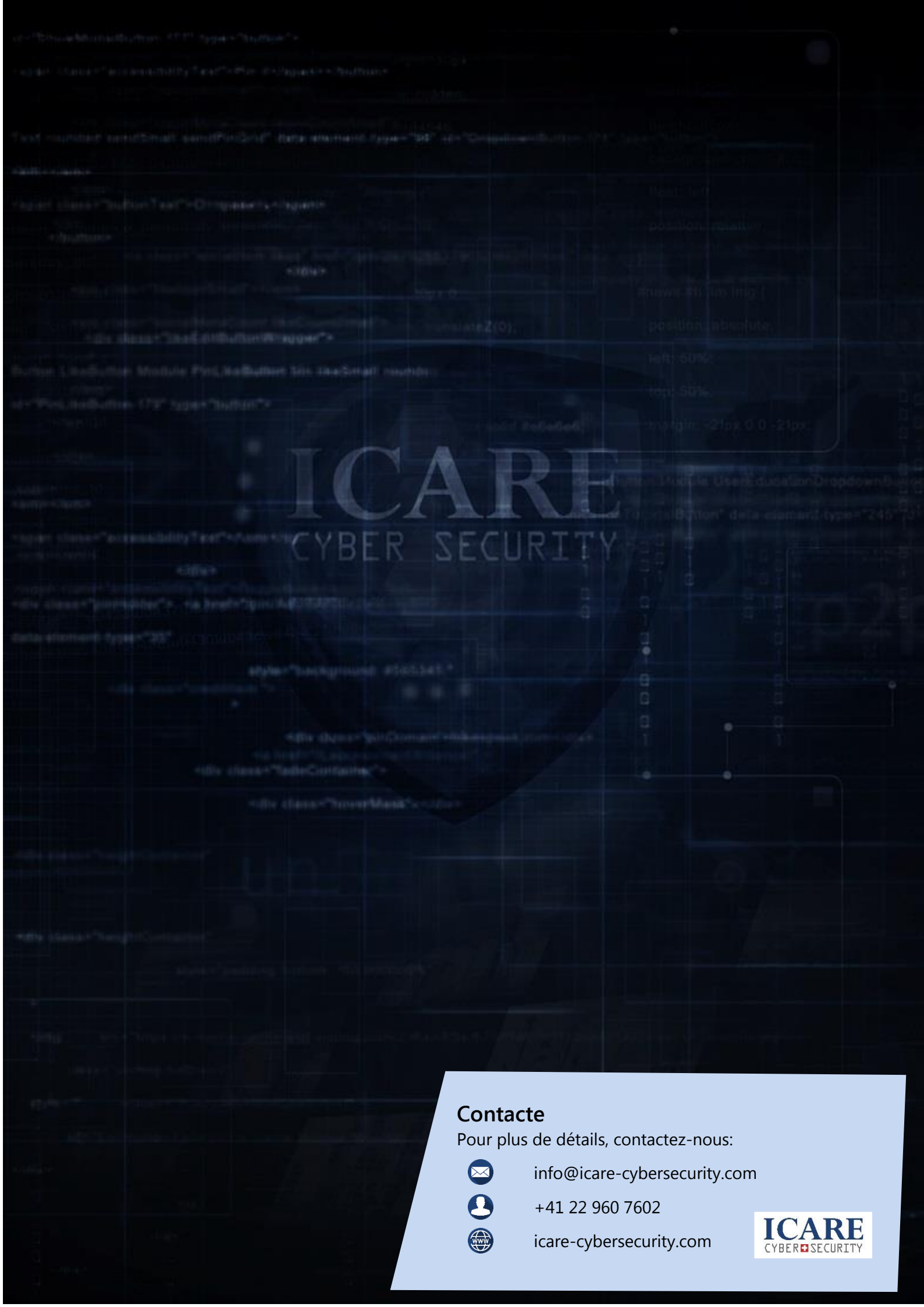
Ensemble nous définissons **l'Etat de Départ** et le **But Final** et vous fournissons une démarche compréhensive et adaptée à vos besoins de la phase d'implémentation jusqu' à la mise en Service.

Analyses de Risques et d'Ecarts	Modèle d'Architecture Sécurisée	Politique de Cyber Securitée	Centre des Opérations de Sécurité	Equipe d'intervention	Cyber Entrainement	SCADA Defense
Environnement Polyvalent	Conformité SCI	Phase d'Implémentation	Surveillance	Infrastructure IT	Infrastructure IT	Détection des Attaques
Bases de Données	Nettoyage de Fichiers	Définir l'adversaire	Détection	Infrastructure OT	Infrastructure OT	OCOS pour Systèmes SCADA
Connexions à Distance	Ségrégation de Réseaux	Vecteurs d'Attaques	Atténuation	Emulateurs d'Environnements	Evaluation des Risques	Conception & Construction du COS
Interconnections Réseaux	Transfert de Données Sécurisé	Engagement de la Direction	Investigation	Modélisation d'Attaques	Surveillances des Risques	Architecture Securisée
Contrôle	Connexions à Distance Sécurisées	Définir les Feuilles de Route Technologiques	Signalisation	Technologie d'Enquêtes	Technologie d'Enquêtes	Consultations
Fuites de Données	Protection en Temps Réel	Avantage	Analyses Post Actions	War Games	Criminalistique	

Nous prenons nos clients étape par étape à travers les mesures nécessaires pour sécuriser leurs infrastructures critiques. Nous recommandons aussi de rapidement mettre en Œuvre les activités de Monitorage qui permettent de comprendre le comportement du réseau de l'entreprise



PREPAREZ-VOUS AVEC L'ACTIVE CYBER COMBAT



Contacte

Pour plus de détails, contactez-nous:

info@icare-cybersecurity.com

+41 22 960 7602

icare-cybersecurity.com

ICARE
CYBER SECURITY