framatome cybersecurity

SIMULATION & VALIDATION PLATFORM

Capacité à répliquer un environnement de production et à valider l'impact des solutions liées à la cybersécurité

La maintenance en conditions de sécurité (MCS) des équipements industriels est une activité de suivi essentielle.

Challenge

Dans un environnement industriel complexe et sensible, maintenir en conditions de sécurité les systèmes de contrôle industriels (ICS) sans impacter cet environnement constitue un véritable défi.

Un autre challenge majeur est de tester et de valider les plans de remédiation en cybersécurité avant leur mise en œuvre sur site. Ne pas perturber les opérations industrielles est l'enjeu clé et une mise en place efficace de ces plans de remédiation permet d'atténuer les risques de cyberattaques.

Solution

La plateforme en cybersécurité de Framatome est basée sur une solution de virtualisation avancée pour la modélisation d'architectures industrielles complexes. Afin de répondre aux contraintes de ces environnements, c'est une plateforme ouverte qui permet de s'interfacer avec des équipements industriels externes (PLC, Switches, Firewall, Data Diode, Passerelle, etc.).

La plateforme permet de:

- Identifier les équipements qui nécessitent une protection.
- Identifier et évaluer les vulnérabilités de ces systèmes.
- Elaborer un plan de remédiation.
- Réaliser des tests d'intrusions dans un environnement maîtrisé.
- Tester et valider le plan de remédiation dans un environnement sécurisé:
    - Durcissement.
    - Déploiement de correctifs.
    - Tests de non régression.
- Préparer et valider le processus de mise en œuvre à réaliser sur site.

Bénéfices clients

- Réaliser les opérations à risque dans un environnement maitrisé et isolé.
- Gagner du temps et des coûts sur la configuration, l'intégration et la validation pour se concentrer sur les objectifs opérationnels.
- Mieux coordonner les équipes de maintenance et d'exploitation.

Votre performance, notre engagement de tous les jours

@ Plateforme de Framatome

Informations Techniques

- **Virtualisation** d'environnements complexes composés de dizaines ou centaines de machines virtuelles ou conteneurs.
- **Hardware in the loop :** Intégration d'équipements ou systèmes physiques.
- **Trames réseau :** Génération de trafic permettant de simuler des intrusions.
- **Scenario d'attaques :** Mise en place de scenarii pour vérifier la défense en profondeur de systèmes.

Chiffres clés

60% des cyberattaques ont eu des conséquences avérées sur le business.

24% avec des perturbations sur la production.

25% des entreprises déclarent avoir subi au moins une attaque par rançongiciel.

Baromètre du CESIN de 2023 (Club des Experts de la Sécurité de l'Information et du Numérique

Contact: cyber-services@framatome.com
www.framatomecybersecurity.com