Cybersécurité : enjeux pour l'usine du futur

En lien avec H2020 DS7-07-2017

FPC Ingénierie

- Société d'ingénierie en Contrôle-Commande (ICS), 10 personnes
- Au contact du monde industriel et académique
- Sens de la solution à apporter sur les problématiques nouvelles en Informatique Industrielle
  - Architectures
  - Etudes de fiabilité
  - Méthodes de gestion technique des projets
- Souci de présenter les problématiques selon les impacts / contraintes client

Développement Cybersécurité industrielle

- Lauréat H2020 SME Phase 2 : 1,7 M € de subvention pour développer un système de détection d'intrusion (IDS)
- Développement d'une offre de formation à la cybersécurité industrielle, déjà plus de 100 personnes formées
- Offre de prestations dédiées cyber-sécurité industrielle:
  - Analyse de risques
  - Audit
  - Accompagnement sur les mesures de sécurité

-> Connaissance détaillées des enjeux, contraintes, besoins

Les points durs de la cybersécurité industrielle (1)

- Hétérogénéité entre pays européens
- Infrastructures critiques versus industries : obligations réglementaires ou incitations fortes dans un cas, quelle motivation pour les autres ?
- Confrontation IT / OT :
  - Solutions IT intéressantes et non suffisantes
  - Pratiques OT contraignantes et parfois mauvaises
  - Langage automaticiens / informaticiens
- Limites des analyses de risque : complétude, proportionnalité des mesures par rapport aux risques
- Solutions techniques et organisationnelles non matures

Les points durs de la cybersécurité industrielle (2)

- La cybersécurité industrielle (OT) vue depuis la cybersécurité informatique (IT) ne suffit pas – voire même, ne convient pas.
- Les systèmes industriels ne sont pas administrés ni monitorés.
- Le bon fonctionnement en continu reste l'objectif numéro 1, devant la cybersécurité
- L'opacité et la méconnaissance du système sont les sources de beaucoup de failles (voire toutes).
- Sécuriser par rapport aux menaces amène à être toujours vulnérable.

Les axes de progrès du moment

- Import et application intelligente des mesures d'hygiène informatique
- Découverte de l'hygiène de configuration des systèmes
- « Situation Awareness » : recouvre
  - La contextualisation des situations
  - La capacité de connaitre le fonctionnement interne des ICS
  - En contradiction avec le chiffrement !
- Les architectures
- Les « appliances »
- Le durcissement des équipements
- Code sûr

Focus sur l'industrie du futur

- IoT divergent de la ségrégation en zones (62443)
- Limite d'intervention / d'ingérence du RSSI ?
- « Fractalisation » de la surface d'attaque
- Cycle de vie : système en perpétuelle évolution
- Beaucoup de petites solutions mais pas de solution
- Dilution des responsabilités Cyber
- Convergence Sûreté – cyber-sécurité mise à mal

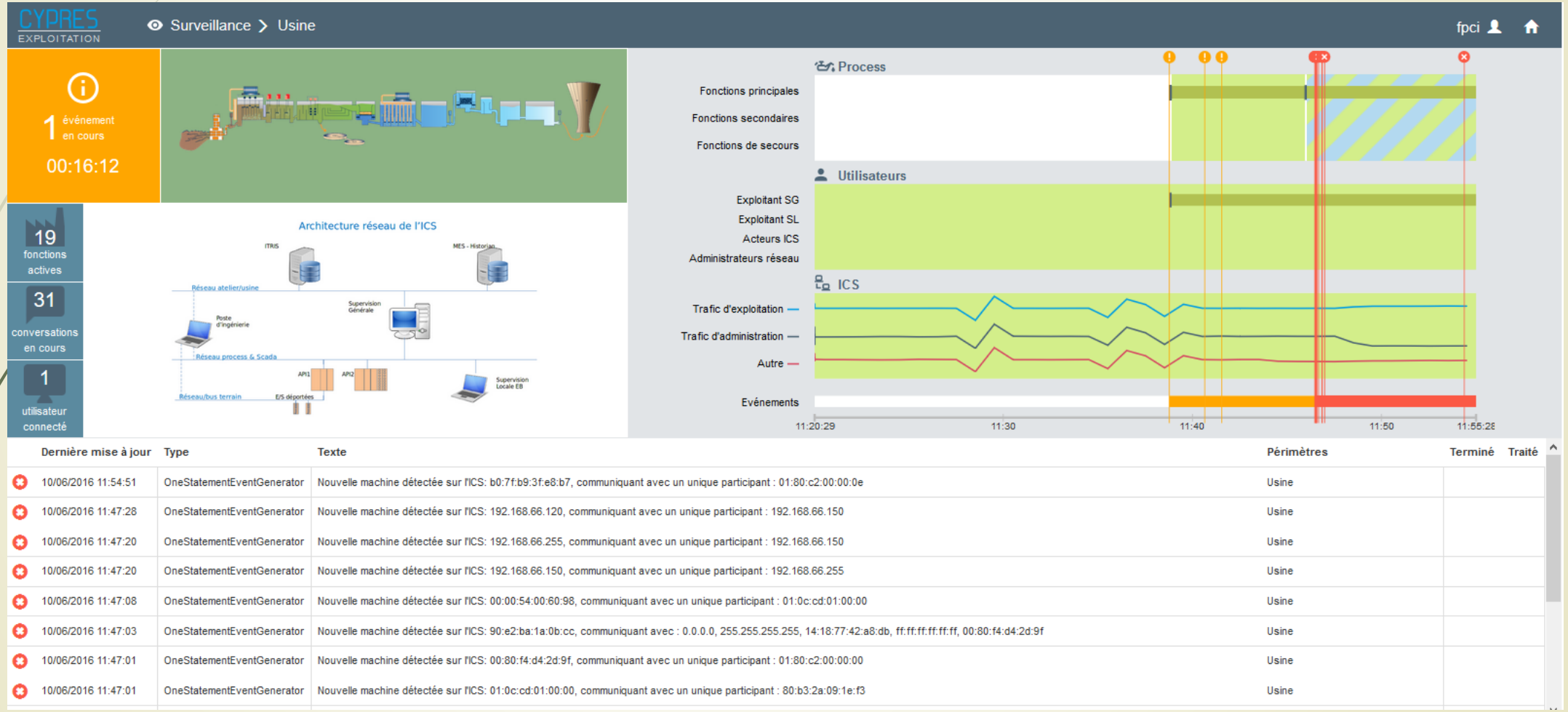
Les perspectives intéressantes du moment

- Canalisation des communications
  - Log, trace, audit trails, forensic tools
- Protection réseau
  - Protocoles, comportement, cartographie, Network System Management (62351)
  - Technologies de pare-feu, diodes
- Analyse comportementale plutôt que virale
  - Détection y compris en cas d'exploit de faille 0-day
- Technologies de défense passives (honey pot) et actives (reroutage sur attaque DOS)
- Evolutions dans l'authentification

Points forts de FPC Ingénierie par le développement de CYPRES

- Contextualisation forte
- Analyse comportementale
- Enregistrements et visualisation adaptées aux exploitants, automaticiens autant qu'aux RSSI
- Produit de détection d'intrusion qualifié
- Capacité à générer des contre-mesures et des systèmes d'entraînement aux attaques
- Capacité à renforcer un système ancien ou vulnérable depuis l'architecture jusqu'aux Forensic Tools

Compagnon SCADA et IDS



Dernière mise à jour	Type	Texte	Périmètres	Terminé	Traité
10/06/2016 11:54:51	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: b0:7f:b9:3f:e8:b7, communiquant avec un unique participant : 01:80:c2:00:00:0e	Usine		
10/06/2016 11:47:28	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 192.168.66.120, communiquant avec un unique participant : 192.168.66.150	Usine		
10/06/2016 11:47:20	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 192.168.66.255, communiquant avec un unique participant : 192.168.66.150	Usine		
10/06/2016 11:47:20	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 192.168.66.150, communiquant avec un unique participant : 192.168.66.255	Usine		
10/06/2016 11:47:08	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 00:00:54:00:60:98, communiquant avec un unique participant : 01:0c:cd:01:00:00	Usine		
10/06/2016 11:47:03	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 90:e2:ba:1a:0b:cc, communiquant avec : 0.0.0.0, 255.255.255.255, 14:18:77:42:a8:db, ff:ff:ff:ff:ff:ff, 00:80:f4:d4:2d:9f	Usine		
10/06/2016 11:47:01	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 00:80:f4:d4:2d:9f, communiquant avec un unique participant : 01:80:c2:00:00:00	Usine		
10/06/2016 11:47:01	OneStatementEventGenerator	Nouvelle machine détectée sur l'ICS: 01:0c:cd:01:00:00, communiquant avec un unique participant : 80:b3:2a:09:1e:f3	Usine		

Questions et Réponses