Nouvelles vulnérabilités, nouvelles menaces, nouvelles solutions

Grenoble mardi et mercredi 30 et 31 janvier 2018

Détection d'intrusion dans les réseaux industriels par modélisation de la normalité et détection d'anomalie

Jean-Christophe Testud

Sentryo

Tel : 33 9 70 75 34 80 – jean-christophe.testud@sentryo.net

Mots clés : cybersécurité, réseaux industriels, machine learning, détection d'anomalies

Résumé :

Avec l'avènement de l'Industrie 4.0, les usines subissent une forte transformation en adoptant une connectivité forte et la mise en réseau des composants industriels (automates, robots, IoT). Cela représente un terrain de jeu de choix pour des acteurs malveillants, pouvant mettre à l'arrêt ou saboter une usine. Afin de comprendre des attaques réelles, nous nous sommes basés sur la cyber kill chain qui démontre clairement les étapes par lesquelles un attaquant passe pour atteindre son but (de la phase de reconnaissance jusqu'à l'altération sur le processus industriel). Nous avons créé des scénarios grâce à des retours d'expériences des attaques industrielles comme Stuxnet en Iran, les multiples attaques contre les centrales électriques ukrainiennes, ou celles contre les chaînes d'assemblage de Renault.

Pour détecter ces différents scénarios, nous avons développé plusieurs approches complémentaires. Un objectif majeur étant de donner un maximum de contexte et « d'interprétabilité » aux alertes générées. Ces algorithmes que nous présenterons reposent sur le principe de la détection d'anomalies par rapport au fonctionnement nominal du réseau:

1. Un premier algorithme repose sur la création d'une activité réseau de référence basée sur la connaissance métier des experts. Cette référence permet de détecter les activités 100 % nouvelles ou la disparition d'activités connues.
2. Afin de détecter des changements de comportement plus subtils, il est possible de modéliser les comportements réseau sur des axes déjà connus, et d'en suivre les variations. Nous présenterons une représentation de ces déviations. Grâce à une représentation de ces variations, il est possible de repérer des phases caractéristiques du trafic et d'isoler les périodes où le réseau aurait un comportement qui dévie (de manière brutale ou étalée dans le temps), sans connaissance préalable du réseau.
3. Enfin, nous présenterons un algorithme de *Machine Learning* permettant le suivi du processus industriel via les variables qui le décrivent. Cet algorithme peut par exemple détecter des injections malicieuses de variables industrielles.