Contribution ID: **31** Type: **Roundtable Member**

A proactive approach: Stopping insiders' threats with machine-learning technology

Monday, 5 November 2018 16:25 (5 minutes)

Abstract –Insiders' threats initiated covertly or overtly are foremost challenges for nuclear safeguards and security. In safeguards, covert insiders' activities include theft and diversion of special nuclear materials; misuse of process and equipment; deliberately tempering with IAEA surveillance equipment; or systematic concealment of malicious activities for nuclear weapons development. With the advance in digital and cyber technologies, malicious insiders' activities become ever more sophisticated and difficult to uncover, hampering efforts by the international safeguards regime.

A "game changer" involving the recent malware attack against the TRICONEX safety system at an industrial complex in the Middle East serves as a wakeup call for the cyber defense of malicious attacks initiated externally or by insiders. The attack was the first to target an engineering system dedicated to protecting people and the environment. Though not successful, the implications cast a long shadow over the doubt on the adequacy of a defense based on cyber analysts adopting information technology (IT).

A defensive approach with IT based on lessons-learned (after an attack) is problematic, and hence inadequate as insiders are always steps ahead of defenders. In a long run, an artificial intelligent (AI) approach based on machine learning would be proactive and preferred. Such defensive approach is now possible due to the advances in AI technologies, aided by the exponential increase in the ability to collect big data and to perform massive computations.

With a machine learning approach, it would trace the attack vectors and identify defensive tasks, and show how many of these tasks can be automated, and even deployed in real time to catch the insiders/intruders before any damage is done. For example, machine learning would be able to identify unusual traffic on the network, and shut down these connections as they occur. It can identify abnormal standard operating procedures requested by insiders attempting to steal sensitive information or materials, and sound an alarm to alert the plant responders to prevent the theft. Also, machine learning implemented for containment and surveillance would recognize patterns of concealment by insiders, and alert the IAEA inspection to stop the malicious activities.

Which "Key Question" does your Abstract address?

CHA2.1

Which alternative "Key Question" does your Abstract address? (if any)

CHA2.2

Topics

CHA2

Primary author: Dr CHOI, Jor-Shan (Lawrence Livermore National Laboratory (retired))

Presenter: Dr CHOI, Jor-Shan (Lawrence Livermore National Laboratory (retired))

Session Classification: [CHA] Keeping Pace with IT Security - Threat Intelligence for the IAEA/Nuclear Regulatory World

Track Classification: Addressing Growing Safeguards Challenges (CHA)