Contribution ID: **120**　　Type: **Poster**

Common Criteria for Nuclear Cyber Security

The nuclear industry is just one of many industry verticals (e.g. automotive, medical, oil & gas etc.) grappling with the challenge of addressing cyber risk in the supply chain. The Common Criteria (ISO/IEC 15408) is the only well established and internationally recognized standard for the security evaluation of IT products –a vital part of the supply chain. Uniquely, the Common Criteria provides a flexible but structured framework that can be customized and adopted for a variety of industry vertical use cases, threat models and assurance levels. Coupled with the standard itself, there exists a world-wide network of Common Criteria schemes and labs that can be leveraged by the nuclear industry.
In his presentation, Mr. Turner will provide the following information to delegates:
• Basic introduction to Common Criteria
• Relationship between Common Criteria and EU Cyber Act (as this will be of interest to many of the delegates)
• Using Protection Profiles to specify security requirements
• Examples of how Technical Communities collaborate to create Protection Profiles
• Examples of how test automation is being leveraged to speed up Common Criteria evaluations
• Applying Protection Profiles and Technical Communities collaboration in the Nuclear context (a concrete example of how CC can work in the Nuclear context)
• Regulatory examples and recommendations

The three key points that Mr. Turner wishes to leave with the delegates are:
1. Don't re-invent the wheel. The Common Criteria (ISO/IEC 15408) is the only well established and internationally recognized standard for IT product security evaluation –and it is improving all the time. There is tremendous value in the world-wide network of schemes and accredited labs that can be leveraged for your industry. Uniquely, the Common Criteria provides a flexible but structured framework that can be customized and adopted for a variety of industry vertical use cases, threat models and assurance levels.
2. Industry collaboration is critical. The Common Criteria is like a tool box –one must know which tools to use. To get real value from Common Criteria, industry participants must collaborate to:
a. Create a market demand (or regulator requirement) for Common Criteria –vendors will not go to the trouble of certification if there is no demand.
b. Create tailored requirements to address the specific industry needs –leverage the Common Criteria User Forum to establish Technical Communities that are focused on sharing threat intelligence and specifying security requirements (both functional and across the product life-cycle) for technologies that are critical to your industry –i.e. via Protection Profiles.
3. Automation is here. It is only through industry adoption of test automation that the Common Criteria process will scale and be able to adequately address the current shortcomings that prevent the wider adoption of the standard for other verticals –namely time, cost and demonstrable reduction of risk.

Gender

Male

State

Canada

Author: Mr TURNER, Lachlan

Presenter: Mr TURNER, Lachlan

Track Classification: CC: Information and computer security considerations for nuclear security