Tuesday, February 14, 2023
2:40 PM – 3:00 PM
Overcoming the IT/OT Disconnect: Tips, Tricks, and Traps

James Stanger
Chief Technology Evangelist
CompTIA

John Mongeon
Senior Manger of Business Development
CompTIA

Abstract:
There is a long-standing divide between Information Technology (IT) and Operational Technology (OT) equipment, protocols, and support professionals. Governments and militaries worldwide have tolerated - and even encouraged - the IT/OT divide.

This practice flies in the face of ongoing trends. Today, we're seeing more traditional IT technology embedded within OT devices. We have also seen how IT and OT devices have become active targets in an organization's attack surface. We will quickly demonstrate various tools in this presentation, including Nmap, Metasploit, Security Onion, and OT-based honey pots. The goal is to help workers and policy makers understand practical ways to protect legacy and modern infrastructure.

In this presentation, we will demonstrate ways that governments and militaries worldwide have recognized the IT / OT divide as a dangerous disconnect. We will also discuss reasons why this disconnect is both long-standing and dangerous. For example, we will discuss how traditional OT protocols tend to "talk" differently than typical IT protocols. We will also deconstruct and discuss how OT devices tend to be perceived by military and government workers. We will do this by demonstrating how typical IT and OT protocols respond to typical security audits, analytics applications, and pen testing procedures. We will then discuss ways that organizations have overcome the IT / OT divide.

The presentation will discuss procedural, organizational, and technical changes that the most successful teams have used. Discussion points will include:

- Understanding traditional IT and OT perspectives
- How to re-organize technical teams
- Recognizing how to manage and secure legacy and (post)modern OT devices

One of the typical issues involved when monitoring, auditing, and securing OT and SCADA equipment is that workers and business leaders alike tend to think about these devices as functional parts of buildings, conveyor belts, and robotics equipment. We will discuss ways to change traditional perspectives so that devices are seen as technology that simply "talks" with a different dialect. We will demonstrate various tools in this presentation, including Nmap, Metasploit, Security Onion, and OT-based honey pots. The goal is to help workers and policy makers understand practical ways to protect legacy and modern infrastructure.

Finally, we will discuss ways that IT, OT, and cloud resources are increasingly used by organizations in their quest to turn data into actionable information. As part of this discussion, we will outline ways to manage the security of data at rest and in transit, not only from a technical, but also from a managerial perspective.