2:15 p.m. - 2:45 p.m.

A Behind-the-Headlines Look at Cyber-Attacks on a Military Control System

Charlene Mowery
Director of DoD Accounts
Ultra Electronics, 3eTI

Few have missed the headlines, or failed to appreciate the repercussions, associated with the Stuxnet, BlackEnergy, Havex, Sandworm and Triton/Hatman malware that has been discovered across the globe. In this presentation, 3eTI will show how attack vectors associated with identity compromise, social engineering and other factors can open a military industrial control system (ICS) to intrusions with the potential to cripple base operations. There is a perception that only nation-states are capable of launching a cyber-attack against automated and control systems. This presentation will show that the reality is anyone can do it, from an entry-level civilian employee to contractor to hacktivist team.

TAKEAWAYS > Appreciation for the unique vulnerabilities of a military ICS > Awareness of methods that can succeed for penetrating a military facility network > Actions and solutions available for comprehensive system cybersecurity

PURPOSE & OBJECTIVES This presentation is focused on the issues of cybersecurity for ICS. It introduces recommended standards with practical ways for implementing DHS and DoD guidance as part of a complete risk management strategy. The audience will gain a stronger appreciation of the security challenges and operations opportunities that are central to ICS organizations worldwide. At the presentation's conclusion, audiences will more fully understand the unique characteristics of industrial cybersecurity, and how security is effectively implemented across both the operational and IT domains. Those present will: > Develop an understanding of ICS security risks, vulnerabilities and attack vectors > Become more familiar with military security standards > Appreciate and recognize state-of-the-art hacker trends, techniques and technologies > Distinguish among the likelihoods for real-world impacts of breaches to ICS cybersecurity > Recognize central vulnerabilities relative to ICS protocols such as OPC, Modbus, DNP3, and Ethernet/IP

MAJOR POINTS TO BE COVERED > How to breach a firewall-protected network > Where military networks are vulnerable > How to identify attacks > Assessing opportunities for damage > Mitigating potentially catastrophic intrusions